ServiceNow for Tenable.io User Guide

Last Revised: June 19, 2018

Table of Contents

Overview

These applications are designed to help customers who use both Tenable.io and ServiceNow. The Tenable.io for Assets application integrates Tenable assets with the ServiceNow Configuration Management Database (CMDB). This application, once configured, allows you to bring Tenable asset data into ServiceNow as Configuration Items (CI) and to push ServiceNow CIs to Tenable.io as assets. The Tenable.io for Vulnerability Response application integrates Tenable vulnerability findings with the ServiceNow Security Operations Vulnerability Response module. This application, once configured, syncs all of Tenable vulnerability findings into ServiceNow Vulnerable Items (VIs) and Tenable Plugin details into ServiceNow Third Party Vulnerabilities.

This guide covers ServiceNow integration with:

- Tenable.io for Assets
- Tenable.io for Vulnerability Response

Tenable.io for Assets

Tenable.io for Assets seamlessly syncs and reconciles assets between Tenable.io and ServiceNow Configuration Management Database (CMDB). With Tenable's sophisticated discovery and scanning technology and ServiceNow's extensive CMDB you can now accurately track all of your assets.

Major Features

- Customize how Tenable assets are matched to ServiceNow CIs
- Create custom rules that automatically create ServiceNow CIs from Tenable assets
- Review unmatched Tenable.io assets and manually match them to existing ServiceNow CIs.
- Review unmatched Tenable.io assets and manually create new ServiceNow CIs.
- Define which ServiceNow CIs are sent to Tenable.io as assets
- Customize data mapping while keeping app upgradability
- Report which assets are synced between Tenable and ServiceNow
- Report which assets are not synced between Tenable and ServiceNow

Application Dependencies

- ServiceNow Kingston Platform
- ServiceNow Configuration Management Database (CMDB)
- (Optional) ServiceNow MID Server - This is only required for Tenable.io On-Premises
- Tenable.io
- Tenable.io API Library (ServiceNow App) - This app is a prerequisitie for all other Tenable.io apps in the ServiceNow store.
- Tenable.io for Assets (This app)

Integration Configuration

The following steps outline the configuration process to allow ServiceNow, through the use of the application, to poll and retrieve vulnerability data from Tenable.io. You must be logged in with a ServiceNow account that has the x_tsirm_tio_cmdb.admin role to perform the setup process.

The setup process involves these major steps, spelled out below in greater detail:

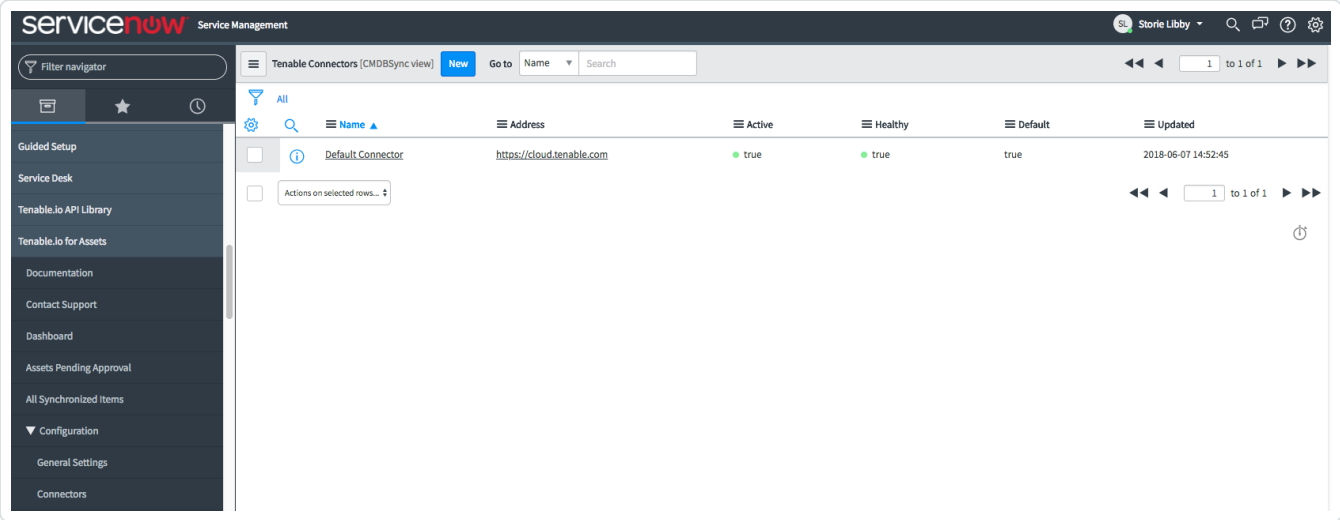
- Create Tenable.io API keys
- Create a Connector
- Configure the connection in Tenable.io for assets via an outbound sync
- Configure CIs to push to Tenable.io

Create Tenable.io API Keys

1. Log into Tenable.io.
2. Create an administrator account dedicated for use with this ServiceNow application. This account is used by ServiceNow to connect to Tenable.io to retrieve asset data.
3. Generate API Keys and save them for use with ServiceNow.

Configure ServiceNow and Tenable.io Asset Connector

1. Log into the ServiceNow console.
2. In the left-hand pane, navigate to **Tenable.io for Assets** > **Configuration** > **Connectors.**



3. Click **Default Connector**.
4. On the **Tenable Connector** page, select the **Active** check box.
5. In the **Access Key** field, type the value associated with your Tenable.io instance.

   > **Tip:** Use the API Key generated in the Create Tenable.io API Keys section of this document.

6. In the **Secret Key** field, type the value associated with your Tenable.io instance.

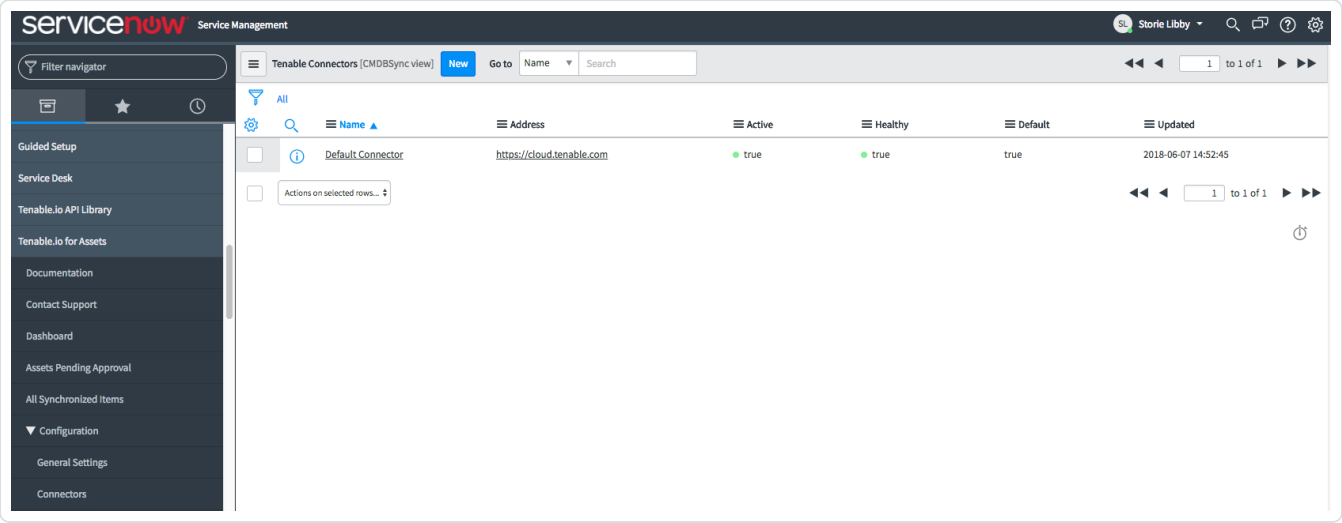
   > **Tip:** Use the Secret Key generated in the Create Tenable.io API Keys section of this document.

7. Click **Update**.

   Within minutes, the connector starts syncing ServiceNow configuration items to Tenable.io.

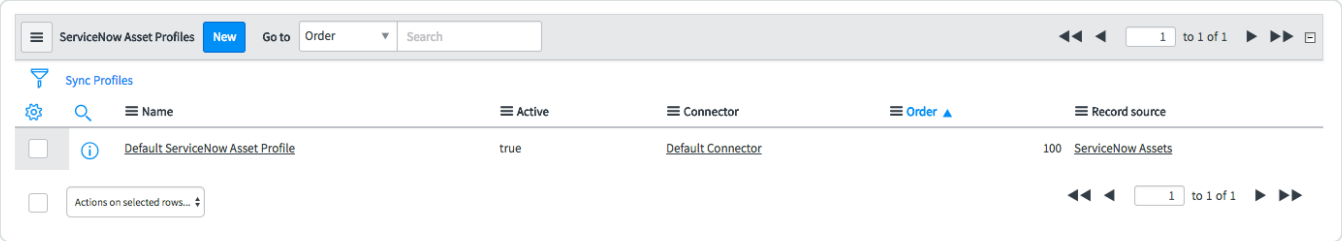
Configure Assets to be Synced from ServiceNow to Tenable.io

1. In ServiceNow, navigate to **Tenable.io for Assets** > **Configuration** > **Connectors**.



2. Click the connector for which you wish to configure an outbound sync.

3. At the bottom of the page, in the **ServiceNow Asset Profiles** list, click the asset profile for which you wish to configure an outbound sync.



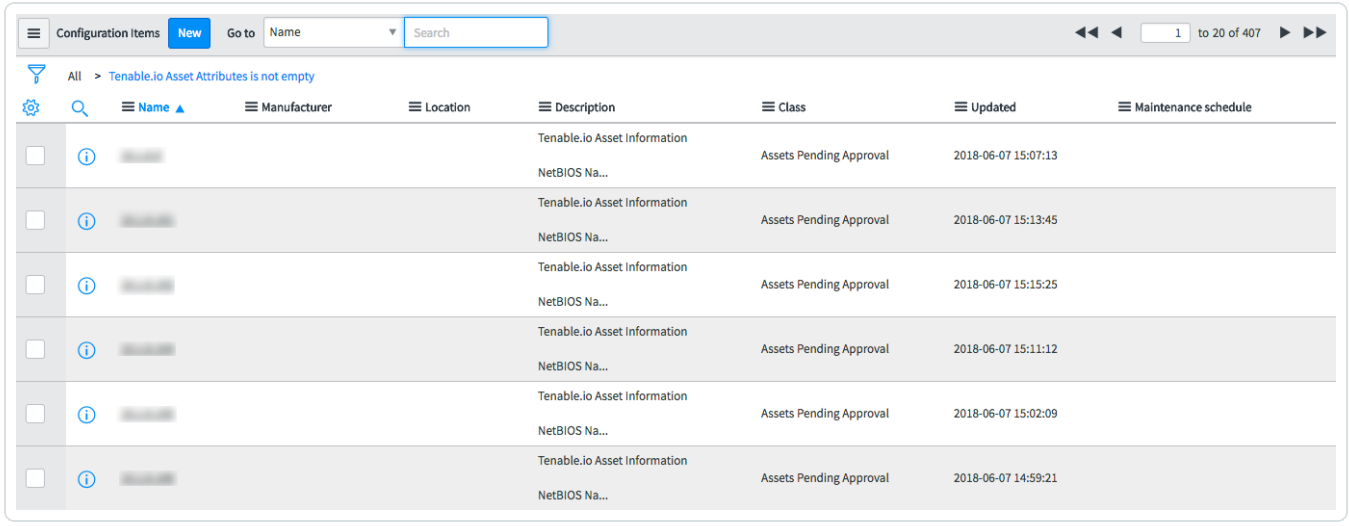
> **Note:** Optionally, to create a new asset profile, at the top of the page, click **New**.

The **Profile** page appears, where you can view the **Conditions**, **Default Chunk Size**, and the number of assets that will be synced based on your set conditions. Additionally, you can enable, disable, or set the profile to default.

4. Select the **Active** check box.

5. To view ServiceNow configuration items synced to Tenable.io, in ServiceNow, navigate to **Tenable.io for Assets** > **All Synchronized Items**.

   A list of all configuration items in ServiceNow that have a related record for the Tenable.io synced asset attributes appears.



Additional Settings

Settings can be changed for more control and troubleshooting.

1. In ServiceNow, navigate to **Tenable.io for Assets** > **Configuration** > **General Settings**.
2. Select the **Show Advanced Settings** check box.

   Advanced Settings include:

   - Max job log age (days)
   - Max job wait time (days)
   - New record sync frequency (minutes)

Custom Mapping of Data Received from ServiceNow

In the **Application** menu, administrators can access modules for administering the application:

- **API Data Mappings**
  - **Default Transform Map**: Defines how fields are mapped as records are brought back into update ServiceNow records.
  - **Default Import Set Table**: Temporary table into which data is brought before it is transformed to create/update ServiceNow records.
  - **Default Outbound Map**: Maps definitions of how ServiceNow fields map to Tenable.io fields for when outbound syncing occurs
  - **CI Matching Rules**: Rules for matching assets with configuration items as they come into ServiceNow.
  - **CI Creating Rules**: Rules for creating configuration items from Tenable.io assets as they come into ServiceNow.
- **Diagnostics**
  - **Tenable.io Jobs**: Jobs and their statuses.
  - **Queued Actions**.

Create a Matching Rule

See the Assets Optional Configuration section.

Create a Create Rule

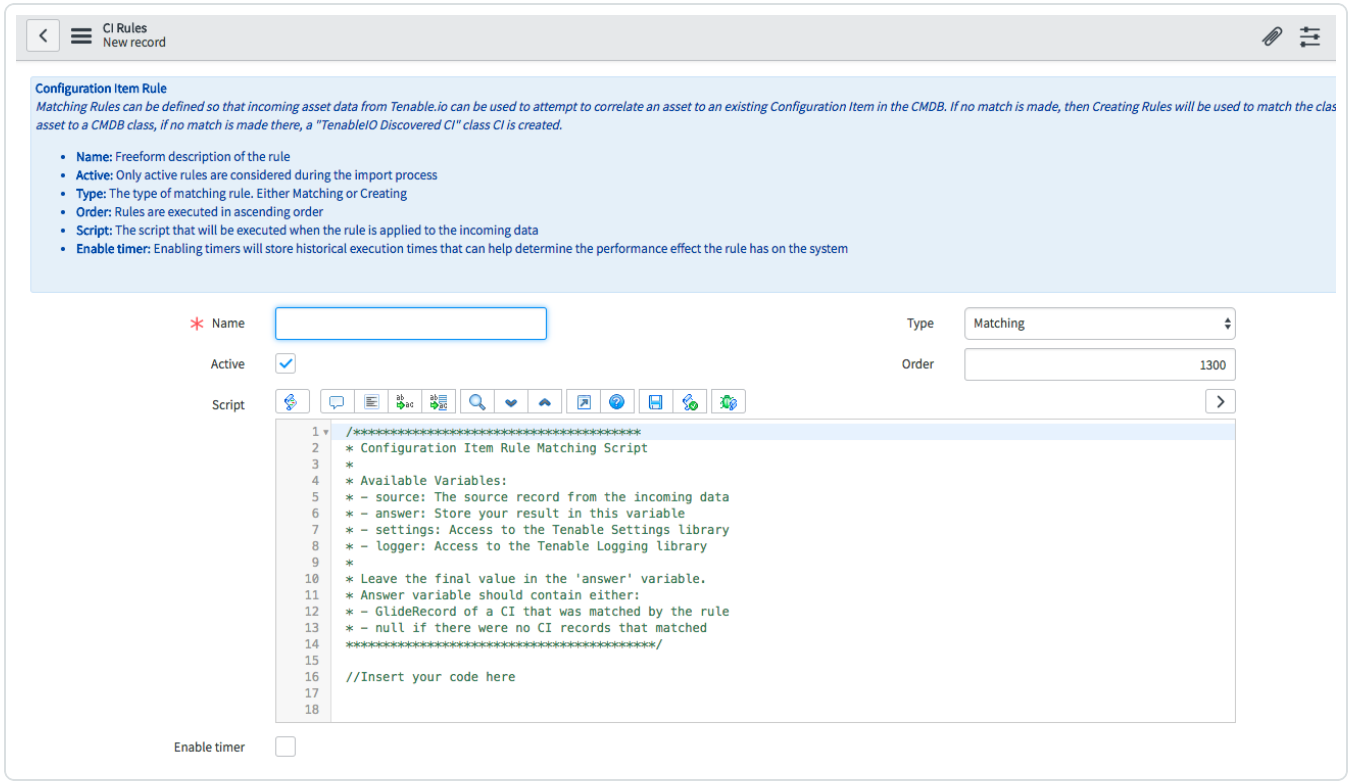
See the Assets Optional Configuration section.

Optional Configuration

Create a Matching Rule

1. In ServiceNow, navigate to **Tenable.io for Assets** > **API Data Mappings** > **CI Matching Rules**.
2. At the top of the page, click **New**.

   The **New Record** page appears.

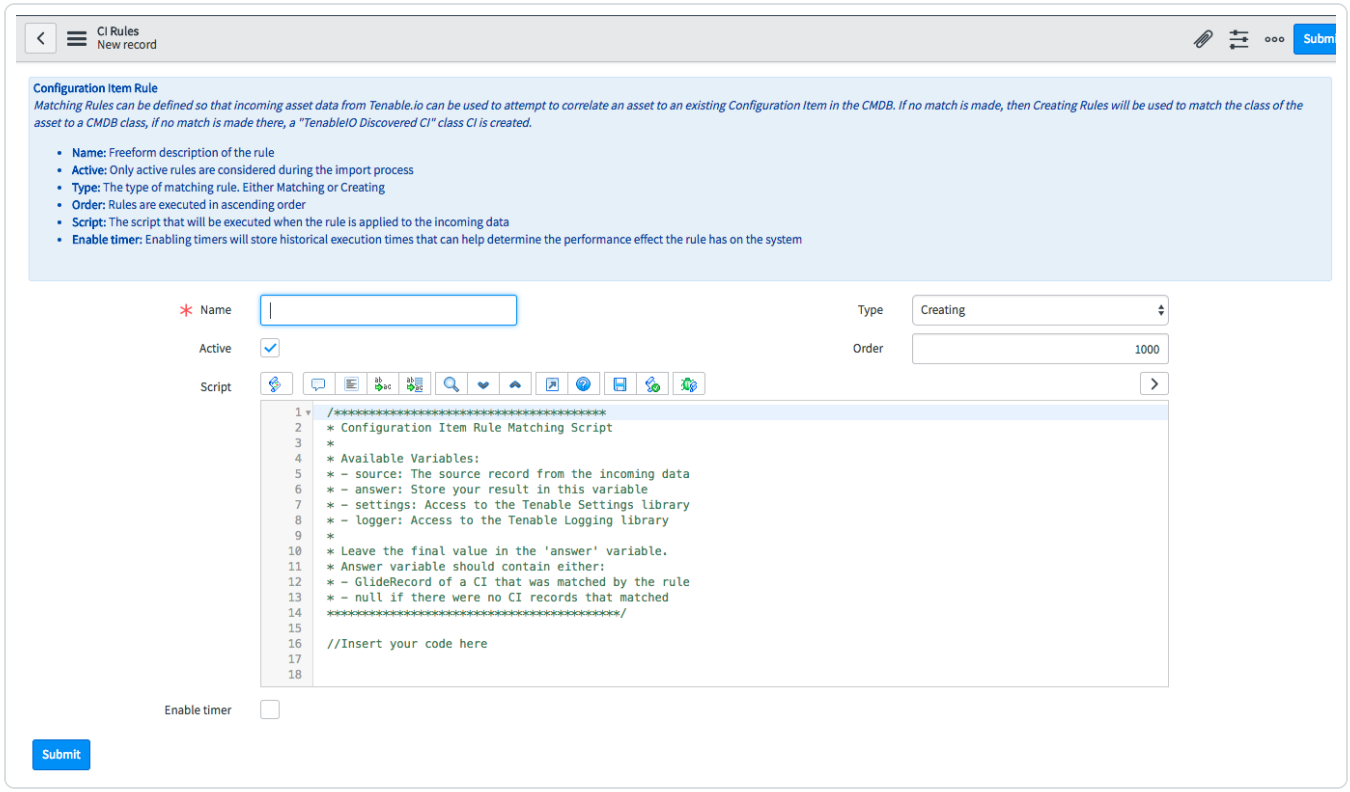


3. In the **Name** field, type a name for the matching rule.
4. From the **Type** drop-down, select **Matching**.
5. Select the **Active** check box.
6. To reorder the matching rule, edit its **Order** field. Matching rules are tried in ascending order (lowest to highest).
7. Click **Submit**.

Create a Creating Rule

1. In ServiceNow, navigate to **Tenable.io for Assets** > **API Data Mappings** > **CI Creating Rules**.
2. At the top of the page, click **New**.

   The **New Record** page appears.



3. In the **Name** field, type a name for the creating rule.
4. From the **Type** drop-down, select **Creating**.
5. Select the **Active** check box.
6. To reorder the matching rule, edit its **Order** field. Creating rules are tried in ascending order (lowest to highest).
7. Click **Submit**.

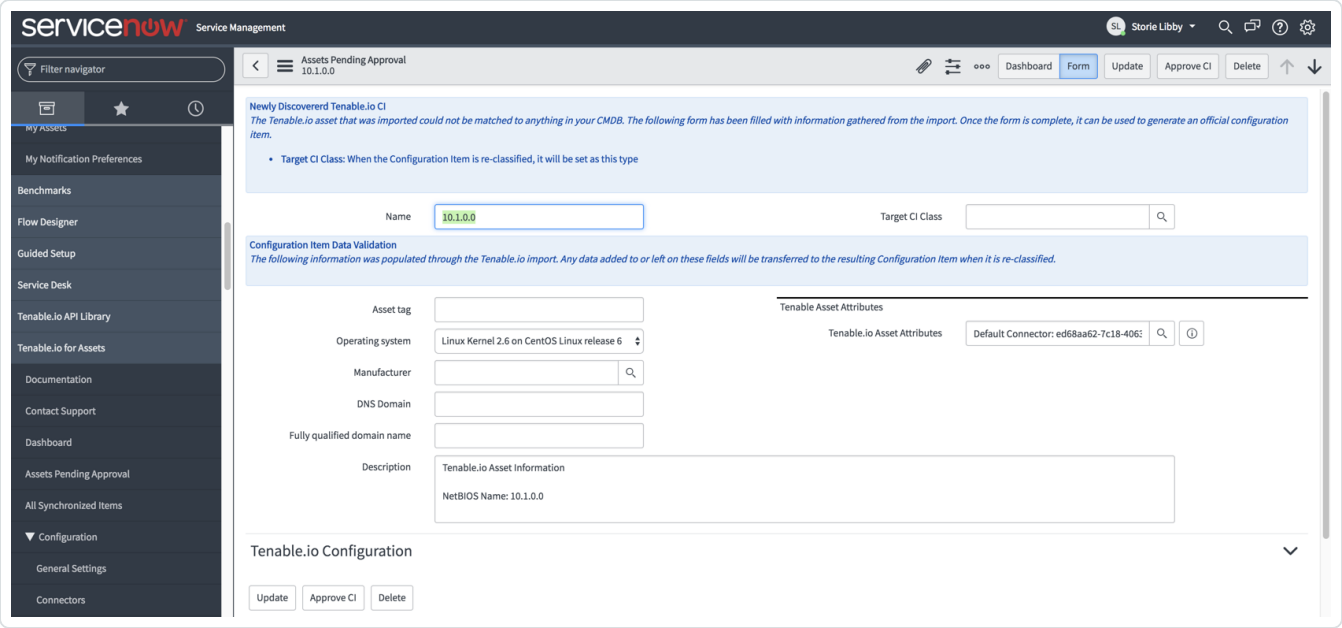
Assets Pending Approval

Pending Approval indicates that as an asset is synced, it cannot be classified as a certain type of configuration item (computer, printer, etc.). These assets must be manually approved.

1. In ServiceNow, navigate to **Tenable.io for Assets** > **Assets Pending Approval**.

To approve one asset:

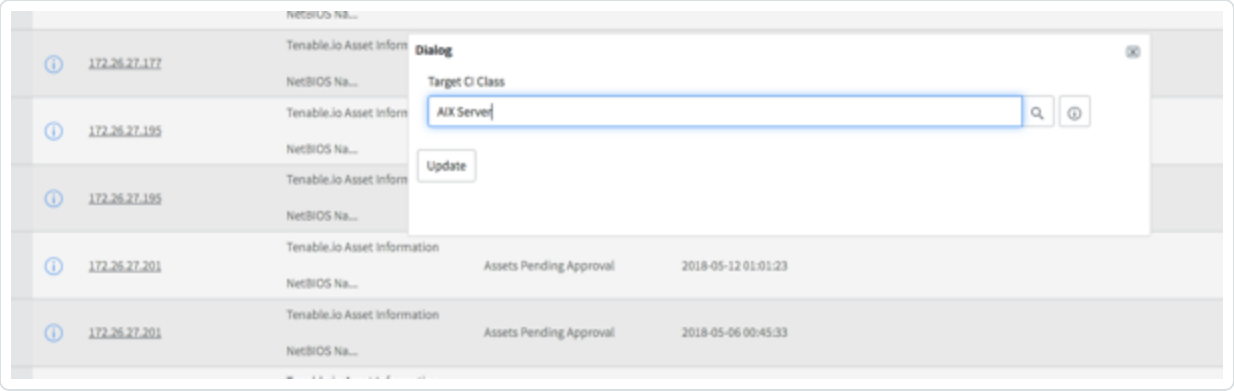
1. Click the asset(s) you wish to approve.
2. From the **Target CI Class** field, select a value for the asset.



3. Click **Approve CI**.

To approve multiple assets:

1. Select the check boxes next to the assets you wish to approve.
2. From the **Action** menu, select **Approve CIs**.
3. From the **Target CI Class** field, select a value for the assets.



4. Click **Update**.

Tenable.io for Vulnerability Response

The integration of Tenable.io for Vulnerability Response with ServiceNow's Vulnerability Response module reduces your cyber risk by allowing you to rapidly prioritize and automate the remediation of critical vulnerabilities across your most important assets.

Major Features:

- Create ServiceNow 3rd party vulnerabilities from Tenable Plugins
- Create Vulnerable Items from Tenable findings
- Customize data mapping while keeping app upgradability
- Choose which findings severities to sync from Tenable
- Automatically close vulnerable items after a Tenable remediation scan has validated the fix
- Reopen previously closed vulnerable items if they are found again at a later date.
- Limit the plugin families you want to import from Tenable findings
- Ensure the vulnerabilities are properly linked in ServiceNow CIs

Application Dependencies

- ServiceNow Kingston Platform
- ServiceNow Security Operations Vulnerability Response
- (Optional) ServiceNow MID Server - This is only required for Tenable.io On-Premises
- Tenable.io
- Tenable.io API Library (ServiceNow App) - This app is a prerequisite for all other Tenable.io apps in the ServiceNow store.
- Tenable.io for Assets (ServiceNow App)
- Tenable.io for Vulnerability Response (this app)

Integration Configuration

The following steps outline the configuration process to allow ServiceNow, through the use of the application, to poll and retrieve vulnerability data from Tenable.io. You must be logged in with a ServiceNow account that has the x_tsirm_tio_vr.admin role to perform the setup process.

The setup process involves these major steps, spelled out below in greater detail:

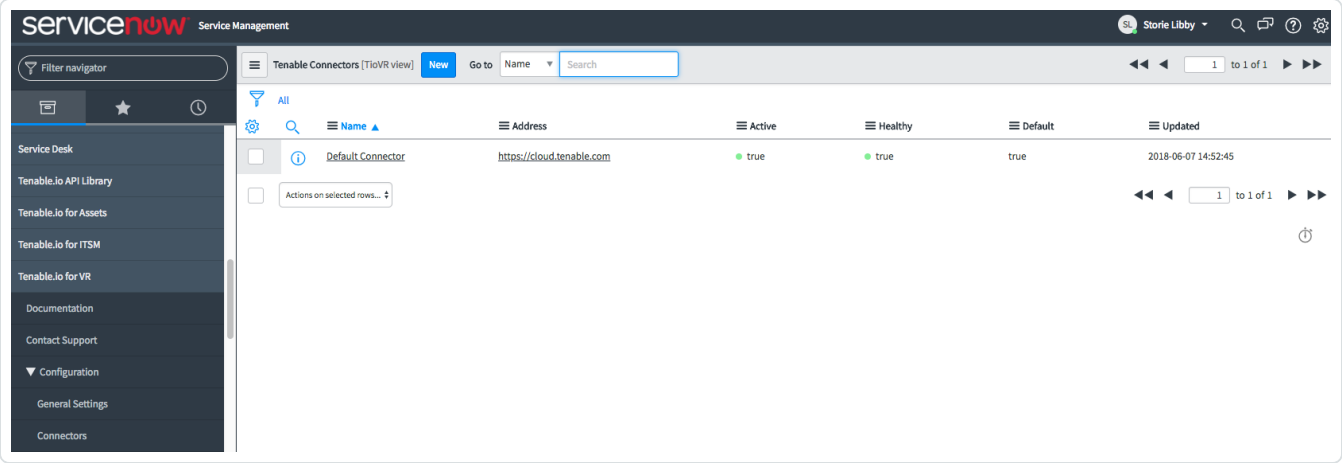
- Create a Connector
- Configure the connection in Tenable.io for VR
- Schedule an import

Configure Asset Connector

Complete the Asset Configuration steps before configuring a VR connection in ServiceNow.

Configure the ServiceNow and Tenable.io VR Connector

1. In the ServiceNow application, in the left-hand pane, navigate to **Tenable.io for VR** > **Configuration** > **Connectors**.



2. Click **Default Connector**.
3. On the **Tenable Connector** page, select the **Active** check box.
4. Click **Update**.

   By default, that evening the connector starts syncing ServiceNow vulnerabilities to Tenable.io.

Schedule an Import

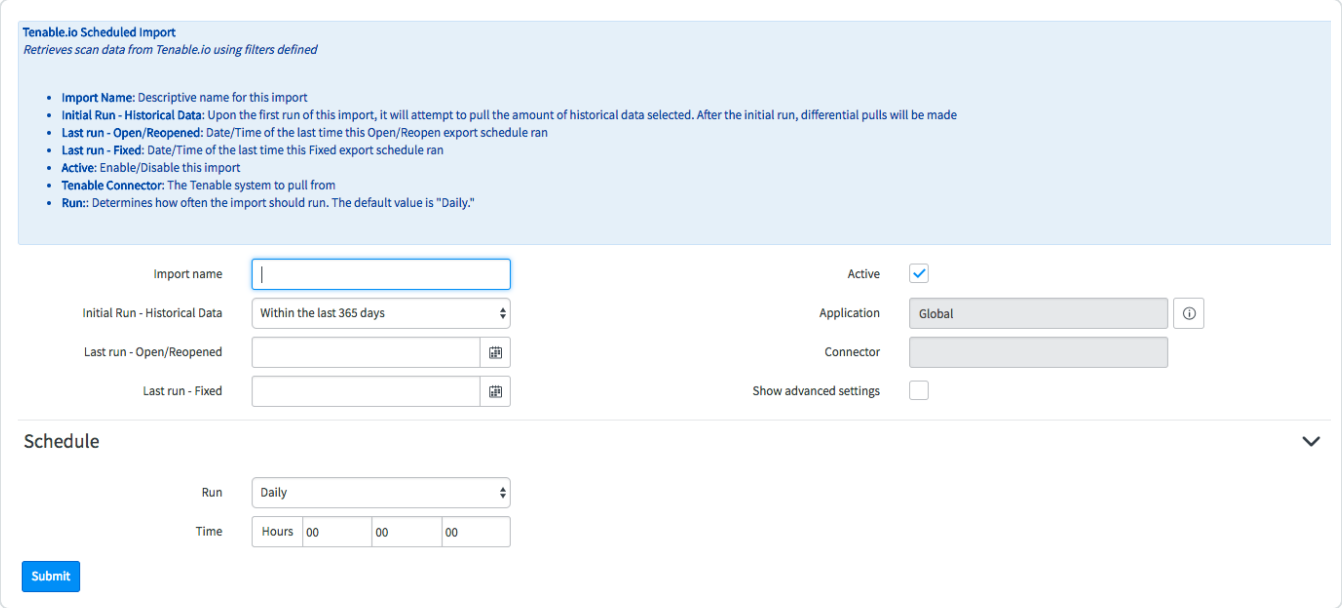
When the connection is configured, the **Open/Reopened** and **Fixed** import jobs start. The **Fixed** import job always waits for the **Open/Reopened** import job to finish so the vulnerabilities are set properly.

> **Note:** If the **Fixed** chunks have no records, the **Fixed** import job is automatically marked complete.

To create a new import job:

1. In ServiceNow, navigate to **Tenable.io for VR** > **Configuration** > **Scheduled Imports**.
2. At the top of the page, click **New**.

   The **New Record** page appears.



3. In the **Import Name** field, type a name for the import.
4. Select the **Active** check box.
5. In the **Initial Run - Historical Data** field, specify how far back (in days) to import when this Scheduled Import runs for the first time. For example, if Within 30 days is selected, vulnerabilities that were observed 15 or 25 days ago are imported into ServiceNow. After the first import, Tenable for Security Operations only requests as many days as needed to catch up with SecurityCenter as a matter of efficiency.
6. From the **Tenable Connector** drop-down, select the connector for the import.

7. In the **Schedule** section, in the Run and Time fields, select how often to request new vulnerability data from Tenable.io.
8. Click **Submit**.
9. If you want to begin the import now, visit the new scheduled import and click **Execute Now**.

Once the vulnerability import is complete, the following items appear in ServiceNow:

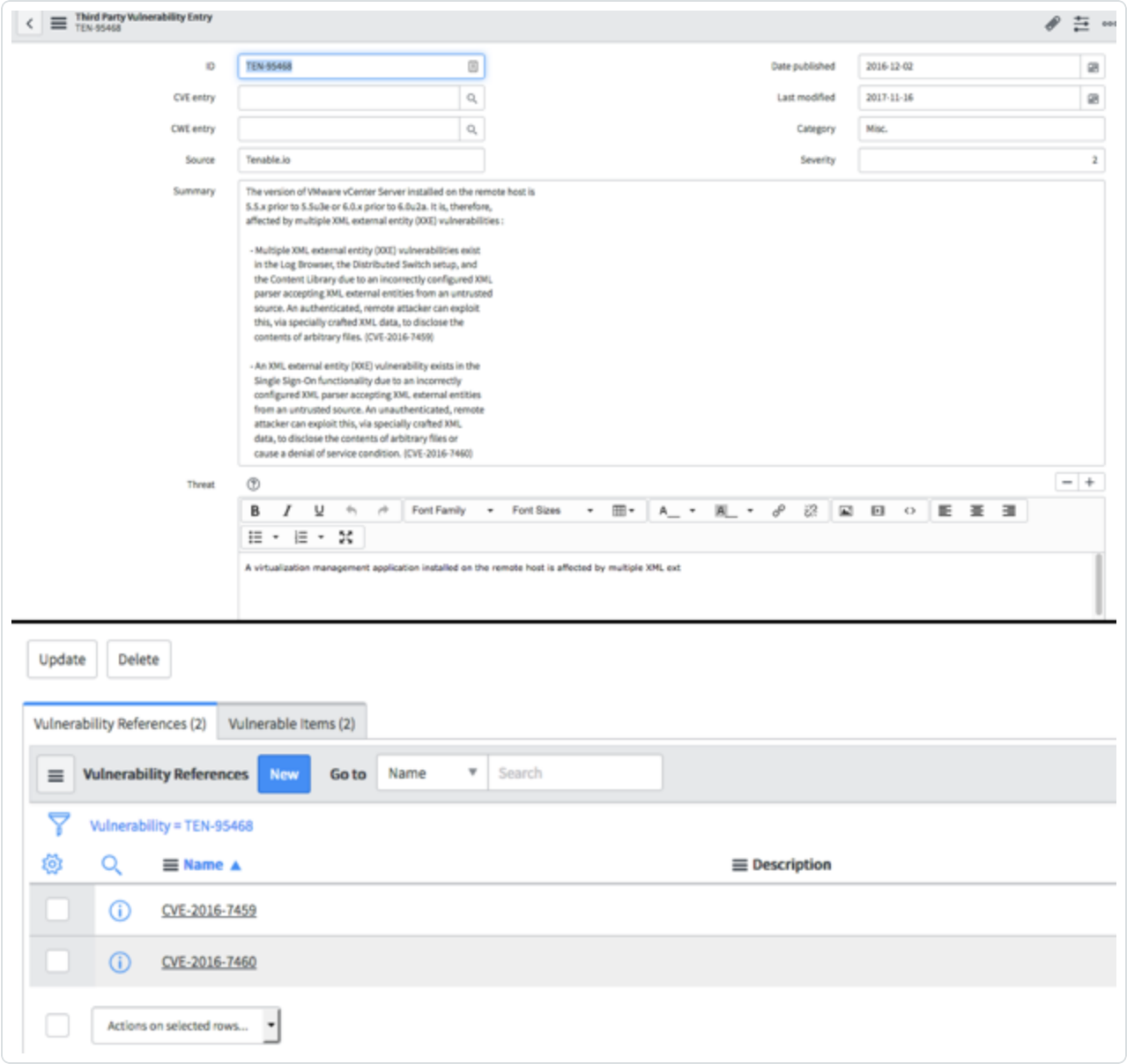
Third Party Vulnerabilities

To view Third Party Vulnerabilities:

1. Navigate to **Vulnerability** > **Libraries** > **Third Party**.

   Any vulnerabilities that include **TEN-** were imported from Tenable.io. Click a vulnerability to view the details.

   > **Note:** The bottom of the page includes Vulnerability Items and lists of CVE information linked during the import.



Configuration Items (Assets from Tenable.io)

To view Configuration Items:

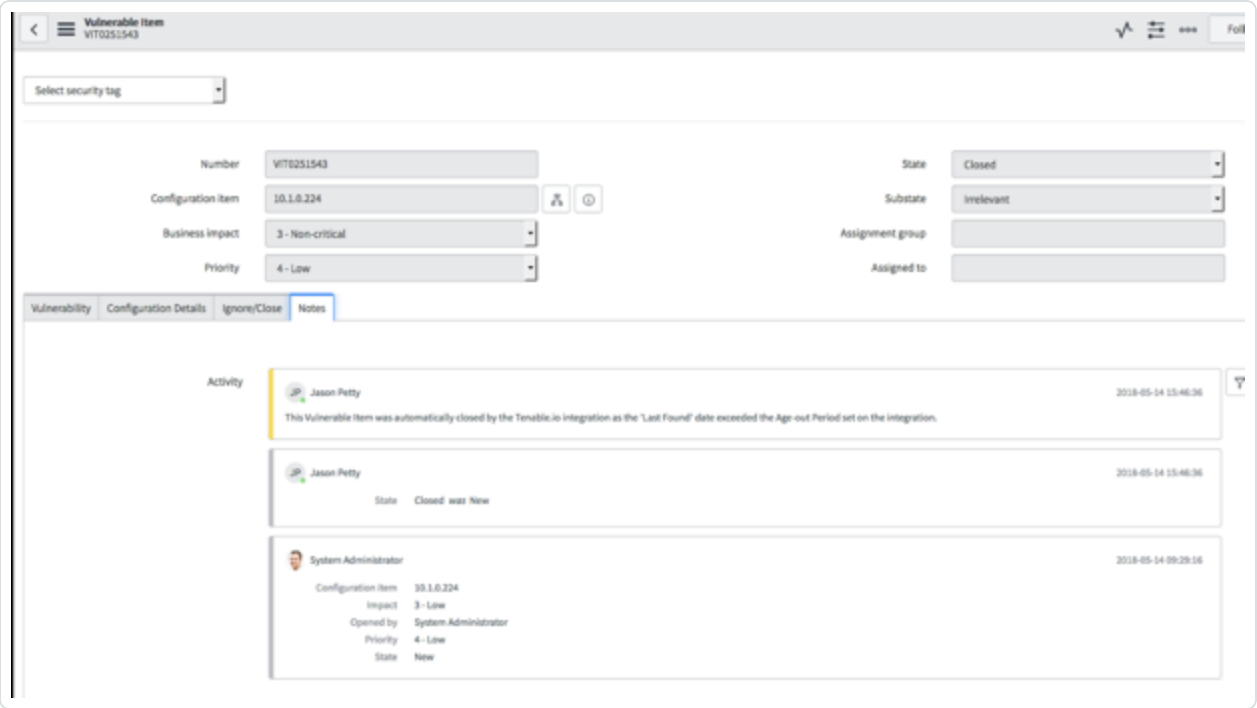
1. Navigate to **Tenable.io for Assets** > **All Synchronized Items** and **Tenable.io for Assets** > **Assets Pending Approval**.

Vulnerability Items (The linked Vulnerability and Configuration Items)

To view Vulnerability Items:

1. Navigate to **Vulnerability** > **Vulnerabilities** > **Vulnerable Items**.
2. Click any items that include **TEN-** in the name to view details.

> **Note:** If a Vulnerability Item is closed, then the fields are disabled. In the **Notes** section, you can view the notes regarding why the item is closed.



Additional Settings

Settings can be changed for more control and troubleshooting.

1. In ServiceNow, navigate to **Tenable.io for Assets** > **Configuration** > **General Settings**.

   Here you can view/edit:

   - Logging level
   - Advanced Settings
     - Age out period (days).
     - **Analysis import set name:** Name of the Scheduled Import Set that is used to import data.

2. In the **Application** menu, administrators can access modules for administering the application:

   - **API Data Mappings**
     - **Default VR Data Source:** The Data Source Object that takes one chunk record at a time and processes them into ServiceNow.
     - **Default Transform Map:** Defines how fields are mapped as records and brought back in to update ServiceNow records.
     - **Default Import Set Table:** Temporary table that data is brought into before it is transformed to create/update ServiceNow records.
   - **Diagnostics**
     - **Queued Actions**

       > **Note:** Queued actions are available to users as well as administrators.

Support

Tenable provides support for Tenable SecurityCenter and provides commercially reasonable help for the Tenable-written application components that reside within the ServiceNow platform. Because each ServiceNow instance is highly customizable, Tenable Customer Support cannot help with ServiceNow customizations such as reporting, data transformation, and workflow logic. This application is only designed to make the process easier for getting Tenable SecurityCenter vulnerability data to your ServiceNow Operations Manager.

Contacting Tenable Support

- Support Hours of Operation: 24 hours a day
- Support Days of Operation: 7 days a week
- Contact Method: Phone, Support Portal, Email, Chat
- Contact Details: 1-855- 267-7044 (Toll Free) 1-443- 545-2104 (Direct), support@tenable.com, https://support.tenable.com
- Follow the **Contact Tenable Support** link in the application to go directly to the Tenable Support Portal

Troubleshooting

How do I tell if my Assets are Syncing between ServiceNow and Tenable.io?

1. In ServiceNow, navigate to **Tenable.io for Assets** > **Diagnostics** > **Queued Actions**. Actions should appear in the **New** and **Processing** states before being removed from the list.
2. Navigate to Tenable.io.
3. Click **Assets**.
4. From the **Filter** drop-down, select **Source** equals **ServiceNow**.

   Synced assets from ServiceNow appear in the list.

How can I view the progress of my scheduled import?

1. Navigate to **Tenable.io for VR** > **Configuration** > **Scheduled Imports** > **Default Scheduled Import** > **Tenable.io Import Job Details** list.

The status of these jobs updates throughout the progress of the import:

a. Initially, the status is set to **New**.

b. While the job is running, the status updates to **Identifying Chunks**.

c. When the export job finishes and ServiceNow begins receiving chunk data from Tenable.io, the status changes to **Receiving Chunk Data**.

   Each chunk is attached to a .json file in ServiceNow. Chunks are listed under their associated job.

d. Once all the chunk data is retrieved, the status changes to **Importing**. Each chunk imports into ServiceNow one at a time.

e. Once importing is complete, the job is marked as **Complete** or **Complete with Errors**.

   Note: If a job is marked **Complete with Errors**, the job is attempted again on the next schedule.

How can I adjust the Log Level?

1. In ServiceNow, navigate to **Tenable.io for Assets** > **Configuration** > **General Settings**.
2. From the **Logging Level** drop-down, select the logging level you wish to employ.

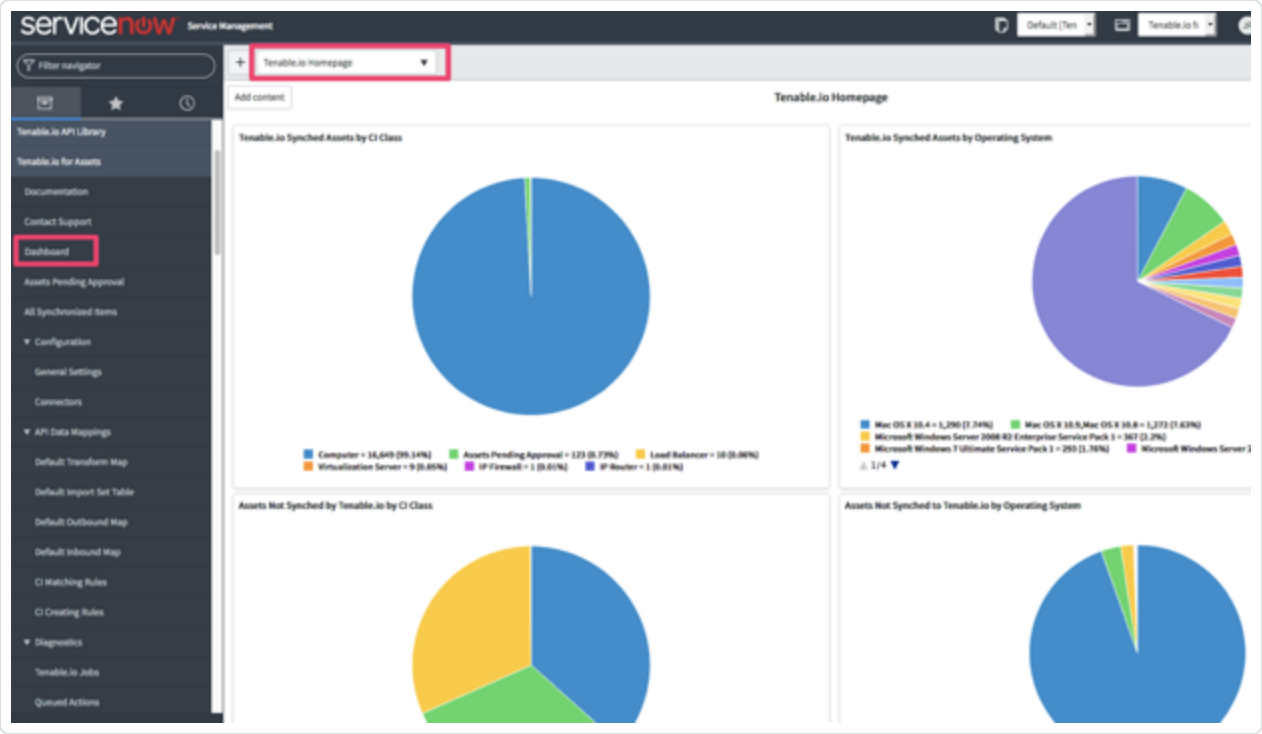
How can I Ensure my VR Connection is Active?

1. Navigate to **Tenable.io for VR** > **Diagnostics** > **Queued Actions**. Actions should appear in the **New** and **Processing** states before being removed from the list.

How can I set Tenable.io for Assets as my ServiceNow home screen?

1. Navigate to **Tenable.io for Assets** > **Dashboard**.

   Tenable.io for Assets is set as the ServiceNow home screen.



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.