# Table of Contents

**Welcome to Tenable for ServiceNow 4.x.x** .......................................................... 4

Before You Begin ......................................................................................................... 5

Application Dependencies ......................................................................................... 8

Get Started with Tenable for ServiceNow ................................................................. 9

**Install** ..................................................................................................................... 10

**Upgrade to 4.x.x Tenable Applications** ............................................................... 11

Upgrade the Tenable Applications Overview ......................................................... 13

Upgrade the Tenable Applications ........................................................................... 14

**Configure** ............................................................................................................... 17

Configure the Tenable Connector ............................................................................. 18

Disable or Enable Connectors ................................................................................. 22

Assets Configuration and Schedule Import ......................................................... 25

**Configure** ............................................................................................................... 17

VR Configuration and Schedule Import ............................................................... 32

ITSM Configuration and Schedule Import ............................................................ 37

**Settings** ................................................................................................................. 50

General Settings .................................................................................................... 51

Assets Settings ...................................................................................................... 52

VR Settings ........................................................................................................... 53

ITSM Settings ...................................................................................................... 55

Configure CI to SC Asset Group .............................................................................. 56

**Tenable Applications** .......................................................................................... 57

Tenable for Assets ................................................................................................. 58
Welcome to Tenable for ServiceNow 4.x.x

Tenable applications are designed to help customers who use ServiceNow with Tenable.io or Tenable.sc.

In the Tenable for ServiceNow 4.x.x, all configuration and import scheduling is done via the connectors. Therefore, you must properly configure your connectors for the Assets, Vulnerability Response (VR), or Information Technology Service Management (ITSM) applications to function properly.

The Tenable for Assets application integrates Tenable assets with the ServiceNow Configuration Management Database (CMDB) to use the ServiceNow Identification Reconciliation Engine (IRE). This application, once configured, allows you to bring Tenable asset data into ServiceNow as CIs and to push ServiceNow CIs to Tenable as assets.

The Tenable 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 (VI) and Tenable Plugin details into ServiceNow Third Party Vulnerabilities.

The Tenable for ITSM application integrates Tenable high and critical vulnerability findings into a custom table that can then be used to create incidents from the vulnerabilities. This application, once configured, syncs all of Tenable vulnerability findings into a custom vulnerabilities table and Tenable Plugin details into a second custom table.

This guide covers ServiceNow integration with:

- **Tenable Connector**
- **Assets Configuration and Schedule Import**
- **VR Configuration and Schedule Import**
- **ITSM Configuration and Schedule Import**
Before You Begin

You must complete the following steps before you can use the Tenable for ServiceNow application.

Configure ServiceNow Applications

Tenable recommends that you work with your internal ServiceNow Administrator or ServiceNow Consultant to help setup the applications and follow ServiceNow’s process for development which uses a development > test > production model:

- Install your development instance and tune as necessary.
- Create any modifications using update sets.
- Install the applications on a test environment and promote those update set changes for quality assurance in your test environment.
- Once approved in your test environment, install the Tenable applications on a production environment and apply the update sets.

**Note:** You need unique credentials for each ServiceNow environment.

Configure ServiceNow MID Server

The ServiceNow MID Server application facilitates communication and movement of data between the platform and external applications, data sources, and services. There can be several MID servers in an environment with some dedicated for development/testing and others dedicated to production. If your Tenable.sc resides behind a firewall on your internal network, you must use the MID server to access its data.

- Review the [MID server](#) section in the ServiceNow documentation.
- Ensure your system meets the MID server system requirements, as described in the [MID Server System requirements](#) in the ServiceNow documentation.
- Ensure your system meets the MID Server memory requirements, as described in the [Set the MID Server JVM memory size](#) section in the ServiceNow documentation.

ServiceNow Scoped Application

---

---
Application scoping protects applications by identifying and restricting access to application files and data. For more information, see the Application Scope section in the ServiceNow documentation.

Enabling the Application picker under the developer tab in the ServiceNow UI configuration menu simplifies the Tenable for ServiceNow application configuration. For more information, see the System settings for the user interface (UI) section in the ServiceNow documentation.

**Configure Users in Tenable Applications**

Tenable requires creating individual ServiceNow users in Tenable.io/Tenable.sc for each of your ServiceNow instances. This helps prevent rate limiting, data collision, etc.

Examples:

- sn_dev
- sn_test
- sn_prod

By segmenting the users, you can also limit the amount of data used in your development and test environments.

In Tenable.io, you can set up an Access Group and limit the data to specific assets to simplify the import and testing of data.

In Tenable.sc, you can create a query that limits the data presented to the development and test users. To determine the best dataset to use for your development and test environments, speak with your Tenable administrator. They can also help you ensure ServiceNow displays the best data by setting up appropriate scan cadences.

**Generate Tenable.io API Keys**

If you want to integrate ServiceNow with Tenable.io, you must generate API keys.

**Note:** You must create unique API keys for use with ServiceNow.

1. Log in to Tenable.io.
2. **Create administrator accounts** (e.g., development, test, production) dedicated for use with ServiceNow. These accounts are used by ServiceNow to connect to Tenable.io to retrieve asset data.

3. **Generate API keys** and save them for use with ServiceNow.

   **Note:** For your Tenable.io integration:
   - You must generate an API key in Tenable.io to complete the configuration. See the [Tenable.io user guide](https://www.tenable.com/docs/TenantGuide) for instructions on how to generate an API key. (Do not use this API key for any other third party or custom-built application or integration. It must be unique for each installed instance of the integration.)

4. Navigate to **Settings > Access Groups**.

5. Click the **All Assets** group.

6. Do one of the following:

   - If the **All Users** toggle is enabled, do nothing.
   - If the **All Users** toggle is disabled:
     a. Click the **+** button.
     b. Add the ServiceNow users you created in step 2.

### Generate Tenable.sc API Keys

If you want to integrate Tenable.sc with ServiceNow, you must create API keys.

**Note:** You must create unique API users for use with ServiceNow.

1. Log in to Tenable.sc.

2. **Create security manager accounts** or **Create security analyst accounts** (e.g., development, test, production) with full access dedicated for use with ServiceNow. These accounts are used by ServiceNow to connect to Tenable.sc to retrieve data and kick off remediation scans.

3. **Generate API keys** and save them for use with ServiceNow.
**Application Dependencies**

The Tenable apps for ServiceNow have the following application dependencies:

- ServiceNow Orlando, Paris, or Quebec
- ServiceNow Configuration Management Database (CMDB)
- Integration Commons for CMDB
- CMDB CI Class Models
- Tenable.io or Tenable.sc 5.7+
- Tenable Connector (ServiceNow Application) - This application is a prerequisite for all other Tenable.io applications in the ServiceNow store
- Tenable Assets - This application is dependent on Tenable Connector
- Tenable VR - This application is dependent on Tenable Assets and ServiceNow VR
- Tenable ITSM - This application is dependent on Tenable Assets
Get Started with Tenable for ServiceNow

Use the following getting started sequence to configure your Tenable for ServiceNow integration.

**Note:** It is important to configure Tenable ServiceNow applications in the following order. You must install and configure connectors before any other application. If the connectors are not properly installed, those errors will impact all subsequent application installations and configurations.

**Tip:** Tenable recommends using the tabbed view in ServiceNow to easily navigate the Tenable applications. To use this setting, go to **Settings > Forms.** Enable the **Tabbed forms** toggle.

1. **Install** the Tenable applications you want to use in ServiceNow.
   
   **Note:** Tenable Connector and Tenable Assets are required.

2. **Configure the** [Tenable Connector](#).

3. **Configure the** [Tenable for Assets](#) application. You can schedule imports in this step.
   
   **Note:** It is important to accurately configure the **Tenable for Asset** application. If this is not set up correctly, the integration does not work properly.

4. (Optional) **Configure the** [Tenable for VR](#) application. You can schedule imports in this step.

5. (Optional) **Configure the** [Tenable for ITSM](#) application. You can schedule imports in this step.

6. **Configure advanced options.**
Install

To download the Tenable applications, go to the ServiceNow App Store. For more information on how to download applications from the App Store, see the ServiceNow documentation.

The following Tenable applications are available in the ServiceNow App Store:

- Tenable Connector (Required)
- Tenable for Assets (Required)
- Tenable for Vulnerability Response (VR) (Optional)
- Tenable for ITSM (Optional)
Upgrade to 4.x.x Tenable Applications

Step 1: Upgrade the Applications

While the upgrade is seamless from an application perspective, we have moved from a custom CI matching/create engine to the ServiceNow Identification Reconciliation Engine (IRE). This change means that you must first understand IRE and plan for testing to ensure that IRE works as expected before upgrading production and/or vulnerability data.

Two major items take place during application upgrade:

- All CIs that are in the Assets Pending Approval class are moved to one of the following new ServiceNow classes:
  - Unclassified Hardware
  - Incomplete IP

  This allows Tenable to utilize out-of-the-box CI classes and remove our custom CI classes in subsequent versions of the application.

- The upgrade generates IRE payloads for every CI with Tenable asset attributes. This ensures that any previous matches continue working as they did prior to the upgrade.

While IRE provides a standardized engine for bringing third-party asset data into ServiceNow, there are some limitations in IRE. These limitations are not specific to Tenable or Tenable data, but rather are part of the design/functionality of the IRE. You must extensively test and tune how Tenable assets are brought in using IRE. If you have questions or need assistance with tuning IRE, please contact your ServiceNow representative.

It is important that every unique Tenable asset translates to a unique CI in ServiceNow. Otherwise, you are guaranteed to lose Tenable vulnerability data when it imports into ServiceNow.

Moving forward, be sure to follow the Asset application setup procedures. For more information, see the IRE Rules instructions in the Assets Configuration section.

Step 2: Review the Upgrade History and Resolve Conflicts

If there are problems with your upgrade, you must review the Upgrade History and manually resolve any conflicts.
To manually resolve conflicts with your upgrade:

1. Log in to ServiceNow.
2. In the left panel, in the Filter Navigator, type "Upgrade History".
3. Click Upgrade History.
   
   The Upgrade History page appears.
4. In the To box, type "x_tsirm*".
5. On your keyboard, press Enter.
   
   A list of system upgrades appears.
6. Locate item in the list with a value in the Change skipped column.
7. For each of these items, in the From column, click n/a.
8. Manually review and merge each skipped change.

**Note:** When opening a support case, you must provide proof that the above steps have been completed, as most issues revolve around the incorrect completion of these steps.

---

**Step 3: Delete Leftover Artifacts**

Occasionally, older application files, or artifacts, may not get deleted even after performing the tasks in Step 2: Review the Upgrade History and Resolve Conflicts. If you encounter this problem, view this Knowledge Base article to manually delete any leftover artifacts.

**Note:** When opening a support case, you must provide the output of this script, as most issues revolve around the incorrect completion of this step.
Upgrade the Tenable Applications Overview

Upgrades are periodically made to the ServiceNow Tenable Applications. When these updates are made, you must upgrade the platform to ensure the updates are applied to your system.

To upgrade the ServiceNow Tenable Applications:

1. Disable the Tenable connectors.

2. Upgrade the platform.
   
   For more information, see the ServiceNow documentation.

3. For each of the Tenable Applications you installed, complete the Upgrade the Tenable Applications steps.
   
   • Upgrade the Tenable Connector
   
   • Upgrade Tenable for Assets
   
   • Upgrade Tenable for VR (if using)
   
   • Upgrade Tenable for ITSM (if using)

4. Enable the Tenable connectors.
Upgrade the Tenable Applications

Step 1: Update the Tenable Application Version

To update the version of your Tenable application:

1. In the ServiceNow filter search bar, type `system applications`.
   
   The system applications results appear.


   ![ServiceNow filter search bar](image)

   The `All Applications` page appears.

3. In the search filter, type "Tenable".
A list of installed Tenable applications appear.

4. Next to the installed application, click the version drop-down.

A list of available version updates appear.

5. Select the version that you want to update to.

6. Click **Update**.

The application updates to the version you selected.

**Step 2: Review the Upgrade History and Resolve Conflicts**

If there are problems with your upgrade, you must review the Upgrade History and manually resolve any conflicts.

To manually resolve conflicts with your upgrade:
1. Log in to ServiceNow.

2. In the left panel, in the Filter Navigator, type "Upgrade History".

3. Click Upgrade History.

   The Upgrade History page appears.

4. In the To box, type "x_tsirm*".

5. On your keyboard, press Enter.

   A list of system upgrades appears.

6. Locate item in the list with a value in the Change skipped column.

7. For each of these items, in the From column, click n/a.

8. Manually review and merge each skipped change.

Step 3: Delete Leftover Artifacts

Occasionally, older application files, or artifacts, may not get deleted even after performing the tasks in Step 2: Review the Upgrade History and Resolve Conflicts. If you encounter this problem, view this Knowledge Base article to manually delete any leftover artifacts.
Configure your Tenable application.

1. Configure the Tenable Connector
2. Configure Tenable for Assets
3. (Optional) Configure Tenable for VR
4. (Optional) Configure Tenable for ITSM
Configure the Tenable Connector

The Tenable Connector provides all API interactions between your Tenable applications (Tenable.io or Tenable.sc) and ServiceNow instance.

**Note:** In ServiceNow, you must have the x_tsirm_api_access admin role to perform the basic connector setup process.

**Note:** The ServiceNow configuration only supports Tenable.sc versions 5.7 and later.

Before you begin:

For Tenable.io:

**Required User Role:** Administrator

- You must have your Tenable.io API keys.

**Note:** For your Tenable.io integration:

- You must generate an API key in Tenable.io to complete the configuration. See the [Tenable.io user guide](#) for instructions on how to generate an API key. (Do not use this API key for any other third party or custom built application or integration. A unique API key is required for each installed instance of the integration.)

For Tenable.sc:

**Required User Role:** Security Analyst

To configure the Tenable connector for Tenable.io or Tenable.sc:

1. Log in to ServiceNow.
2. In the left navigation pane, click Tenable Connector > Connectors.
   
   The Tenable Connectors page appears.
3. Click New.
4. From the Tenable Product drop-down box, select Tenable.io or Tenable.sc.
5. If you are in a domain separated environment, in the **Domain** box, type the domain into which to bring connector data.

6. Select the **Active** check box.

7. In the **Scheduled Job Run As** box, type the username of the user with which you want to import data.

   **Note:** If you are in a domain separated environment, this field is required. The user must be part of the domain specified in step 5.

8. In the **Name** text box, type a name for the connector.

9. Complete the configurations for your selected Tenable application.

**For Tenable.io:**

![Image of Tenable Connector configuration](image)

- **Tenable Product**
  - **Tenable.io**

- **Active**
  - **Default**

- **Name**

- **Address**
  - `https://cloud.tenable.com`

- **Access Key**

- **Secret Key**

   **a.** In the **Address** text box, type an IP address or DNS name for the connector. ServiceNow populates this with the Tenable.io IP address.

      **Note:** You must type `https://` before the IP or DNS name.

   **b.** In the **Access Key** text box, type the access key provided by your Tenable administrator.

   **c.** In the **Secret Key** text box, type the secret key provided by your Tenable administrator.

**For Tenable.sc:**
a. Next to **Address**, click the lock button.

b. In the **Address** text box, type an IP address or DNS name for the connector.

   **Note:** You must type `https://` before the IP or DNS name.

c. Click the lock button to lock the address.

d. In the **MID Server** text box, search for and select a MID server that can access your Tenable.sc server.

e. Do one of the following:

   - If you check the **Use User/Password** check box:
     
     i. In the **API Username** text box, type the API username provided by your Tenable administrator.

     ii. In the **API Password** text box, type the API password provided by your Tenable administrator.

   - If you do not check the **Use User/Password** check box:

     i. In the **Access Key** text box, type the API access key provided by your Tenable administrator.

     ii. In the **Secret Key** text box, type the API secret key provided by your Tenable administrator.

   **Tip:** To save your selected configuration options without navigating away from the page:
1. Right click in the top menu that contains the Tenable Connector heading and menu. A list of options appears.

2. Click **Save**.

10. (Optional) In the **General Settings** section, you can specify your **Max ECC Wait Time** (in seconds) and **Request Timeout** (in seconds) for each of your configured connectors.

11. In the **Asset Settings** section, you can set the **Asset Logging Level**, **Asset Max Cumulative Log Entries**, and **Asset Max Cumulative Log Sizes**. The default setting for the logging levels is **Errors Only**.

12. In the **Additional Asset Settings** section, you can set **New Record Sync Frequency** (in minutes), **Record Update Sync Frequency** (in minutes), **Asset Max Job Log** (in days), and **Asset Max Job Wait** (in days).

**Note:** You may have additional settings options on your connector page depending on the Tenable applications you have installed (e.g., Tenable Assets [**Assets Settings**], Tenable VR [**VR Settings**], and Tenable ITSM [**ITSM Settings**]).

**Note:** For more information about ServiceNow settings, see the [ServiceNow documentation](#).

13. Click **Test the Connector**.

**Note:** If the connector test fails, check your username, password, and API Keys and retest the connector.

14. Click **Update**.
Disable or Enable Connectors

You can enable or disable your Tenable connectors.

**Disable Connector**

**Enable Connector**

To disable your Tenable Connector:

1. In the ServiceNow filter search bar, type *Tenable*.
   
The Tenable applications appear.

2. In the left-hand menu, click *Tenable Connector*.

3. In the sub-menu, click *Connectors*.
   
   Your configured Tenable connectors appear.

4. Select your Tenable connector.

   ![Tenable Connectors](image)

   The selected connector page appears.

5. At the top of the page, deselect the **Active** checkbox.
6. Click **Update**.

The **Tenable Connector** is deactivated.

7. Repeat this to deactivate all your connectors.

To enable your Tenable Connector:

1. In the ServiceNow filter search bar, type *Tenable*.

   The Tenable applications appear.

2. In the left-hand menu, click **Tenable Connector**.

3. In the sub-menu, click **Connectors**.

   Your configured Tenable connectors appear.

4. Select your Tenable connector.

   The selected connector page appears.

5. At the top of the screen, select the **Active** checkbox.
6. Click **Update**.

   The **Tenable Connector** is activated.

7. Repeat this to activate all your connectors.
Assets Configuration and Schedule Import

**Note:** Tenable for Assets only supports Tenable.sc versions 5.7 and later.

The asset integration allows ServiceNow to retrieve and accurately match Tenable assets to your existing CIs. Tenable for VR and ITSM both rely on this app for finding the correct asset related to vulnerabilities from Tenable.

**Note:** It is extremely important that you completely setup and tune this integration to correctly match Tenable Assets to ServiceNow CIs before moving on to Tenable for VR or Tenable for Assets.

To setup the asset integration configuration, you must:

- [Configure the Tenable Connector](#)
- [Configure Assets to Sync from Tenable to ServiceNow](#)
- [Configure IRE Rules](#)
- [(Optional) Configure Assets to Sync from ServiceNow to Tenable.io](#)

**Configure Assets to Sync from Tenable to ServiceNow**

1. Log in to ServiceNow.
2. Go to the Tenable Connector Application.
3. In the left-hand menu, click **Tenable Connector**.
4. In the sub-menu, click **Connectors**.
   - The **Tenable Connectors** page appears.
5. Click the Tenable connector you want to use: **Tenable.io** or **Tenable.sc**.
   - The **Tenable Connector** page appears.
6. In the **Scheduled Jobs** section, click **New**.
   - The **Tenable Scheduled Import** page appears. By default, the **Tenable Product** and **Connector** fields populate with the Tenable application/connector you selected in step 3.
7. From the **Tenable Application** drop-down box, select **Tenable for Assets**.
8. From the **Tenable Job Type** drop-down box, select the appropriate job type.

9. If you are in a domain separated environment, in the **Domain** box, type the domain into which to bring connector data.

10. (For Tenable.io) From the **Import Export** drop-down box, select **Import**. Import is selected by default.

11. In the **Name** text box, type a unique name for this scheduled job.

12. Configure the options for your import.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Update Pull</td>
<td>Sets a date and time for the next pull.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This field is set by the scheduled job as it runs.</td>
</tr>
<tr>
<td>Active</td>
<td>If selected, an asset sync is automatically queued when you submit the import or export. Default setting: selected.</td>
</tr>
<tr>
<td>Order</td>
<td>Prioritizes when the import should run. (This option populates when you select the <strong>Tenable Application</strong> in step 6. However, you can modify it by typing in the text box.)</td>
</tr>
<tr>
<td>-------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Default Chunk Size</td>
<td>The number of records pulled in segments during the import. (This option populates when you select the <strong>Tenable Application</strong> in step 6. However, you can modify it by typing in the text box.)</td>
</tr>
<tr>
<td>SC Query</td>
<td>(Only for Tenable.sc) Select the Tenable.sc query to use for the import.</td>
</tr>
<tr>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>Record Update Sync Frequency</td>
<td>The frequency of pulling assets (in minutes). The default setting is once a day (1,440 minutes).</td>
</tr>
</tbody>
</table>

**Note:** This option is hard coded and can only be changed via the code.

13. Click **Submit**.

**Note:** Ensure that you accurately configure the assets. Asset configuration is key in making the integration work properly. Errors in these configuration steps, effect all future configurations.

**Configure IRE Rules**

Be sure to review the [ServiceNow 3.0.x upgrade instructions](#) to ensure the IRE will work in your environment.

**Note:** By default, Tenable data updates CI fields on each import. If you are using ServiceNow Paris or later, you can use [reconciliation rules](#) to control what asset data updates.

1. Log in to ServiceNow.

2. In the left panel, in the **Filter navigator**, type "CI Class Manager".

3. Click **CI Class Manager**.

The **CI Class Manager** page opens.
4. Click **Open Hierarchy**.

   The **CI Classes** panel opens.

5. In the **CI Classes** panel, click **Hardware (2032)**.

   The **Hardware** page appears.

6. In the **Class Info** section, click **Identification Rule**.

   The **Identification Rule** page appears.

7. Clone or edit the **Serial Number** rule.

   The **Edit Identifier Entry** window appears.

8. Click **Advanced Options**.

9. In the **Advanced Options** section, deselect the **Enforce exact count match** check box.

10. Click **Save**.

    You return to the **Identification Rule** page.

11. Clone or edit the **Network Adapter** rule.

    The **Edit Identifier Entry** window appears.

12. Repeat steps 8-10 for the **Network Adapter** rule.

**What to do next:**

Clean the correlation data to ensure IRE rule changes are applied on the next import.

Below are example background scripts that you can run to clean direct correlations between Tenable data, the CMDB, and IRE data. When you make changes to the IRE rules to better match third party data to your existing ServiceNow CIs, you must clean up old relationships to ensure the updated rules are applied.

```javascript
//Asset Attributes cleanup
var assetInfo = new GlideMultipleDelete('x_tsirm_tio_cmdb_asset_attributes');
assetInfo.execute();
// Cleanup source uniqueness
This will force IRE matching
```
var assetSysSource = new GlideMultipleDelete("sys_object_source");
assetSysSource.addQuery("name", "STARTSWITH", "Tenable");
assetSysSource.execute();

(Optional) Configure Assets to Sync from ServiceNow to Tenable.io

**Note:** Please work with your ServiceNow administrator to perform the following task. The information provided below should be used as a guideline. Your administrator can assist in tuning the export to achieve your desired results.

1. Log in to ServiceNow.
2. In the left-hand menu, click **Tenable Connector**.
3. In the sub-menu, click **Connectors**.
   
   The **Tenable Connectors** page appears.
4. Click the Tenable connector you want to use: **Tenable.io** or **Tenable.sc**.
   
   The **Tenable Connector** page appears.
5. In the **Scheduled Jobs** section, click **New**.
   
   The **Tenable Scheduled Import** page appears. By default, the **Tenable Product** and **Connector** fields populate with the Tenable application/connector you selected in step 3.
6. From the **Tenable Application** drop-down box, select **Tenable for Assets**.
7. From the **Tenable Job Type** drop-down box, select the appropriate job type.
8. If you are in a domain separated environment, in the **Domain** box, type the domain into which to bring connector data.
9. (For Tenable.io) From the **Import Export** drop-down box, select **Import**. Import is selected by default.
10. In the **Name** text box, type a name for the export.
11. Configure the options for your export.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Update Pull</td>
<td>Sets a date and time for the next pull.</td>
</tr>
<tr>
<td>Active</td>
<td>If selected, an asset sync is automatically queued when you submit the import or export. Default setting: selected.</td>
</tr>
<tr>
<td>Order</td>
<td>The order that the import should run. (This option populates when you select the <strong>Tenable Application</strong> in step 6. However, you can modify it by typing in the text box.)</td>
</tr>
<tr>
<td>Default Chunk Size</td>
<td>The number of records pulled in segments during the import. (This option populates when you select the <strong>Tenable Application</strong> in step 6. However, you can modify it by typing in the text box.)</td>
</tr>
</tbody>
</table>

**Configuration**

<table>
<thead>
<tr>
<th>Record Update Sync Frequency</th>
<th>The frequency of pulling assets (in minutes). The default setting is once a day (1,440 minutes).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
<td>This option is hard coded and can only be changed via the code.</td>
</tr>
</tbody>
</table>

| Source table and Conditions  | Select source tables and use filter conditions to specify export information.                   |

12. Click **Submit**.
VR Configuration and Schedule Import

This section describes how to configure Tenable for VR.

**Note:** The Tenable for Vulnerability Response application only supports Tenable.sc versions 5.7 and later.

The VR integration configuration allows ServiceNow to poll and retrieve vulnerability data from Tenable.

Before you begin:

- In ServiceNow, you must have an account that has the `x_tsirm_tio_vr.admin` role complete the setup.

- **Configure the Tenable Connector**

  **Note:** You must completely configure and tune Tenable for Assets to correctly match Tenable Assets with ServiceNow CIs. If you do not do this first, you will have issues with VR.

Configure the ServiceNow and Tenable VR Connector

1. Log in to ServiceNow.

2. In the left-hand menu, click **Tenable Connector**.

3. In the sub-menu, click **Connectors**.

   The **Tenable Connectors** page appears.

4. Click the Tenable connector you want to use: **Tenable.io** or **Tenable.sc**.

   The **Tenable Connector** page appears.

5. In the **Scheduled Jobs** section, click **New**.

   The **Tenable Scheduled Import** page appears. By default, the **Tenable Product** and **Connector** fields populate with the Tenable application/connector you selected in step 3.

6. From the **Tenable Application** drop-down box, select **Tenable for VR**.

   Tenable.io
7. From the **Tenable Job Type** drop-down box, select the appropriate job type.

8. If you are in a domain separated environment, in the **Domain** box, type the domain into which to bring connector data.

9. (For Tenable.io) From the **Import Export** drop-down box, select **Import**. Import is selected by default.

10. In the **Name** text box, type a name for the VR.

11. Configure the options for your import.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initial Run Historical Data</strong></td>
<td>Specifies how far back (in days) to import when run for the first time. For example, if <strong>Within 30 days</strong> is selected, vulnerabilities that were observed 15 or 25 days ago are imported into ServiceNow. After the first import, Tenable only requests as many days as needed to catch up with Tenable.io or Tenable.sc.</td>
</tr>
<tr>
<td><strong>Run Fixed Query on Initial Run</strong></td>
<td>Pulls fixed vulnerabilities from the past on the first import. This allows for more complete reporting in ServiceNow for prior fixed vulnerabilities. Default setting: deselected.</td>
</tr>
<tr>
<td><strong>Last Run - Opened/Reopened</strong></td>
<td>The date and time that the open/reopened import was last run.</td>
</tr>
<tr>
<td><strong>Last run - Fixed</strong></td>
<td>The date and time that the fixed import was last run.</td>
</tr>
<tr>
<td><strong>Active</strong></td>
<td>If selected, an asset sync is automatically queued when you submit the import or export. Default setting: selected.</td>
</tr>
<tr>
<td><strong>Default Chunk Size</strong></td>
<td>The number of records pulled in segments during the import. (This option populates when you select the <strong>Tenable Application</strong> in step 6. However, you can modify it by typing in the text box.) (For Tenable.io, you should not change this unless Tenable advises you to do so.)</td>
</tr>
</tbody>
</table>
Included Severities  | (Only for Tenable.io) Select the severity levels to import. If not specified, all severity levels are imported.
---|---
Included Plugin Family Names  | (Only for Tenable.io) Select plugin family names to include in the import. If not specified, all families are imported.
SC Query  | (Only for Tenable.sc) The Tenable.sc query used for the import or export.

**Schedule**

| Run | The frequency with which you want the import to run. |
| Time | The set time (hh/mm/ss) to run the import. |

12. In the **Access Key** text box, type the access key provided by your Tenable administrator.

13. In the **Secret Key** text box, type the secret key provided by your Tenable administrator.

14. Click **Update**.

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

### Third Party Vulnerabilities

To view third party vulnerabilities:

- Navigate to **Vulnerable Items > Libraries > Third Party**.

Vulnerabilities that include **TEN-** were imported from Tenable.io or Tenable.sc. 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.
Vulnerability Items (Linked Vulnerability and Configuration Items)

To view vulnerability items:

- Navigate to **Vulnerabilities > Vulnerable Items**.

Vulnerabilities that include **TEN-** were imported from Tenable.io and Tenable.sc. Click a vulnerability to view the details.

**Note:** If a vulnerability item is closed, the text boxes are disabled. In the **Notes** section, you can view information about why the item is closed.
ITSM Configuration and Schedule Import

This section describes how to configure Tenable for ITSM.

**Note:** The ITSM app only pulls in Critical and High vulnerabilities. If you require more flexibility/customization, you can upgrade to the free Tenable for Vulnerability Response application.

**Note:** The ServiceNow configuration only supports Tenable.sc versions 5.7 and later.

The ITSM integration configuration allows ServiceNow to poll and retrieve vulnerability data from Tenable.io/Tenable.sc.

Before you begin:

In ServiceNow, you must have the `x_tsirm_tio_itsm.admin` role to complete the setup.

**Note:** You must completely configure and tune Tenable for Assets to correctly match Tenable Assets with ServiceNow CIs. If you do not do this first, you will have issues with ITSM.

To setup the ITSM integration configuration, you must:

- Configure the Tenable Connector
- Create the ServiceNow and Tenable.io ITSM Connector
- Create an Incident Rule
- ITSM Configuration and Schedule Import

Create the ServiceNow and Tenable.io ITSM Connector

1. Log in to ServiceNow.

2. In the left-hand menu, click **Tenable Connector**.

3. In the sub-menu, click **Connectors**.

   The **Tenable Connectors** page appears.

4. Click the Tenable connector you want to use: **Tenable.io** or **Tenable.sc**.

   The **Tenable Connector** page appears.
5. In the **Scheduled Jobs** section, click **New**.

   The **Tenable Scheduled Import** page appears. By default, the **Tenable Product** and **Connector** fields populate with the Tenable application/connector you selected in step 3.

6. From the **Tenable Application** drop-down box, select **Tenable for ITSM**.

---

### Tenable Scheduled Import

**Tenable Application**: Tenable for ITSM

**Tenable Product**: Tenable.io

**Connector**: T.io Small

**Name**: 

**Initial Run - Historical Data**

- **Run Fixed Query on Initial Run**
- **Default chunk size**: 50

**Schedule**

- **Run**: Daily

---

**Tenable.sc**
7. If you are in a domain separated environment, in the **Domain** box, type the domain into which to bring connector data.

8. (For Tenable.io) From the **Import Export** drop-down box, select **Import**. Import is selected by default.

9. In the **Name** text box, type a name for the import.

10. Configure the options for your import.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Run - Historical Data</td>
<td>The amount of time (in days) of how far back you want to pull data.</td>
</tr>
<tr>
<td>Run Fixed Query on Initial Run</td>
<td>Pulls fixed vulnerabilities on the first import. Default setting: deselected.</td>
</tr>
<tr>
<td>Last Run - Opened/Reopened</td>
<td>The date and time that the open/reopened import was last run.</td>
</tr>
<tr>
<td>Last run - Fixed</td>
<td>The date and time that the fixed import was last run.</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td>Active</td>
<td>If selected, an asset sync is automatically queued when you submit the import or export. Default setting: selected.</td>
</tr>
<tr>
<td>Default Chunk Size</td>
<td>The number of records pulled in segments during the import. (This option populates when you select the <strong>Tenable Application</strong> in step 6. However, you can modify it by typing in the text box.) (For Tenable.io, you should not change this unless Tenable advises you to do so.)</td>
</tr>
<tr>
<td>SC Query</td>
<td>(Only for Tenable.sc) The Tenable.sc query used for the import or export.</td>
</tr>
</tbody>
</table>

**Schedule**

<table>
<thead>
<tr>
<th>Run</th>
<th>The frequency with which you want the import to run.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>The set time (hh/mm/ss) to run the import.</td>
</tr>
</tbody>
</table>

11. Click **Update**.

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

**Create an Incident Rule**

Incident Rules must be created/enabled for the integration to create incidents. By default, a disabled example rule comes with the application.

1. From the left navigation pane, navigate to **Tenable for ITSM > Configuration > Incident Rules**.

   The **Incident Rules** page appears.

2. Click **New**.

   The **New record** page appears.
3. In the **Name** text box, type a name for the matching rule.

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

5. (Optional) If you want to use scripting to create this rule, click the **Advanced** check box and type the desired script.

### Incident rule field options

<table>
<thead>
<tr>
<th>Column label</th>
<th>Column name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sys ID</td>
<td>sys_id</td>
<td>Sys ID (GUID)</td>
</tr>
<tr>
<td>acceptRisk</td>
<td>u_acceptrisk</td>
<td>String</td>
</tr>
<tr>
<td>asset</td>
<td>u_asset</td>
<td>String</td>
</tr>
<tr>
<td>asset/agent_uuid</td>
<td>u_asset_agent_uuid</td>
<td>String</td>
</tr>
<tr>
<td>asset/bios_uuid</td>
<td>u_asset_bios_uuid</td>
<td>String</td>
</tr>
<tr>
<td>asset/device_type</td>
<td>u_asset_device_type</td>
<td>String</td>
</tr>
<tr>
<td>Field</td>
<td>Uppercase Field</td>
<td>Type</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------</td>
<td>------</td>
</tr>
<tr>
<td>cvssVector</td>
<td>u_cvssvector</td>
<td>String</td>
</tr>
<tr>
<td>exploitAvailable</td>
<td>u_exploitavailable</td>
<td>String</td>
</tr>
<tr>
<td>exploitEase</td>
<td>u_exploitease</td>
<td>String</td>
</tr>
<tr>
<td>exploitFrameworks</td>
<td>u_exploitframeworks</td>
<td>String</td>
</tr>
<tr>
<td>family</td>
<td>u_family</td>
<td>String</td>
</tr>
<tr>
<td>family/id</td>
<td>u_family_id</td>
<td>String</td>
</tr>
<tr>
<td>first_found</td>
<td>u_first_found</td>
<td>String</td>
</tr>
<tr>
<td>fqdn</td>
<td>u_fqdn</td>
<td>String</td>
</tr>
<tr>
<td>hasBeenMitigated</td>
<td>u_hasbeenmitigated</td>
<td>String</td>
</tr>
<tr>
<td>hostname</td>
<td>u_hostname</td>
<td>String</td>
</tr>
<tr>
<td>hostUniqueness</td>
<td>u_hostuniqueness</td>
<td>String</td>
</tr>
<tr>
<td>id</td>
<td>u_id</td>
<td>String</td>
</tr>
<tr>
<td>interfaces</td>
<td>u_interfaces</td>
<td>String</td>
</tr>
<tr>
<td>ips</td>
<td>u_ips</td>
<td>String</td>
</tr>
<tr>
<td>job_type</td>
<td>u_job_type</td>
<td>String</td>
</tr>
<tr>
<td>last_fixed</td>
<td>u_last_fixed</td>
<td>String</td>
</tr>
<tr>
<td>last_found</td>
<td>u_last_found</td>
<td>String</td>
</tr>
<tr>
<td>name</td>
<td>u_name</td>
<td>String</td>
</tr>
<tr>
<td>netbiosName</td>
<td>u_netbiosname</td>
<td>String</td>
</tr>
<tr>
<td>operating_system</td>
<td>u_operating_system</td>
<td>String</td>
</tr>
<tr>
<td>output</td>
<td>u_output</td>
<td>String</td>
</tr>
<tr>
<td>patchPubDate</td>
<td>u_patchpubdate</td>
<td>String</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------</td>
<td>----------</td>
</tr>
<tr>
<td>plugin</td>
<td>u_plugin</td>
<td>String</td>
</tr>
<tr>
<td>pluginText</td>
<td>u_plugintext</td>
<td>String</td>
</tr>
<tr>
<td>plugin_bid</td>
<td>u_plugin_bid</td>
<td>String</td>
</tr>
<tr>
<td>plugin/canvas_package</td>
<td>u_plugin_canvas_package</td>
<td>String</td>
</tr>
<tr>
<td>plugin/checks_for_malware</td>
<td>u_plugin_checks_for_malware</td>
<td>String</td>
</tr>
<tr>
<td>plugin/checks_for_default_account</td>
<td>u_plugin_checkefault_account</td>
<td>String</td>
</tr>
<tr>
<td>plugin/cpe</td>
<td>u_plugin_cpe</td>
<td>String</td>
</tr>
<tr>
<td>plugin_cve</td>
<td>u_plugin_cve</td>
<td>String</td>
</tr>
<tr>
<td>plugin/cvss3_vector/availability_impact</td>
<td>u_plugin_cvss3_ability_impact</td>
<td>String</td>
</tr>
<tr>
<td>plugin/cvss3_base_score</td>
<td>u_plugin_cvss3_base_score</td>
<td>String</td>
</tr>
<tr>
<td>plugin/cvss3_temporal_vector/remediation_level</td>
<td>u_plugin_cvss3_ediation_level</td>
<td>String</td>
</tr>
<tr>
<td>plugin/cvss3_vector/access_complexity</td>
<td>u_plugin_cvss3_access_complexity</td>
<td>String</td>
</tr>
<tr>
<td>plugin/cvss3_temporal_vector/exploitability</td>
<td>u_plugin_cvss3_exploitability</td>
<td>String</td>
</tr>
<tr>
<td>plugin/cvss3_temporal_vector/report_confidence</td>
<td>u_plugin_cvss3_report_confidence</td>
<td>String</td>
</tr>
<tr>
<td>plugin/cvss_temporal_vector/raw</td>
<td>u_plugin_cvss__raw_vector_raw</td>
<td>String</td>
</tr>
<tr>
<td>plugin/cvss_vector/integrity_impact</td>
<td>u_plugin_cvss__integrity_impact</td>
<td>String</td>
</tr>
<tr>
<td>plugin/cvss_vector/confidentiality</td>
<td>u_plugin_cvss__confidentiality</td>
<td>String</td>
</tr>
<tr>
<td>Impact</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td><code>plugin/cvss_vector/access_vector</code></td>
<td>u_plugin_cvss___access_vector</td>
<td>String</td>
</tr>
<tr>
<td><code>plugin/description</code></td>
<td>u_plugin_description</td>
<td>String</td>
</tr>
<tr>
<td><code>plugin/exploitability_ease</code></td>
<td>u_plugin_exploitability_ease</td>
<td>String</td>
</tr>
<tr>
<td><code>plugin/exploited_by_malware</code></td>
<td>u_plugin_exploited_by_malware</td>
<td>String</td>
</tr>
<tr>
<td><code>plugin/exploited_by_nessus</code></td>
<td>u_plugin_exploited_by_nessus</td>
<td>String</td>
</tr>
<tr>
<td><code>plugin/exploit_available</code></td>
<td>u_plugin_exploit_available</td>
<td>String</td>
</tr>
<tr>
<td><code>plugin/exploit_framework_canvas</code></td>
<td>u_plugin_explo_amework_canvas</td>
<td>String</td>
</tr>
<tr>
<td><code>plugin/exploit_framework_core</code></td>
<td>u_plugin_explo_framework_core</td>
<td>String</td>
</tr>
<tr>
<td><code>plugin/exploit_framework_expoithub</code></td>
<td>u_plugin_explo_ork_expoithub</td>
<td>String</td>
</tr>
<tr>
<td><code>plugin/exploit_framework_metasploit</code></td>
<td>u_plugin_explo_ork_metasploit</td>
<td>String</td>
</tr>
<tr>
<td><code>plugin/exploit_framework_d2_elliot</code></td>
<td>u_plugin_explo_work_d2_elliot</td>
<td>String</td>
</tr>
<tr>
<td><code>plugin/family</code></td>
<td>u_plugin_family</td>
<td>String</td>
</tr>
<tr>
<td><code>plugin/family_id</code></td>
<td>u_plugin_family_id</td>
<td>String</td>
</tr>
<tr>
<td><code>plugin/family_type</code></td>
<td>u_plugin_family_type</td>
<td>String</td>
</tr>
<tr>
<td><code>plugin/has_patch</code></td>
<td>u_plugin_has_patch</td>
<td>String</td>
</tr>
<tr>
<td><code>plugin/id</code></td>
<td>u_plugin_id</td>
<td>String</td>
</tr>
<tr>
<td><code>plugin/info</code></td>
<td>u_plugin_info</td>
<td>String</td>
</tr>
<tr>
<td><code>plugin/in_the_news</code></td>
<td>u_plugin_in_the_news</td>
<td>String</td>
</tr>
<tr>
<td><code>plugin/metasploit_name</code></td>
<td>u_plugin_metasploit_name</td>
<td>String</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>--------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>plugin/modification_date</td>
<td>u_plugin_modification_date</td>
<td>String</td>
</tr>
<tr>
<td>plugin/name</td>
<td>u_plugin_name</td>
<td>String</td>
</tr>
<tr>
<td>plugin/patch_publication_date</td>
<td>u_plugin_patch_blication_date</td>
<td>String</td>
</tr>
<tr>
<td>plugin/publication_date</td>
<td>u_plugin_publication_date</td>
<td>String</td>
</tr>
<tr>
<td>plugin/risk_factor</td>
<td>u_plugin_risk_factor</td>
<td>String</td>
</tr>
<tr>
<td>plugin/see_also</td>
<td>u_plugin_see_also</td>
<td>String</td>
</tr>
<tr>
<td>plugin/solution</td>
<td>u_plugin_solution</td>
<td>String</td>
</tr>
<tr>
<td>plugin/stig_severity</td>
<td>u_plugin_stig_severity</td>
<td>String</td>
</tr>
<tr>
<td>plugin/synopsis</td>
<td>u_plugin_synopsis</td>
<td>String</td>
</tr>
<tr>
<td>plugin/type</td>
<td>u_plugin_type</td>
<td>String</td>
</tr>
<tr>
<td>plugin/unsupported_by_vendor</td>
<td>u_plugin_unsupported_by_vendor</td>
<td>String</td>
</tr>
<tr>
<td>plugin/version</td>
<td>u_plugin_version</td>
<td>String</td>
</tr>
<tr>
<td>plugin/vpr</td>
<td>u_plugin_vpr</td>
<td>String</td>
</tr>
<tr>
<td>plugin/vpr/drivers</td>
<td>u_plugin_vpr_drivers</td>
<td>String</td>
</tr>
<tr>
<td>plugin/vpr/drivers/cvss3_impact_</td>
<td>u_plugin_vpr_d_3_impact_score</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td>score</td>
<td></td>
</tr>
<tr>
<td>plugin/vpr/drivers/cvss_impact_</td>
<td>u_plugin_vpr_d_core_predicted</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td>score_predicted</td>
<td></td>
</tr>
<tr>
<td>plugin/vpr/drivers/threat_recency_</td>
<td>u_plugin_vpr_d_cy_lower_bound</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td>lower_bound</td>
<td></td>
</tr>
<tr>
<td>plugin/vpr/drivers/threat_recency_</td>
<td>u_plugin_vpr_d_cy_upper_bound</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td>upper_bound</td>
<td></td>
</tr>
<tr>
<td>Field Name</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>plugin/vpr/drivers/age_of_vuln/lower_bound</td>
<td>u_plugin_vpr_d_ln_lower_bound</td>
<td>String</td>
</tr>
<tr>
<td>plugin/vpr/drivers/age_of_vuln/upper_bound</td>
<td>u_plugin_vpr_d_ln_upper_bound</td>
<td>String</td>
</tr>
<tr>
<td>plugin/vpr/drivers/product_coverage</td>
<td>u_plugin_vpr_d_oduct_coverage</td>
<td>String</td>
</tr>
<tr>
<td>plugin/vpr/drivers/age_of_vuln</td>
<td>u_plugin_vpr_d_rs_age_of_vuln</td>
<td>String</td>
</tr>
<tr>
<td>plugin/vpr/drivers/threat_sources_last28</td>
<td>u_plugin_vpr_d_sources_last28</td>
<td>String</td>
</tr>
<tr>
<td>plugin/vpr/drivers/threat_intensity_last28</td>
<td>u_plugin_vpr_d_tensity_last28</td>
<td>String</td>
</tr>
<tr>
<td>plugin/vpr/drivers/threat_recency</td>
<td>u_plugin_vpr_d_threat_recency</td>
<td>String</td>
</tr>
<tr>
<td>plugin/vpr/drivers/exploit_code_maturity</td>
<td>u_plugin_vpr_d__code_maturity</td>
<td>String</td>
</tr>
<tr>
<td>plugin/vpr/score</td>
<td>u_plugin_vpr_score</td>
<td>String</td>
</tr>
<tr>
<td>plugin/vpr/updated</td>
<td>u_plugin_vpr_updated</td>
<td>String</td>
</tr>
<tr>
<td>plugin/vuln_publication_date</td>
<td>u_plugin_vuln_publication_date</td>
<td>String</td>
</tr>
<tr>
<td>plugin/xrefs</td>
<td>u_plugin_xrefs</td>
<td>String</td>
</tr>
<tr>
<td>port</td>
<td>u_port</td>
<td>String</td>
</tr>
<tr>
<td>port/port</td>
<td>u_port_port</td>
<td>String</td>
</tr>
<tr>
<td>port/protocol</td>
<td>u_port_protocol</td>
<td>String</td>
</tr>
<tr>
<td>port/service</td>
<td>u_port_service</td>
<td>String</td>
</tr>
<tr>
<td>product_type</td>
<td>u_product_type</td>
<td>String</td>
</tr>
<tr>
<td>recastRisk</td>
<td>u_recastrisk</td>
<td>String</td>
</tr>
<tr>
<td>Column Name</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------</td>
<td>--------</td>
</tr>
<tr>
<td>recast_reason</td>
<td>u_recast_reason</td>
<td>String</td>
</tr>
<tr>
<td>recast_rule_uuid</td>
<td>u_recast_rule_uuid</td>
<td>String</td>
</tr>
<tr>
<td>repository</td>
<td>u_repository</td>
<td>String</td>
</tr>
<tr>
<td>repository_data_format</td>
<td>u_repository_data_format</td>
<td>String</td>
</tr>
<tr>
<td>repository_id</td>
<td>u_repository_id</td>
<td>String</td>
</tr>
<tr>
<td>riskFactor</td>
<td>u_riskfactor</td>
<td>String</td>
</tr>
<tr>
<td>scan</td>
<td>u_scan</td>
<td>String</td>
</tr>
<tr>
<td>scan/completed_at</td>
<td>u_scan_completed_at</td>
<td>String</td>
</tr>
<tr>
<td>scan/schedule_uuid</td>
<td>u_scan_schedule_uuid</td>
<td>String</td>
</tr>
<tr>
<td>scan/started_at</td>
<td>u_scan_started_at</td>
<td>String</td>
</tr>
<tr>
<td>scan/uuid</td>
<td>u_scan_uuid</td>
<td>String</td>
</tr>
<tr>
<td>scunique</td>
<td>u_scunique</td>
<td>String</td>
</tr>
<tr>
<td>seeAlso</td>
<td>u_seealso</td>
<td>String</td>
</tr>
<tr>
<td>severity</td>
<td>u_severity</td>
<td>String</td>
</tr>
<tr>
<td>severity_default_id</td>
<td>u_severity_default_id</td>
<td>String</td>
</tr>
<tr>
<td>severity_id</td>
<td>u_severity_id</td>
<td>String</td>
</tr>
<tr>
<td>severity_modification_type</td>
<td>u_severity_modification_type</td>
<td>String</td>
</tr>
<tr>
<td>state</td>
<td>u_state</td>
<td>String</td>
</tr>
<tr>
<td>stigSeverity</td>
<td>u_stigseverity</td>
<td>String</td>
</tr>
<tr>
<td>system_type</td>
<td>u_system_type</td>
<td>String</td>
</tr>
<tr>
<td>temporalScore</td>
<td>u_temporalscore</td>
<td>String</td>
</tr>
<tr>
<td>Uniqueness</td>
<td>u_uniqueness</td>
<td>String</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------</td>
<td>--------</td>
</tr>
<tr>
<td>uuid</td>
<td>u_uuid</td>
<td>String</td>
</tr>
<tr>
<td>vprContext</td>
<td>u_vprcontext</td>
<td>String</td>
</tr>
<tr>
<td>vprScore</td>
<td>u_vprscore</td>
<td>String</td>
</tr>
<tr>
<td>xref</td>
<td>u_xref</td>
<td>String</td>
</tr>
</tbody>
</table>

6. In the **Asset field** text box, select the appropriate asset for the rule.

7. In the **Operator** text box, select the appropriate operator for the rule.

8. In the **Value** text box, type the value for the rule.

9. (Optional) To reorder the incident rule, update the value in the **Order** text box. Incident rules are tried in ascending order (lowest to highest).

10. If you are in a domain separated environment, in the **Domain** box, type the domain into which to bring connector data.

11. Click **Submit**.

**Plugins**

To view plugins:

- Navigate to **Tenable for ITSM > Plugins**.

**Vulnerabilities**

To view vulnerabilities:

- Navigate to **Tenable for ITSM > Vulnerabilities**.

**Incidents**

To view incidents:

- Navigate to **Tenable for ITSM > Incidents**.
Settings

General Settings
Assets Settings
ITSM Settings
VR Settings
General Settings

Use the settings options to maximize control and troubleshoot.

To access the General Settings:

1. Log in to ServiceNow.
2. In the left-hand menu, click **Tenable Connector**.
3. In the sub-menu, click **Connectors**.
   The **Tenable Connectors** page appears.
4. Click the Tenable connector you want to use: **Tenable.io** or **Tenable.sc**.
   The **Tenable Connector** page appears.
5. In the **General Settings** section, you can view/edit:
   - Max ECC Wait Time (sec)
   - Request Timeout (sec)
   - Max Attachment Records
   - Default Chunk Size
   - Connector Logging Level
Assets Settings

Use the settings options to maximize control and troubleshoot.

To access the Asset Settings:

1. Log in to ServiceNow.
2. In the left-hand menu, click Tenable Connector.
3. In the sub-menu, click Connectors.
   
   The Tenable Connectors page appears.
4. Click the Tenable connector you want to use: Tenable.io or Tenable.sc.
   
   The Tenable Connector page appears.
5. In the Asset Settings section, you can view/edit:
   
   - Logging level
   - Max Cumulative Log Entries
   - Max Cumulative Log Size
   - Additional Settings
     - New Record sync frequency (min)
     - Record update sync frequency (min)
     - Asset Max Job Age (days)
     - Asset Max Job Wait Time (days)
VR Settings

Use the settings options to maximize control and troubleshoot.

To access the VR Settings:

1. Log in to ServiceNow.
2. In the left-hand menu, click Tenable Connector.
3. In the sub-menu, click Connectors.
   The Tenable Connectors page appears.
4. Click the Tenable connector you want to use: Tenable.io or Tenable.sc.
   The Tenable Connector page appears.
5. In the VR Settings section, you can view/edit:
   - VR Logging level
   - VR Max Job Log Age (days)
   - VR Plugin Chunk Size
   - VR Vulnerability Chunk Size
   - VR Max Cumulative Log Entries
   - VR Max Cumulative Log Size
   - VR Plugin Import Thread Limit
   - VR Vulnerability Import Thread Limit

Furthermore, in the left-hand menu, you can configure the following settings:

- Advanced
  - Transform Maps: Defines how fields are mapped as records and brought back in to update ServiceNow records.
Caution: We do not support changes made to Transform Maps. If you want to customize your Transform Maps options, we recommend you contact your ServiceNow Administrator.

- **Diagnostics**
  - Dashboard
  - VR Logs
ITSM Settings

Use the settings options to maximize control and troubleshoot.

To access the ITSM Settings:

1. Log in to ServiceNow.
2. In the left-hand menu, click Tenable Connector.
3. In the sub-menu, click Connectors.
   
   The Tenable Connectors page appears.
4. Click the Tenable connector you want to use: Tenable.io or Tenable.sc.
   
   The Tenable Connector page appears.
5. In the ITSM Settings section, you can view/edit:
   
   - ITSM Logging Level
   - ITSM Plugin Chunk Size
   - ITSM Plugin Import Thread Limit
   - ITSM Max Cumulative Log Entries
   - ITSM Max Cumulative Log Size
   - ITSM Vulnerability Chunk Size

6. In the ITSM Additional Settings section, you can view/edit:
   
   - ITSM Age Out Period
   - ITSM Max Job Log Age (days)

Create an Incident from a Record

See the ITSM Optional Configuration section.
Configure CI to SC Asset Group

You can configure CI to Sync from ServiceNow to Tenable.sc Asset Groups.

**Note:** Please work with your ServiceNow administrator to perform the following task. The information provided below should be used as a guideline. Your administrator can assist in tuning the export to achieve your desired results.

To configure CI to SC Asset Group:

1. Log in to ServiceNow.
2. In the left-hand menu, click **Tenable Connector**.
3. In the sub-menu, click **Connectors**.
   
   The **Tenable Connectors** page appears.
4. Click the Tenable connector you want to use: **Tenable.io** or **Tenable.sc**.
   
   The **Tenable Connector** page appears.
5. In the **Scheduled Jobs** section, click **New**.
   
   The **Tenable Scheduled Import** page appears. By default, the **Tenable Product** and **Connector** fields populate with the Tenable application/connector you selected in step 3.
6. From the **Tenable Application** drop-down, select **Tenable for Assets**.
7. From the **Tenable Job Type** drop-down, select **Push Assets**.
8. In the **Name** text box, type a name for the export.
9. In the **Group Name** box, type a name for the asset group.
10. From the **Group Type** drop-down, select the type of asset group to create.
11. In the **Conditions** section, filter the records you want to export.
12. Click **Submit**.
Tenable Applications

Tenable for Assets

Tenable for ITSM

Tenable for Vulnerability Response
Tenable for Assets

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

Note: Tenable for Assets only supports Tenable.sc versions 5.7 and later.

- Customize how Tenable assets are matched to ServiceNow CIs
- Define which ServiceNow CIs are sent to Tenable as assets
Tenable for Assets for ServiceNow

Description

Tenable.io offers continuous monitoring and vulnerability management that protects critical applications, devices, and infrastructures. The Tenable for Assets application is purpose-built for ServiceNow’s Vulnerability Response offering, allowing you to import your Tenable.io vulnerability data and manage it within ServiceNow.

Application Menu

Tenable for Assets

Primary Role Required: x_tsirm_tio_cmdb.user

<table>
<thead>
<tr>
<th>Title</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documentation</td>
<td>x_tsirm_tio_cmdb.user</td>
</tr>
<tr>
<td>Contact Support</td>
<td>x_tsirm_tio_cmdb.user</td>
</tr>
<tr>
<td>Dashboard</td>
<td>x_tsirm_tio_cmdb.user</td>
</tr>
<tr>
<td>Assets Pending Approval</td>
<td>x_tsirm_tio_cmdb.user</td>
</tr>
<tr>
<td>All Synchronized Items</td>
<td>x_tsirm_tio_cmdb.user</td>
</tr>
<tr>
<td>Configuration</td>
<td>x_tsirm_tio_cmdb.admin</td>
</tr>
<tr>
<td>General Settings</td>
<td>x_tsirm_tio_cmdb.admin</td>
</tr>
<tr>
<td>Connectors</td>
<td>x_tsirm_tio_cmdb.admin</td>
</tr>
<tr>
<td>API Data Mappings</td>
<td>x_tsirm_tio_cmdb.user</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>x_tsirm_tio_cmdb.admin</td>
</tr>
<tr>
<td>Asset Outbound Jobs</td>
<td>x_tsirm_tio_cmdb.admin</td>
</tr>
<tr>
<td>Asset Inbound Jobs</td>
<td>x_tsirm_tio_cmdb.admin</td>
</tr>
<tr>
<td>Queued Actions</td>
<td>x_tsirm_tio_cmdb.admin</td>
</tr>
</tbody>
</table>
Primary Roles

x_tsirm_tio_cmdb.admin

**Description:** An administrative user of the application.

x_tsirm_tio_cmdb.user

**Description:** A basic user of the application.

Business Rules

Update Job and Chunk Status

**Description:** Business rule that sets the status of jobs and chunks.

Push Asset Update to Tenable.io

**Description:** Sends asset update information to Tenable.io by creating an async request queue action entry.

Set Name

**Description:** Sets the name of the asset attribute record if the connector or Asset UUID change.

Set Tenable Values when Done Processing

**Description:** On complete outbound jobs, this sets values on the asset attribute record.

Update Job Percent Complete

**Description:** Updates the job percent complete as records get processed.

Create Settings if None exist

**Description:** Automatically creates a general settings record with default values if one doesn’t exist.

Calc Job State

**Description:** Calculates the job state based on happenings with chunks.
On Job State Change

**Description:** Inbound job total records and percent complete, when the state of the job changes.

Notify About Limitations on Out of Box Rules

**Description:** Shows UI message explaining that out of box CI rules are not editable.

Push Asset Update to Tenable.io (Update)

**Description:** Sends asset update information to Tenable.io by creating an async request queue action entry.
Tenable for ITSM

Tenable for IT Service Management (ITSM) provides the ability to import Tenable vulnerability findings and transform them into ServiceNow incidents without the need for ServiceNow Vulnerability Response. This helps you move from manual email and spreadsheet processes to a repeatable workflow in ServiceNow. As your needs expand or you need more flexibility and customization, you can easily transition to Vulnerability Response.

The Tenable ITSM Process

Tenable for ITSM uses Tenable for Assets to find the correct asset/CI to link a vulnerability to. It is extremely important that you completely test and tune Tenable for assets before configuring Tenable for ITSM. Tenable for ITSM uses the connector you specify to download vulnerabilities and create them in a custom ServiceNow table. The application uses configurable incident rules to create ServiceNow incidents for each vulnerability that can be used by IT administrators to assign remediation work to their teams.

The application creates vulnerabilities as follows:

- The Tenable ITSM app uses the Tenable for Assets app to match vulnerable assets to ServiceNow CI’s.
- For every high and critical vulnerability finding, it creates a unique vulnerability entry in the Tenable ITSM app.
- Unique vulnerability entries are determined by coalescing on ServiceNow CI, plugin id, port and protocol.
- If a vulnerability is fixed in Tenable, both the vulnerability and incident close in ServiceNow.
- If a vulnerability is manually closed, but is found in the future, Tenable reopens the vulnerability and incident in ServiceNow.

The application can create incidents as follows:

- You can manually create a ServiceNow incident from the vulnerability form.
- You can create incident rules to automatically spawn incidents:
- Use the selector form for simple rule creation using asset fields and values.
- Use advanced scripting to manipulate data for more granular selection.
Tenable.io for ITSM for ServiceNow

Tenable.io offers continuous monitoring and vulnerability management that protects critical applications, devices, and infrastructures. The Tenable for ITSM application is purpose built for ServiceNow’s Vulnerability Response offering, allowing you to import your Tenable.io vulnerability data and manage it within ServiceNow.

Application Menu

Tenable.io for ITSM

Primary Role Required: x_tsirm_tio_itsm.user

<table>
<thead>
<tr>
<th>Title</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documentation</td>
<td>x_tsirm_tio_itsm.user</td>
</tr>
<tr>
<td>Contact Support</td>
<td>x_tsirm_tio_itsm.user</td>
</tr>
<tr>
<td>Plugins</td>
<td>x_tsirm_tio_itsm.user</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>x_tsirm_tio_itsm.user</td>
</tr>
<tr>
<td>Incidents</td>
<td>x_tsirm_tio_itsm.user</td>
</tr>
<tr>
<td>Configuration</td>
<td>x_tsirm_tio_itsm.user</td>
</tr>
<tr>
<td>General Settings</td>
<td>x_tsirm_tio_itsm.admin</td>
</tr>
<tr>
<td>Connectors</td>
<td>x_tsirm_tio_itsm.admin</td>
</tr>
<tr>
<td>Scheduled Imports</td>
<td>x_tsirm_tio_itsm.user</td>
</tr>
<tr>
<td>Incident Rules</td>
<td>x_tsirm_tio_itsm.admin</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>x_tsirm_tio_itsm.admin</td>
</tr>
<tr>
<td>Queued Actions</td>
<td>x_tsirm_tio_itsm.admin</td>
</tr>
<tr>
<td>Documentation</td>
<td>x_tsirm_tio_itsm.user</td>
</tr>
<tr>
<td>Contact Support</td>
<td>x_tsirm_tio_itsm.user</td>
</tr>
<tr>
<td>Title</td>
<td>Required Role</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Plugins</td>
<td>x_tsirm_tio_itsm.user</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>x_tsirm_tio_itsm.user</td>
</tr>
<tr>
<td>Incidents</td>
<td>x_tsirm_tio_itsm.user</td>
</tr>
</tbody>
</table>

### Primary Roles

**x_tsirm_tio_itsm.admin**

**Description:** An administrative user of the application.

**x_tsirm_tio_itsm.user**

**Description:** A basic user of the application.

### Business Rules

**Calc Job State**

**Description:** Calculates the job state based on happenings with chunks.

**On Job State Change**

**Description:** Inbound job total records and percent complete, when the state of the job changes.

**Create Settings if None Exist**

**Description:** Automatically creates a general settings record with default values if one doesn’t exist.
Tenable for Vulnerability Response (VR)

The integration of Tenable for Vulnerability Response with ServiceNow’s Vulnerability Response module takes your Tenable platform findings and syncs them into ServiceNow Vulnerability Response tables and data structures. This integration allows you to reduce your cyber risk by allowing you to rapidly prioritize and automate the remediation of critical vulnerabilities across your most important assets.

**Note:** The Tenable for Vulnerability Response application only supports Tenable.sc versions 5.7 and later.

With Tenable for Vulnerability Response, you can:

- Leverage the Tenable for Assets application to properly link vulnerabilities to ServiceNow CIs
- Create ServiceNow third party vulnerabilities from Tenable Plugins
- Create Vulnerable Items from Tenable findings
- Customize data mapping while keeping app upgradability
- Configure vulnerabilities to sync from your Tenable platform
- Automatically close vulnerable items once Tenable finds them to be resolved
- Reopen previously closed vulnerable items if they are found again at a later date.
Tenable for VR

Tenable for VR allows you to fully integrate your Tenable data with ServiceNow creating closed loop remediation. This application has grouping functionality and risk calculators. In addition, it creates tickets for IT staff according to specified machines, allows reallocation, closing, and reopening.

Application Menu

Tenable for VR

Primary Role Required: x_tsirm_tio_vr.user

<table>
<thead>
<tr>
<th>Title</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documentation</td>
<td>x_tsirm_tio_vr.user</td>
</tr>
<tr>
<td>Contact Support</td>
<td>x_tsirm_tio_vr.user</td>
</tr>
<tr>
<td>Configuration</td>
<td>x_tsirm_tio_vr.user</td>
</tr>
<tr>
<td>General Settings</td>
<td>x_tsirm_tio_vr.admin</td>
</tr>
<tr>
<td>Connectors</td>
<td>x_tsirm_tio_vr.admin</td>
</tr>
<tr>
<td>Scheduled Imports</td>
<td>x_tsirm_tio_vr.user</td>
</tr>
<tr>
<td>API Data Mappings</td>
<td>x_tsirm_tio_vr.admin</td>
</tr>
<tr>
<td>Default VR Data Source</td>
<td>x_tsirm_tio_vr.admin</td>
</tr>
<tr>
<td>Transform Maps</td>
<td>x_tsirm_tio_vr.admin</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>x_tsirm_tio_vr.admin</td>
</tr>
<tr>
<td>Queued Actions</td>
<td>x_tsirm_tio_vr.admin</td>
</tr>
<tr>
<td>Documentation</td>
<td>x_tsirm_tio_vr.user</td>
</tr>
<tr>
<td>Contact Support</td>
<td>x_tsirm_tio_vr.user</td>
</tr>
<tr>
<td>Configuration</td>
<td>x_tsirm_tio_vr.user</td>
</tr>
</tbody>
</table>
### Primary Roles

**x_tsirm_tio_vr.admin**

**Description:** An administrative user of the application.

**x_tsirm_tio_vr.user**

**Description:** A basic user of the application.

### Business Rules

#### Calc Job State

**Description:** Calculates the job state based on happenings with chunks.

#### Run Plugin Families Populate on Activate

**Description:** Runs the script to run the API call to get plugin families from Tenable when a connector is activated.

#### On Job State Change

**Description:** Inbound job total records and percent complete, when the state of the job changes.

#### Create Settings if None Exist

**Description:** Automatically creates a general settings record with default values if one doesn’t exist.
# Available Data

## Tenable.io Data Map

The following table compares Tenable.io data field names with the equivalent names used in the ServiceNow applications.

<table>
<thead>
<tr>
<th>Tenable.io</th>
<th>ServiceNow</th>
</tr>
</thead>
<tbody>
<tr>
<td>bios_uuid</td>
<td>bios_uuid</td>
</tr>
<tr>
<td>fqdns</td>
<td>fqdn</td>
</tr>
<tr>
<td>ipv4s/ipv6s/network_interfaces</td>
<td>ipv4/ipv6</td>
</tr>
<tr>
<td>last_authenticated_scan_date</td>
<td>lastAuthenticatedScanDate</td>
</tr>
<tr>
<td>mac_addresses</td>
<td>mac_address</td>
</tr>
<tr>
<td>mcafee_epo_guid</td>
<td>mcafee_epo_guid</td>
</tr>
<tr>
<td>netbios_names</td>
<td>netbios_name</td>
</tr>
<tr>
<td>agent_uuid</td>
<td>agent_uuid</td>
</tr>
<tr>
<td>id</td>
<td>asset_uuid</td>
</tr>
<tr>
<td>has_agent</td>
<td>has_agent</td>
</tr>
<tr>
<td>has_plugin_results</td>
<td>has_plugin_results</td>
</tr>
<tr>
<td>created_at</td>
<td>created_at</td>
</tr>
<tr>
<td>terminated_at</td>
<td>terminated_at</td>
</tr>
<tr>
<td>terminated_by</td>
<td>terminated_by</td>
</tr>
<tr>
<td>updated_at</td>
<td>updated_at</td>
</tr>
<tr>
<td>deleted_at</td>
<td>deleted_at</td>
</tr>
<tr>
<td>deleted_by</td>
<td>deleted_by</td>
</tr>
</tbody>
</table>

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective companies.
<table>
<thead>
<tr>
<th>first_seen</th>
<th>first_seen</th>
</tr>
</thead>
<tbody>
<tr>
<td>last_seen</td>
<td>last_seen</td>
</tr>
<tr>
<td>last_scan_time</td>
<td>last_scan_time</td>
</tr>
<tr>
<td>lastLicensed_scan_date</td>
<td>last Licensed scan date</td>
</tr>
<tr>
<td>azure_vm_id</td>
<td>azure_vm_id</td>
</tr>
<tr>
<td>azure_resource_id</td>
<td>azure_resource_id</td>
</tr>
<tr>
<td>aws_ec2_instance_ami_id</td>
<td>aws ec2_instance_ami_id</td>
</tr>
<tr>
<td>aws_ec2_instance_id</td>
<td>aws ec2_instance_id</td>
</tr>
<tr>
<td>aws_owner_id</td>
<td>aws_owner_id</td>
</tr>
<tr>
<td>aws_availability_zone</td>
<td>aws availability zone</td>
</tr>
<tr>
<td>aws_region</td>
<td>aws_region</td>
</tr>
<tr>
<td>aws_vpc_id</td>
<td>aws_vpc_id</td>
</tr>
<tr>
<td>aws_ec2_instance_group_name</td>
<td>aws ec2 instance group name</td>
</tr>
<tr>
<td>aws_ec2_instance_state_name</td>
<td>aws ec2 instance state name</td>
</tr>
<tr>
<td>aws_ec2_instance_type</td>
<td>aws ec2 instance type</td>
</tr>
<tr>
<td>aws_subnet_id</td>
<td>aws_subnet_id</td>
</tr>
<tr>
<td>aws_ec2_product_code</td>
<td>aws ec2 product code</td>
</tr>
<tr>
<td>aws_ec2_name</td>
<td>aws_ec2_name</td>
</tr>
<tr>
<td>mcafee_epo_agent_guid</td>
<td>mcafee epo agent guid</td>
</tr>
<tr>
<td>servicenow_sysid</td>
<td>servicenow_sysid</td>
</tr>
<tr>
<td>agent_names</td>
<td>agent_names</td>
</tr>
<tr>
<td>mac_addresses</td>
<td>mac_addresses</td>
</tr>
<tr>
<td>Tenable.sc</td>
<td>ServiceNow</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>biosGUID</td>
<td>bios_uuid</td>
</tr>
<tr>
<td>dnsName</td>
<td>fqdn</td>
</tr>
<tr>
<td>ip</td>
<td>ipv4/ipv6</td>
</tr>
<tr>
<td>lastAuthRun</td>
<td>last_authenticated_scan_date</td>
</tr>
<tr>
<td>lastUnauthRun</td>
<td>last_unauthenticated_scan_date</td>
</tr>
<tr>
<td>macAddress</td>
<td>mac_address</td>
</tr>
<tr>
<td>mcafeeGUID</td>
<td>mcafee_epo_guid</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>netbiosName</td>
<td>netbios_name</td>
</tr>
<tr>
<td>osCPE</td>
<td>os_cpe</td>
</tr>
<tr>
<td>uniqueness</td>
<td>uniqueness</td>
</tr>
<tr>
<td>uuid</td>
<td>agent_uuid</td>
</tr>
<tr>
<td>repository.dataFormat</td>
<td>repository_data_format</td>
</tr>
<tr>
<td>repository.description</td>
<td>repository_description</td>
</tr>
<tr>
<td>repository.id</td>
<td>repository_id</td>
</tr>
<tr>
<td>repository.name</td>
<td>repository_name</td>
</tr>
</tbody>
</table>
Support

The Tenable for ServiceNow applications are highly customizable as every ServiceNow environment tends to be very different. However, Tenable cannot provide ServiceNow specific customization support. This guide provides information for basic customization scenarios. Tenable cannot troubleshoot or support items such as custom CI rules, custom transform maps, and custom field mapping.

Many customers utilize a deployment partner to help set up their instance appropriately for their customer needs. If you are interested, contact your Tenable representative to get information on other companies that have extensive experience with the Tenable for ServiceNow applications.

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), [Tenable Community Site](#)
- Follow the [Contact Tenable Support](#) link in the application to go directly to the [Tenable Community Site](#)
**Troubleshooting**

How can I view the progress of my scheduled import?

1. Navigate to **Tenable Connector > Connector > Job Logs**

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 Connector > Connector > Asset/VR/ITSM Settings**.

2. From the **Logging Level** drop-down, select the logging level you wish to employ.