Tenable and ServiceNow 5.x.x Integration Guide

Last Revised: September 11, 2023

Table of Contents

Welcome to Tenable for ServiceNow 5.x.x

Caution: Tenable's Vulnerability Response (VR) integration app for Tenable Vulnerability Management and Tenable Security Center is deprecated and the last day of support is April 14th, 2023. Tenable recommends that you migrate to ServiceNow's integration app for Tenable Vulnerability Management or Tenable Security Center before this date. For more information, see the Tenable bulletin. This application continues to be available for Tenable OT Security and is renamed as “Tenable OT Security for VR."

Tenable applications are designed to help customers who use ServiceNow with Tenable Vulnerability Management, Tenable Security Center, or Tenable OT Security.

In the Tenable for ServiceNow 5.x.x and later, the Tenable Connectors handle all configuration and import scheduling. Therefore, you must properly configure your Tenable Connectors for the Assets, Vulnerability Response (VR) for Tenable OT Security, or Information Technology Service Management (ITSM) applications to function properly.

The Service Graph Connector for Tenable for Assets application integrates Tenable assets with the ServiceNow Configuration Management Database (CMDB). Assets are imported into the CMDB through ServiceNow's 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 OT Security for Vulnerability Response application integrates Tenable vulnerability findings with the ServiceNow Security Operations Vulnerability Response module. This application, once configured, syncs all of Tenable OT Security vulnerability findings into ServiceNow Vulnerable Items (VI) and Tenable Plugin details into ServiceNow Third-Party Vulnerabilities.

The Tenable for ITSM application integrates Tenable vulnerability findings into a custom table 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

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 to development or testing, and others dedicated to production. If your Tenable Security Center or Tenable OT Security 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 user interface configuration menu simplifies the Tenable for ServiceNow application configuration.

Tenable requires creating individual ServiceNow users in Tenable Vulnerability Management/Tenable Security Center/Tenable OT Security 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 Vulnerability Management, you can set up an Access Group and limit the data to specific assets to simplify the import and testing of data.

> **Note**: Tenable is converting all access groups into permission configurations. For more information, see Access Groups and Permissions in the Tenable Vulnerability Management User Guide.

In Tenable Security Center, 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.

In Tenable OT Security, you can create users by navigating to **Local Settings** > **Users and Roles** > **Local Users** > **Add User**.

Generate Tenable Vulnerability Management API Keys

To generate unique API keys to integrate ServiceNow with Tenable Vulnerability Management:

1. Log in to Tenable Vulnerability Management.
2. Create administrator accounts (For example, development, test, production) dedicated for use with ServiceNow. ServiceNow uses these accounts to connect to Tenable Vulnerability Management to retrieve asset data.
3. Generate API keys and save them for use with ServiceNow.

   Note: For your Tenable Vulnerability Management integration:

   - Generate an API key in Tenable Vulnerability Management to complete the configuration. See the Tenable Vulnerability Management 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. 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 Security Center API Keys

Create unique API keys to integrate Tenable Security Center with ServiceNow:

1. Log in to Tenable Security Center.
2. Create security manager accounts or Create security analyst accounts (e.g., development, test, production) with full access dedicated for use with ServiceNow. ServiceNow uses these accounts to connect to Tenable Security Center to retrieve data and kick off remediation scans.
3. Generate API keys and save them for use with ServiceNow.

In Tenable OT Security, you can create API keys by navigating to **Local Settings** > **System Configuration** > **API Keys** > **Generate Key**.

Application Dependencies

The Tenable apps for ServiceNow have the following application dependencies:

- Tenable Vulnerability Management, Tenable Security Center 5.7+, or Tenable OT Security
- ServiceNow Utah, Tokyo, or San Diego

Applications

Note: Each application name is linked to its ServiceNow store listing. Click the link to see more detailed dependency information.

Tenable Connector: This application is a prerequisite for all of the following Tenable applications in the ServiceNow store.

Service Graph Connector for Tenable for Assets:

- Tenable Connector
- ServiceNow Configuration Management Database (CMDB)
- Integration Commons for CMDB
- CMDB CI Class Models
- ITOM Licensing (com.snc.itom.license)
- ITOM Discovery License (com.snc.itom.discovery.license)

Note: Service Graph Certified apps are required to have the following dependencies: ITOM Licensing (com.snc.itom.license) and ITOM Discovery License (com.snc.itom.discovery.license). You may request to have the com.snc.itom.license plugin installed on your instance from the ServiceNow Support Portal. Contact your ServiceNow representative for more information.

Tenable OT Security for Vulnerability Response:

- Tenable Connector
- Service Graph Connector for Tenable for Assets
- ServiceNow Vulnerability Response

Tenable for ITSM:

- Tenable Connector
- Service Graph Connector for Tenable for Assets
- ServiceNow Incident (ITSM)

Get Started with Tenable for ServiceNow

To configure your Tenable for ServiceNow integration:

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

Tip: Tenable recommends using the tabbed view in ServiceNow to 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 Service Graph Connector for Tenable for Assets are required.

2. Configure the **Tenable Connector**.
3. Configure the Service Graph Connector for Tenable for Assets application. You can schedule imports in this step.

   Note: It is important to configure the **Service Graph Connector for Tenable for Assets** application with accurate parameters. Otherwise, the integration may not work as designed.

4. (Optional) Configure the **Tenable OT Security 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.

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)
- Service Graph Connector for Tenable for Assets (Required)
- Tenable OT Security for Vulnerability Response (VR) (Optional)
- Tenable for ITSM (Optional)

Tenable Applications Upgrade Overview

Tenable's ServiceNow applications get upgrades periodically. Tenable recommends that you upgrade the platform to ensure your system remains up to date.

Supported Upgrade Paths

Version 3.1 and earlier

Tenable does not support direct upgrades to the current version of the application for customers currently using Tenable apps version 3.1 and earlier. To upgrade to the newest version of the Tenable applications, delete your current Tenable applications and data and then reinstall the newest version of the applications.

For more information, see Deleting Tenable Applications and Data.

Version 4.0 and later

Tenable supports direct upgrades to the current version of the application for customers using Tenable apps version 4.0 and later. For more information, see Upgrade Tenable Applications.

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 Service Graph Connector for Tenable for Assets
   - Upgrade Tenable OT Security for VR (if using)
   - Upgrade Tenable for ITSM (if using)
4. Enable the Tenable connectors.

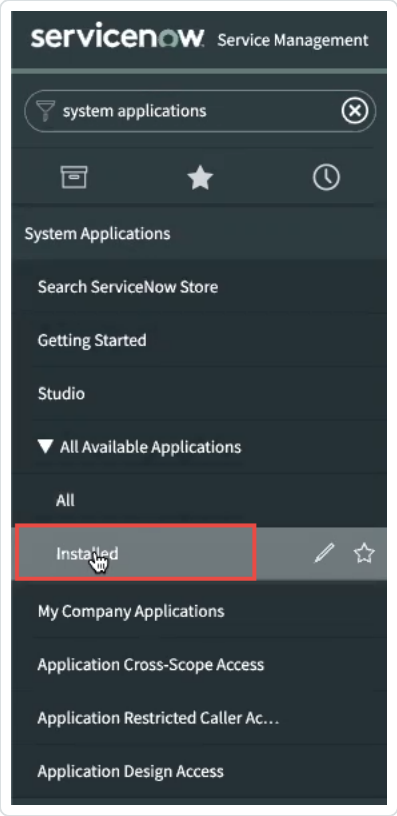
Upgrade the Tenable Applications

To update the Tenable application version:

1. In the ServiceNow filter search bar, type *system applications*.

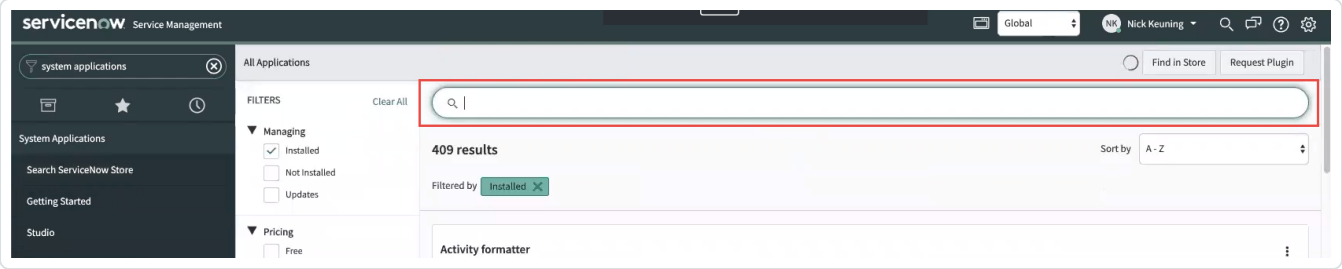
   The system applications results appear.

2. Under **System Applications**, select **Installed**.



   The **All Applications** page appears.

3. Type *Tenable* in the **search filter box**.

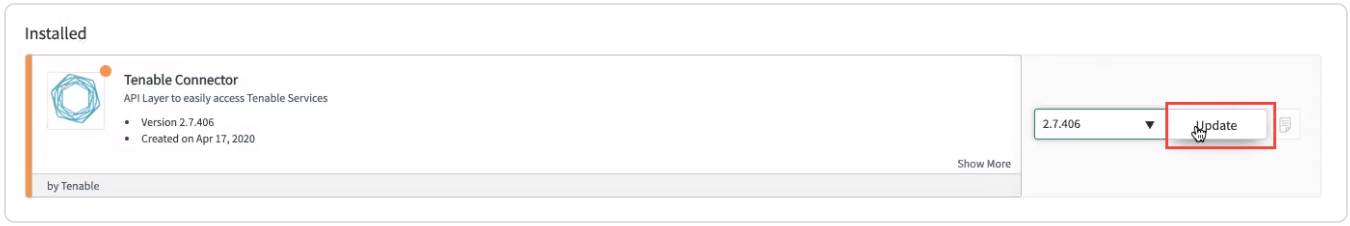


A list of installed Tenable applications appears.

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

   A list of available version updates appears.

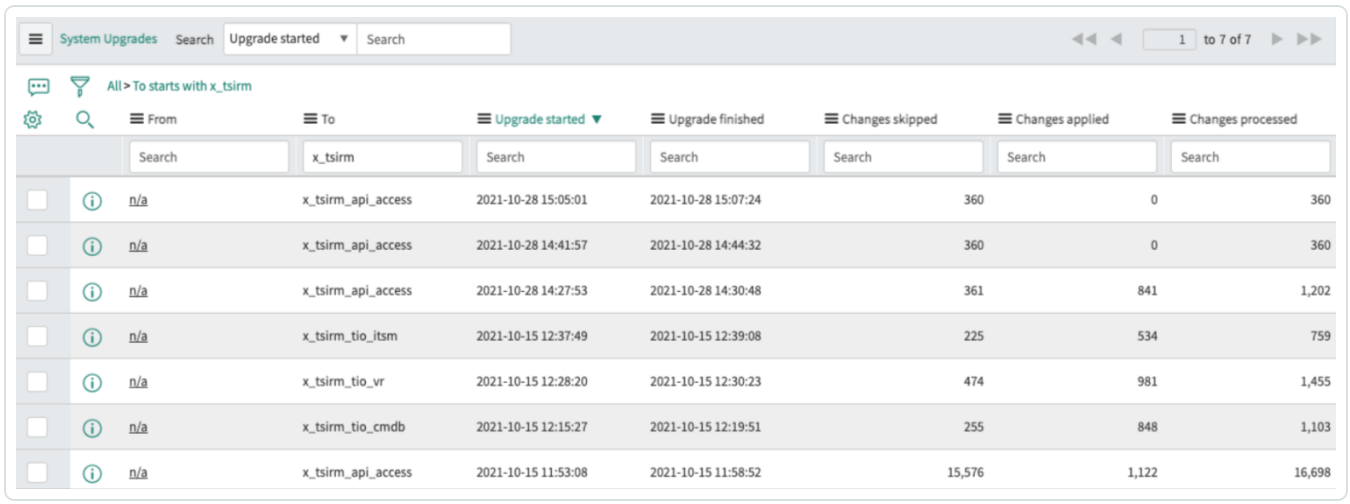
5. For each Tenable app (Tenable Connector, Service Graph Connector for Tenable for Assets, Tenable OT Security for VR, or Tenable for ITSM), select the latest version.
6. Click **Update**.



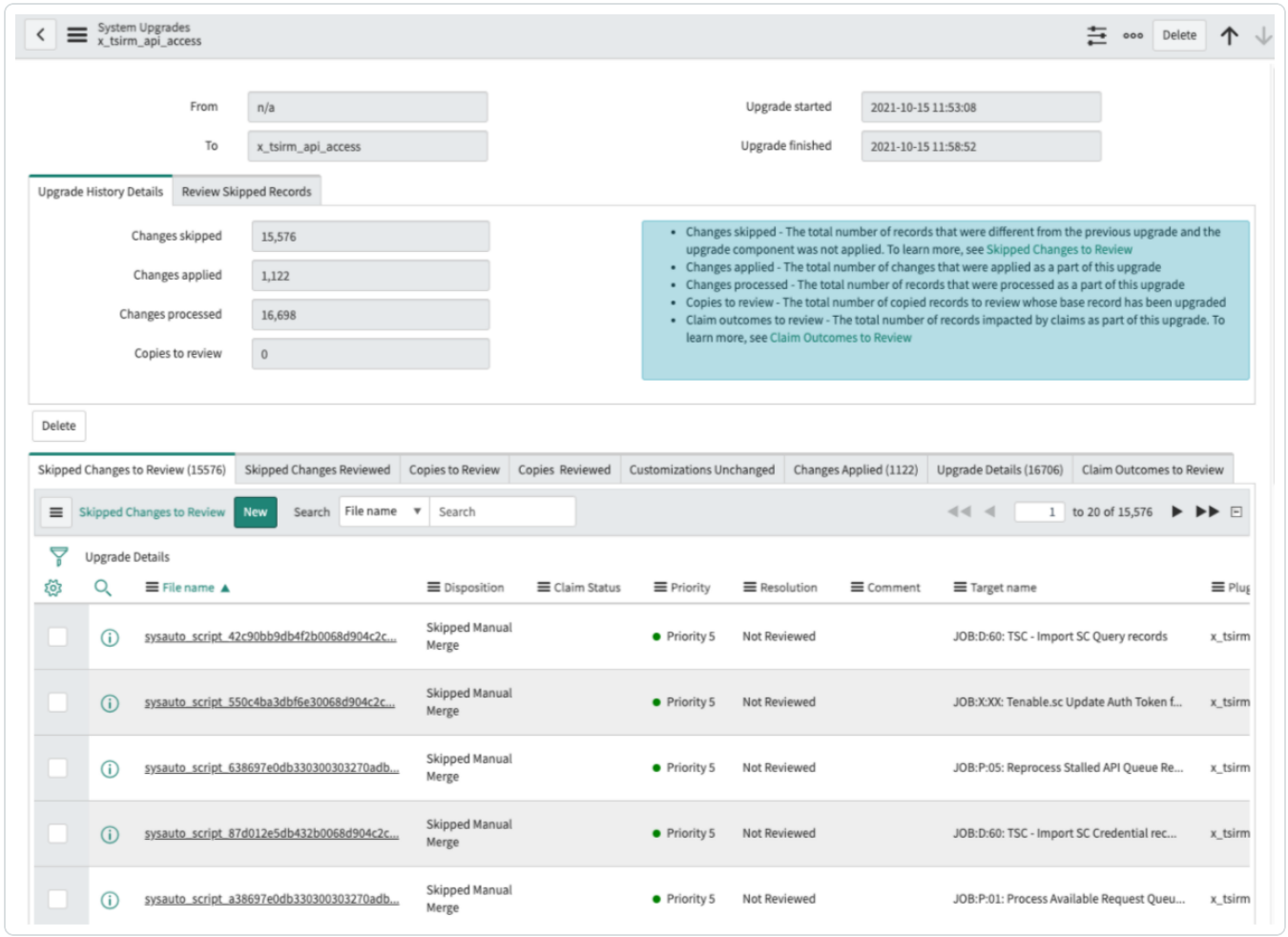
   The application updates to the version you selected.

Review and Resolve All Upgrade Skipped Changes

1. Navigate to **System Diagnostics > Upgrade History**.
2. Search for “x_tsirm” in the **To** field.



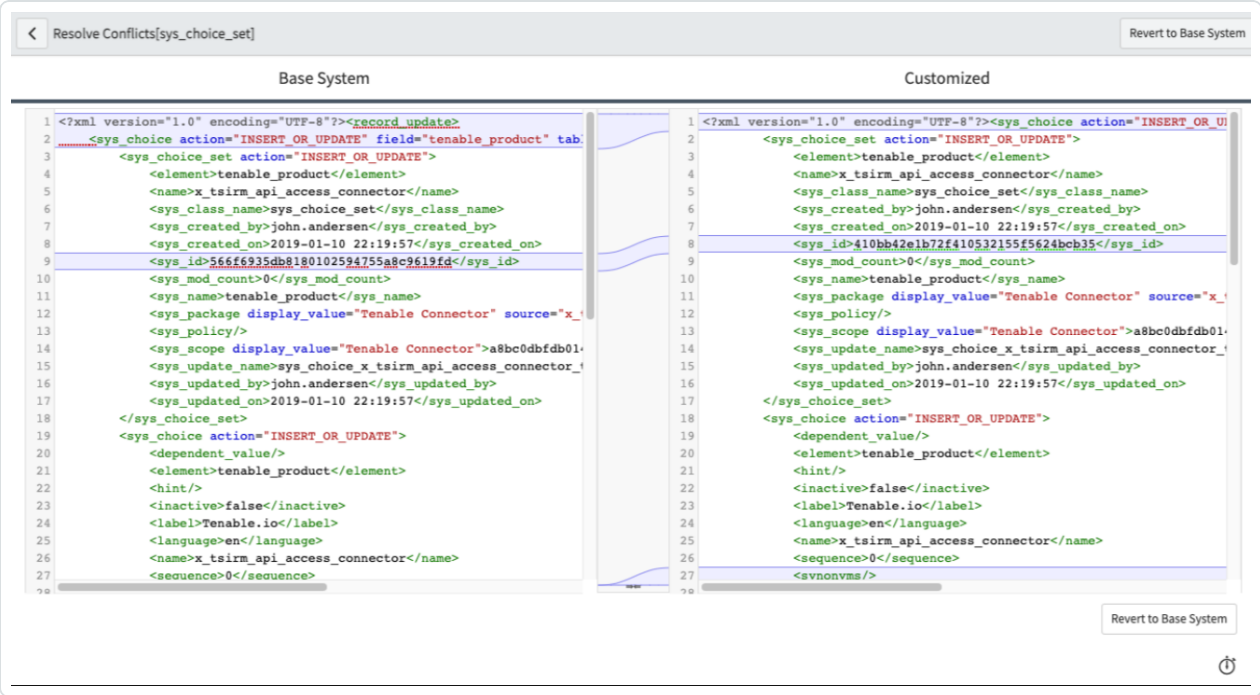
3. For each updated Tenable app, open the upgrade record and look at the **Skipped Changes to Review** tab.



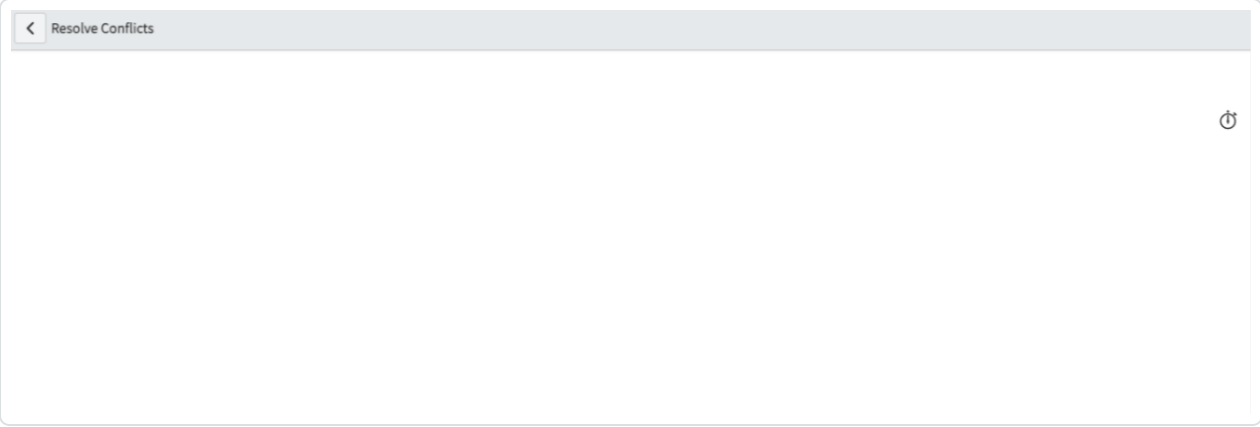
4. For each skipped change in this list, complete the following steps:

a. Open the skipped change and select **Resolve Conflicts**.

b. Select the option to **Revert to Base System**, if present. The app automatically marks the skipped change record as **Reviewed and Reverted**.



c. If you see a blank screen without an option to **Revert to Base System**, then there is no action to take on the skipped change. Mark the skipped change record as **Reviewed**.



After you review all skipped changes in all Tenable apps, the upgrade is complete.

Delete Leftover Artifacts

Occasionally, older application files, or artifacts, may not get deleted even after performing the tasks in **Review and Resolve All Upgrade Skipped Changes**. If you encounter this problem, view this knowledge base article to delete any leftover artifacts.

How to Verify a Successful Upgrade

Tenable supports the most recent version of Tenable applications within ServiceNow, and unsuccessful upgrades cause most support issues. If requesting support, perform the following steps to provide proof that you have successfully updated Tenable applications within ServiceNow to the newest available version.

Caution: To complete a successful upgrade, it is important to review manually each of the skipped changes and follow the instructions. If you batch update the resolution field of these records instead of manually reviewing and resolving each one, then the upgrade fails and you must perform the upgrade again. To redo an upgrade, you need to repair each of the Tenable apps and complete the skip log process again.

Method 1: Support Collection Script

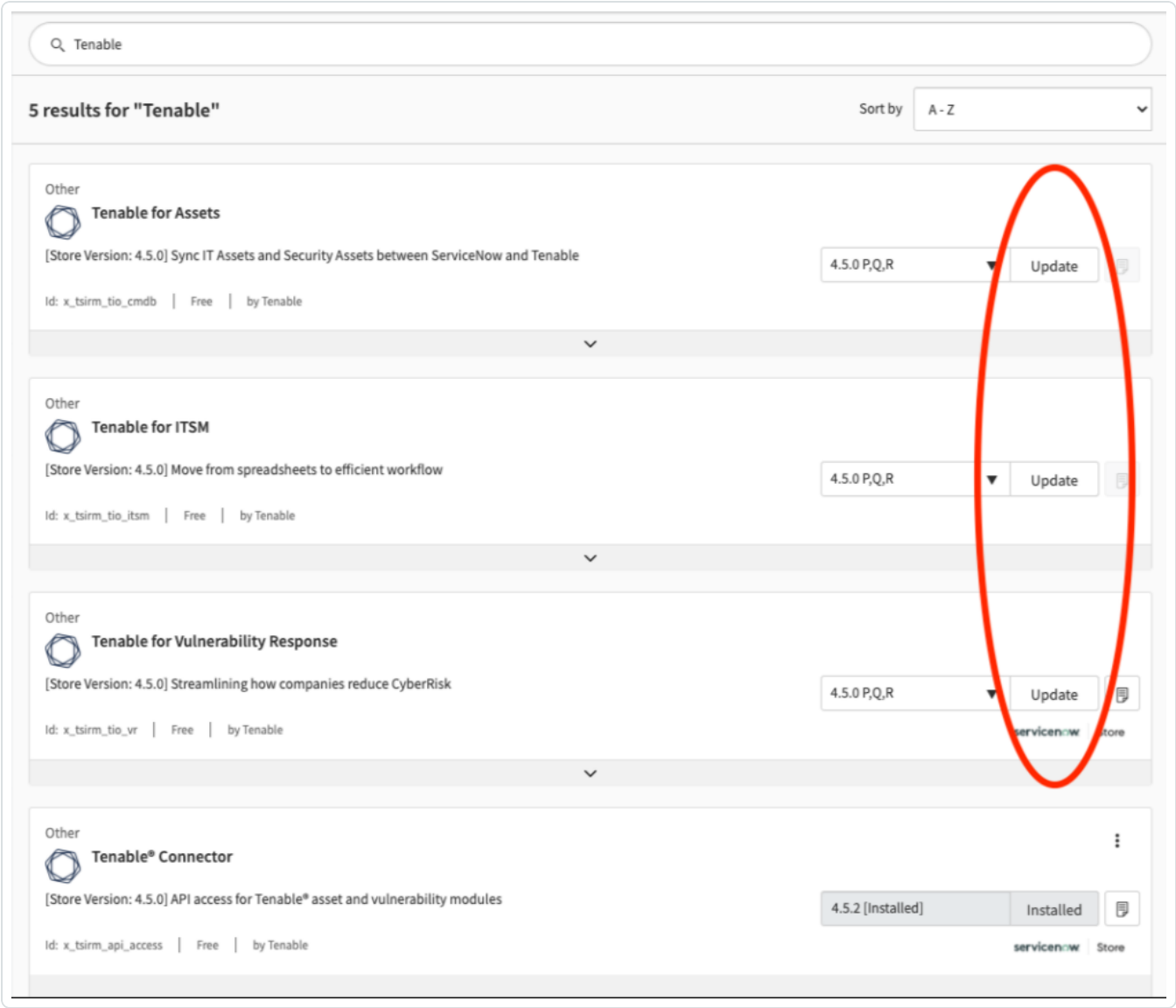
Tenable support provides a script on our support page to gather upgrade information without the need for you to provide any screenshots as verification:

Tenable Service Now App Support Collection Script

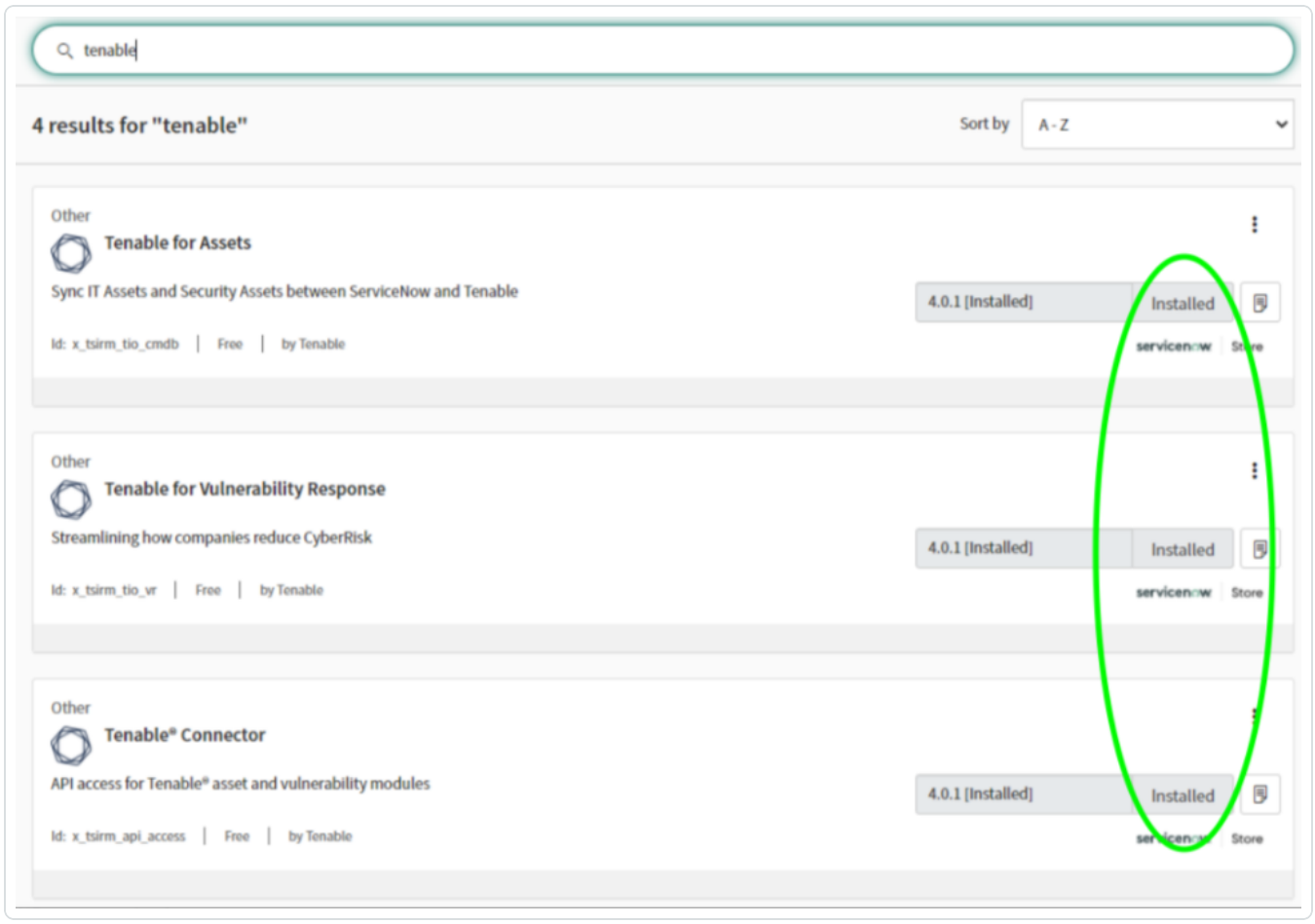
Method 2: Provide Verification Screenshots

If you are unable to run the support collection script, you can provide screenshots to show completed the successful upgrade.

1. Provide a screenshot of the current version of the Tenable plugins.

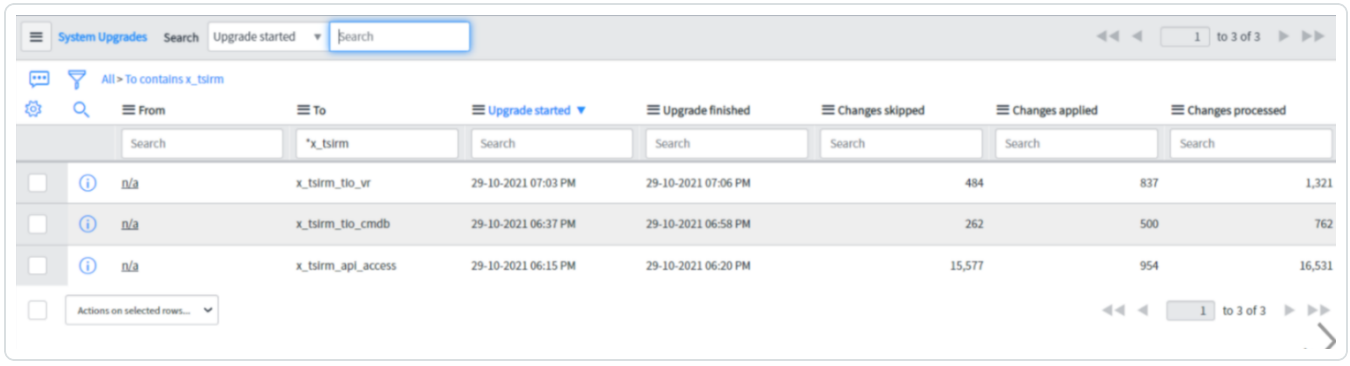


Note: This screenshot shows the user has not updated all of their plugins to the latest version. They need to update to the newest version to receive support.

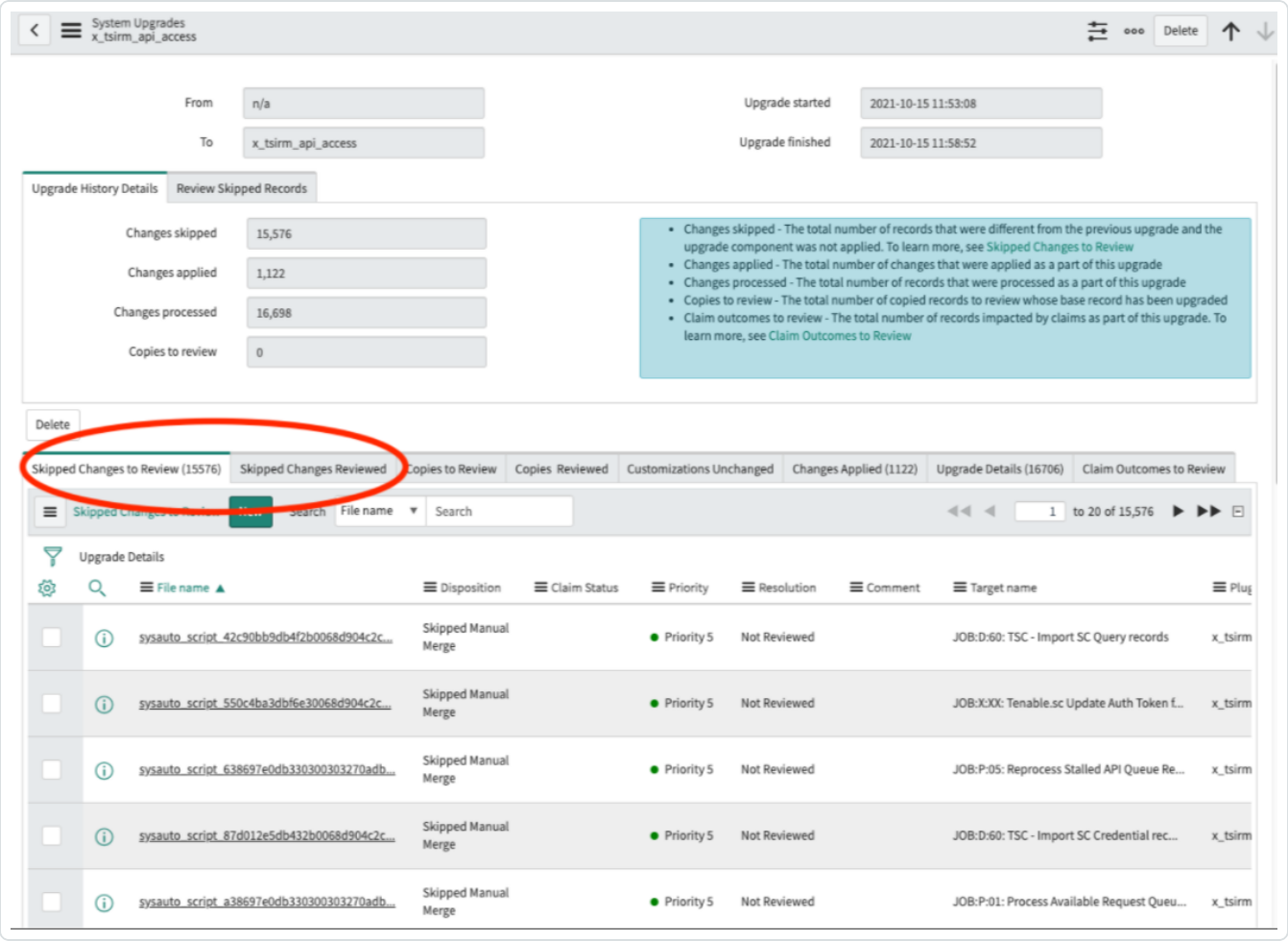


Note: This screenshot shows the user has updated all of their plugins to the latest version.

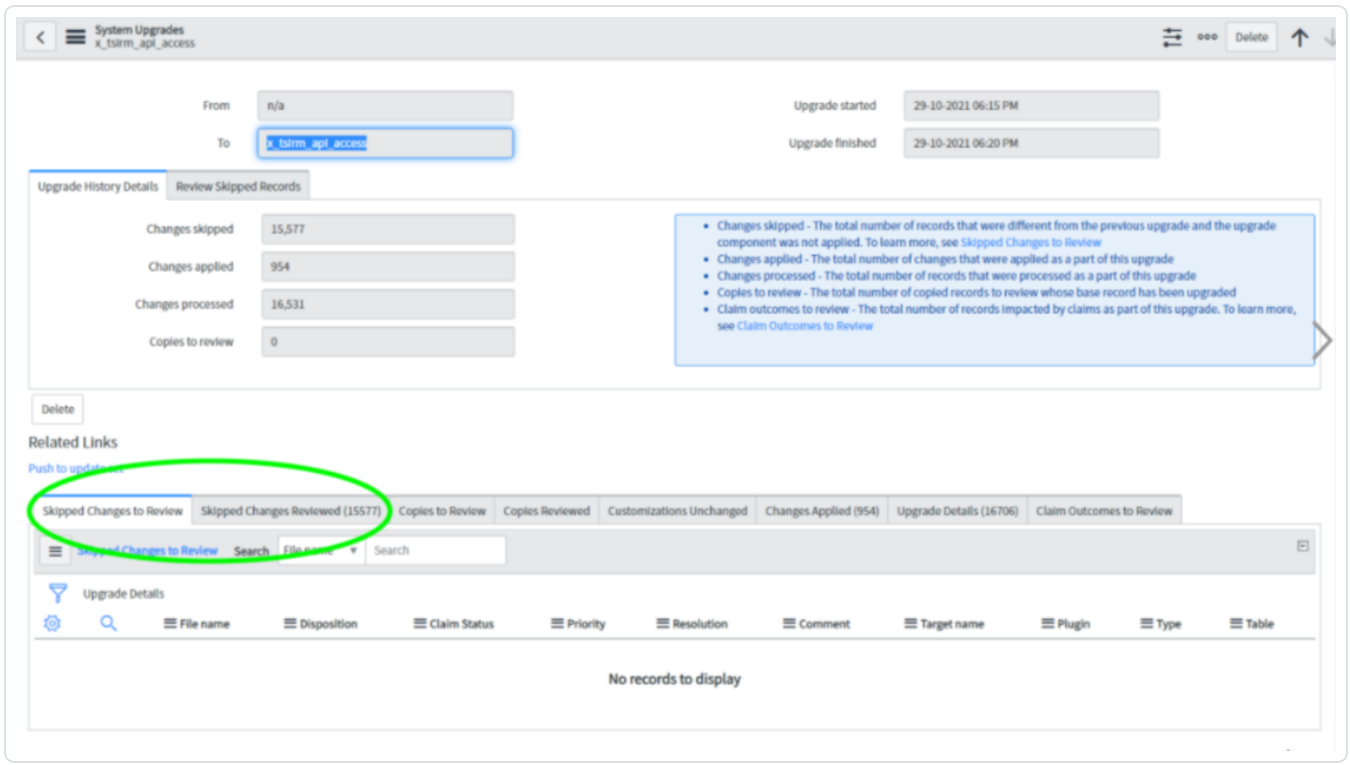
2. Provide screenshots of the **Upgrade History** and **Reviewed Skip Logs** for each plugin.



Note: This screenshot shows that the user has not reviewed the skipped changes.



Note: This screenshot shows the user has not manually reviewed all skipped changes. They need to complete this step to upgrade successfully and receive support.



Note: This screenshot shows the user has reviewed all skipped changes.

Unsuccessful Upgrades

If you are unsuccessful with your Tenable App for ServiceNow upgrade, you can complete it again:

1. Navigate to **System Definition > Plugins** and search for the Tenable apps.
2. For each Tenable app (Tenable Connector, Service Graph Connector for Tenable for Assets, Tenable OT Security for VR, or Tenable for ITSM), click the **Menu** icon on the application tile.
3. Click **Repair**.
4. In the **Activate Plugin** dialog box, click **Repair**.
5. After you repair the apps, they are back to a newly installed state, and you can review the skipped changes again. See *Review and Resolve Skipped Changes* in the Upgrade the Tenable Applications documentation.

Common Reasons for Failed Upgrade

Not reviewing skipped changes:

If you do not review the **Skipped Changes** after an upgrade, the apps will not work properly and the upgrade will be unsuccessful.

Incorrectly reviewing skipped changes:

The Tenable application does not apply changes, function properly, and the upgrade fails, when you do not manually open, review, and resolve each individual skipped change, and/or only update the **Resolution** field of the **Skipped Changes** list to **Reviewed and Reverted** (or to another resolved value).

For more information, see Upgrade the Tenable Applications.

Deleting Tenable Applications and Data

You may need to delete your Tenable applications and data when upgrading ServiceNow from versions 3.0 and earlier to versions 4.0 and later.

To delete current Tenable applications and data:

1. Disable all Tenable connectors and their associated or scheduled jobs.
2. Run the following commands in **Scripts** > **Background** to delete records:
    a. Delete all **Assets Pending Approval** (Tenable-specific legacy asset class).

```
//Assets Pending Approval cleanup x_tsirm_tio_cmdb_tio_disc_ci
var apa = new GlideMultipleDelete('x_tsirm_tio_cmdb_tio_disc_ci');
apa.execute();
```

    b. Delete all **Tenable Asset Attribute** records.

```
//Asset Attributes cleanup x_tsirm_tio_cmdb_asset_attributes
var assetInfo = new GlideMultipleDelete('x_tsirm_tio_cmdb_asset_
attributes');
assetInfo.execute();
```

    c. Delete all Tenable-specific IRE records.

```
//Clean up source uniqueness. This will force IRE matching
var assetSysSource = new GlideMultipleDelete(“sys_object_source”);
assetSysSource.addQuery(“name”, “STARTSWITH”, “Tenable”);
assetSysSource.execute();
```

    d. Delete all Tenable vulnerability items.

```
var vi = new GlideMultipleDelete('sn_vul_vulnerable_item');
 vi.addQuery(“source”, “STARTSWITH”, “Tenable”);
```

```
vi.execute();
```

3. Uninstall the Tenable applications.

This process provides a cleaner starting point and removes any corrupted data, if present. From here, you can either reinstall the Tenable applications, or install the ServiceNow-built Vulnerability Response (VR) app.

Reinstall Tenable-built Applications

Choose this option if you are not using ServiceNow's VR application. For more information, see the Install page.

Tenable Applications

Service Graph Connector for Tenable for Assets

Tenable for ITSM

Tenable OT Security for Vulnerability Response (VR)

Service Graph Connector for Tenable for Assets

Service Graph Connector for Tenable for Assets syncs and reconciles assets between Tenable Vulnerability Management, Tenable Security Center, Tenable OT Security, 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.

With Service Graph Connector for Tenable for Assets, you can:

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

Note: Service Graph Connector for Tenable for Assets only supports Tenable Security Center versions 5.7 and later.

Note: The Tenable ServiceNow Application for Assets push job to Tenable Vulnerability Management only creates assets and does not assign tags to assets.

For more information, see Assets Configuration and Schedule Import.

Service Graph Connector for Tenable for Assets for ServiceNow

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

Note: The Service Graph Connector for Tenable for Assets ServiceNow app asset push job uses the POST /import/assets API endpoint to create new assets in Tenable Vulnerability Management. This endpoint creates an asset import job that is managed by Tenable Vulnerability Management and is referred to as an async request in several rule descriptions.

Application Menu

- **Service Graph Connector for Tenable for Assets**: Primary Role Required: x_tsirm_tio_cmdb.user

Title	Required Role
Documentation	x_tsirm_tio_cmdb.user
Contact Support	x_tsirm_tio_cmdb.user
Dashboard	x_tsirm_tio_cmdb.user
Assets Pending Approval	x_tsirm_tio_cmdb.user
All Synchronized Items	x_tsirm_tio_cmdb.user
Configuration	x_tsirm_tio_cmdb.admin
General Settings	x_tsirm_tio_cmdb.admin
Connectors	x_tsirm_tio_cmdb.admin
API Data Mappings	x_tsirm_tio_cmdb.user
Diagnostics	x_tsirm_tio_cmdb.admin
Asset Outbound Jobs	x_tsirm_tio_cmdb.admin

Title	Required Role
Asset Inbound Jobs	x_tsirm_tio_cmdb.admin
Queued Actions	x_tsirm_tio_cmdb.admin

Primary Roles

- **x_tsirm_tio_cmdb.admin**: An administrative user of the application.
- **x_tsirm_tio_cmdb.user**: A basic user of the application.

Business Rules

- **Update Job and Chunk Status**: Business rule that sets the status of jobs and chunks.
- **Push Asset Update to Tenable.io**: Sends asset update information to Tenable Vulnerability Management by creating an async request queue action entry.
- **Set Name**: Sets the name of the asset attribute record of the connector or Asset UUID change.
- **Set Tenable Values when Done Processing**: On complete outbound jobs, this sets values on the asset attribute record.
- **Update Job Percent Complete**: Updates the job percent complete as records get processed.
- **Create Settings if None exist**: Automatically creates a general settings record with default values if one does not exist.
- **Calc Job State**: Calculates the job state based on happenings with chunks.
- **On Job State Change**: Inbound job total records and percent complete, when the state of the job changes.
- **Notify About Limitations on Out of Box Rules**: Shows user interface message explaining that out of box CI rules are not editable.
- **Push Asset Update to Tenable.io (Update)**: Sends asset update information to Tenable Vulnerability Management by creating an async request queue action entry.

Tenable for ITSM

Tenable for IT Service Management (ITSM) provides you with 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.

The Tenable ITSM Process

Tenable for ITSM uses Service Graph Connector for Tenable for Assets to find the correct asset/CI to link a vulnerability to. It is important that you completely test and tune Service Graph Connector for 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 to be used by IT administrators to assign remediation work to their teams.

The application creates vulnerabilities as follows:

- The Tenable ITSM app uses the Service Graph Connector for Tenable for Assets app to match vulnerable assets to ServiceNow CI's.
- For every vulnerability finding, it creates a unique vulnerability entry in the Tenable ITSM app.
- Coalescing on ServiceNow CI, plugin id, port, and protocols determine unique vulnerability entries.
- If a vulnerability is fixed in Tenable, both the vulnerability and incident close in ServiceNow.
- If a vulnerability is closed manually, but 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 for ITSM for ServiceNow

Tenable Vulnerability Management offers 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 Vulnerability Management vulnerability data and manage it within ServiceNow.

Application Menu

- **Tenable for ITSM**: Primary Role Required: x_tsirm_tio_itsm.user

Title	Required Role
Documentation	x_tsirm_tio_itsm.user
Contact Support	x_tsirm_tio_itsm.user
Plugins	x_tsirm_tio_itsm.user
Vulnerabilities	x_tsirm_tio_itsm.user
Incidents	x_tsirm_tio_itsm.user
Configuration	x_tsirm_tio_itsm.user
General Settings	x_tsirm_tio_itsm.admin
Connectors	x_tsirm_tio_itsm.admin
Scheduled Imports	x_tsirm_tio_itsm.user
Incident Rules	x_tsirm_tio_itsm.admin
Diagnostics	x_tsirm_tio_itsm.admin
Queued Actions	x_tsirm_tio_itsm.admin
Documentation	x_tsirm_tio_itsm.user
Contact Support	x_tsirm_tio_itsm.user
Plugins	x_tsirm_tio_itsm.user

Title	Required Role
Vulnerabilities	x_tsirm_tio_itsm.user
Incidents	x_tsirm_tio_itsm.user

Primary Roles

- **x_tsirm_tio_itsm.admin**: An administrative user of the application.
- **x_tsirm_tio_itsm.user**: A basic user of the application.

Business Rules

- **Cali Job State**: Calculates the job state based on happenings with chunks.
- **On Job State**: Change Inbound job total records and percent complete, when the state of the job changes.
- **Create Settings if None Exist**: Automatically creates a general settings record with default values if one doesn't exist.

Tenable OT Security for Vulnerability Response (VR)

The integration of Tenable OT Security for VR 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 prioritize rapidly and automate the remediation of critical vulnerabilities across your most important assets.

> **Note:** The Tenable OT Security for VR application only supports Tenable OT Security.

With Tenable OT Security for Vulnerability Response, you can:

- Leverage the Service Graph Connector for Tenable for Assets application to 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 later.

Tenable OT Security for VR

Tenable OT Security for VR allows you to 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.

Note: Run the import asset job before running the import vulnerabilities job in Tenable OT Security for VR.

Application Menu

Tenable OT Security for VR: Primary Role Required: x_tsirm_tio_vr.user

Title	Required Role
Documentation	x_tsirm_tio_vr.user
Contact Support	x_tsirm_tio_vr.user
Configuration	x_tsirm_tio_vr.user
General Settings	x_tsirm_tio_vr.admin
Connectors	x_tsirm_tio_vr.admin
Scheduled Imports	x_tsirm_tio_vr.user
API Data Mappings	x_tsirm_tio_vr.admin
Default VR Data Source	x_tsirm_tio_vr.admin
Transform Maps	x_tsirm_tio_vr.admin
Diagnostics	x_tsirm_tio_vr.admin
Queued Actions	x_tsirm_tio_vr.admin
Documentation	x_tsirm_tio_vr.user
Contact Support	x_tsirm_tio_vr.user
Configuration	x_tsirm_tio_vr.user

Title	Required Role
General Settings	x_tsirm_tio_vr.admin
Connectors	x_tsirm_tio_vr.admin
Scheduled Imports	x_tsirm_tio_vr.user

Primary Roles

x_tsirm_tio_vr.admin: An administrative user of the application.

x_tsirm_tio_vr.user: A basic user of the application.

Business Rules

Calc Job State: Calculates the job state based on happenings with chunks.

Run Plugin Families Populate on Activate: Runs the script to run the API call to get plugin families from Tenable when a connector is activated.

On Job State Change: Inbound job total records and percent complete, when the state of the job changes.

Create Settings if None Exist: Automatically creates a general settings record with default values if one doesn't exist.

ServiceNow Data Maps

The logic for mapping Assets to ServiceNow Configuration Items is available in the following pages:

- Tenable OT Security available data
- Tenable Security Center available data
- Tenable Vulnerability Management available data

Available Data Tenable OT Security

Tenable OT Security Asset Import Data Map

Logic for mapping Tenable OT Security Assets to ServiceNow Configuration Items.

Asset import sequence:

1. ServiceNow queries Tenable OT Security for assets.
2. Data is attached to ServiceNow Job Chunk.
3. Data is transformed into a format useable for ServiceNow Identification and Reconciliation Engine (IRE).
4. Data is submitted to IRE which creates CIs in CMDB.
5. OT Assets are created for certain CIs.

Data Transformation in ServiceNow

For each Asset imported from Tenable OT Security into ServiceNow, multiple records are created.

Main CI

A main CI record (cmdb_ci_incomplete_ip, cmdb_ci_unclassed_hardware, or cmdb_ci_computer) is created for every Tenable OT Security Asset imported into ServiceNow.

ServiceNow Field	Details (Tenable OT Security fields in bold)	CMDB Class
Class	1. "Operational Technology (OT)" 2. Specific OT Class • If there is a known ServiceNow CI class map for that Tenable OT Security type	All classes
Name	**details.name**	All classes
Serial Number	**details.serial**	All classes
Description	**details.description**	All classes

Operating System	**details.osNamel**	All classes
Backplane ID	**details.backplane**	All classes
Backplane Name	**details.backplane**	All classes
Firmware version	**details.firmwareVersion**	All classes
Model number	**details.modelName**	All classes
Discovery Source	“SG-TenableForAssets”	All classes
IP Address	**details.ips[0]**	All classes
Most recent discovery	**details.lastSeen**	All classes
First discovered	**details.firstSeen**	All classes
Vendor	**details.vendor**	All classes
Manufacturer	**details.vendor**	All classes
Tenable Asset Attributes	Reference to Tio CMDB Asset Attributes table with Tenable OT Security specific fields	All classes

Child Network Adapter CIs

Related Network Adapter CI records (cmdb_ci_network_adapter) are created for Tenable OT Security Assets since there is no network interface information pulled from Tenable.

ServiceNow field	Details (Tenable OT Security fields in bold)
Class	“Network Adapter”
Name	**details.macs**
MAC Address	**details.macs**

Configuration Item	Reference to Main CI
Discovery Source	“SG-TenableForAssets”

Child IP Address CIs

Related IP Address CI records (cmdb_ci_ip_address) are created for each IP address associated with a Main CI.

ServiceNow field	Details (Tenable OT Security fields in bold)
Class	“IP Address”
Name	**details.ips**
IP Address	**details.ips**
IP Version	“4”
Network Partition Identifier	**details.extendedSegments.nodes[0].id**
Discovery Source	“SG-TenableForAssets”

Tenable Asset Attributes Records

A Tenable Asset Attributes record (x_tsirm_tio_cmdb_asset_attributes) is created for every Main CI.

ServiceNow filed	Details (Tenable OT Security fields in bold)
Hostname	Main CI name
Connector	Reference to connector record
Tenable Uniqueness	**id**
Asset UUID	**id**
Raw Data	Raw JSON Data
Sources	“OT for” + Tenable App Name
Source Native Key	**id**
Attributes	Raw JSON Data in ServiceNow format

ServiceNow filed	Details (Tenable OT Security fields in bold)
Name	Connector.Name + ". " + **id**
Related CI	Reference to Main CI

OT Asset Records

An OT Asset record (cmdb_ot_entity) is created for every Main CI.

ServiceNow field	Details (Tenable OT Security fields in bold)
OT asset	Reference to Main CI
OT asset type	Specific asset type • If there is a known ServiceNow OT asset type map for that Tenable OT Security **type**.
OT discovery source ID	**id**
Purdue level	**details.purdueLevel**
Asset criticality	**details.criticality**
OT discovery source name	“SG-TenableForAssets”

CMDB Relationship Records

A CMDB Relationship record (cmdb_rel_ci) is created for every parent/child relationship between the Main CI and a Network Adapter CI or an IP Address CI.

ServiceNow field	Details
Parent	Reference to Main CI
Child	Reference to Network Adapter or IP Address CI
Type	“Owns::Owned by”

Discovery Source Records

A Discovery Source record (sys_object_source) is created for every new CI created in ServiceNow with information about the source and the unique identifier of the CI.

ServiceNow field	Details
ID	id
Last Scan	Date/time of last Tenable OT Security import
Target Sys ID	Reference to Main CI
Target Table	Table of Main CI
Name	“SG-TenableForAssets”
Source Feed	“Tenable”

API Calls to Tenable OT Security

Query Assets

Input: first, after

- **Example:** `{"operationName": "getAssets", "variables": {"first": chunkSize, "after": afterCursor, "sort": [{ "direction": "AscNullFirst", "field": "lastSeen" }] }, "query": "query getAssets($filter: AssetExpressionsParams, $search: String, $sort: [AssetSortParams!], $slowCount: Boolean, $after: String, $first: Int) { assets(filter: $filter sort: $sort search: $search slowCount: $slowCount after: $after first: $first) { pageInfo { ...pageInfo __typename } nodes { ...inventoryAsset __typename } count: totalCount __typename } } fragment pageInfo on PageInfo { startCursor endCursor hasNextPage hasPreviousPage __typename } fragment inventoryAsset on Asset { id superType type details segments { nodes { ...segmentName __typename } __typename } __typename } fragment segmentName on SegmentGroup { id name type assetType subnet systemName system isPredefinedName __typename}" }`

Output: Use GraphiQL Playground or review Asset object documentation for possible asset values.

Available Data Tenable Security Center

Tenable Security Center Asset Import Data Map

Logic for mapping Tenable Security Center Assets to ServiceNow Configuration Items.

Asset import sequence:

1. ServiceNow queries Tenable Security Center for assets.
2. Data is attached to ServiceNow Job Chunk.
3. Data is transformed into a format useable for ServiceNow Identification and Reconciliation Engine (IRE).
4. Data is submitted to IRE which creates CIs in CMDB.

Data Transformation in ServiceNow

For each Asset imported from Tenable Security Center into ServiceNow, multiple records are created.

Main CI

A main CI record (cmdb_ci_incomplete_ip, cmdb_ci_unclassed_hardware, or cmdb_ci_computer) is created for every Tenable Security Center Asset imported into ServiceNow.

ServiceNow Field	Details (Tenable Security Center fields in bold)	CMDB Class
Class	• Incomplete IP Identified Device If **ip** is received from Tenable Security Center. • Unclassed Hardware If 1, plus **dnsName** or **netbiosNames** are received from Tenable Security Center. • Computer If 2, plus **osCPE** are received from Ten-	All classes

	able Security Center.	
Name	1. **netbiosName** 2. **fqdn** 3. **dnsName** 4. **ip** 5. **macAddress**	All classes
Description	Information about how name was identified	All classes
Discovery Source	“SG-TenableForAssets”	All classes
Tenable Asset Attributes	Reference to Tio CMDB Asset Attributes table with Tenable Security Center specific fields	Computer and Unclassed Hardware classes only
Mac Address	**macAddress**	Computer and Unclassed Hardware classes only
Operating System	**osCPE**	Computer class only
Name	**ip**	Incomplete IP class only
Network Partition Identifier	**repository_name**	Incomplete IP class only

Child Network Adapter CIs

Related Network Adapter CI records (cmdb_ci_network_adapter) are NOT created for Tenable Security Center Assets since there is no network interface information pulled from Tenable.

Child IP Address CIs

Related IP Address CI records (cmdb_ci_ip_address) are created for each IP address associated with a Main CI.

ServiceNow field	Details (Tenable Security Center fields in bold)
Class	“IP Address”
Name	**ip**
IP Address	**ip**
IP Version	“4”
Network Partition Identifier	**repository.name**
Discovery Source	“SG-TenableForAssets”

Tenable Asset Attributes Records

A Tenable Asset Attributes record (x_tsirm_tio_cmdb_asset_attributes) is created for every Main CI.

ServiceNow filed	Details (Tenable Security Center fields in bold)
Hostname	Main CI name
Connector	Reference to connector record
SC Uniqueness	1. **uniqueness** 2. **hostUniqueness**
OS CPE	**osCPE**
Repository Data Format	**repository.dataFormat**
Sources	“SC for” + Tenable App Name
Source Native Key	1. **uniqueness** 2. **hostUniqueness**
Attributes	Raw JSON Data in ServiceNow format
Name	Connector.Name ": " + SC Uniqueness
Related CI	Reference to Main CI

CMDB Relationship Records

A CMDB Relationship record (cmdb_rel_ci) is created for every parent/child relationship between the Main CI and a Network Adapter CI or an IP Address CI.

ServiceNow field	Details
Parent	Reference to Main CI
Child	Reference to Network Adapter or IP Address CI
Type	“Owns::Owned by”

Discovery Source Records

A Discovery Source record (sys_object_source) is created for every new CI created in ServiceNow with information about the source and the unique identifier of the CI.

ServiceNow field	Details
ID	**id**
Last Scan	Date/time of last Tenable Security Center import
Target Sys ID	Reference to Main CI
Target Table	Table of Main CI
Name	“SG-TenableForAssets”
Source Feed	“Tenable”

API Calls to Tenable Security Center

Request Analyst Results

Input: type, query, sortDir, sortField, sourceType, startOffset, endOffset

- **Example:** `{"type":"vuln","query":{"name":"","-type":"vuln","tool":"sumip","description":"","context":"","groups":[],"startOffset":0,"endOffset":1500,"filters":[{"filterName":"repository","operator":"=","value":[{"id":"3","-name":"Staged-Small","description":"","type":"Local","uuid":"5AEA0478-0F1A-`

4B02-87D6-1F6131443F9C"},{"id":"1","-
name":"Live","description":"","type":"Local","uuid":"504D0D4E-7A95-4AA8-
BFC2-98009FE702E1"},{"id":"4","name":"Staged-Agent-
s","description":"","type":"Local","uuid":"9F68370D-1EC9-4005-8555-
23B1DF2FCF5B"}]},{"fil-
terName":"lastSeen","operator":"=","id":"lastSeen","value":"1670364343-
1670450742"}]},"sortField":"score","sortDir":"asc","-
sourceType":"cumulative"}

Output: Open link and review Example Response for possible asset values.

Available Data Tenable Vulnerability Management

Tenable Vulnerability Management Asset Import Data Map

Logic for mapping Tenable Vulnerability Management Assets to ServiceNow Configuration Items.

Asset import sequence:

1. ServiceNow queries Tenable Vulnerability Management for assets.
2. Data is attached to ServiceNow Job Chunk.
3. Data is transformed into a format useable for ServiceNow Identification and Reconciliation Engine (IRE).
4. Data is submitted to IRE which creates CIs in CMDB.

Data Transformation in ServiceNow

For each Asset imported from Tenable Vulnerability Management into ServiceNow, multiple records are created.

Main CI

A main CI record (cmdb_ci_incomplete_ip, cmdb_ci_unclassed_hardware, or cmdb_ci_computer) is created for every Tenable Vulnerability Management Asset imported into ServiceNow.

ServiceNow Field	Details (Tenable Vulnerability Management fields in bold)	CMDB Class
Class	• Incomplete IP Identified Device If **ipv4s** or **ipv6s** are received from Tenable Vulnerability Management. • Unclassed Hardware If 1., plus **hostnames**, **netbios_names**, or **fqdns** are received from Tenable Vulnerability Management. • Computer	All classes

	If 2., plus **aws_ec2_instance_id**, **gcp_instance_id**, **azure_resource_id**, or **operating_systems** are received from Tenable Vulnerability Management.	
Name	1. **netbios_names** 2. **hostnames** 3. **fqdns** 4. **ipv4s** 5. **ipv6s** 6. **mac_addressses**	All classes
Description	Information about how name was identified	All classes
Discovery Source	“SG-TenableForAssets”	All classes
Tenable Asset Attributes	Reference to Tio CMDB Asset Attributes table with Tenable Vulnerability Management specific fields	All classes
Is Virtual	If **aws_ec2_instance_id, gcp_instance_id**, **azure_resource_id** is received from Tenable Vulnerability Management	Computer class only
Operating System	**operating_systems**	Computer class only
IP Address	**ipv4s**	Incomplete IP class only
IP Version	“4”	Incomplete IP class only
Network Partition Identifier	**network_name**	Incomplete IP class only

Child Network Adapter CIs

Related Network Adapter CI records (cmdb_ci_network_adapter) are created for each MAC address associated with a Main CI.

ServiceNow field	Details (Tenable Vulnerability Management fields in bold)
Class	“Network Adapter”
Name	**network_interfaces.name**
MAC Address	**network_interfaces.mac_addresses**
Fully Qualified Domain Name	**network_interfaces.fqdns**
Configuration Item	Reference to Main CI
Discovery Source	“SG-TenableForAssets”

Child IP Address CIs

Related IP Address CI records (cmdb_ci_ip_address) are created for each IP address associated with a Main CI.

ServiceNow field	Details (Tenable Vulnerability Management fields in bold)
Class	“Network Adapter”
Name	1. **network_interfaces.ipv4s** or **network_interfaces.ipv6s** 2. **ipv4s or ipv6s**
IP Address	1. **network_interfaces.ipv4s** or **network_interfaces.ipv6s** 2. **ipv4s or ipv6s**
IP Version	“4” or “6”
Network Partition Identifier	**network_name**
Nic	Reference to Network Adapter (if exists)
Discovery Source	“SG-TenableForAssets”

Tenable Asset Attributes Records

A Tenable Asset Attributes record (x_tsirm_tio_cmdb_asset_attributes) is created for every Main CI.

ServiceNow filed	Details (Tenable Vulnerability Management fields in bold)
Hostname	Main CI name
Connector	Reference to connector record
Tenable Uniqueness	**id**
Asset UUID	**id**
Raw Data	Raw JSON data
Sources	“IO for ” + Tenable App Name
Source Native Key	**id**
Has Agent	**has_agent**
Has Plugin Results	**has_plugin_results**
Created At	**created_at**
Terminated At	**terminated_at**
Terminated By	**terminated_by**
Updated At	**updated_at**
Deleted At	**deleted_at**
Deleted By	**deleted_by**
First Seen	**first_seen**
Last Seen	**last_seen**
First Scan Time	**first_scan_time**
Last Scan Time	**last_scan_time**
Last Authenticated Scan Date	**last_auhenticated_scan_date**
Last Licensed Scan Date	**last_licensed_scan_date**
Last Scan ID	**last_scan_id**

ServiceNow filed	Details (Tenable Vulnerability Management fields in bold)
Last Schedule ID	**last_schedule_id**
Azure Instance ID	**azure_vm_id**
GCP Project ID	**gcp_project_id**
GCP Zone	**gcp_zone**
GCP Instance ID	**gcp_instance_id**
AWS EC2 Instance ID	**aws_ec2_instance_id**
Agent UUID	**agent_uuid**
BIOS UUID	**bios_uuid**
Network ID	**network_id**
AWS Owner ID	**aws_owner_id**
McAfee EPO GUID	**mcafee_epo_guid**
McAfee EPO Agent GUID	**mcafee_epo_agent_guid**
Bigfix Asset ID	**bigfix_asset_id**
Agent Names	**agent_names**
Netbios Name	**netbios_names**
Operating Systems	**operating_systems**
System Type	**system_types**
SSH Fingerprints	**ssh_fingerprints**
Qualys Asset ID	**qualys_asset_ids**
Qualys Host IDs	**qualys_host_ids**
Manufacturer TPM ID	**manufacturer_tpm_ids**
Symantec EP Hardware Key	**symantec_ep_hardware_keys**

ServiceNow filed	Details (Tenable Vulnerability Management fields in bold)
Sources	**sources**
Tags	**tags**
ACR Score	**acr_score**
Exposure Score	**exposure_score**
Attributes	Raw JSON data in ServiceNow format
Name	Connector.Name + ": " + **id**
Related CI	Reference to Main CI

CMDB Relationship Records

A CMDB Relationship record (cmdb_rel_ci) is created for every parent/child relationship between the Main CI and a Network Adapter CI or an IP Address CI.

ServiceNow field	Details
Parent	Reference to Main CI
Child	Reference to Network Adapter or IP Address CI
Type	“Owns::Owned by”

Discovery Source Records

A Discovery Source record (sys_object_source) is created for every new CI created in ServiceNow with information about the source and the unique identifier of the CI.

ServiceNow field	Details
ID	**id**
Last Scan	Date/time of last Tenable Vulnerability Management import
Target Sys ID	Reference to Main CI
Target Table	Table of Main CI

Name	“SG-TenableForAssets”
Source Feed	“Tenable”

API Calls to Tenable Vulnerability Management

Generate Tenable Assets Export

Input: chunk_size, filters

- **Example:** `{"chunk_size":1500,"filters":{"updated_at":1657660668,"is_deleted":false,"is_licensed":true}}`

Output: export_uuid

Query for Asset Export Status

Input: export_uuid

Output: status, chunks_available

Download Tenable Assets Export Chunk

Input: export_uuid, chunk_id

Output: Open link and select the 200 response for all possible asset values.

Tenable Security Center Data Map

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

Tenable Security Center	ServiceNow
biosGUID	bios_uuid
dnsName	fqdn
ip	ipv4/ipv6
lastAuthRun	last_authenticated_scan_date
lastUnauthRun	last_unauthenticated_scan_date

macAddress	mac_address
mcafeeGUID	mcafee_epo_guid
netbiosName	netbios_name
osCPE	os_cpe
uniqueness	uniqueness
uuid	agent_uuid
repository.dataFormat	repository_data_format
repository.description	repository_description
repository.id	repository_id
repository.name	repository_name

Configure

Configure your Tenable application.

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

Configure the Tenable Connector

The Tenable Connector provides all API interactions between your Tenable applications (Tenable OT Security, Tenable Vulnerability Management, or Tenable Security Center) 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 Security Center versions 5.7 and later.

Before you begin:

For Tenable Vulnerability Management:

Required User Role: Administrator

- You must have your Tenable Vulnerability Management API keys.

  Note: For your Tenable Vulnerability Management integration:

  - Generate an API key in Tenable Vulnerability Management to complete the configuration. See the Tenable Vulnerability Management 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 a requirement for each installed instance of the integration.)

For Tenable Security Center:

Required User Role: Security Analyst

For Tenable OT Security:

Required User Role: Read Only

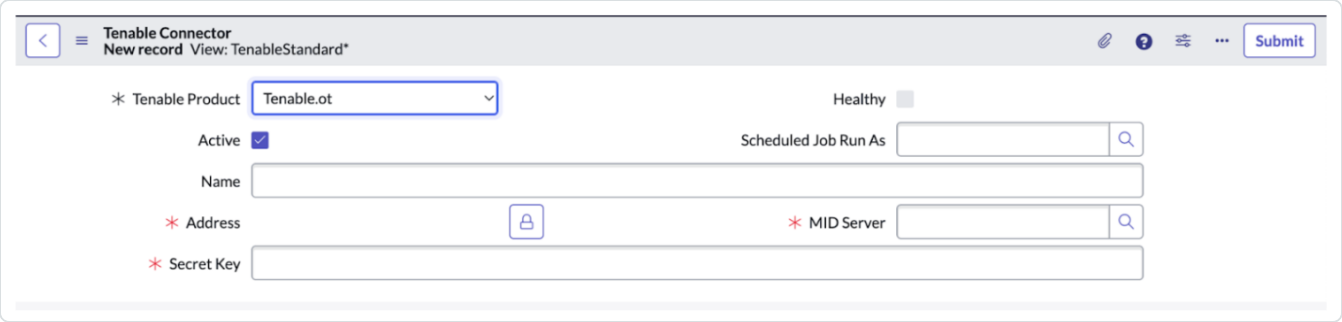
To configure the Tenable connector for Tenable Vulnerability Management, Tenable Security Center, or Tenable OT Security:

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.ot**, **Tenable.io**, or **Tenable Security Center**.
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 a requirement. 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 OT Security:

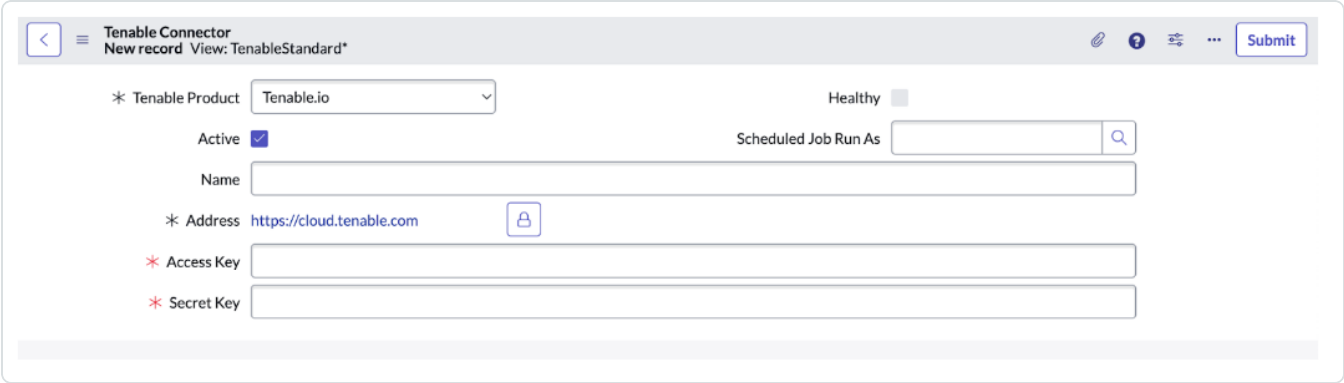
   a. In the **Address** text box, type an IP address or DNS name for the connector.

      Note: Type *https://* before the IP or DNS name.

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

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

For Tenable Vulnerability Management:



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

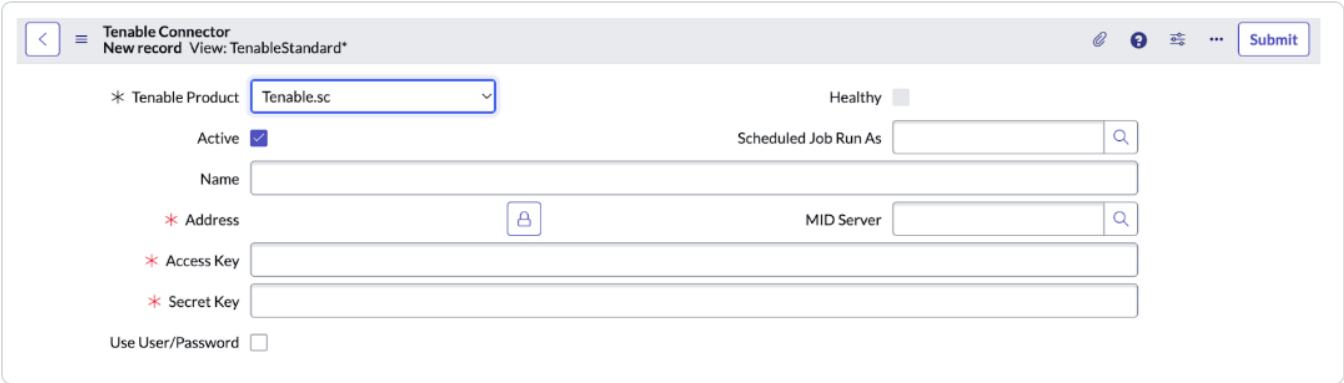
ServiceNow populates this with the Tenable Vulnerability Management IP address.

> **Note:** 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 Security Center:



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:** 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 Security Center 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 more settings options on your connector page depending on the Tenable applications you have installed (For example, Service Graph Connector for Tenable for Assets [**Assets Settings**], Tenable OT Security for VR [**VR Settings**], and Tenable ITSM **[ITSM Settings**]).

> **Note:** For more information about ServiceNow settings, see the ServiceNow documentation.

13. Click **Update**.

14. Click **Test the Connector**.

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

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*.

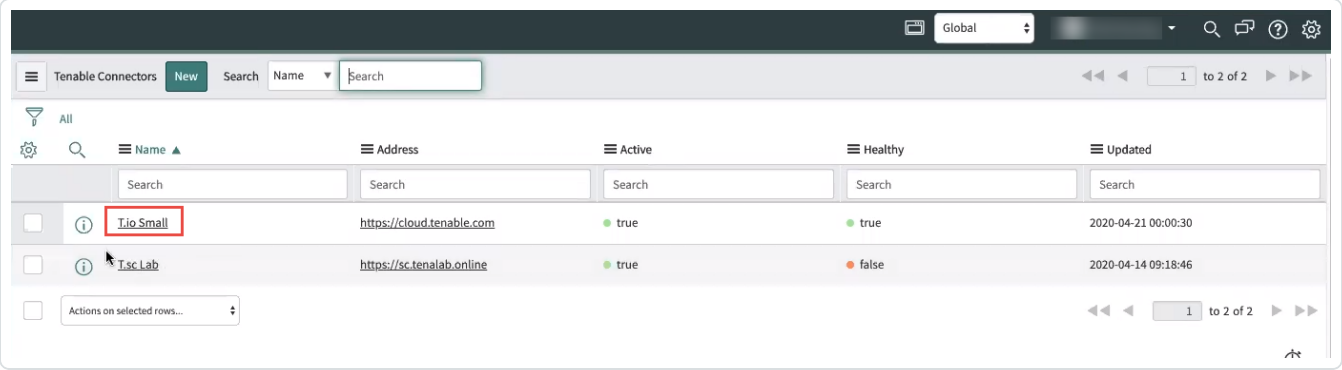
   The Tenable applications appear.

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

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

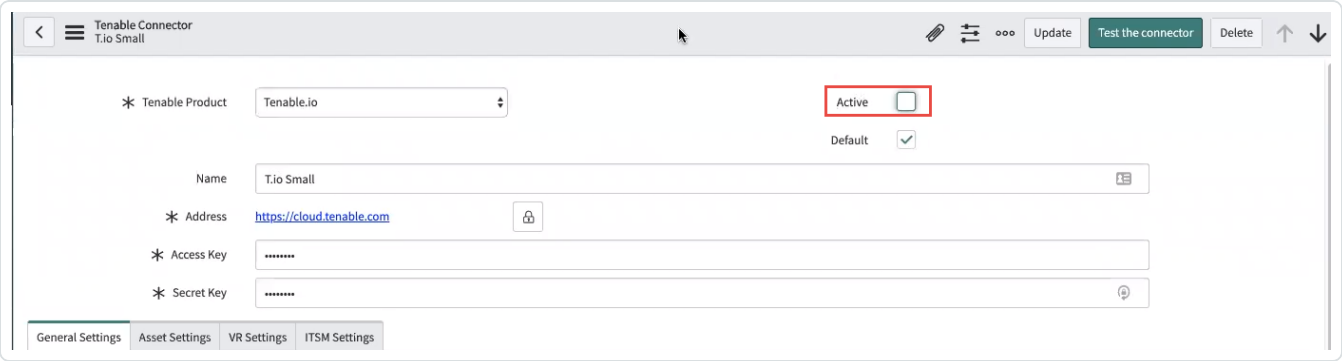
   Your configured Tenable connectors appear.

4. Select your Tenable connector.



   The selected connector page appears.

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



6. Click **Update**.

   The **Tenable Connector** deactivates.

7. Repeat this to deactivate all your connectors.

To enable your Tenable Connector:

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

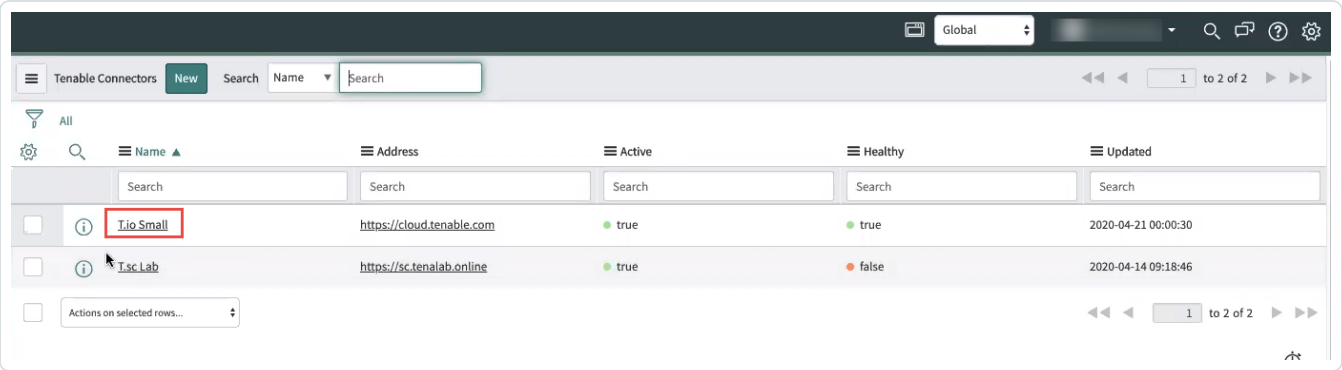
   The Tenable applications appear.

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

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

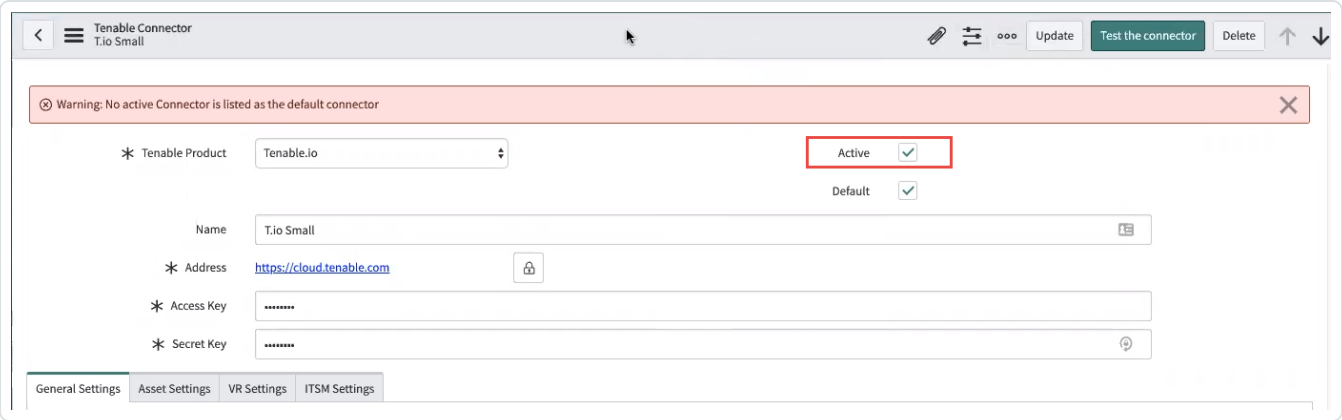
   Your configured Tenable connectors appear.

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** activates.

7. Repeat this to activate all your connectors.

Assets Configuration and Schedule Import

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

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

Note: It is important that you completely set up and tune this integration to match Tenable Assets to ServiceNow CIs before moving on to Tenable OT Security for VR or Tenable for ITSM.

To set up the asset integration configuration, you must:

- Configure the Tenable Connector
- Configure Assets to Sync from Tenable to ServiceNow
- Configure IRE Rules
- Import Operational Technology (OT) Devices
- (Optional) Configure Assets to Sync from ServiceNow to Tenable Vulnerability Management
- (Optional) Configure Assets to Sync from ServiceNow to Tenable Security Center

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 Vulnerability Management**, **Tenable Security Center**, or **Tenable.ot**.

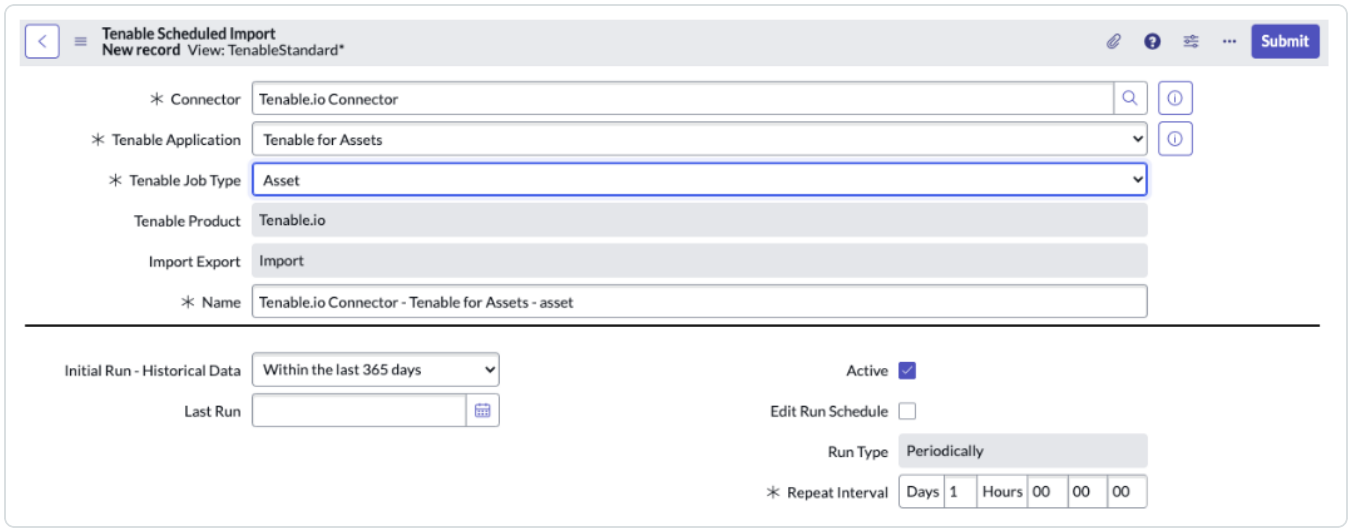
   The **Tenable Connector** page appears.

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

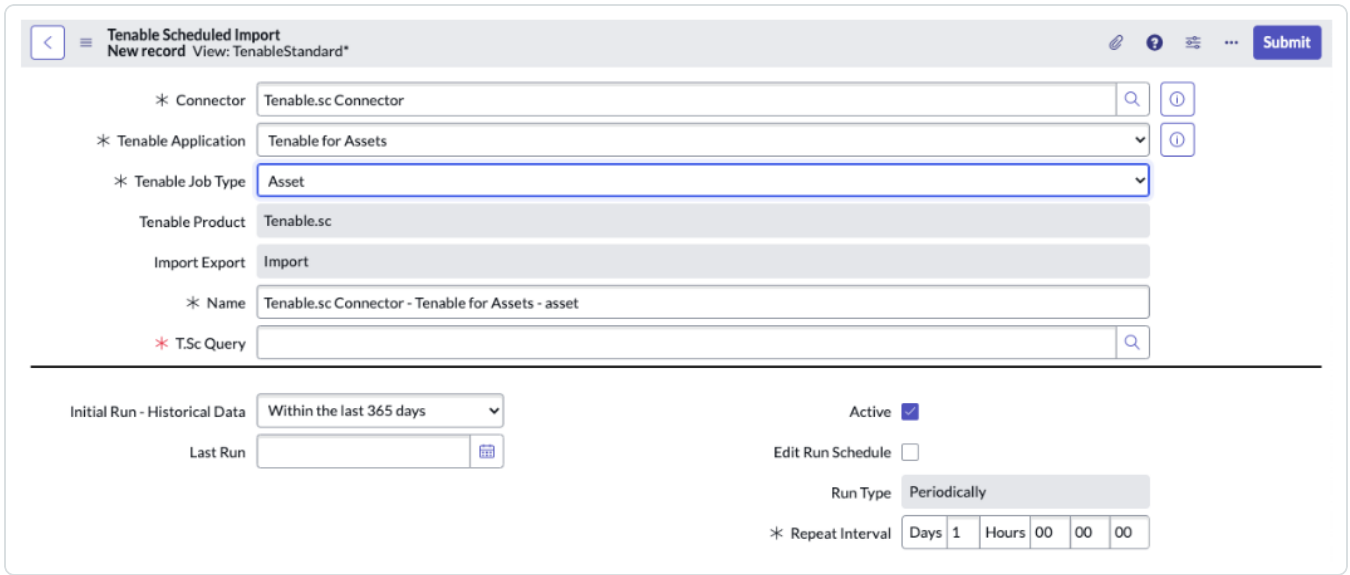
   The **Tenable Scheduled Import** page appears. By default, the **Tenable Product** and **Connector** fields populate with the Tenable application/connector you selected in step 5.

7. From the **Tenable Application** drop-down box, select **Service Graph Connector for Tenable for Assets**.

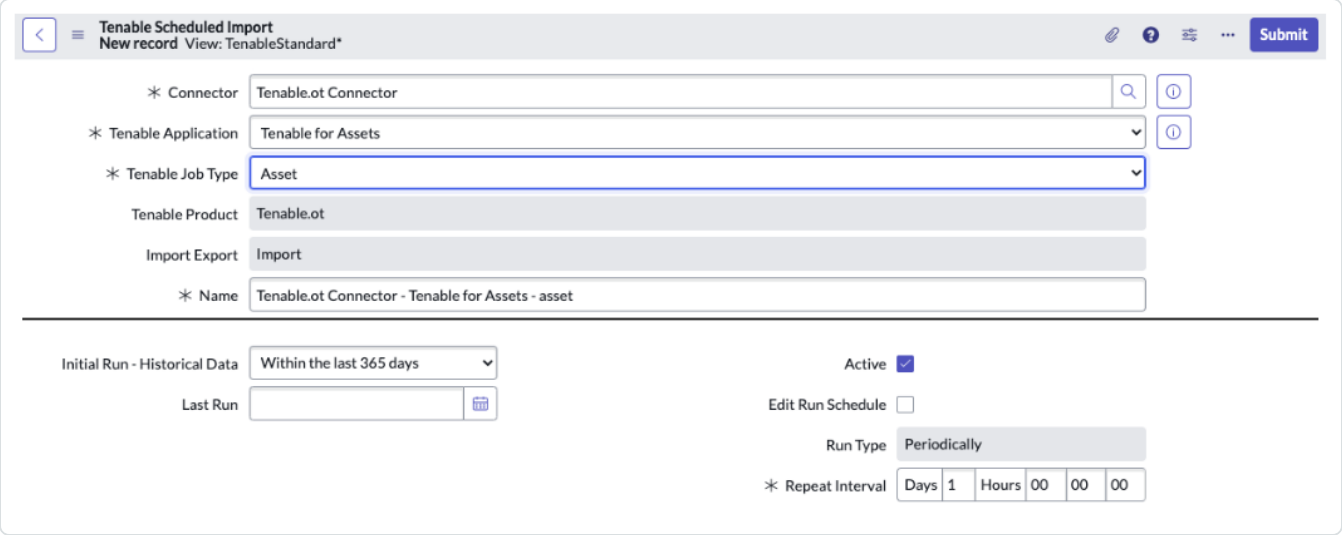
   Tenable Vulnerability Management



   Tenable Security Center



   Tenable.ot



8. From the **Tenable Job Type** drop-down box, select the **Asset** job type.

   Note: If you are in a domain-separated environment, the Domain is set to the same value that is on the **Connector** record. If this is not correct, create a new **Connector** record in the correct Domain.

9. From the **Import Export** drop-down box, select **Import**. Import is selected by default.

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

11. Configure the options for your import.

Option	Description
T.sc Query	(Only for Tenable Security Center) Select the query to use for the import. **Note:** If no queries are available, see Queries in the Tenable Security Center documentation to add a new query. Then, execute the Queries Scheduled Import to pull it into ServiceNow. Once that is complete, then you can select the new query here
Initial Run - Historical Data	The amount of time (in days) of historical data you would like to pull for your first import.
Last Run	The date and time that the import was last run.

Active	If selected, the scheduled job runs on the configured schedule. If Run Type = Periodically and Active = true, then an asset sync is automatically executed when you submit the import or export. By default, this setting is selected.
Schedule	
Edit Run Schedule	Select this box if you want to edit the Run Type and Repeat Interval / Time.
Run Type	The frequency that you want the import to run.
Repeat Interval / Time	The set time (hh/mm/ss) to run the import.

12. 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 affect all future configurations.

Configure IRE Rules

The Identification and Reconciliation Engine (IRE) is ServiceNow's system for identifying matches in the CMDB and determining if CIs can be created and what CI fields can be updated by different sources. Refer to ServiceNow's documentation to ensure IRE is configured correctly for your environment before importing assets from Tenable.

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. You can use data source rules to prevent Tenable from creating new CIs.

Note: ServiceNow provides some general Identification Rules out-of-the-box. However, you may need to customize these rules for your specific environment. By default, CI fields are updated with Tenable data on each import. You can use reconciliation rules to control what CI fields can be updated by Tenable. By default, Tenable is able to create new CIs in your CMDB. You can use Data Source Rules to prevent Tenable from creating new CIs. By default, your CIs will not be automatically reclassified if a match is found in a different CI class. Read more about CI reclassification here. To change this behavior, modify the `x_tsirm_tio_cmdb.updateWithoutDowngrade` and `x_tsirm_tio_cmdb.updateWithoutSwitch` system properties.

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:

Ensure IRE rule changes are applied on the next import and clean the correlation data.

The following background scripts are examples that you can run to clean direct correlations between Tenable data, the CMDB, and IRE data. When you change the IRE rules to improve the match with third-party data to your existing ServiceNow CIs, you must apply the updated rules and clean up old relationships.

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

Import Operational Technology (OT) Devices

Note: You must have a license from ServiceNow to import OT devices from Tenable OT Security. Refer to the *OT Subscription Unit Overview* in the ServiceNow documentation and contact your ServiceNow account team for details.

Before you begin:

1. Submit a request to ServiceNow support to install the *com.snc.itom.license* plugin on your production instance. This allows ServiceNow to report on your OT assets.
2. Run the fix script included in Tenable assets to register Tenable as an asset source with ServiceNow.

To run the fix script for OT devices in the ServiceNow user interface:

1. In the **Filter navigator**, type *Fix Scripts*.
2. In the left-side navigation pane, click **Fix Scripts**.

   The page populates with available fix scripts.
3. In the search box, search by name for **Add Tenable.ot to ITOM License**.
4. In the search results, click **Add Tenable.ot to ITOM License**.
5. In the upper-right, click **Run Fix Script**.

   The fix script runs.

Configure Assets to Sync from ServiceNow to Tenable Security Center

You can configure CIs to Sync from ServiceNow to Tenable Security Center static IP list assets, or to DNS name list assets. For more information, see Tenable Security Center Assets documentation.

Note: Work with your ServiceNow administrator to perform the following task. Use the following information as a guideline. Your administrator can help with tuning the export to achieve your desired results.

To configure ServiceNow to Tenable Security Center:

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 Security Center**.

   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 4.
6. From the **Tenable Application** drop-down, select **Service Graph Connector for 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**.

Configure Assets to Sync from ServiceNow to Tenable Vulnerability Management

You can configure CIs to Sync from ServiceNow to Tenable Vulnerability Management.

Note: Work with your ServiceNow administrator to perform the following tasks. Use the information provided in the following process as a guideline. Your administrator can help with tuning the export to achieve your desired results.

Note: To sync assets from ServiceNow to Tenable Security Center, see 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**.

   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 **Service Graph Connector for Tenable for Assets**.
7. From the **Tenable Job Type** drop-down box, select the **Push Asset** job type.

   Note: If you are in a domain-separated environment, the Domain is set to the same value that is on the Connector record. If this is not correct, create a new Connector record in the correct Domain.
8. 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 export.
10. Configure the options for your export.

Option	Description
Last Run	The date and time that the import was last run.
Active	If selected, the scheduled job runs on the configured schedule. If Run Type = Periodically and Active = true, then an asset sync is automatically executed when you submit the import or export. By default, this setting is selected.
Schedule	
Edit Run Schedule	Select this box if you want to edit the Run Type and Repeat Interval / Time.
Run Type	The frequency that you want the import to run.
Repeat Interval / Time	The set time (hh/mm/ss) to run the import.
Conditions	
Configuration Item Source Table	The table to search to query the CIs you want exported to Tenable. By default, this is set to `cmdb_ci`
Conditions	Filter conditions for the CIs you want exported to Tenable. By default, this is set to `Any Computer CIs that have not already been imported into ServiceNow from Tenable`

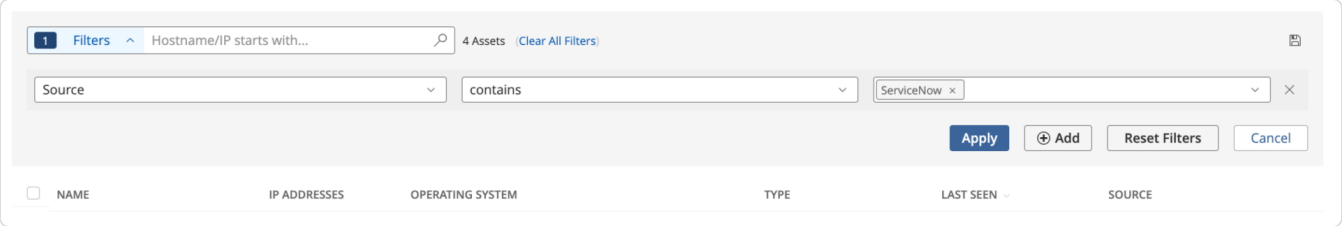
11. Click **Submit**.

Verification

1. Launch your Tenable user interface.
2. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.
3. In the left navigation plane, in the **Asset View** section, click **Assets**.

4. Filter your assets by **Source**contains**ServiceNow**.



The **ServiceNow** option only shows up in the filter box if the integration was successful.

For more information on filtering assets, see View Assets in the Tenable Vulnerability Management documentation.

VR Configuration and Schedule Import

This section describes how to configure Tenable OT Security for VR.

> **Note:** The Tenable OT Security for VR application supports only Tenable OT Security.

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 to complete the setup.
- Configure the Tenable Connector

  > **Note:** Completely configure and tune Service Graph Connector for Tenable for Assets to match Tenable Assets with ServiceNow CIs. If you do not do this first, issues may occur with VR.

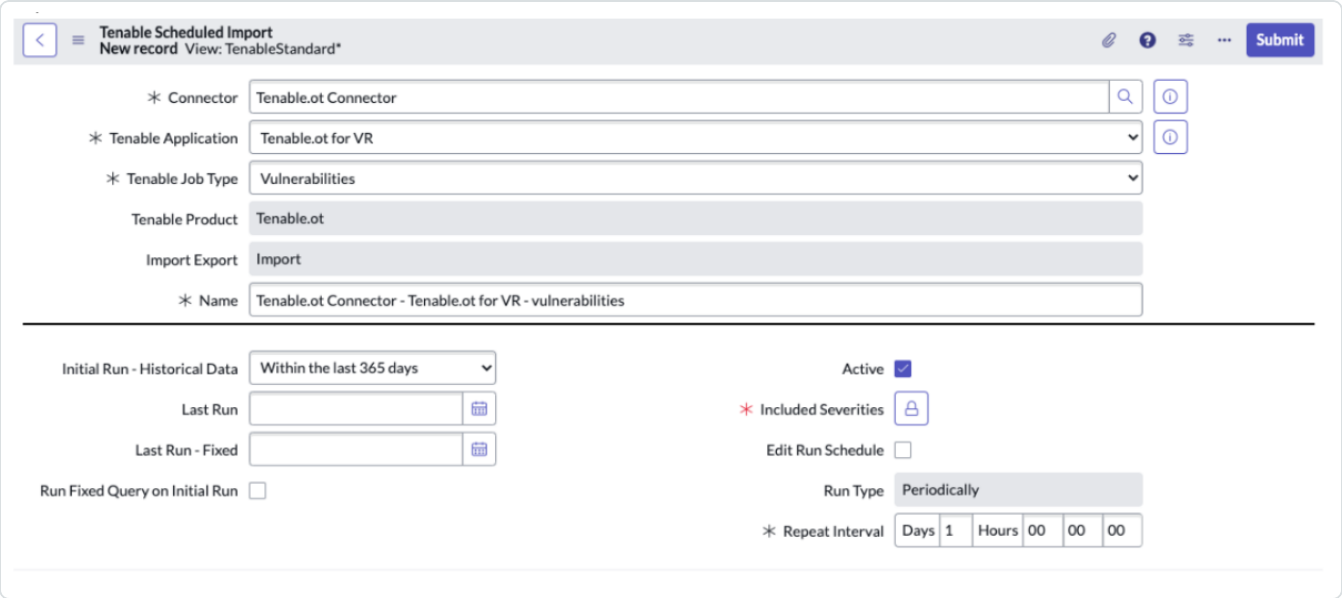
Configure the ServiceNow and Tenable OT Security for VR Connector

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.ot**.

   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 4.
6. From the **Tenable Application** drop-down box, select **Tenable.ot for Vulnerability Response**.



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

   Note: If you are in a domain-separated environment, the **Domain** is set to the same value that is on the **Connector** record. If this is not correct, create a new **Connector** record in the correct **Domain**.

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 Vulnerability Management) 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.

Option	Description
Initial Run Historical Data	Specifies how far back (in days) to import when run for the first time. For example, if you select the **Within 30 days** option, observed vulnerabilities within 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.
Last Run -Opene-	The date and time that the Open/Reopened import was last

d/Reopened	run.
Last run - Fixed	The date and time that the fixed import was last run.
Run Fixed Query on Initial Run	Pulls fixed vulnerabilities from the past on the first import. This allows for more complete reporting in ServiceNow for prior fixed vulnerabilities. By default, this setting is not selected.
Active	If selected, the scheduled job runs on the configured schedule. If `Run Type = Periodically and Active = true`, then an asset sync is automatically executed when you submit the import or export. By default, this setting is selected.
Included Severities	Specify the severities you want to be imported. By default, this is set to High, Critical
Schedule	
Edit Run Schedule	Select this box if you want to edit the Run Type and Repeat Interval / Time.
Run Type	The frequency that you want the import to run.
Repeat Interval / Time	The set time (hh/mm/ss) to run the import.

12. Click **Update**.

    By default, connector starts syncing vulnerabilities from Tenable to ServiceNow.

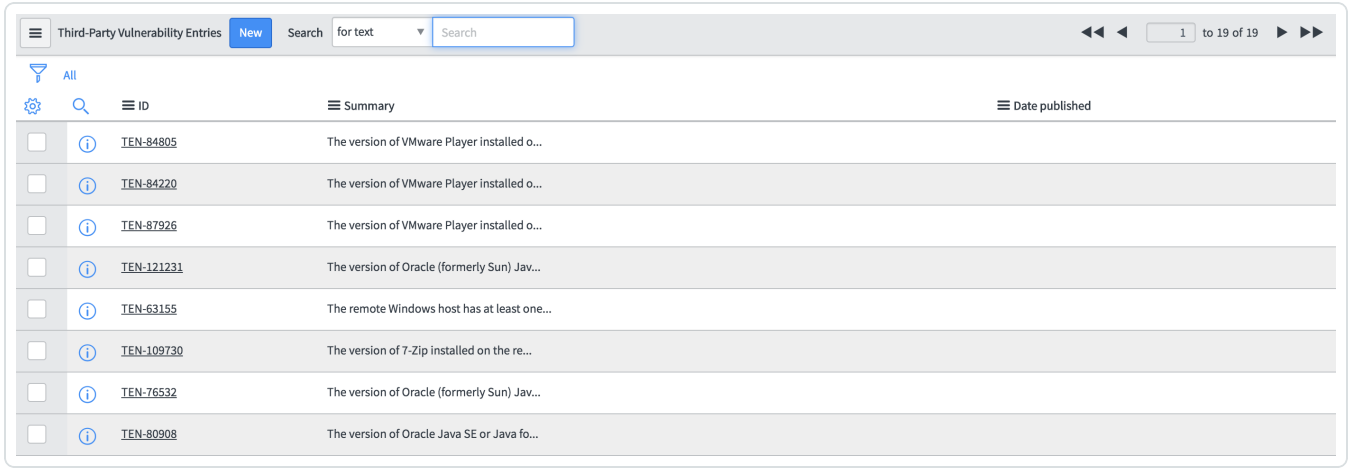
Third-Party Vulnerabilities

To view third-party vulnerabilities:

- Navigate to **Vulnerability Response** > **Libraries** > **Third-Party**.

  Vulnerabilities that include **TEN-** were imported from Tenable OT Security. 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.



Vulnerable Items (Linked Vulnerability and Configuration Items)

To view vulnerable items:

- Navigate to **Vulnerability Response** > **Vulnerable Items**.

  Vulnerabilities that include **TEN-** were imported from Tenable OT Security. Click a vulnerability to view the details.

  > **Note:** Text boxes are disabled for closed vulnerable items. 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 ServiceNow configuration only supports Tenable Security Center versions 5.7 and later.

The ITSM integration configuration allows ServiceNow to poll and retrieve vulnerability data from Tenable Vulnerability Management/Tenable Security Center.

Before you begin:

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

Note: Configure and tune Service Graph Connector for Tenable for Assets to match Tenable Assets with ServiceNow CIs. If you do not do this first, you may have issues with ITSM.

To set up the ITSM integration configuration, you must:

- Configure the Tenable Connector
- Create the ServiceNow and Tenable for ITSM Connector
- Create an Incident Rule

Create the ServiceNow and Tenable for ITSM Connector

1. Log in to ServiceNow.
2. In the left-hand menu, click **Tenable Connector**.
3. In the sub-menu, click **Connectors**.

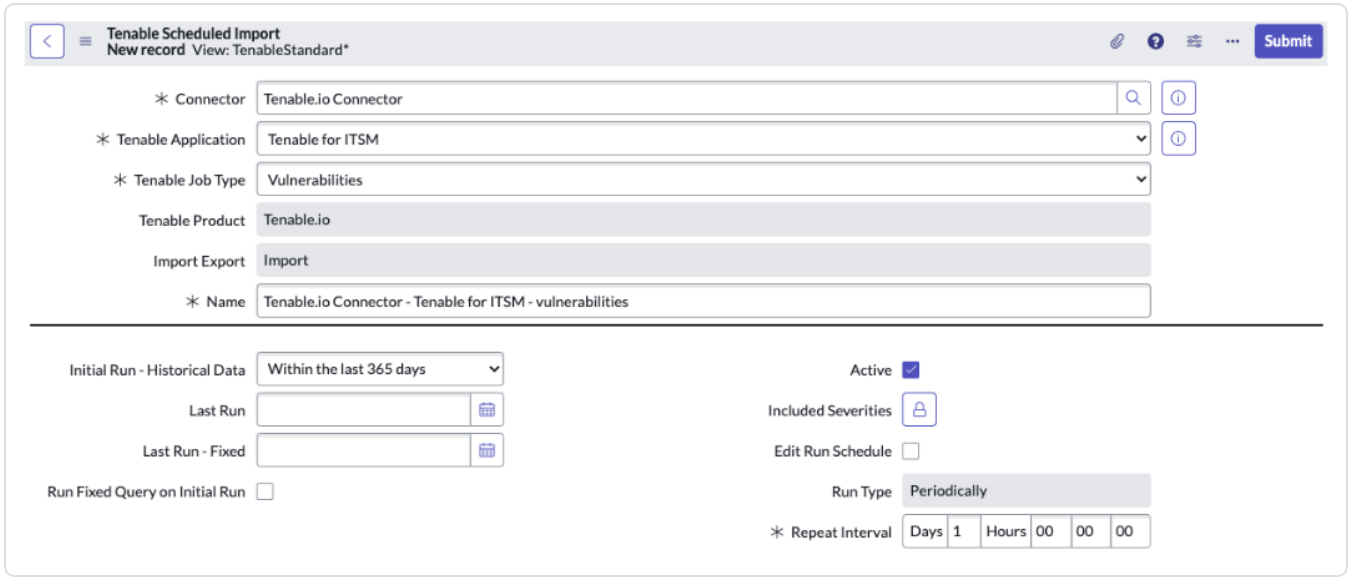
   The **Tenable Connectors** page appears.
4. Click the Tenable connector you want to use: **Tenable.io** or **Tenable Security Center**.

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

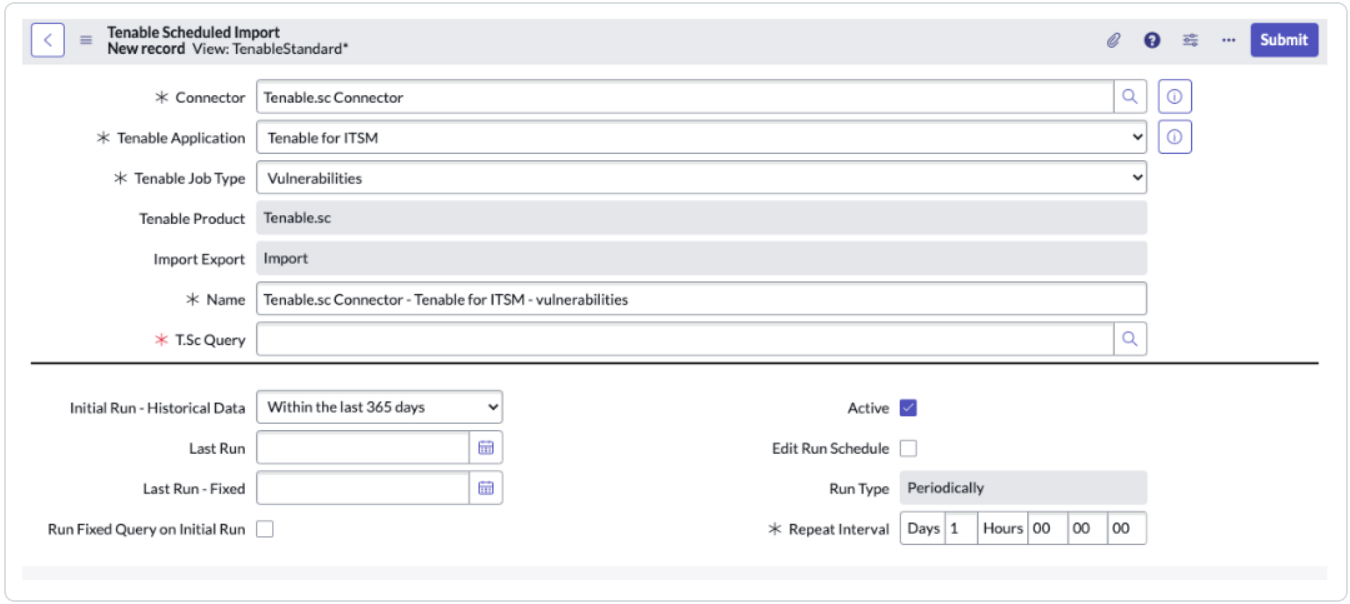
   The **Tenable Scheduled Import** page appears. By default, the **Tenable Product** and **Connector** fields populate with the Tenable application/connector you selected in step 4.

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

   Tenable Vulnerability Management



   Tenable Security Center



7. If you are in a domain-separated environment, the **Domain** is set to the same value that is on the **Connector** record. If this value is not correct, create a new connector record in the correct domain.

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

9. Configure the options for your import.

Option	Description
T.sc Query	(Only for Tenable Security Center) The Tenable Security Center query used for the import or export.
Initial Run - Historical Data	The amount of time (in days) of how far back you want to pull data.
Last Run	The date and time that the open/reopened import was last run.
Last Run - Fixed	The date and time that the fixed import was last run.
Run Fixed Query on Initial Run	Pulls fixed vulnerabilities on the first import. By default, this is set to deselected.
Active	If selected, an asset sync is automatically queued when you submit the import or export. Default setting: selected.
Included Severities	Specify the severities you want to be imported. By default, this is set to High, Critical
Schedule	
Edit Run Schedule	Select this to edit the Run Type and Repeat Interval / Time
Run Type	The frequency with which you want the import to run.
Repeat Interval / Time	The set time (hh/mm/ss) to run the import.

10. Click **Update**.

Create an Incident Rule

Create and enable Incident Rules so that the integration can 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. (Option 1) If you want to use scripting to create this rule, click the **Advanced** check box, and type the desired script. Refer to the default rule provided for an example script.

Incident rule field options

ServiceNow ITSM Vulnerability Import Set Field	Tenable Security Center Vulnerability Analysis Field	Tenable Vulnerability Management Vulnerability Export Field
u_acceptriskrulecomment	acceptRiskRuleComment	
u_acrscore	acrScore	
u_agent_uuid	uuid	asset.agent_uuid
u_asset_hostname	Script - dnsName OR ip*	asset.hostname
u_assetexposurescore	assetExposureScore	
u_bios_uuid		asset.bios_uuid
u_ci	CI SysID*	CI SysID*
u_connector	Connector SysID*	Connector SysID*
u_description	description	description
u_device_type		asset.device_type
u_first_found	firstSeen	first_found
u_first_found_date	firstSeen	first_found
u_fqdn	dnsName	asset.fqdn

u_hasbeenmitigated	hasBeenMitigated	
u_hostname	Script - dnsName OR ip*	
u_hostuniqueness	hostUniqueness	
u_hostuuid	hostUUID	
u_indexed		indexed
u_ip	ip	asset.ipv4
u_ips	ip	
u_job_type	“vuln_data”*	“vuln_data”*
u_keydrivers	keyDrivers	
u_last_fixed		last_fixed
u_last_found	lastSeen	last_found
u_last_found_date	lastSeen	last_found
u_mac_address	macAddress	asset.mac_address
u_netbios_name	netbiosName	asset.netbios_name
u_operating_system	operatingSystem	asset.operating_system
u_operatingsystem	operatingSystem	
u_output	pluginText	output
u_plugin_cve	cve	plugin.cve
u_plugin_description	description	plugin.description
u_plugin_family	family.name	plugin.family
u_plugin_family_type	family.type	
u_plugin_id	pluginID	plugin.id

u_plugin_modification_date	pluginModDate	plugin.modification_date
u_plugin_name	pluginName	plugin.name
u_plugin_publication_date	vulnPubDate	plugin.publication_date
u_plugin_solution	solution	plugin.solution
u_plugin_synopsis	synopsis	plugin.synopsis
u_pluginname	pluginName	
u_port		port
u_port_port	port	port.port
u_port_protocol	protocol	port.protocol
u_priority	Script - 1-4*	Script - 1-4*
u_product_type	“tsc”*	“tio”*
u_recastriskrulecomment	recastRiskRuleComment	
u_reopened	Script - true/false*	Script - true/false*
u_repository_data_format	repository.dataFormat	
u_repository_id	repository.id	
u_repository_name	repository.name	
u_risk_accepted	acceptRisk	
u_risk_recasted	recastRisk	
u_scan		scan
u_scan_completed_at		scan.completed_at
u_scan_started_at		scan.started_at

u_scan_uuid		scan.uuid
u_scunique	Calculated Uniqueness*	
u_severity	severity.name	severity
u_severity_default_id		severity_default_id
u_severity_id	severity.id	severity_id
u_severity_modification_type		severity_modification_type
u_source_name	“Tenable.sc”*	“Tenable.io”*
u_state	Script - OPEN/FIXED*	state
u_substate	Script*	Script*
u_tenable_plugin	Generated Plugin SysID*	Generated Plugin SysID*
u_uniqueness	uniqueness	
u_vpr_score	vprScore	vpr.score
u_vprcontext	vprContext	
u_xref	xref	

6. (Option 2) In the **Asset field** text box, select the appropriate asset field for the rule.
7. (Option 2) In the **Operator** text box, select the appropriate operator for the rule.
8. (Option 2) In the **Value** text box, type the value for the rule.
9. To reorder the incident rule, update the value in the **Order** text box. Incident rules run in ascending order (lowest to highest).

   If you are in a domain-separated environment, the incident rule is created in the current domain.
10. 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

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**, **Tenable Security Center**, or **Tenable.ot**.

   The **Tenable Connector** page appears.
5. In the **General Settings** section, you can view/edit:
   - Max ECC Wait Time (sec)
   - Request Timeout (sec)

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**, **Tenable Security Center**, or **Tenable.ot**.

   The **Tenable Connector** page appears.
5. In the **Asset Settings** section, you can view/edit:
   - CMDB Logging Level
   - CMDB Asset Chunk Size
   - CMDB Asset Import Thread Limit
   - CMDB Outbound map
   - CMDB Max Cumulative Log Entries
   - CMDB Max Cumulative Log Size
   - CMDB Max Job Log Age (days)
   - CMDB Push Asset Record Limit
6. In the left-hand menu, you can configure the following settings:
   - **Advanced**
     - **Default Outbound Map**: Defines the field map when using the Tenable Vulnerability Management Push Asset scheduled export job to send ServiceNow CI data to Tenable Vulnerability Management.

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.ot**.

   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 Vulnerability Asset Chunk Size
   - VR Max Cumulative Log Entries
   - VR Max Cumulative Log Size
   - VR Plugin Import Thread Limit
   - VR Vulnerability Import Thread Limit
6. In the left-hand menu, you can configure the following settings:
   - **Advanced**
     - **Transform Maps**: Defines how VR and Plugin data imports from Tenable are mapped to ServiceNow tables.

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.

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 Security Center**.

   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
   - ITSM Vulnerability Asset Chunk Size
   - ITSM Vulnerability Import Thread Limit
   - ITSM Age Out Period
   - ITSM Max Job Log Age (days)
6. In the left-hand menu, you can configure the following settings:
   - **Advanced**
     - **Transform Maps**: Defines how VR and Plugin data imports from Tenable are mapped to ServiceNow tables.

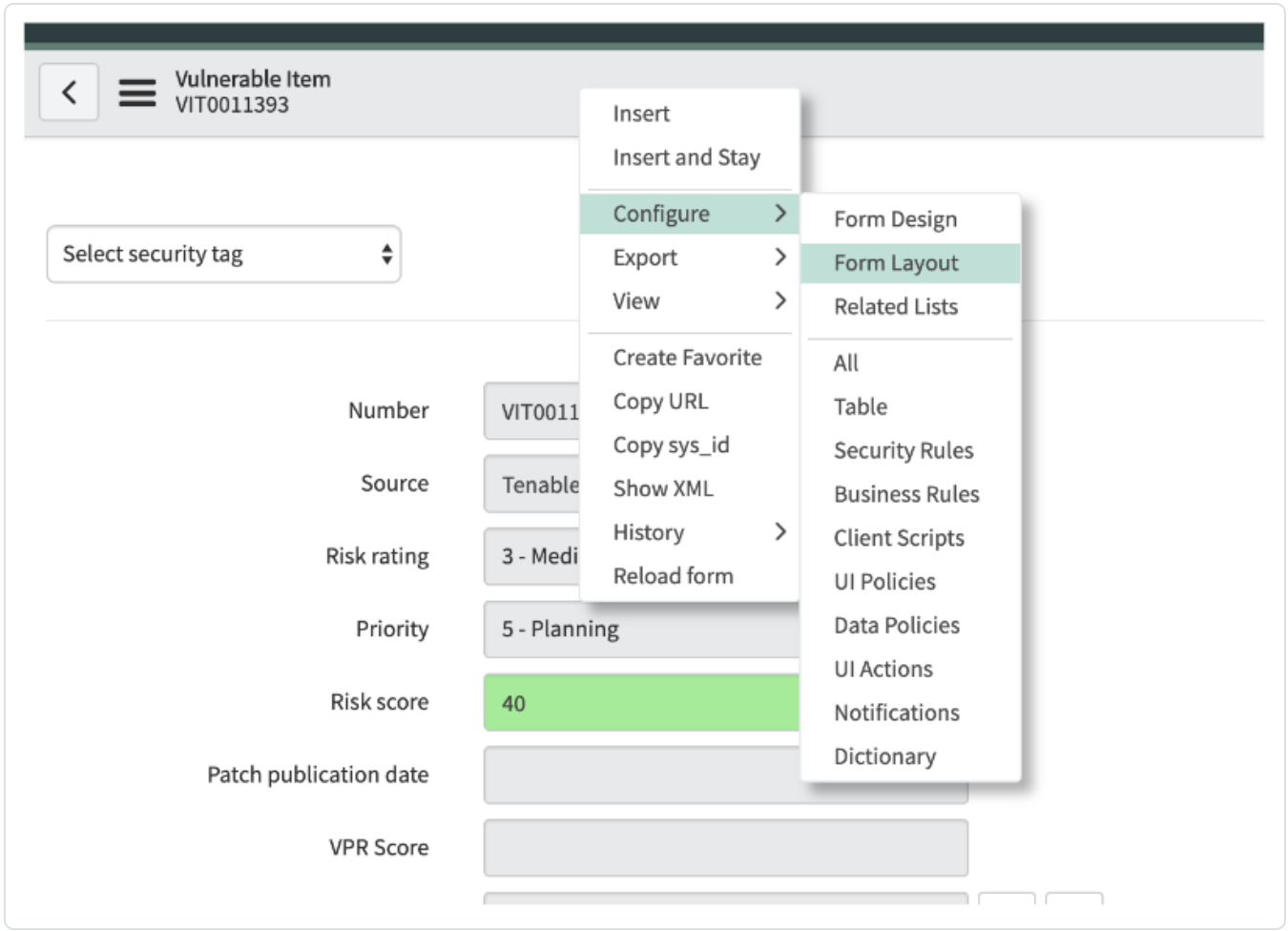
Caution: We do not support changes made to Transform Maps. If you want to customize your Transform Maps options, we recommend you contact your ServiceNow Administrator.

Add Fields to Tables

You can add more fields to your data tables in Service NOW to broaden the scope of information available. In the following example, the VPR Score and Patch publication date are added to the Vulnerability Items table. This can also be done on the Third-Party Table or any table that you choose.

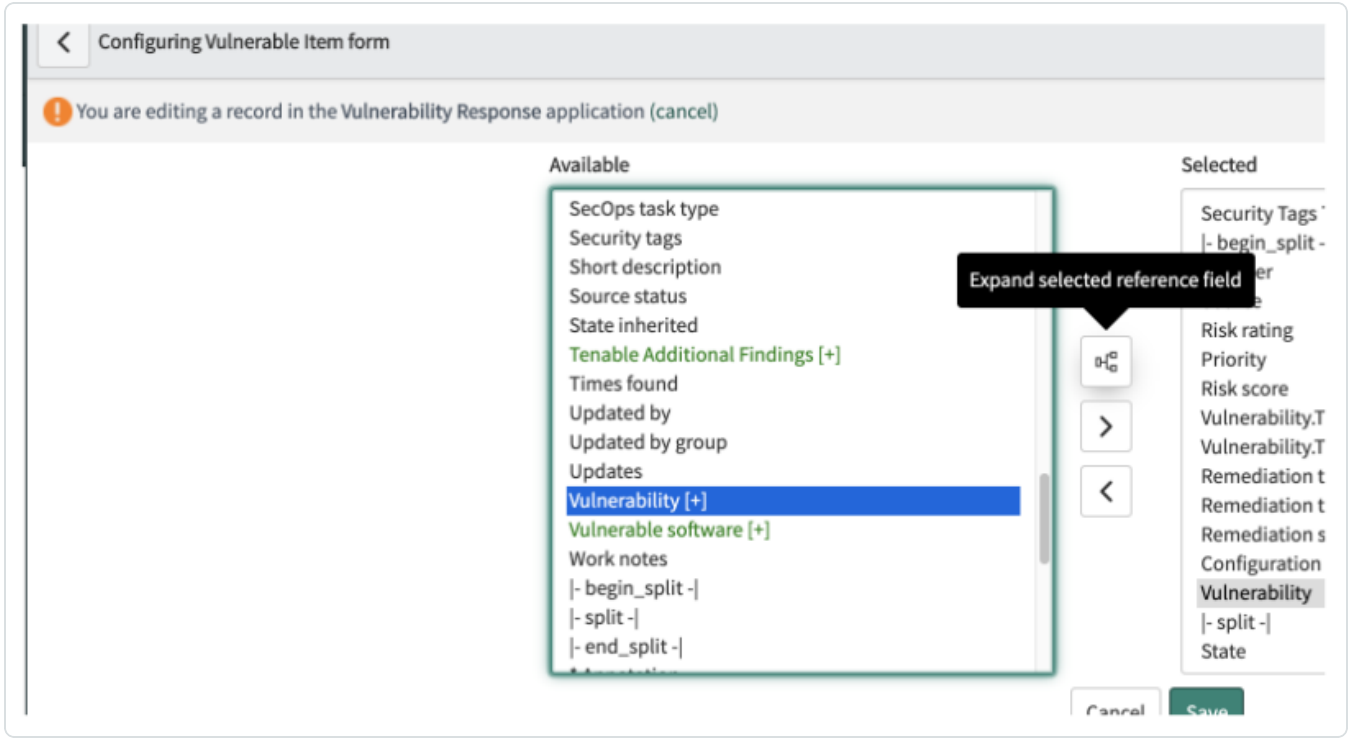
To add more fields to tables:

1. In your **Vulnerability Items** table, select a **Vulnerable Item** entry, right-click on the header and go to **Configure** > **Form Layout**.

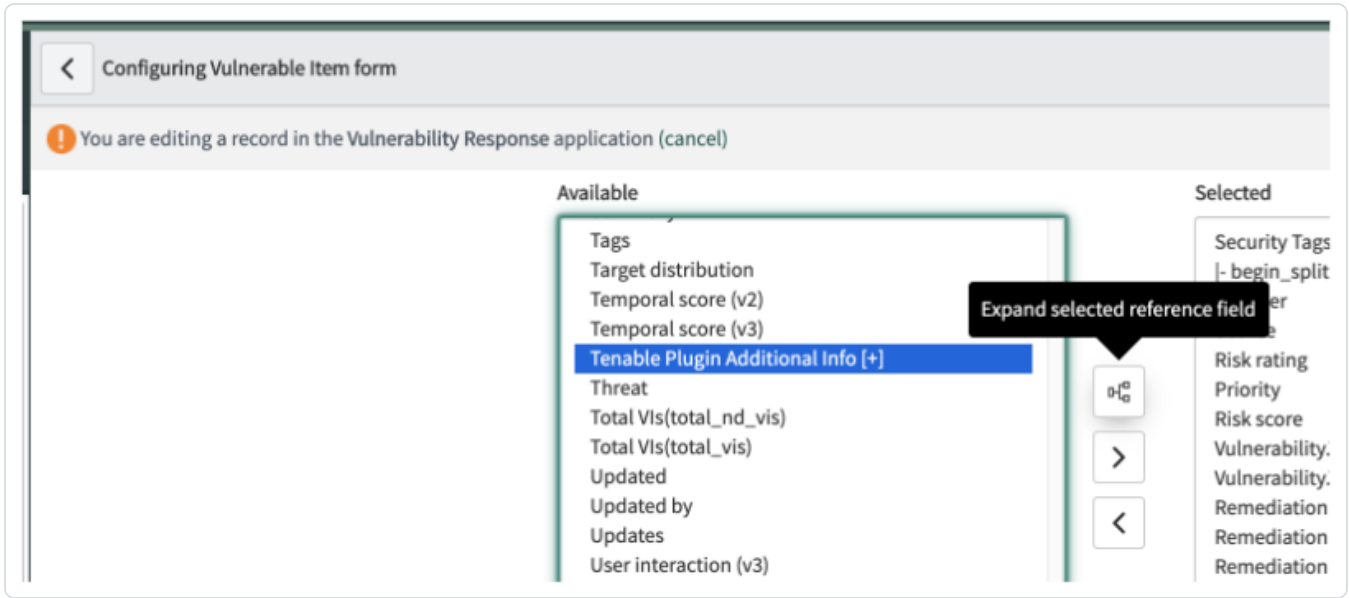


   The **Configuring Vulnerable item form** page appears.

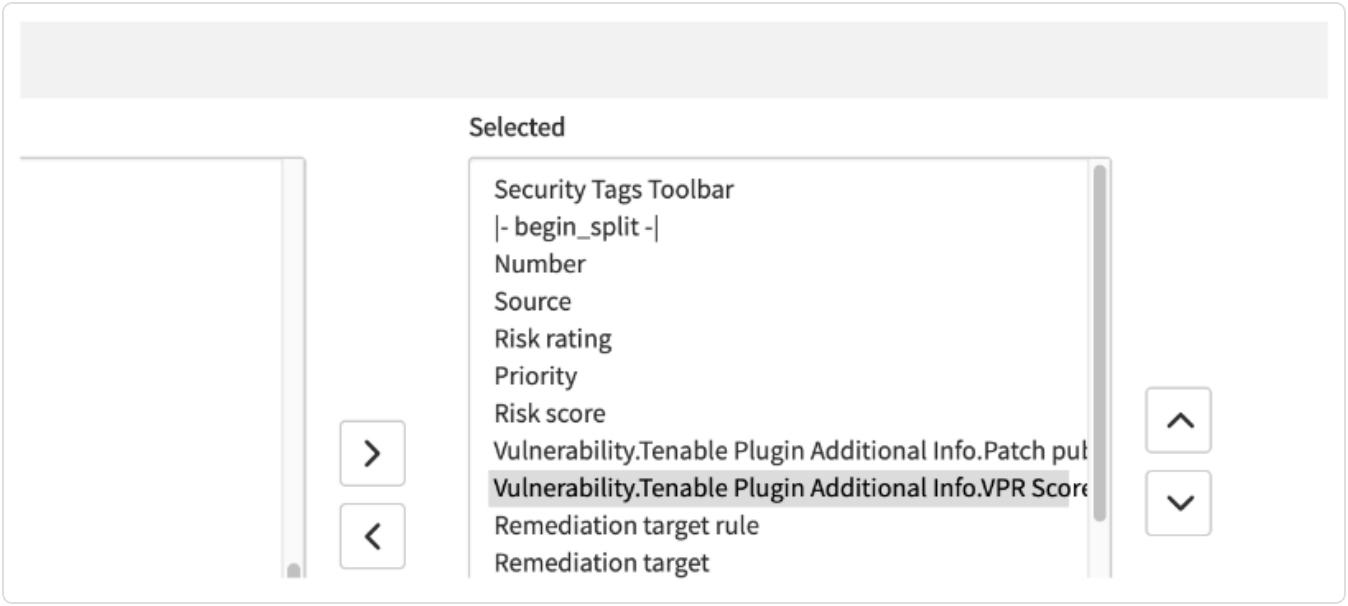
2. In the **Available** box, find **Vulnerability [+]** and expand it.



3. Find **Tenable Plugin Additional Info [+]** and expand it.



4. Select **Vulnerability.TenablePluginAdditionalInfo.VPR Score** and **Vulnerability.Tenable Plugin Additional Info.Patch publication date**, then move those over to the **Selected** box with the **>** button.


Selected
Security Tags Toolbar
|- begin_split -|
Number
Source
Risk rating
Priority
Risk score
Vulnerability.Tenable Plugin Additional Info.Patch pub
Vulnerability.Tenable Plugin Additional Info.VPR Score
Remediation target rule
Remediation target

Support

The Tenable for ServiceNow applications are highly customizable as every ServiceNow environment tends to be unique. 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. When the export job finishes, and ServiceNow begins receiving chunk data from Tenable, the status changes to **Receiving Chunk Data**.

   a. For each chunk of data queried from Tenable, a related Job Chunk record is created with a New status. The raw imported payload is attached as a .json file titled JOB000XXXX-native-0.json in the Job Chunk record.

   b. The raw data is then transformed into a usable format that can be ingested by ServiceNow. This transformed payload is then attached to the Job Chunk record as a .json file titled JOB000XXXX-full-x.json.

   c. The Job Chunk record status is then set to Data Received.

   d. This process repeats until there are no more data chunks to pull from Tenable.

c. Once all the chunk data is retrieved, the Job status changes to Importing. Each Job Chunk import into ServiceNow one at a time. As it is importing, the Job Chunk status is set to Importing and then is set to Complete or Error once finished.

d. Once all of the Job Chunks have completed importing, 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.

---

*The value is generated from scripted logic and not directly from the Tenable Export field.