Tenable and ServiceNow Integration Guide

Last Revised: December 17, 2025

Copyright © 2025 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Table of Contents

Welcome to Tenable for ServiceNow

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

The Service Graph Connector for Tenable 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 Security Center and Tenable Vulnerability Management as assets.

The Tenable OT Security for VR 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.

Tenable Assets Service Graph Connector (ServiceNow App) or ServiceNow Connector for Tenable Exposure Management?

This document covers the standard Tenable integration with ServiceNow. Tenable also now offers the ServiceNow Connector for use with Tenable Exposure Management.

The ServiceNow App allows you to sync assets bi-directionally between Tenable Vulnerability Management (TVM) and Tenable Security Center (TSC). This allows you to create and update configuration items (CIs) in ServiceNow as well as create/update assets (TVM) or asset lists (TSC). Due to limitations in the TVM asset import API, when pushing to TVM the app only passes network details and `servicenow sys_id`.

The ServiceNow Connector for Tenable Exposure Management leverages the entire Tenable Exposure Management data model while the Tenable-provided ServiceNow Integration utilizes the TVM data model. This provides a greater ability to map ServiceNow fields to Tenable Exposure Management fields, and you can also use Tenable Exposure Management custom fields and tags.

The ServiceNow Connector for Tenable Exposure Management is not bi-directional like the ServiceNow App. While the Tenable Exposure Management connector is certainly more robust, setup configuration is much more involved than the ServiceNow App with regard to importing assets to Tenable.

For more information, refer to ServiceNow Connector and Connectors.

Application Dependencies

- Platform compatibility:
  - Tenable Vulnerability Management, Tenable Security Center 5.7+, or Tenable OT Security
  - ServiceNow Yokohama, Zurich
- Plugins required:
  - ITOM Discovery License - 1.0.0
  - ITOM Licensing - 1.0.0
  - CMDB CI Class Models - 1.76.0
  - Integration Commons for CMDB - 2.20.0
  - SGC Central - 2.2.0
  - (Optional - Required when using Domain Separation) Domain Separation
  - (Optional - Required for VR) ServiceNow Vulnerability Response - 23.0.0
  - (Optional - Required for ITSM) Incident - 1.0.0

Application Installation

Users with the System administrator(admin) role can install the application from the ServiceNow Store.

Required User Role: Administrator

To install the application from the ServiceNow Store:

1. Go to https://store.servicenow.com
2. Search for the “Service Graph Connector for Tenable” app in the search tab.
3. Click **Service Graph Connector for Tenable**.
4. Click the **Get** button.
5. Enter the ServiceNow ID credentials of your ServiceNow account.

   A success message appears.
6. Open the instance and navigate to **System Applications** > **All Available Applications** > **All**.
7. Find the application using the filter criteria and search bar.
8. Next to the application listing, click **Install**.

Post-Installation

You can create cross scope privilege records for Tenable for ITSM and “Tenable.ot for VR” apps respectively if they are installed.

Steps to install the application from the ServiceNow Store:

1. Click the globe icon to set the **Application Scope** to **Service Graph Connector for Tenable**.
2. Click the search filter and type "sys_scope_privilege.list."
3. Click **Enter**.
4. Click the **New** button in the top-right corner.

   The **Cross scope privilege New record** form appears.

5. Create six records using values from the following table.

Sr no.	Target Scope	Target Name	Target Type	Operation	Status
1	Tenable for ITSM	x_tsirm_tio_itsm_ vulnerability	Table	Read	Allowed
2	Tenable for ITSM	TenableITSMHelper	Script Include	Execute API	Allowed
3	Tenable for ITSM	TenableITSM	Script Include	Execute API	Allowed
4	Tenable for ITSM	TenableITSMScheduleHelper	Script Include	Execute API	Allowed
5	Tenable.ot for VR	TenableVRScheduleHelper	Script Include	Execute API	Allowed
6	Tenable.ot for VR	TenableVRHelper	Script Include	Execute API	Allowed

6. After creating the records, go to the **Schedule Import** record and click **Execute**.

Upgrade from 5.x Version Apps

If you use the Service Graph Connector for Tenable for Assets and Tenable Connector apps follow the steps outlined here for upgrades to avoid any unexpected issues in the future. This process is not intended for any other applications

Required User Role: Administrator

To upgrade the application from the ServiceNow:

Upgrade the previous Tenable for ITSM and Tenable.ot for VR

1. Log in to the instance and navigate to **System Applications** > **All Available Applications** > **All**.

2. Find the application with the filter criteria and search bar.

3. Next to the application listing, select the version to update.

4. Click **Update**.

Uninstall the previous Tenable Connector and Service Graph Connector for Tenable for Assets app from your instance

1. Navigate to **System Applications** > **All Available Applications** > **All**.

2. A list of applications installed in the instance is displayed.

3. Locate **Tenable Connector and Service Graph Connector for Tenable for Assets**, select it, and under the related links, click **Uninstall**.

Update records created from the previous Tenable apps

1. Navigate to **System definition** > **Scripts - Background**.

2. Run the following scripts:

   - Run the following script in **global** scope.

```
var cmdbGr = new GlideRecord("cmdb_ci");
cmdbGr.addQuery("discovery_source", "SG-TenableForAssets");
cmdbGr.query();
while(cmdbGr.next()) {
      cmdbGr.discovery_source = "SG-Tenable";
      cmdbGr.update();
}
var vrItemsGr = new GlideRecord("sn_vul_vulnerable_item");
vrItemsGr.addQuery("source", "Tenable.ot");
vrItemsGr.query();
while(vrItemsGr.next()) {
      vrItemsGr.source = "Tenable OT Security";
      vrItemsGr.update();
}
var thirdPartyVrGr = new GlideRecord("sn_vul_third_party_entry");
thirdPartyVrGr.addQuery("source", "Tenable.ot");
thirdPartyVrGr.query();
while(thirdPartyVrGr.next()) {
      thirdPartyVrGr.source = "Tenable OT Security";
      thirdPartyVrGr.update();
}
```

Note: This script is to clean the cmdb_ci, vulnerable item and vulnerability entry table records specific to Tenable.

- Run the folllowing script in **x_tsirm_tio_itsm** scope.

```
var itsmVulTvmGr = new GlideRecord("x_tsirm_tio_itsm_vulnerability");
itsmVulTvmGr.addQuery("source", "Tenable.io");
itsmVulTvmGr.query();
while(itsmVulTvmGr.next()) {
      itsmVulTvmGr.source = "Tenable Vulnerability Management";
      itsmVulTvmGr.update();
}
var itsmVulTscGr = new GlideRecord("x_tsirm_tio_itsm_vulnerability");
itsmVulTscGr.addQuery("source", "Tenable.sc");
itsmVulTscGr.query();
while(itsmVulTscGr.next()) {
      itsmVulTscGr.source = "Tenable Security Center";
      itsmVulTscGr.update();
}

var itsmPluginTvmGr = new GlideRecord("x_tsirm_tio_itsm_plugin");
itsmPluginTvmGr.addQuery("source", "Tenable.io");
itsmPluginTvmGr.query();
while(itsmPluginTvmGr.next()) {
      itsmPluginTvmGr.source = "Tenable Vulnerability Management";
      itsmPluginTvmGr.update();
}
var itsmPluginTscGr = new GlideRecord("x_tsirm_tio_itsm_plugin");
itsmPluginTscGr.addQuery("source", "Tenable.sc");
itsmPluginTscGr.query();
while(itsmPluginTscGr.next()) {
      itsmPluginTscGr.source = "Tenable Security Center";
      itsmPluginTscGr.update();
}
```

Note: This script is to clean the **Tenable Vulnerability and Tenable Plugin** table.

- Run the folllowing script in **x_tsirm_tio_vr** scope.

```
var vrAdditionalFindingsGr = new GlideRecord("x_tsirm_tio_vr_ve_info");
vrAdditionalFindingsGr.addQuery("source", "Tenable.ot");
vrAdditionalFindingsGr.query();
while(vrAdditionalFindingsGr.next()) {
      vrAdditionalFindingsGr.source = "Tenable OT Security";
      vrAdditionalFindingsGr.update();
}
```

Note: This script is to clean the **Tenable Plugin Additional Info** table.

User Setup

You can assign users with role privileges according to your needs. Roles are specified according to domain separated instances and non-domain separated instances.

> **Note:** The **x_tsirm_tio_now.import_set_admin** role is used to access import set tables across all the tenable apps. Tenable **does NOT recommend** to give this role to any user.

User Permissions For Non-Domain Separated Instances

User	Role	Permission	Description
System Administrator	admin	Installation of the integration application plugins User Creation Application Log Create the Connection Alias Create the connector Configuration Configure Scheduled Job Resources Process Monitor Support	This user-role is the admin of the ServiceNow Instance and has privileges to perform all the integration-specific actions.
Tenable Application Admin	canvas_user cmdb_inst_admin connection_admin x_tsirm_tio_itsm.admin x_tsirm_tio_now.admin x_tsirm_tio_vr.admin	Create the connector Configuration Configure Scheduled Job Resources Process Monitor Support	This user-role is the admin of the application and is allowed to create the connector, update the configuration, and configure the scheduled job.

Tenable Application User	canvas_user cmdb_inst_admin x_tsirm_tio_itsm.user x_tsirm_tio_now.user x_tsirm_tio_vr.user	Read access of configuration Read access to Connectors, scheduled jobs Support	This user-role is limited to read-only configurations. These users are not able to create or update any configurations.

User Permissions For Domain Separated Instances

User	Role	Permission	Description
System Administrator	admin x_tsirm_tio_now.domain_separation_admin	Installation of the integration application plugins User Creation Application Log Create the Connection Alias Create the connector Configuration Configure Scheduled Job Resources Process Monitor Support	This user-role is the admin of the ServiceNow Instance and has privileges to perform all the integration-specific actions.
Tenable Application Admin	canvas_user cmdb_inst_admin connection_admin x_tsirm_tio_itsm.admin x_tsirm_tio_now.domain_separation_admin x_tsirm_tio_vr.admin	Create the connector Configuration Configure Scheduled Job Resources Process Monitor Support	This user-role is the admin of the application and is allowed to create the connector, update the configuration, and configure the

			scheduled job.
Tenable Application User	canvas_user cmdb_inst_admin x_tsirm_tio_itsm.user x_tsirm_tio_now.user x_tsirm_tio_vr.user	Read access of configuration Read access to Connectors, scheduled jobs Support	This user-role is limited to read-only configurations. These users are not able to create or update any configurations.

Create a User

You can assign create the various Tenable user roles in the ServiceNow platform.

Required User Role: Administrator

User Permissions For Non-Domain Separated Instances

Username (example)	Role
admin	canvas_user cmdb_inst_admin connection_admin x_tsirm_tio_itsm.admin x_tsirm_tio_now.domain_separation_admin x_tsirm_tio_vr.admin

To create a Tenable user and assign the role to it:

1. Navigate to **Organization** > **Users**.
2. Click the **Users** module.

   The **Users** list appears.
3. Click **New**.

   A **New User** form appears.
4. Fill in the form.

   Note: The values for User ID title, and email address shown in the following table are example values.

Field	Description
User ID	The unique user ID for the role in your ServiceNow Platform instance. (For example, "tenable_admin")
First Name	The first name of this user.

Last Name	The last name of this user.
Title	Job title, or role, of this user. (For example, "Tenable admin")
Password	The unique password created for this role.
Email	The unique email address for this user.

5. Click **Submit**.

   > **Note:** Once the **New User** form is submitted, you can assign the role.

6. In the **Users** list in the **User ID** column, click the name of the new user you created.

   The new user record appears and the **Set Password** user interface is visible in the form view of the record.

7. Click the **Set Password** user interface action.

   A new pop-up appears.

8. Click **Generate**.

   > **Note:** This generates a unique password for the created user that must be changed upon first login.

9. Copy and safely store the generated password.
10. Close the pop-up.
11. In the **Users** list in the **User ID** column, click the name of the new user you created.
12. In the Roles section, and click **Edit**.
13. Add the roles in the **Collection** field of the **Edit Member** form.
14. In the **Collection** column, select roles mentioned in the User Permissions For Domain Separated Instances table and move them to the **Roles List**.
15. Click **Save**.

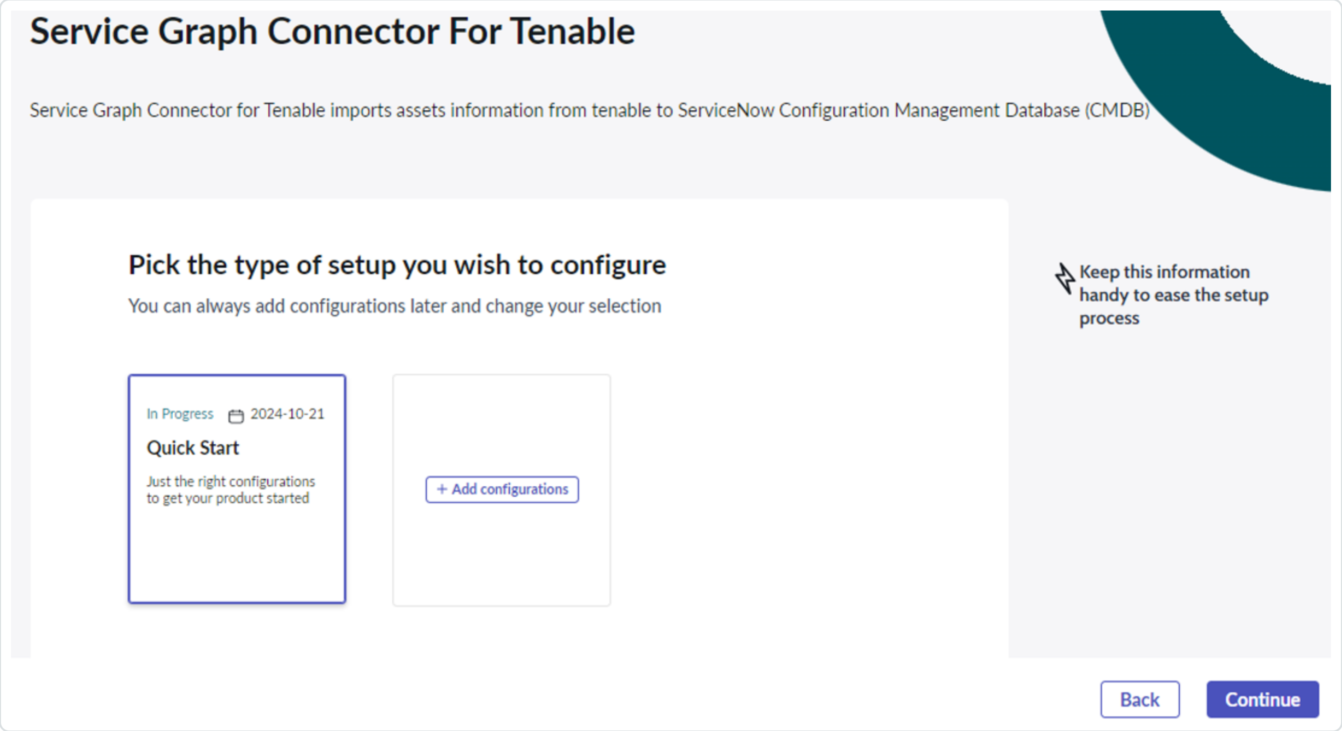
Create a Connection Alias

You can create a connection alias with a guided setup.

Required User Role: Administrator

To create a connection alias:

1. Log in to your ServiceNow instance.
2. Navigate to **Tenable Connector for Assets** > **Guided Setup**.
3. Select the setup type.



Service Graph Connector For Tenable

Service Graph Connector for Tenable imports assets information from tenable to ServiceNow Configuration Management Database (CMDB)

Pick the type of setup you wish to configure

You can always add configurations later and change your selection

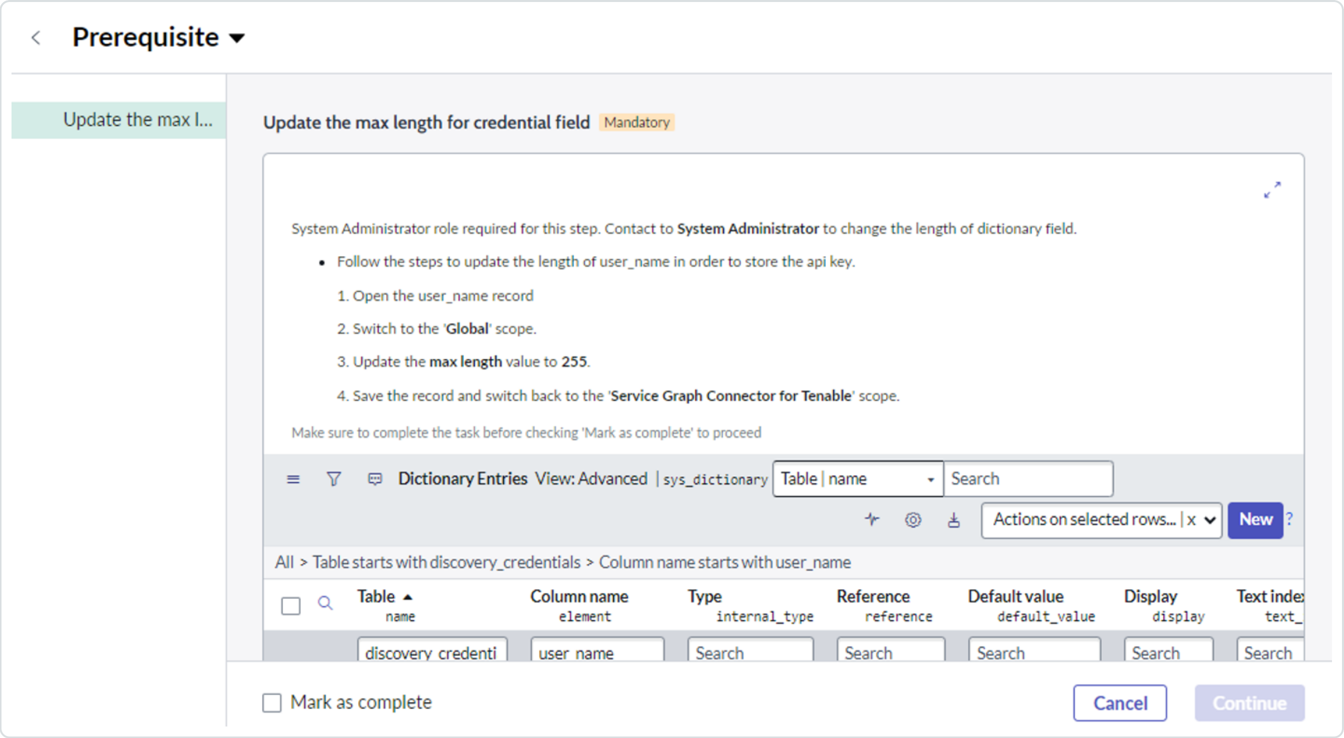
In Progress 2024-10-21

Quick Start

Just the right configurations to get your product started

Keep this information handy to ease the setup process

4. Click **Continue**.
5. In the **Prerequisite** page, select the **Update the max length of credential field** tab and follow the steps in the user interface.



Update the max length for credential field Mandatory

System Administrator role required for this step. Contact to **System Administrator** to change the length of dictionary field.

- Follow the steps to update the length of user_name in order to store the api key.

  1. Open the user_name record
  2. Switch to the '**Global**' scope.
  3. Update the **max length** value to **255**.
  4. Save the record and switch back to the '**Service Graph Connector for Tenable**' scope.

Make sure to complete the task before checking 'Mark as complete' to proceed

Dictionary Entries View: Advanced | sys_dictionary Table | name Search

Actions on selected rows... | x New

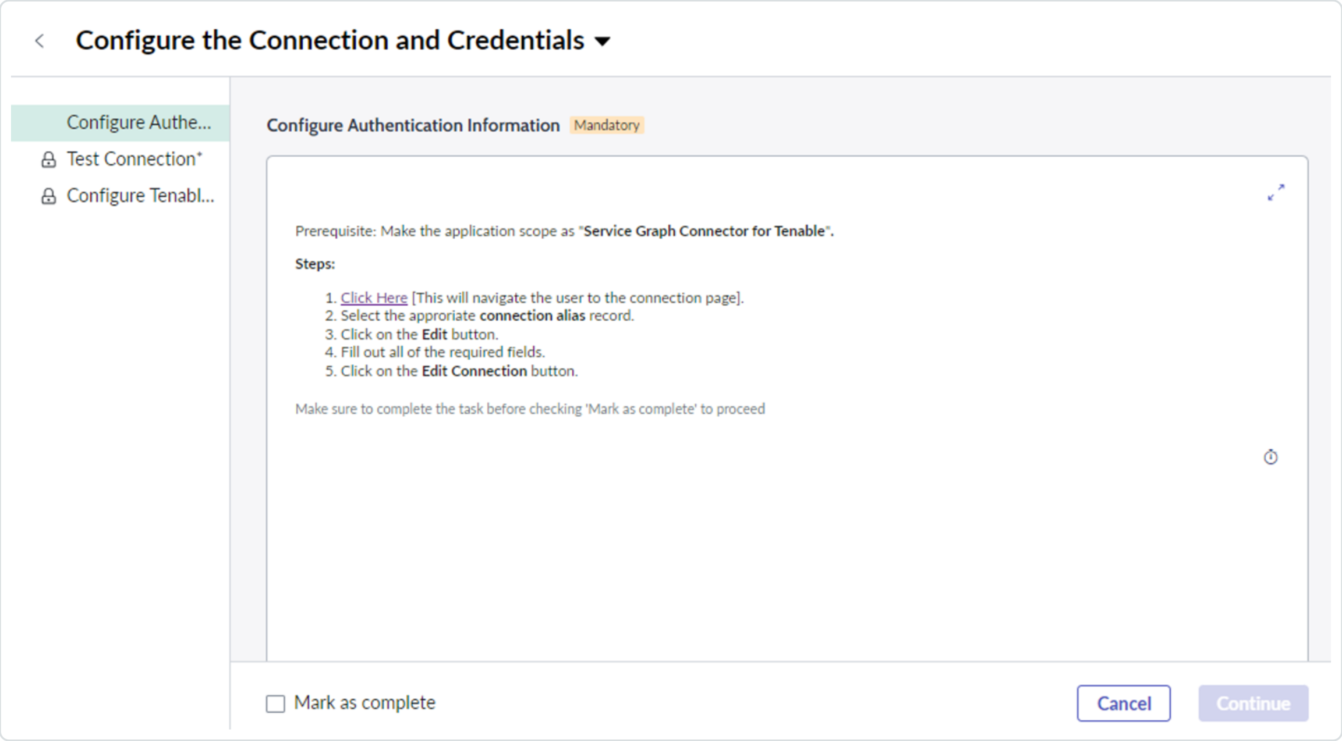
All > Table starts with discovery_credentials > Column name starts with user_name

Table ▲ name	Column name element	Type internal_type	Reference reference	Default value default_value	Display display	Text inde text_
discovery_credenti	user_name	Search	Search	Search	Search	Search

6. Check the **Mark as Complete** checkbox.

7. Click **Continue**.

8. Select the **Configure Authentication Information** tab and follow the steps in the user interface.



Configure the Connection and Credentials
Configure Authe...
Test Connection*
Configure Tenabl...
Configure Authentication Information
Mandatory

Prerequisite: Make the application scope as "**Service Graph Connector for Tenable**".

Steps:

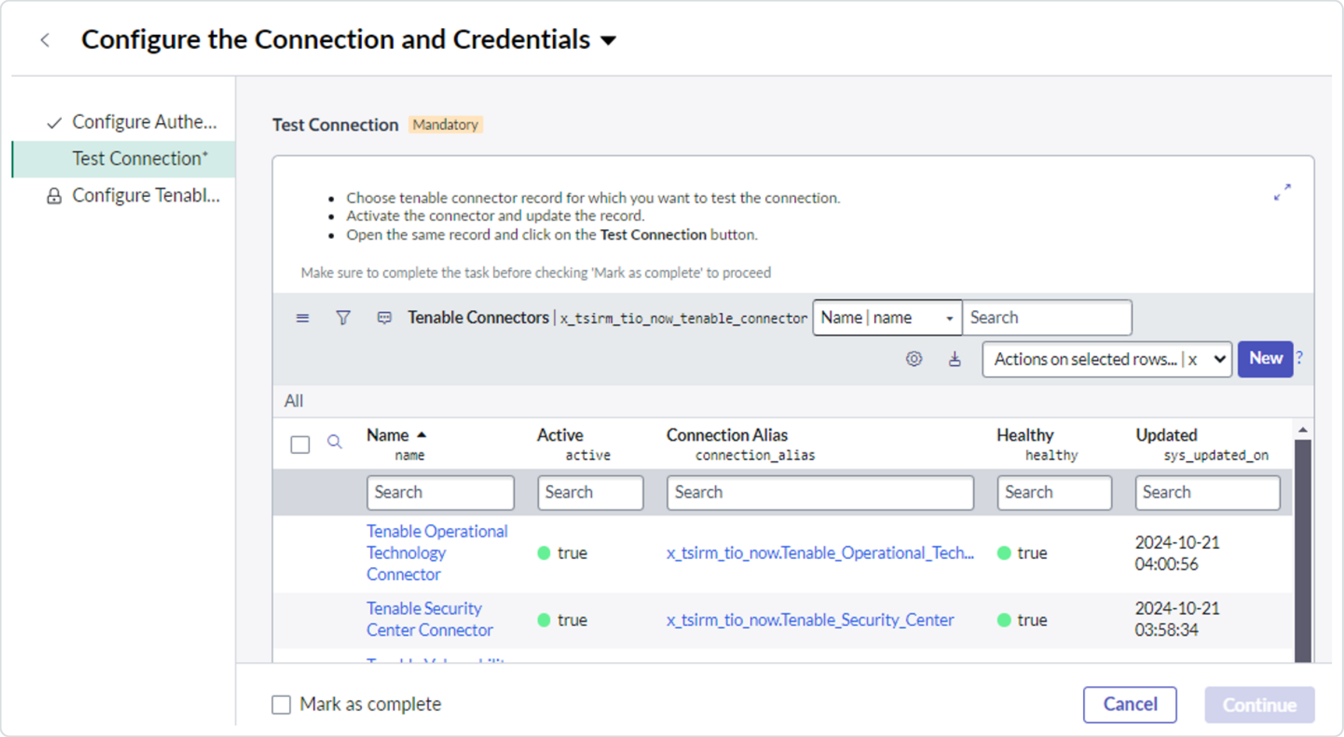
1. Click Here [This will navigate the user to the connection page].
2. Select the approriate **connection alias** record.
3. Click on the **Edit** button.
4. Fill out all of the required fields.
5. Click on the **Edit Connection** button.

Make sure to complete the task before checking 'Mark as complete' to proceed

9. Check the **Mark as Complete** checkbox.

10. Click **Continue**.

11. Select the **Test Connection** tab and follow the steps in the user interface.



Configure the Connection and Credentials

- ✓ Configure Authe...
- Test Connection*
- Configure Tenabl...

Test Connection Mandatory

- Choose tenable connector record for which you want to test the connection.
- Activate the connector and update the record.
- Open the same record and click on the **Test Connection** button.

Make sure to complete the task before checking 'Mark as complete' to proceed

Tenable Connectors | x_tsirm_tio_now_tenable_connector — Name | name — Search

Actions on selected rows... | x — New

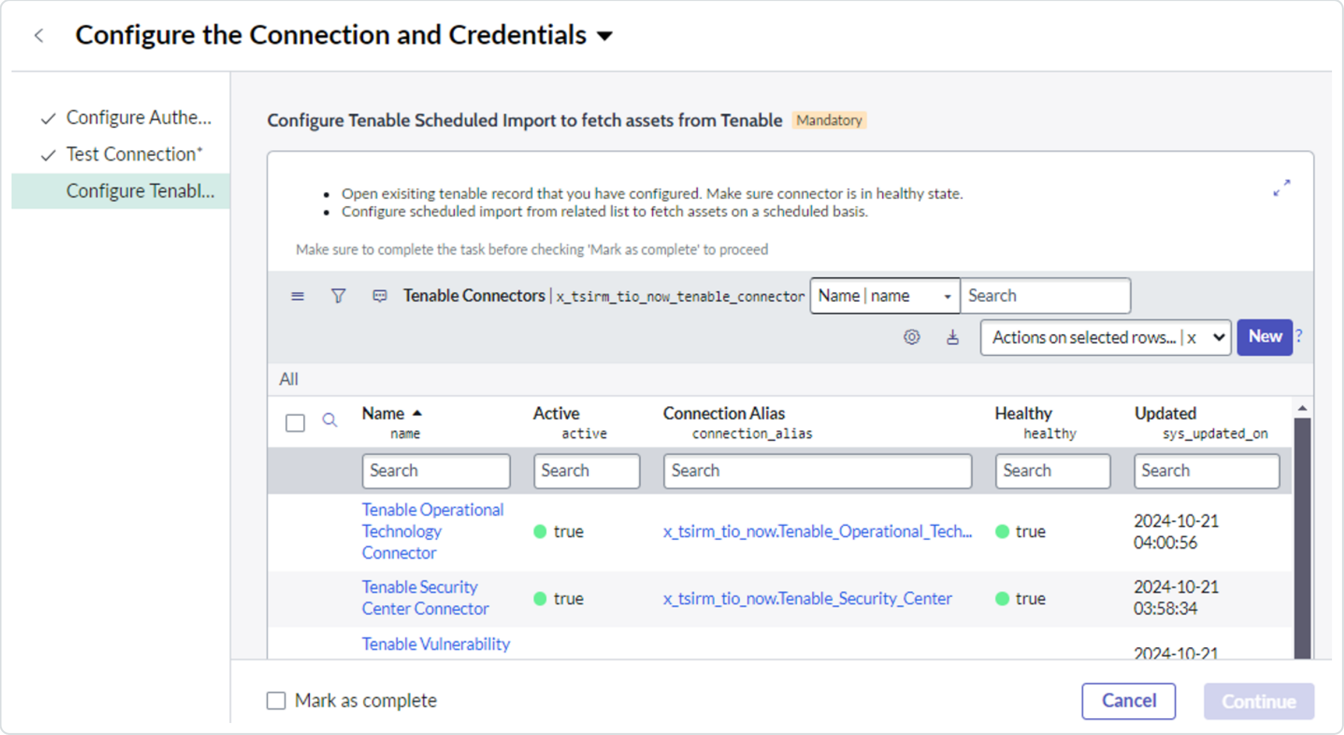
All

Name name	Active active	Connection Alias connection_alias	Healthy healthy	Updated sys_updated_on
Search	Search	Search	Search	Search
Tenable Operational Technology Connector	● true	x_tsirm_tio_now.Tenable_Operational_Tech...	● true	2024-10-21 04:00:56
Tenable Security Center Connector	● true	x_tsirm_tio_now.Tenable_Security_Center	● true	2024-10-21 03:58:34

□ Mark as complete

Cancel Continue

12. To fetch assets from Tenable, select the **Configure Tenable Schedule Import** tab and follow the steps in the user interface.



Configure the Connection and Credentials

- ✓ Configure Authe...
- ✓ Test Connection*
- Configure Tenabl...

Configure Tenable Scheduled Import to fetch assets from Tenable Mandatory

- Open exisiting tenable record that you have configured. Make sure connector is in healthy state.
- Configure scheduled import from related list to fetch assets on a scheduled basis.

Make sure to complete the task before checking 'Mark as complete' to proceed

Tenable Connectors | x_tsirm_tio_now_tenable_connector — Name | name — Search

Actions on selected rows... | x — New

All

Name name	Active active	Connection Alias connection_alias	Healthy healthy	Updated sys_updated_on
Search	Search	Search	Search	Search
Tenable Operational Technology Connector	● true	x_tsirm_tio_now.Tenable_Operational_Tech...	● true	2024-10-21 04:00:56
Tenable Security Center Connector	● true	x_tsirm_tio_now.Tenable_Security_Center	● true	2024-10-21 03:58:34
Tenable Vulnerability				2024-10-21

□ Mark as complete

Cancel Continue

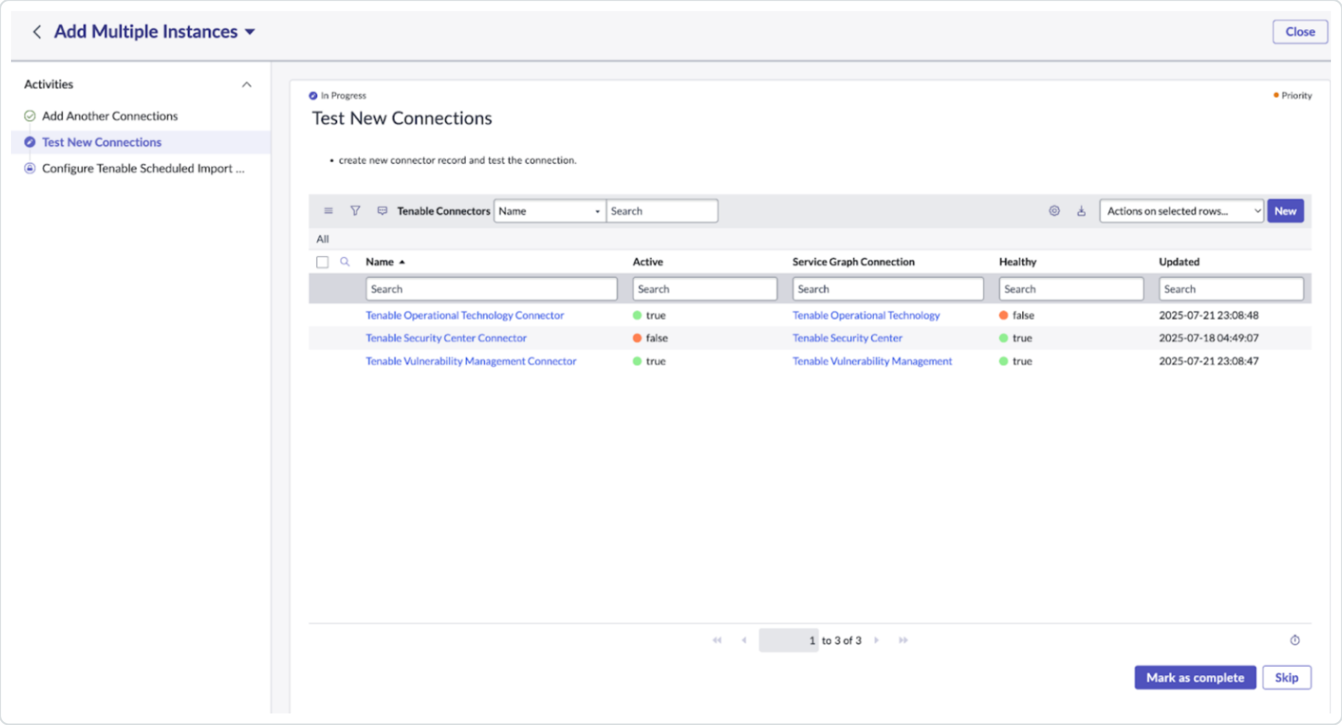
13. Check the **Mark as Complete** checkbox.

14. Click **Continue**.

Add Multiple Instances (Optional)

1. Navigate to **Tenable Connector for Assets** > **Add Multiple Instances**

2. Select the **Add Another Connections** tab and follow the steps in the user interface.



Test New Connections

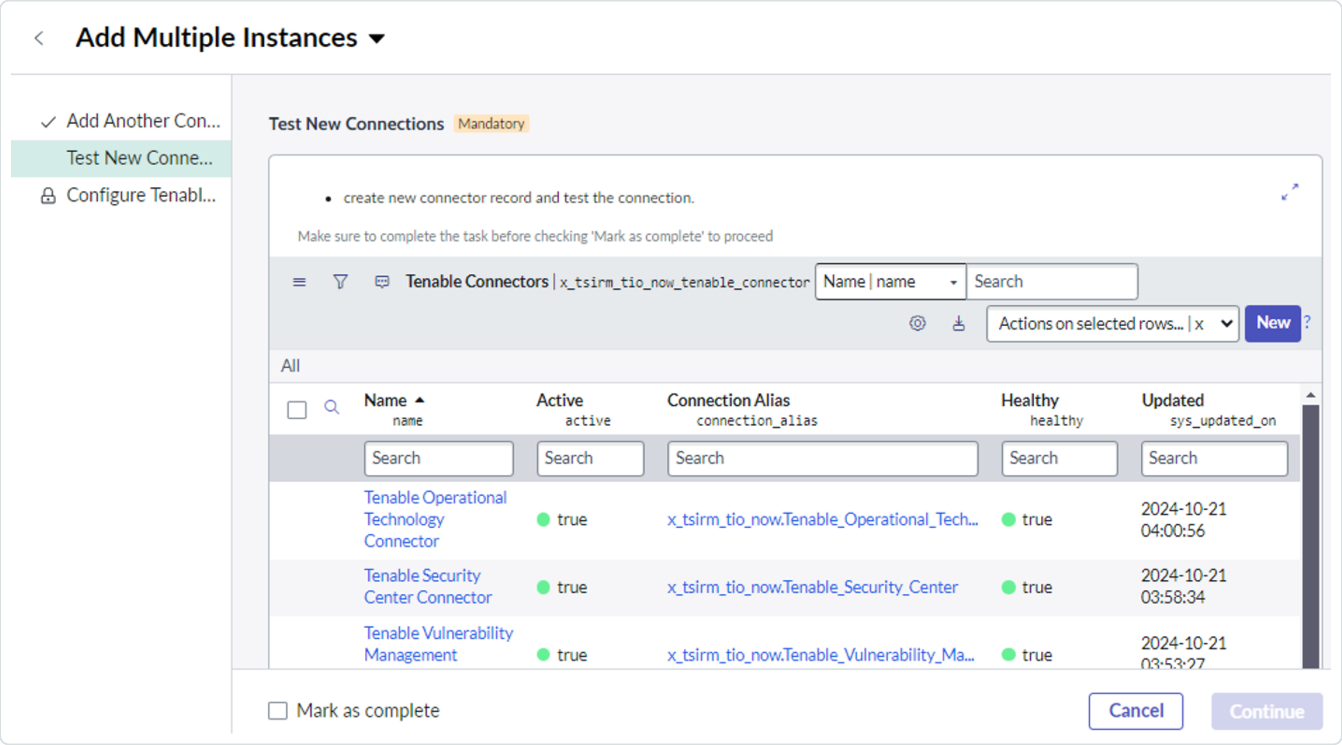
- create new connector record and test the connection.

Name ▲	Active	Service Graph Connection	Healthy	Updated
Tenable Operational Technology Connector	● true	Tenable Operational Technology	● false	2025-07-21 23:08:48
Tenable Security Center Connector	● false	Tenable Security Center	● true	2025-07-18 04:49:07
Tenable Vulnerability Management Connector	● true	Tenable Vulnerability Management	● true	2025-07-21 23:08:47

3. Check the **Mark as Complete** checkbox.

4. Click **Continue**.

5. Select the **Test New Connections** tab and follow the steps in the user interface.



Add Multiple Instances

Test New Connections Mandatory

- create new connector record and test the connection.

Make sure to complete the task before checking 'Mark as complete' to proceed

Tenable Connectors | x_tsirm_tio_now_tenable_connector

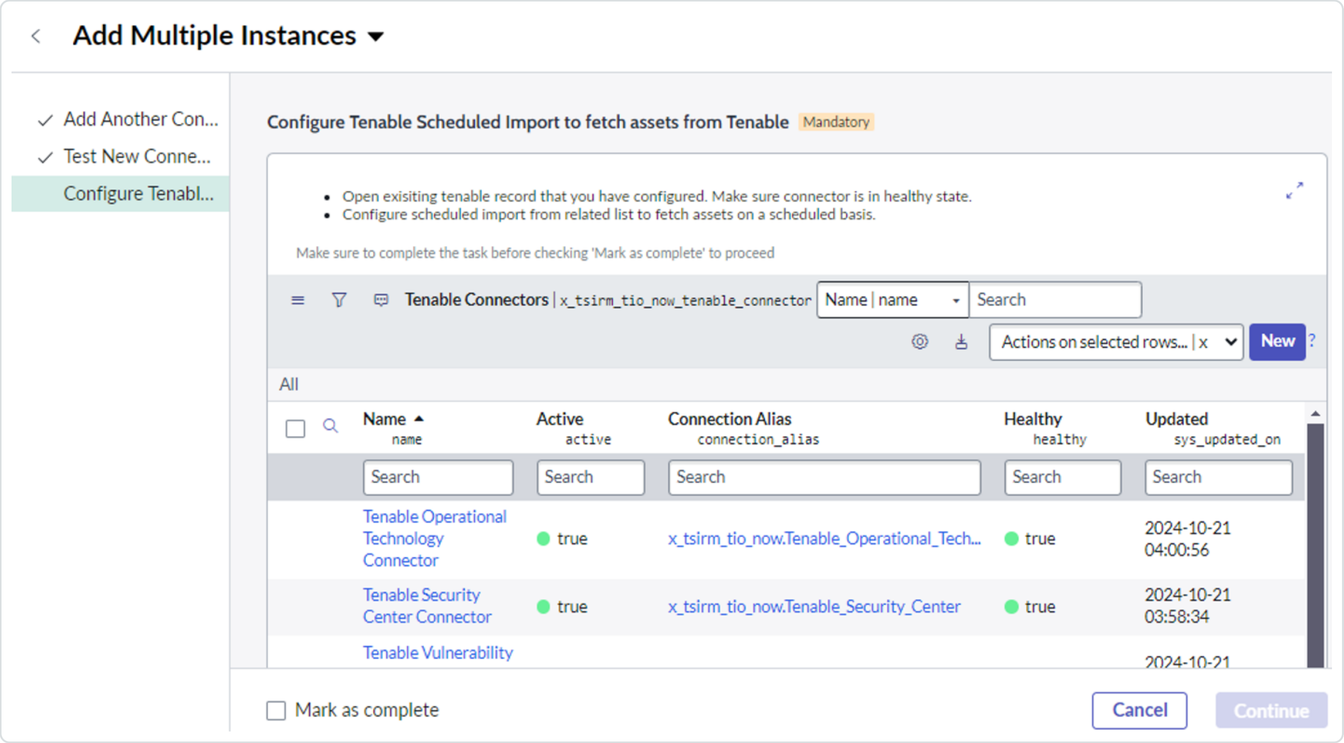
Name	Active	Connection Alias	Healthy	Updated
name	active	connection_alias	healthy	sys_updated_on
Tenable Operational Technology Connector	● true	x_tsirm_tio_now.Tenable_Operational_Tech...	● true	2024-10-21 04:00:56
Tenable Security Center Connector	● true	x_tsirm_tio_now.Tenable_Security_Center	● true	2024-10-21 03:58:34
Tenable Vulnerability Management	● true	x_tsirm_tio_now.Tenable_Vulnerability_Ma...	● true	2024-10-21 03:53:27

□ Mark as complete

6. Check the **Mark as Complete** checkbox.

7. Click **Continue**.

8. To fetch assets from Tenable, select the **Configure Tenable Schedule Import** tab and follow the steps in the user interface.



Add Multiple Instances

✓ Add Another Con...
✓ Test New Conne...
Configure Tenabl...

Configure Tenable Scheduled Import to fetch assets from Tenable Mandatory

- Open exisiting tenable record that you have configured. Make sure connector is in healthy state.
- Configure scheduled import from related list to fetch assets on a scheduled basis.

Make sure to complete the task before checking 'Mark as complete' to proceed

Tenable Connectors | x_tsirm_tio_now_tenable_connector Name | name Search

Actions on selected rows... | x New

All

□	Name ▲ name	Active active	Connection Alias connection_alias	Healthy healthy	Updated sys_updated_on
	Search	Search	Search	Search	Search
	Tenable Operational Technology Connector	● true	x_tsirm_tio_now.Tenable_Operational_Tech...	● true	2024-10-21 04:00:56
	Tenable Security Center Connector	● true	x_tsirm_tio_now.Tenable_Security_Center	● true	2024-10-21 03:58:34
	Tenable Vulnerability				2024-10-21

□ Mark as complete

Cancel Continue

9. Check the **Mark as Complete** checkbox.

10. Click **Continue**.

Map Custom Aliases to the Connector (Optional)

> **Caution:** When you create a new alias for your API keys, you may miss the step of mapping this alias to the **Connector**. This results in the connector defaulting to the wrong alias, causing connection failures and an "Unhealthy" connector status. The procedure to correct this scenario is in the following subsection.

If you have created a new **Connection & Credential Alias** (instead of using the default), you must manually map it to the **Connector**.

To map your custom alias to the connector:

1. Navigate to **Connectors**.

2. Select the relevant Tenable connector.

3. Locate the **Service Graph Connection** field.

4. Click the **lookup** icon.

5. Select your newly created **Connection Alias**.

6. Click **Update**.

   The changes are saved.

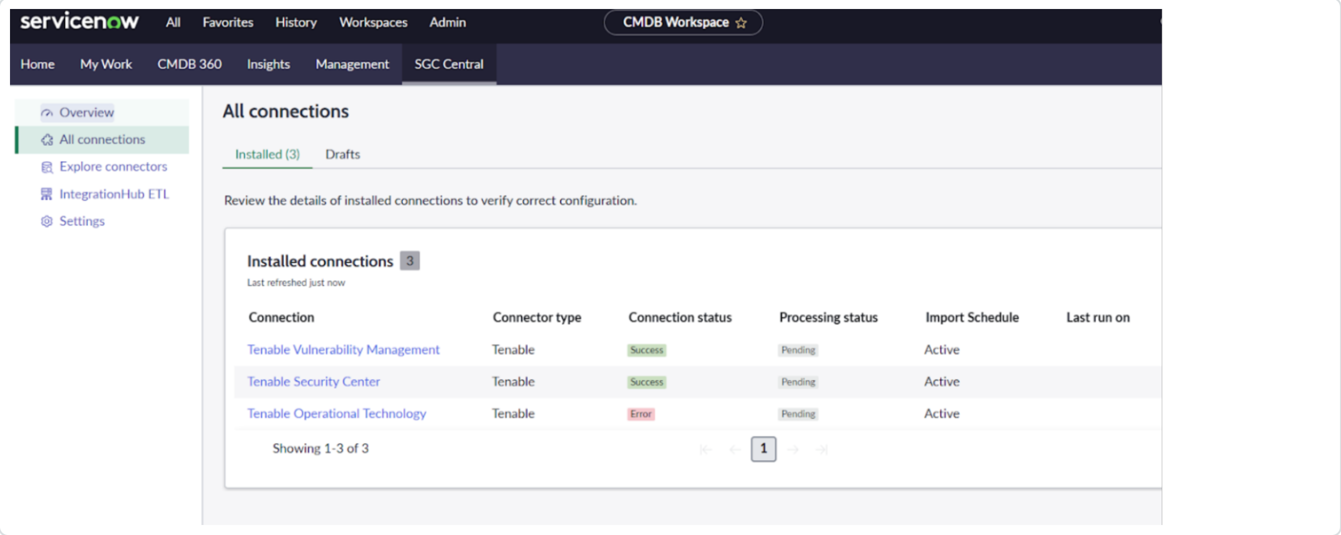
SGC Central Guided Setup

You can create a connection alias with a guided setup.

Required User Role: Administrator

To configure default connections

1. Navigate to **Workspaces** > **CMDB Workspace** > **SGC Central**.



All connections

Installed (3) Drafts

Review the details of installed connections to verify correct configuration.

Installed connections 3

Last refreshed just now

Connection	Connector type	Connection status	Processing status	Import Schedule	Last run on
Tenable Vulnerability Management	Tenable	Success	Pending	Active	
Tenable Security Center	Tenable	Success	Pending	Active	
Tenable Operational Technology	Tenable	Error	Pending	Active	

Showing 1-3 of 3

2. Click **All Connections**.

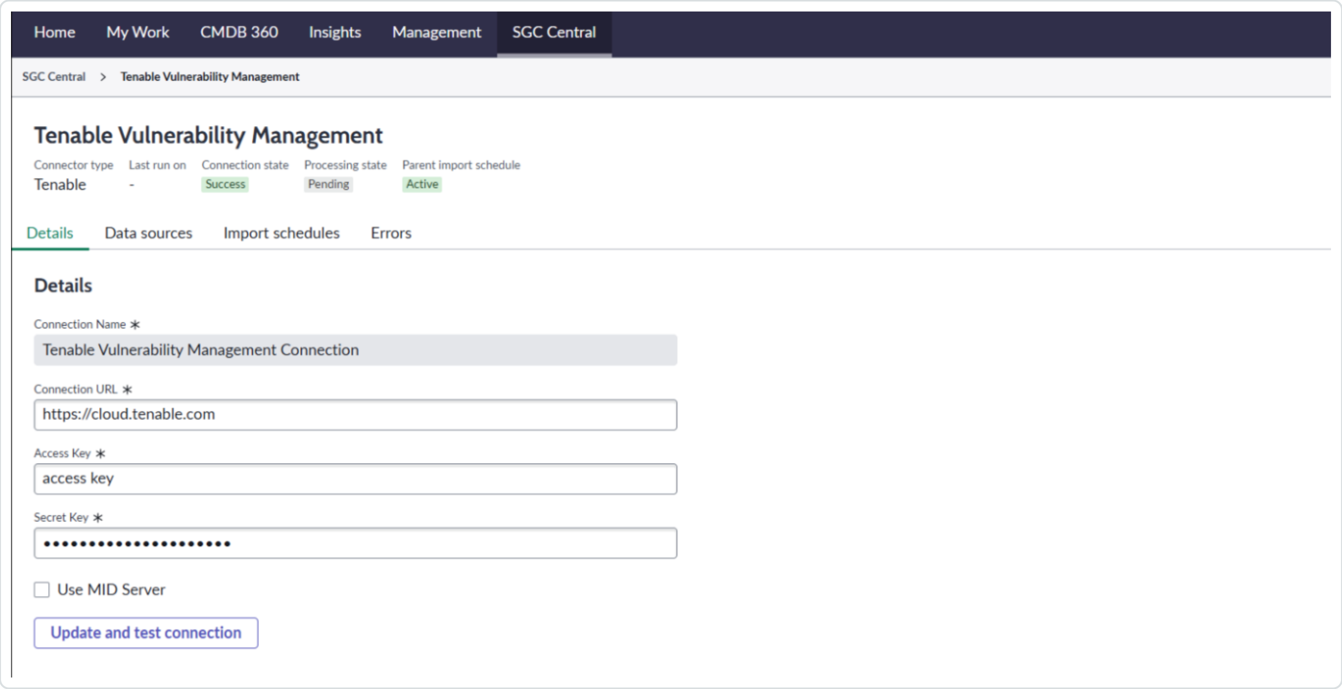
   View the installed connections list here.

3. Update the existing record.

   > **Note:** If the existing setup is in-progress, click the **Drafts** tab, resume your setup of "Tenable," and follow the same steps for configuring multi-instance as shown in the following multi-instance setup section.

4. Click any of the connections..

5. Provide the URL, access key, and secret key.



Tenable Vulnerability Management

Connector type	Last run on	Connection state	Processing state	Parent import schedule
Tenable	-	Success	Pending	Active

Details

Connection Name *: Tenable Vulnerability Management Connection

Connection URL *: https://cloud.tenable.com

Access Key *: access key

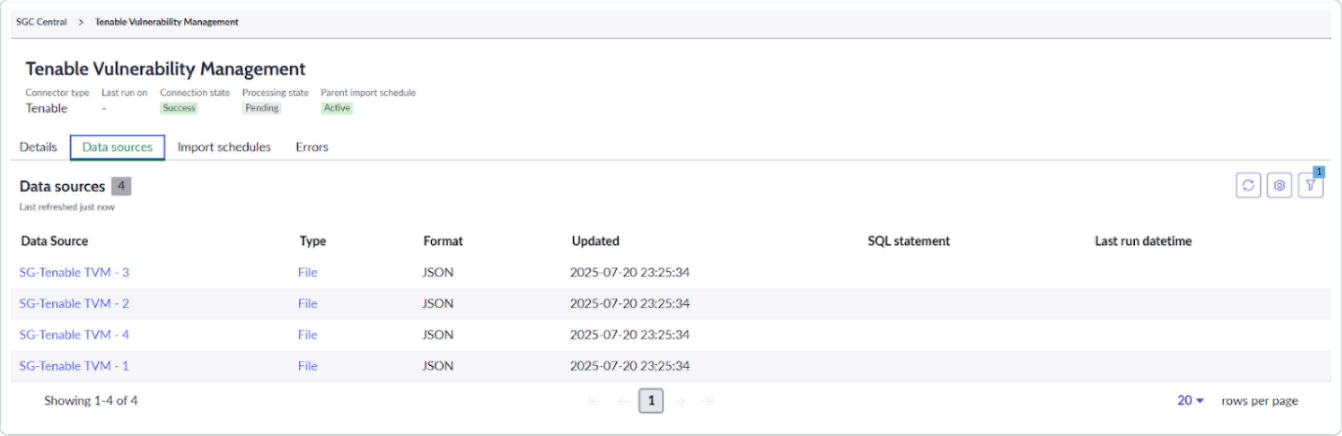
Secret Key *: ••••••••••••••••••••

□ Use MID Server

6. Click **Update and test connection**

   Once the connection test is completed, a **Connection verified** success message appears.

7. View the details of data sources by clicking the **Data sources** tab.



Tenable Vulnerability Management

Connector type	Last run on	Connection state	Processing state	Parent import schedule
Tenable	-	Success	Pending	Active

Data sources 4

Last refreshed just now

Data Source	Type	Format	Updated	SQL statement	Last run datetime
SG-Tenable TVM - 3	File	JSON	2025-07-20 23:25:34		
SG-Tenable TVM - 2	File	JSON	2025-07-20 23:25:34		
SG-Tenable TVM - 4	File	JSON	2025-07-20 23:25:34		
SG-Tenable TVM - 1	File	JSON	2025-07-20 23:25:34		

Showing 1-4 of 4

8. To execute the scheduler, click the **Import Schedules** tab.

Multi-Instance:

1. Navigate to **All Connections**.
2. Click **Create connection**.

3. Select **Tenable**.

4. Click **Create connection**.

> **Note:** As mentioned in the steps, perform the Prerequisite step of updating the max length of the credential field.(If already updated then Click on “Mark as Complete”).

5. Select the **connection alias**.

6. Click **Continue**.

7. Provide the connection name, URL, and tokens.

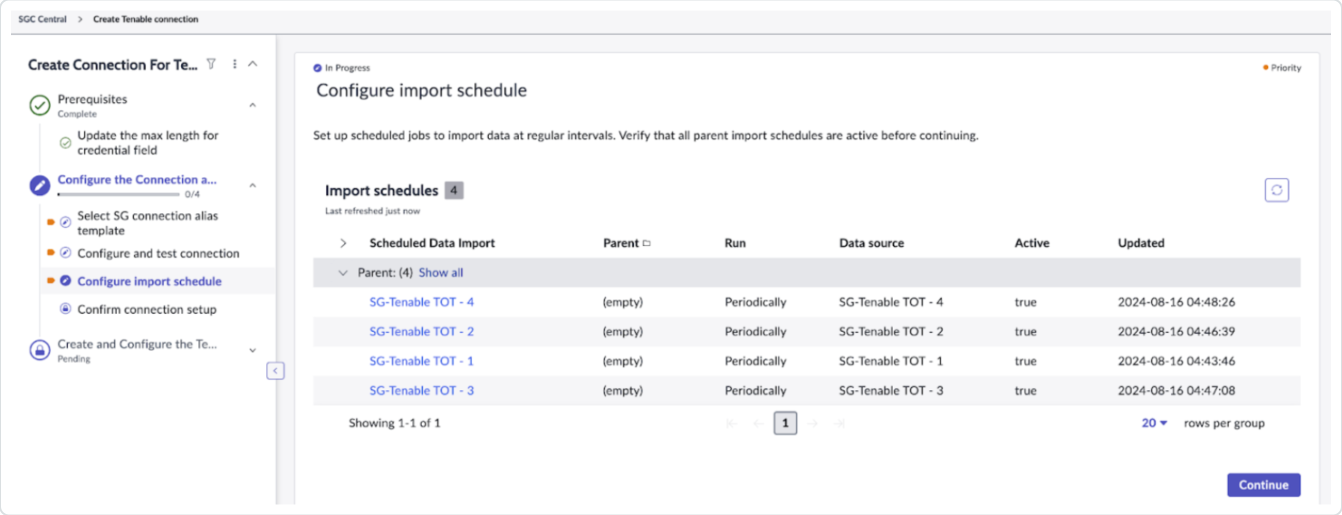
8. Click on the “Create and test connection” button.

   A success message appears.

> **Note:** While creating connection, if you get a "Save credential failed" alert, you can ignore it.

9. Review the four schedule data imports.

10. Click **Continue**.



SGC Central > Create Tenable connection

Create Connection For Te...
Prerequisites
Complete
Update the max length for credential field
Configure the Connection a...
0/4
Select SG connection alias template
Configure and test connection
Configure import schedule
Confirm connection setup
Create and Configure the Te...
Pending
In Progress
Priority

Configure import schedule

Set up scheduled jobs to import data at regular intervals. Verify that all parent import schedules are active before continuing.

Import schedules 4

Last refreshed just now

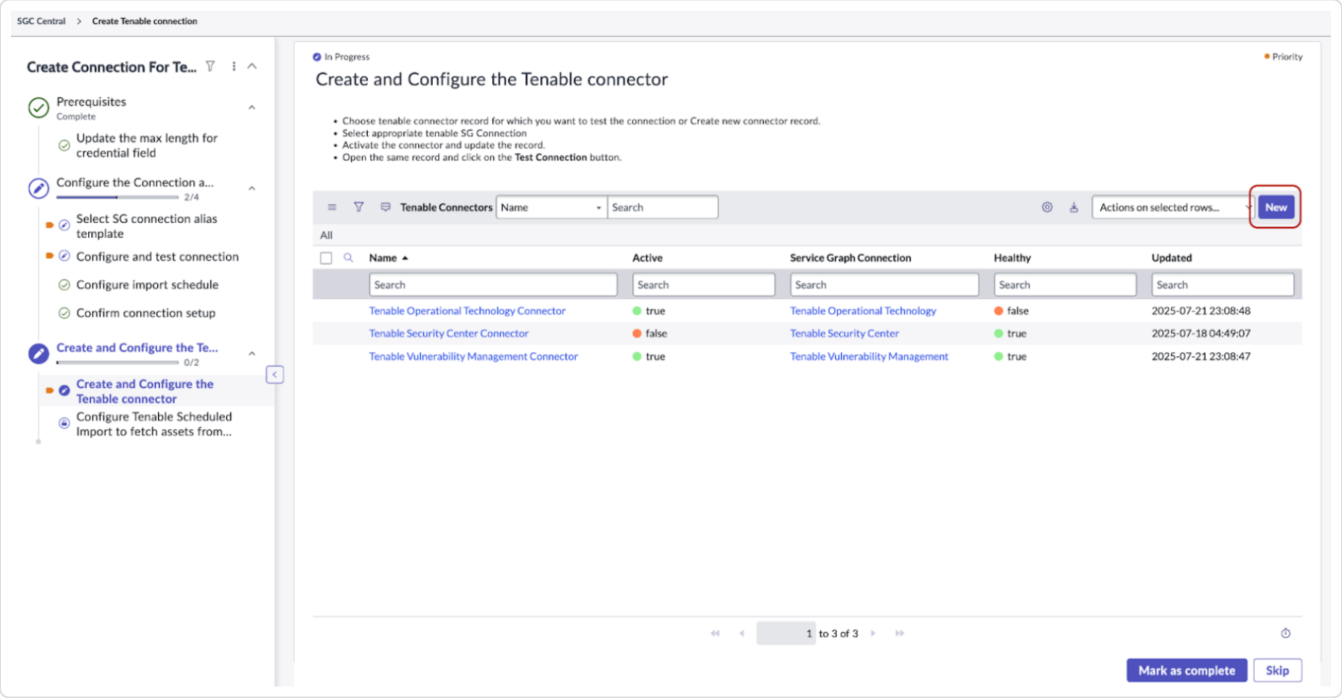
Scheduled Data Import	Parent	Run	Data source	Active	Updated
Parent: (4) Show all					
SG-Tenable TOT - 4	(empty)	Periodically	SG-Tenable TOT - 4	true	2024-08-16 04:48:26
SG-Tenable TOT - 2	(empty)	Periodically	SG-Tenable TOT - 2	true	2024-08-16 04:46:39
SG-Tenable TOT - 1	(empty)	Periodically	SG-Tenable TOT - 1	true	2024-08-16 04:43:46
SG-Tenable TOT - 3	(empty)	Periodically	SG-Tenable TOT - 3	true	2024-08-16 04:47:08

Showing 1-1 of 1

11. Navigate to the **Confirm Connection** tab and click **View All Connections** to see all the added connections.

12. To create the **Tenable Connector**, navigate to the **Next** module and click **New** for the previously created **SG Connection Record**.

13. Provide the required configuration details.



SGC Central > Create Tenable connection
Create Connection For Te...
Prerequisites
Complete
Update the max length for credential field
Configure the Connection a...
2/4
Select SG connection alias template
Configure and test connection
Configure import schedule
Confirm connection setup
Create and Configure the Te...
0/2
Create and Configure the Tenable connector
Configure Tenable Scheduled Import to fetch assets from...
In Progress
Priority

Create and Configure the Tenable connector

- Choose tenable connector record for which you want to test the connection or Create new connector record.
- Select appropriate tenable SG Connection
- Activate the connector and update the record.
- Open the same record and click on the **Test Connection** button.

Tenable Connectors
Name
Search
Actions on selected rows...
New
All

Name ▲	Active	Service Graph Connection	Healthy	Updated
Tenable Operational Technology Connector	● true	Tenable Operational Technology	● false	2025-07-21 23:08:48
Tenable Security Center Connector	● false	Tenable Security Center	● true	2025-07-18 04:49:07
Tenable Vulnerability Management Connector	● true	Tenable Vulnerability Management	● true	2025-07-21 23:08:47

14. Click **Test Connection**.

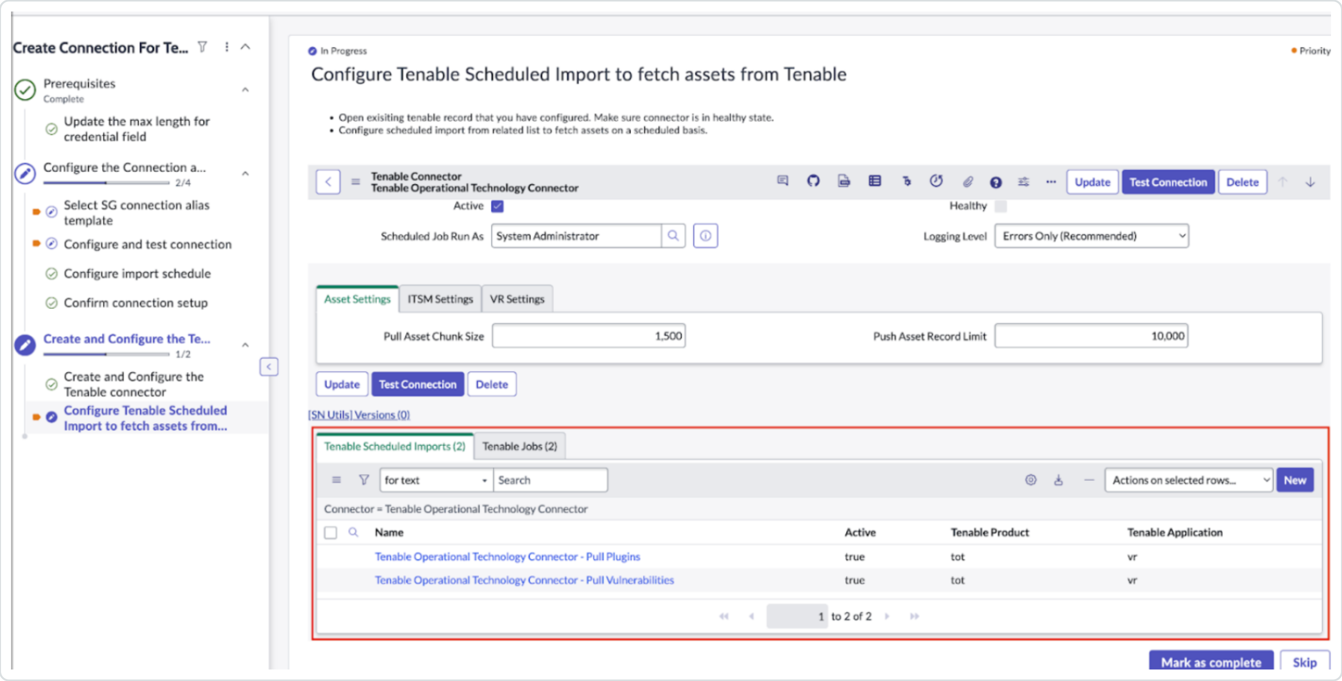
15. Create a **Tenable Schedule Import Job** by opening the Connector Record.

16. Click **New**.

17. Provide the required configuration details.

18. Click **Execute Now** to collect data manually.

19. Click **Mark as Complete**.



Create Connection For Te...
Prerequisites
Complete
Update the max length for credential field
Configure the Connection a...
2/4
Select SG connection alias template
Configure and test connection
Configure import schedule
Confirm connection setup
Create and Configure the Te...
1/2
Create and Configure the Tenable connector
Configure Tenable Scheduled Import to fetch assets from...
In Progress
Priority

Configure Tenable Scheduled Import to fetch assets from Tenable

- Open exisiting tenable record that you have configured. Make sure connector is in healthy state.
- Configure scheduled import from related list to fetch assets on a scheduled basis.

Tenable Connector
Tenable Operational Technology Connector

Update
Test Connection
Delete

Active ☑
Healthy □
Scheduled Job Run As: System Administrator
Logging Level: Errors Only (Recommended)

Pull Asset Chunk Size: 1,500
Push Asset Record Limit: 10,000

Connector = Tenable Operational Technology Connector

Name	Active	Tenable Product	Tenable Application
Tenable Operational Technology Connector - Pull Plugins	true	tot	vr
Tenable Operational Technology Connector - Pull Vulnerabilities	true	tot	vr

1 to 2 of 2

Manage Connections

Required User Role: Administrator

You can create or update existing connections and test the connection. The **Connections** module helps you to manage and monitor connections between various system components.

Key fields in this module include:

Name	Description
Name	The unique identifier for each connection.
Active	Indicates whether the connection is currently active or inactive.
Connection Alias	An alternative name or identifier used to reference the connection.
Message	Contains relevant information or notifications related to the connection.
Status	The current state of the connection, such as success, pending, or failed.
Status Code	The response status code returned from the API call for the using the connection credentials.
Suggestion	Recommendations or actions to address any issues.
Application	The application scope in which the connection is created.
Updated	The date and time when the connection record was last modified.

The Status field indicates the operational state of a connection and can have the following values:

Name	Description
Success	The connection is operating normally and is successfully transmitting data or performing its intended functions.
Error	There is an issue with the connection, which may be affecting its performance or preventing it from functioning as expected.

To manage the connector:

1. Log in to your ServiceNow instance.
2. Navigate to **Tenable Connector for Assets** > **Connectors**.

   The **Tenable Connector** appears.
3. Click **New** or select an existing connection to update.

Service Graph Connections remain in sync with their associated Tenable connectors. When you click **Test Connection**, the status is updated there, and all connectors that use this connection as their Service Graph Connection are marked as healthy or unhealthy based on the outcome of the test connection. Similarly, if you perform the **Test Connection** action from a Tenable connector, the result of that test is also reflected there, and the status is updated accordingly

Create the Connector

You can create several required and optional connections for Tenable products.

Required User Role: Administrator

Connector Configuration Options Matrix

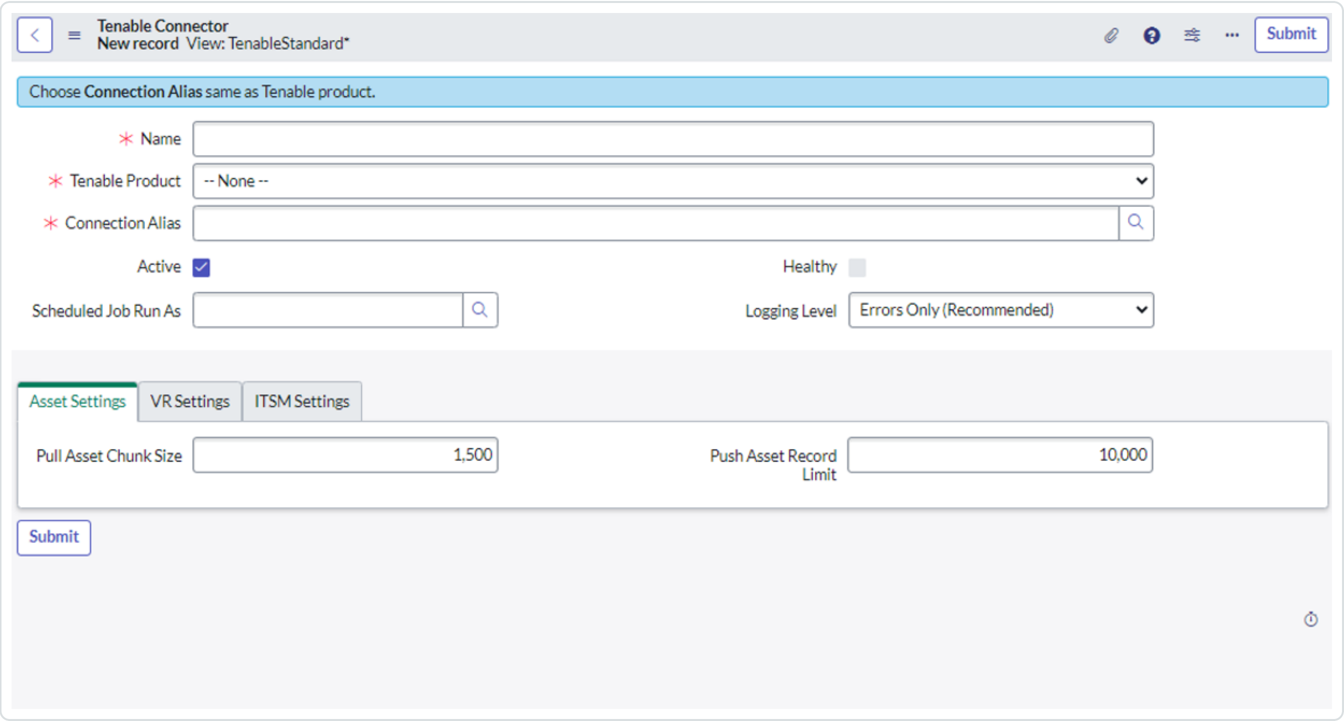
Tenable Product	Module	Job Type
Tenable OT Security (ICP)	Asset	Pull Assets
	VR	Pull Plugins Pull Vulnerabilities
Tenable Security Center	Asset	Pull Assets Push Assets
	ITSM	Pull Vulnerabilities
	SGC for Tenable	Pull Queries
Tenable Vulnerability Management	Asset	Pull Assets Push Assets
	ITSM	Pull Vulnerabilities

To create the connector:

1. Log in to your ServiceNow instance.
2. Navigate to **Tenable Connector for Assets** > **Connectors**.

   The **Tenable Connector** appears.
3. Click **New**.

   A **New User** form appears:



Tenable Connector
New record View: TenableStandard*

Choose Connection Alias same as Tenable product.

* Name			
* Tenable Product	-- None --		
* Connection Alias			
Active	☑	Healthy	□
Scheduled Job Run As		Logging Level	Errors Only (Recommended)

Asset Settings | VR Settings | ITSM Settings

Pull Asset Chunk Size	1,500	Push Asset Record Limit	10,000

4. In the **Name** field, type the name of the connector.

5. From the **Tenable Product** drop-down box, select **Tenable Vulnerability Management**, **Tenable Security Center**, or **Tenable OT Security (ICP)**.

6. Choose the **Service Graph Connection** for the selected **Tenable Product**.

7. Continue to the Optional Connections, or click **Submit**.

Optional Connections

1. Navigate to **Tenable Connector for Assets** > **Add Multiple Instances**.

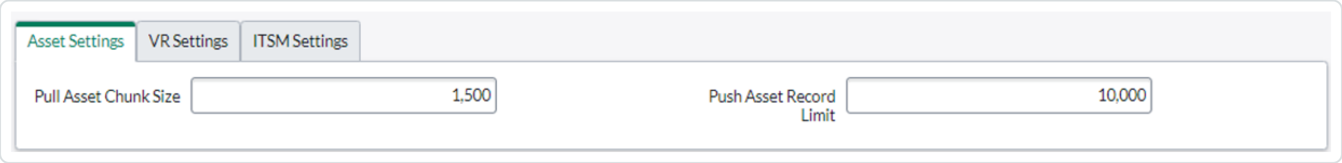
2. Check the **Mark as Complete** checkbox.

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

4. (Optional) Choose **Logging Level** from the dropdown box.

> **Note:**Tenable recommends to use the **Errors Only** level.

5. (Optional) In the **Asset Settings** tab:



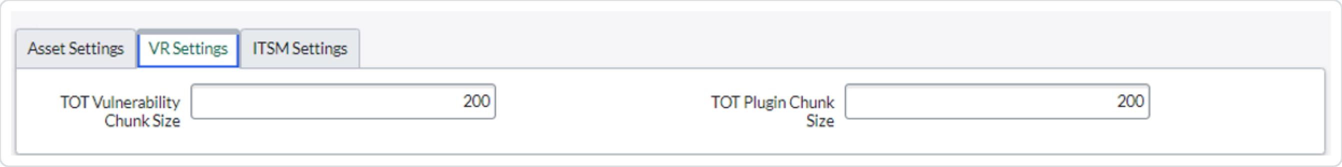
Pull Asset Chunk Size 1,500

Push Asset Record Limit 10,000

Name	Description	Default Value
Pull Asset Chunk Size	The number of records that are pulled per page. Used for the **Pull Assets** job type.	1500
Push Asset Record Limit	The total records that are pushed on the platform at once. Used for the **Push Assets** job type.	10000

Note: The **VR Settings** and **ITSM Settings** tabs are visible only if plugins are activated.

6. (Optional) In the **VR Settings** tab:

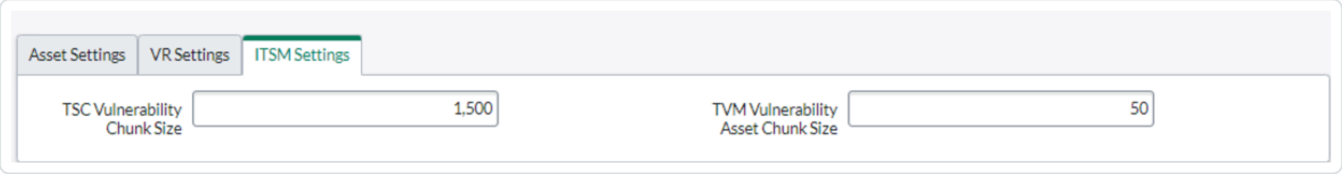


TOT Vulnerability Chunk Size 200

TOT Plugin Chunk Size 200

Name	Description	Default Value
TOT Vulnerability Chunk Size	The number of Vulnerabilities that are pulled per page. Used for TOT Pull Vulnerabilities job type.	200 (also max limit)
Push Asset Record Limit	The total records that are pushed on the platform at once. Used for the **Push Assets** job type.	10000

7. (Optional) In the **ITSM Settings** tab:



TSC Vulnerability Chunk Size 1,500

TVM Vulnerability Asset Chunk Size 50

Name	Description	Default Value
TSC Vulnerability Chunk Size:	The number of vulnerabilities that will be pulled per page. Used for **TSC Pull Vulnerabilities** job type.	1500
TVM Vulnerability Asset Chunk Size	The number of assets for which all of their vulnerabilities will be pulled. Used for **TVM Pull Vulnerabilities** job type.	50 **Note:** Tenable recommends not to change the default value of this field. Increasing the value also increases the amount of data pulled at once. This may create an issue while reading that data.

8. Click **Submit**.

Next steps:

- Configure Tenable Vulnerability Management.
- Configure Tenable Security Center.
- Configure Tenable OT Security.

Configure Tenable Vulnerability Management

Required User Role: Administrator

To configure Tenable Vulnerability Management in ServiceNow:

1. Log in to your ServiceNow instance.
2. Navigate to **Tenable Connector for Assets** > **Connectors**.

   The **Tenable Connector** appears.
3. Navigate to your already existing connector whose Tenable product is Tenable Vulnerability Management.
4. From the **Module** drop-down box, you can select **Asset** or **ITSM**.

   Note: By default, the connector's name is populated.

   Note: For the Asset Module, you can select the **Pull Assets** or **Push Assets** Tenable Job Type. For the ITSM Module, you can select **Pull Vulnerabilities** as the Tenable Job Type.

Asset Module, Tenable Job Type > Pull Assets

The **Pull Assets Schedule Job** fetches the assets from Tenable Vulnerability Management to ServiceNow and stores the asset details in the CMDB Tables (Incomplete IP Identified Device, Unclassed Hardware, Computer, Network Adaptor, IP Address) and the **Custom** table (Tenable Asset Attributes).

Name	Description	Default Value
Active	If selected, the scheduled job runs on the configured schedule.	Disabled
Initial Run - Historical Data	The amount of time (in days) of how far back you want to pull data.	Within the last 365 days

Last Run	The date and time that the import was last run.	N/A
Edit Run Schedule	Select this box if you want to configure the scheduled job run configuration. The following options must be configured: **Note:**Make sure not to set the run frequency too high, as this can result in congested jobs and create performance issues. - **Run:** The frequency that you want the import to run. Possible values are: Daily, Weekly, Monthly, Periodically, Once, On Demand, Business Calendar: Entry Start, or Business Calendar: Entry End. - **Repeat Interval/Time:** Set the time (hh/mm/ss) to run the import. This differs based on the **Run** selection.	If selected, **Daily** is the default value.

Asset Module, Tenable Job Type > Push Assets

The **Push Assets Scheduled Job** pushes the assets from ServiceNow to Tenable Vulnerability Management.

Name	Description	Default Value
Active	If selected, the scheduled job runs on the configured schedule.	Disabled
Initial Run - Historical Data	The amount of time (in days) of how far back you want to pull data.	Within the last 365 days
Last Run	The date and time that the import was last run.	N/A

Edit Run Schedule	Select this box if you want to configure the scheduled job run configuration. The following options must be configured: **Note:** Make sure not to set the run frequency too high, as this can result in congested jobs and create performance issues. • **Run:** The frequency that you want the import to run. Possible values are: Daily, Weekly, Monthly, Periodically, Once, On Demand, Business Calendar: Entry Start, or Business Calendar: Entry End. • **Repeat Interval/Time:** Set the time (hh/mm/ss) to run the import. This differs based on the **Run** selection.	If enabled, **Daily** is the default value.

5. In the **Conditions** > **Configuration Item Source Table** dropdown, select the table on which you want the query to run in order to export the assets to Tenable Vulnerability Management.

6. In the **Conditions** > **Conditions** dropdown, apply the filter conditions on the **Configuration Item Source Table** that you have selected.

7. If you selected the **ITSM Module**, configure the following parameters:

ITSM Module, Tenable Job Type > Pull Vulnerabilities

The **Pull Vulnerabilities Schedule Job** fetches the vulnerabilities from Tenable Vulnerability Management to ServiceNow and stores the vulnerabilities in the **Custom** table (Tenable Vulnerability).

Name	Description	Default Value
Active	If selected, the scheduled job runs on the configured schedule.	Disabled
Initial Run -	The amount of time (in days) of how far back	Within the last 365

Historical Data	you want to pull data.	days
Last Run	The date and time that the import was last run.	N/A
Last Run - Fixed	The date and time that the fixed import was last run. The integration fetches the vulnerabilities from this data and time.	N/A
Run Fixed Query on Initial Run	Pulls fixed vulnerabilities on the first import.	Disabled
Included Severities	Specify the severities for the vulnerabilities being imported.	By default, the value is empty and only vulnerabilities with high and critical severities are fetched.
Edit Run Schedule	Select this box if you want to configure the scheduled job run configuration. The following options must be configured: **Note:** Make sure not to set the run frequency too high, as this can result in congested jobs and create performance issues. • **Run:** The frequency that you want the import to run. Possible values are: Daily, Weekly, Monthly, Periodically, Once, On Demand, Business Calendar: Entry Start, or Business Calendar: Entry End. • **Repeat Interval/Time:** Set the time (hh/mm/ss) to run the import. This differs based on the **Run** selection.	If selected, **Daily** is the default value.

> **Note:** The **Name** text box is automatically populated based on the name of the connector and **Job Type**.

8. Click **Submit**.

Next steps:

- Go to Test Configuration.

ServiceNow ITSM Pro Incident Rule Fields

The ServiceNOW integration with Tenable Vulnerability Management produces incident rule fields and pushes the following asset attributes to ServiceNow ITSM Pro.

Incident Rule Fields and Asset Attributes

Label	Name
cvssV4Supplemental	u_cvssv4supplemental
seolDate	u_seoldate
epssScore	u_epssscore
recastRiskRuleComment	u_recastriskrulecomment
acceptRiskRuleComment	u_acceptriskrulecomment
hostUUID	u_hostuuid
acrScore	u_acrscore
Agent UUID	u_agent_uuid
First Found	u_first_found
IPs	u_ips
Operating System	u_operating_system
Plugin Modification Date	u_plugin_modification_date
Priority	u_priority

Label	Name
Scan	u_scan
severity_modification_type	u_severity_modification_type
XREF	u_xref
Description	u_description
indexed	u_indexed
Netbios Name	u_netbios_name
Plugin Family Type	u_plugin_family_type
Port Port	u_port_port
risk_accepted	u_risk_accepted
severity_default_id	u_severity_default_id
VPR Context	u_vprcontext
Configuration Item	u_ci
Hostname	u_hostname
Last Found Date	u_last_found_date
Plugin Description	u_plugin_description
Plugin Synopsis	u_plugin_synopsis
Repository ID	u_repository_id
SC Unique	u_scunique
Tenable Plugin ID	u_tenable_plugin
FQDN	u_fqdn
last_fixed	u_last_fixed
pluginName	u_pluginname

Label	Name
Plugin Publication Date	u_plugin_publication_date
Reopened	u_reopened
Scan Started At	u_scan_started_at
State	u_state
vulnUniqueness	u_vulnuniqueness
vulnUUID	u_vulnuuid

Incident Rule Fields and Asset Attributes (cont'd)

Label	Name
cvssV4BaseScore	u_cvssv4basescore
cgiScanEnabled	u_cgiscanenabled
keyDrivers	u_keydrivers
assetExposureScore	u_assetexposurescore
thoroughScanEnabled	u_thoroughscanenabled
paranoidScanEnabled	u_paranoidscanenabled
finding_id	u_finding_id
BIOS UUID	u_bios_uuid
hasBeenMitigated	u_hasbeenmitigated
Last Found	u_last_found
Plugin CVE	u_plugin_cve
Plugin Solution	u_plugin_solution
Repository Data Format	u_repository_data_format

Label	Name
Scan UUID	u_scan_uuid
Substate	u_substate
Asset Hostname	u_asset_hostname
First Found Date	u_first_found_date
Job Type	u_job_type
Output	u_output
Plugin Name	u_plugin_name
Product Type	u_product_type
Scan Completed At	u_scan_completed_at
Source Name	u_source_name
Device Type	u_device_type
IP	u_ip
operatingSystem	u_operatingsystem
Plugin ID	u_plugin_id
Port Protocol	u_port_protocol
Risk Recasted	u_risk_recasted
Severity ID	u_severity_id
VPR Score	u_vpr_score
source	u_source
Connector	u_connector
hostUniqueness	u_hostuniqueness
MAC Address	u_mac_address

Label	Name
Plugin Family	u_plugin_family
Port	u_port
Repository Name	u_repository_name
Severity	u_severity
uniqueness	u_uniqueness
attachment	u_attachment
cvssV4Vector	u_cvssv4vector
cvssV4ThreatScore	u_cvssv4threatscore
cvssV4ThreatVector	u_cvssv4threatvector

Configure Tenable Security Center

Required User Role: Administrator

To configure Tenable Security Center in ServiceNow:

1. Log in to your ServiceNow instance.
2. Navigate to **Tenable Connector for Assets** > **Connectors**.

   The **Tenable Connector** appears.
3. Navigate to your already existing connector whose Tenable product is Tenable Security Center.
4. From the **Module** drop-down box, you can select **Asset**, **ITSM**, or **SGC for Tenable**.

   Note: By default, the connector's name is populated.

   Note: For the Asset Module, you can select the **Pull Assets** or **Push Assets** Tenable Job Type. For the ITSM Module, you can select **Pull Vulnerabilities** as the Tenable Job Type.

   Asset Module, Tenable Job Type > Pull Assets

   The **Pull Assets Schedule Job** fetches the assets from Tenable Security Center to ServiceNow and stores the asset details in the CMDB Tables (Incomplete IP Identified Device, Unclassed Hardware, Computer, Network Adaptor, IP Address) and the **Custom** table (Tenable Asset Attributes).

Name	Description	Default Value
TSC Query	The selected filter is used to pull vulnerabilities or assets from Tenable Security Center.	Disabled
Active	If selected, the scheduled job runs on the configured schedule.	Disabled

Initial Run - Historical Data	The amount of time (in days) of how far back you want to pull data.	Within the last 365 days
Last Run	The date and time that the import was last run.	N/A
Edit Run Schedule	Select this box if you want to configure the scheduled job run configuration. The following options must be configured: **Note:** Make sure not to set the run frequency too high, as this can result in congested jobs and create performance issues. • **Run:** The frequency that you want the import to run. Possible values are: Daily, Weekly, Monthly, Periodically, Once, On Demand, Business Calendar: Entry Start, or Business Calendar: Entry End. • **Repeat Interval/Time:** Set the time (hh/mm/ss) to run the import. This differs based on the **Run** selection.	If selected, **Daily** is the default value.

Asset Module, Tenable Job Type > Push Assets

The **Push Assets Scheduled Job** pushes the assets from ServiceNow to Tenable Security Center. In Tenable Security Center, the data is pushed in the group that you specify when creating the schedule job. A new group is created on the platform, if the specified one is not already present.

Name	Description	Default Value
Active	If selected, the scheduled job runs on the configured schedule.	Disabled

Initial Run - Historical Data	The amount of time (in days) of how far back you want to pull data.	Within the last 365 days
Last Run	The date and time that the import was last run.	N/A
Edit Run Schedule	Select this box if you want to configure the scheduled job run configuration. The following options must be configured: **Note:** Make sure not to set the run frequency too high, as this can result in congested jobs and create performance issues. • **Run:** The frequency that you want the import to run. Possible values are: Daily, Weekly, Monthly, Periodically, Once, On Demand, Business Calendar: Entry Start, or Business Calendar: Entry End. • **Repeat Interval/Time:** Set the time (hh/mm/ss) to run the import. This differs based on the **Run** selection.	If enabled, **Daily** is the default value.

5. In the **Conditions** > **Configuration Item Source Table** dropdown, select the table on which you want the query to run in order to export the assets to Tenable Security Center.

> **Note:** By default, this value is set to `cmdb_ci`. For the group type **Static IP Address**, the **Configuration Item Source Table** should be the parent table of "CMDB CI IP Address."

6. In the **Conditions** > **Group Name** text box, enter the name of the group.

> **Note:** This named group is created in Tenable Security Center while pushing the assets records. You can identify these records based on the group name on the platform.

7. In **Conditions** > **Group Type** dropdown, select **DNS** or **Static IP Address**, based on which type of data you would like to push.

> **Note:** For **Static IP Address**, you need to set the **IP Version** and **IP's To Send** options. Only unique IP addresses are stored on the Tenable Security Center. However, in the Tenable job's **Total Record** field, you may see more records than the number actually stored on the platform. This discrepancy occurs because the job does not check for uniqueness, whereas the platform does. The scheduled job first retrieves the record from the selected table, then checks the parent-child relationship in the `cmdb_rel_ci` table. If the relationship is not satisfied, the IP is not pushed to the platform. If the relationship is satisfied, the child IP is pushed to the platform.

8. In the **Conditions** > **Conditions** dropdown, apply the filter conditions on the Configuration Item Source Table that you have selected.

9. If you selected the **ITSM Module**, configure the following parameters:

ITSM Module, Tenable Job Type > Pull Vulnerabilities

The **Pull Vulnerabilities Schedule Job** fetches the vulnerabilities from Tenable Security Center to ServiceNow and stores the vulnerabilities in the **Custom** table (Tenable Vulnerability).

Name	Description	Default Value
TSC Query	The selected filter is used to pull vulnerabilities or assets from Tenable Security Center.	Disabled
Active	If selected, the scheduled job runs on the configured schedule.	Disabled
Initial Run - Historical Data	The amount of time (in days) of how far back you want to pull data.	Within the last 365 days
Last Run	The date and time that the import was last run.	N/A
Last Run - Fixed	The date and time that the fixed import was last run. The integration fetches the vulnerabilities from this data and time.	N/A

	Note: This field is for the **Fixed** job mode.	
Run Fixed Query on Initial Run	Pulls fixed vulnerabilities on the first import.	Disabled
Edit Run Schedule	Select this box if you want to configure the scheduled job run configuration. The following options must be configured: **Note:** Make sure not to set the run frequency too high, as this can result in congested jobs and create performance issues. • **Run:** The frequency that you want the import to run. Possible values are: Daily, Weekly, Monthly, Periodically, Once, On Demand, Business Calendar: Entry Start, or Business Calendar: Entry End. • **Repeat Interval/Time:** Set the time (hh/mm/ss) to run the import. This differs based on the **Run** selection.	If selected, **Daily** is the default value.

Note: The **Name** text box is automatically populated based on the name of the connector and **Job Type**.

10. Click **Submit**.

Next steps:

- Go to Test Configuration.

Configure Tenable OT Security

Required User Role: Administrator

To configure Tenable OT Security in ServiceNow:

1. Log in to your ServiceNow instance.
2. Navigate to **Tenable Connector for Assets** > **Connectors**.

   The **Tenable Connector** appears.
3. Navigate to your already existing connector whose Tenable product is Tenable OT Security.
4. From the **Module** drop-down box, you can select **Asset** or **VR**.

   Note: By default, the connector's name is populated.

   Note: For the Asset Module, you can select the **Pull Assets** Tenable Job Type. For the VR Module, you can select the **Pull Vulnerabilities** as the Tenable Job Type. The **Pull Plugins Tenable Job Type** is automatically created by the **Pull Vulnerabilities** job.

   Asset Module, Tenable Job Type > Pull Assets

   The **Pull Assets Schedule Job** fetches the assets from Tenable OT Security to ServiceNow and stores the asset details in the CMDB Tables (IP Address, Network Adapter, OT Control Systems, Incomplete IP Identified Device, Operational Technology (OT), Network Gear, Industrial Sensors) and the **Custom** table (Tenable Asset Attributes).

Name	Description	Default Value
Active	If selected, the scheduled job runs on the configured schedule.	Disabled
Initial Run - Historical Data	The amount of time (in days) of how far back you want to pull data.	Within the last 365 days

Last Run	The date and time that the import was last run.	N/A
Edit Run Schedule	Select this box if you want to configure the scheduled job run configuration. The following options must be configured: **Note:**Make sure not to set the run frequency too high, as this can result in congested jobs and create performance issues. • **Run:** The frequency that you want the import to run. Possible values are: Daily, Weekly, Monthly, Periodically, Once, On Demand, Business Calendar: Entry Start, or Business Calendar: Entry End. • **Repeat Interval/Time:** Set the time (hh/mm/ss) to run the import. This differs based on the **Run** selection.	If selected, **Daily** is the default value.

5. If you selected the **VR Module**, configure the following parameters:

> **Note:** This module is only be visible if the "Tenable.ot for VR" integration is installed.

VR Module, Tenable Job Type > Pull Plugins

The **Pull Plugins Schedule Job** fetches the assets from Tenable OT Security to ServiceNow and stores the plugin details in the **Custom** table (Plugin Import and Tenable Plugin Additional Info).

> **Note:** This **Scheduled** job is automatically created when the **Pull Vulnerabilities** job is created.

Name	Description	Default Value
Active	If selected, the scheduled job runs on the configured	Disabled

	schedule.	
Initial Run - Historical Data	The amount of time (in days) of how far back you want to pull data.	Within the last 365 days
Last Run	The date and time that the import was last run.	N/A
Last Run - Fixed	The date and time that the fixed import was last run. The integration fetches the vulnerabilities from this data and time. **Note:** This field is for the **Fixed** job mode.	N/A
Run Fixed Query on Initial Run	Pulls fixed vulnerabilities on the first import.	Disabled
Edit Run Schedule	Select this box if you want to configure the scheduled job run configuration. The following options must be configured: **Note:** Make sure not to set the run frequency too high, as this can result in congested jobs and create performance issues. • **Run:** The frequency that you want the import to run. Possible values are: Daily, Weekly, Monthly, Periodically, Once, On Demand, Business Calendar: Entry Start, or Business Calendar: Entry End. • **Repeat Interval/Time:** Set the time (hh/mm/ss) to run the import. This differs based on the **Run** selection.	If selected, **Daily** is the default value.

VR Module, Tenable Job Type > Pull Vulnerabilities

The **Pull Vulnerabilities Schedule Job** fetches the vulnerabilities from Tenable OT Security to ServiceNow and stores the vulnerabilities in the ServiceNow able **Vulnerable Item**.

Name	Description	Default Value
Active	If selected, the scheduled job runs on the configured schedule.	Disabled
Initial Run - Historical Data	The amount of time (in days) of how far back you want to pull data.	Within the last 365 days
Last Run	The date and time that the import was last run.	N/A
Last Run - Fixed	The date and time that the fixed import was last run. The integration fetches the vulnerabilities from this data and time. **Note:** This field is for the **Fixed** job mode.	N/A
Run Fixed Query on Initial Run	Pulls fixed vulnerabilities on the first import.	Disabled
Edit Run Schedule	Select this box if you want to configure the scheduled job run configuration. The following options must be configured: **Note:** Make sure not to set the run frequency too high, as this can result in congested jobs and create performance issues. • **Run:** The frequency that you want the import to run. Possible values are: Daily, Weekly, Monthly, Periodically, Once, On Demand, Business Calendar: Entry Start, or Business Calendar: Entry	If selected, **Daily** is the default value.

	End. - **Repeat Interval/Time:** Set the time (hh/mm/ss) to run the import. This differs based on the **Run** selection.	

Note: The **Name** text box is automatically populated based on the name of the connector and **Job Type**.

6. Click **Submit**.

Next steps:

- Go to Test Configuration.

Test the Configuration

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 and testing, and others dedicated to production.

Configuration checks:

- If your Tenable Security Center resides behind a firewall on your internal network, you must use the MID server to access its data.
- For Tenable Operational Technology MID Server is mandatory.
- 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.

FAQ

Why am I unable to install an application from the ServiceNow Store?

1. Verify you have the system administrator (admin) role.
2. Navigate to **System Applications** > **All Available Applications** > **All**.
3. Verify the application appears under the **Installed** tab.

How can I create a new user?

- Perform the steps the steps in User Administration.

Why am I getting an error related to ECC Queue timeout?

1. Navigate to **sys_properties.LIST**.
2. Update the following system properties with given values:
   a. `glide.http.outbound.max_timeout.enabled` = false
   b. `glide.http.outbound.max_timeout.enabled` = false
   c. `glide.http.outbound.max_timeout` = 60 (or increase the time as per requirement)
3. Run the scheduled script again.

Why am I unable to Create the Connection Alias?

- Verify you have the system administrator (admin) role.

Why am I Unable to Create the Connector?

1. Verify you have the system administrator (admin) role or Application Admin role.

Why is the Connector unhealthy?

1. Check the credentials and the endpoint of the **Connection Alias**. Make sure not to add a '/' after the endpoint.

2. (For TSC and TOT) Verify that the MID is running. (Mandatory for TOT)

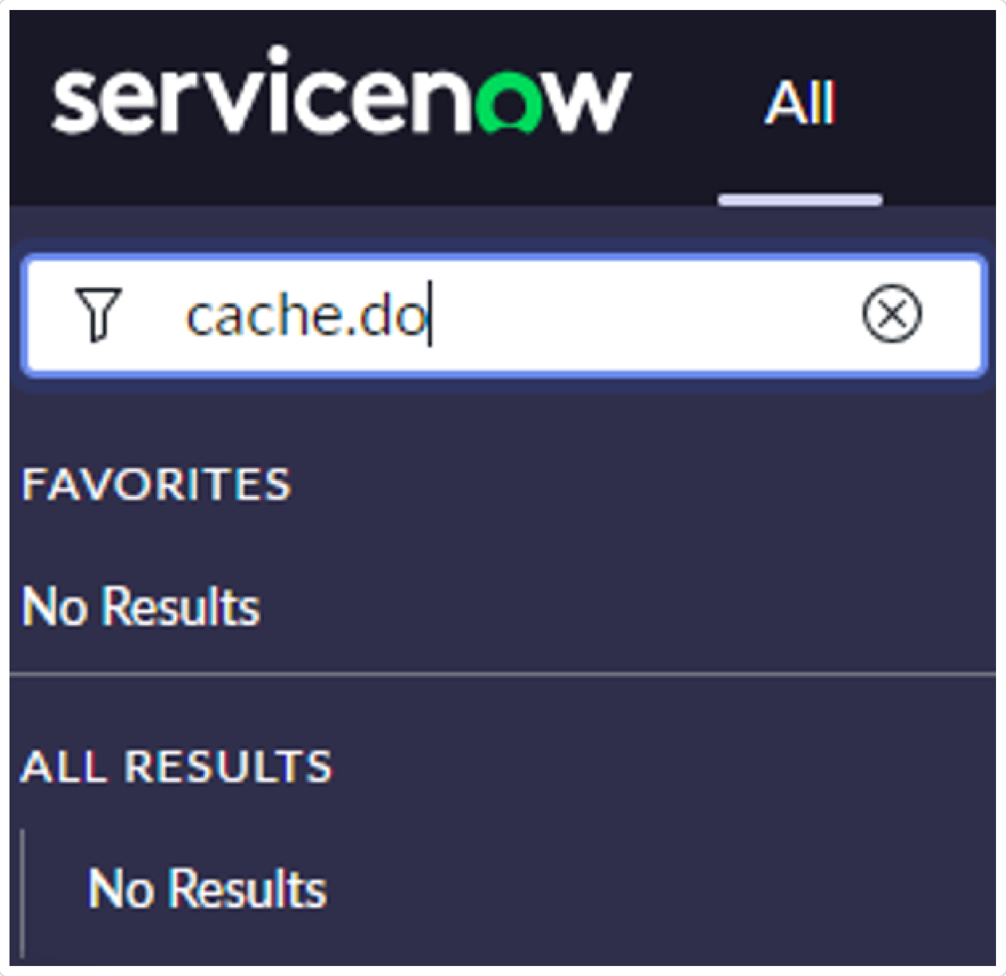
Why am I unable to see options in the Tenable Scheduled Import Form view?

1. Clear cache from your browser or create the **Scheduled Import Job** from Incognito.

2. Clear cache from your ServiceNow instance:

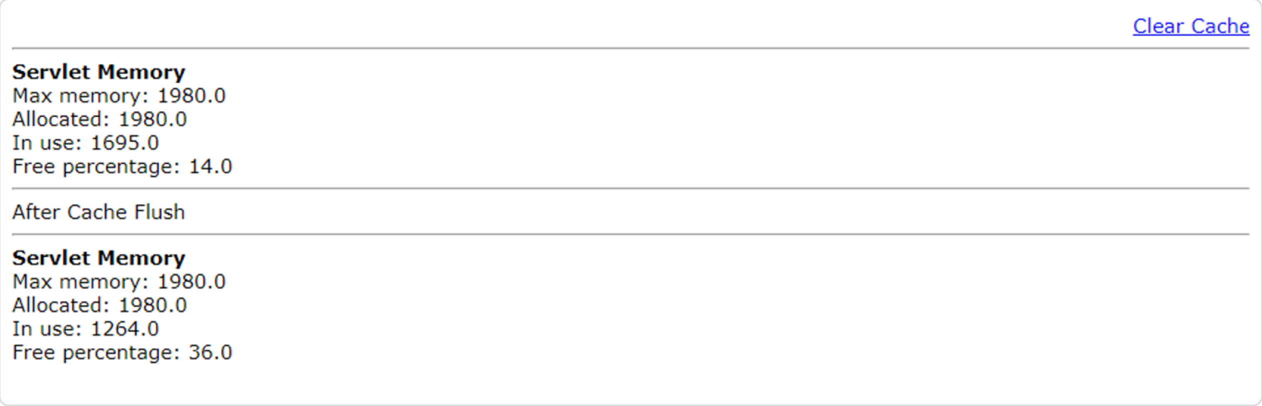
    a. Login to your ServiceNow instance.

    b. Type "cache.do" in the filters tab.



    c. Click **Enter**

d. On the following page click **Clear Cache**.



Clear Cache

Servlet Memory
Max memory: 1980.0
Allocated: 1980.0
In use: 1695.0
Free percentage: 14.0

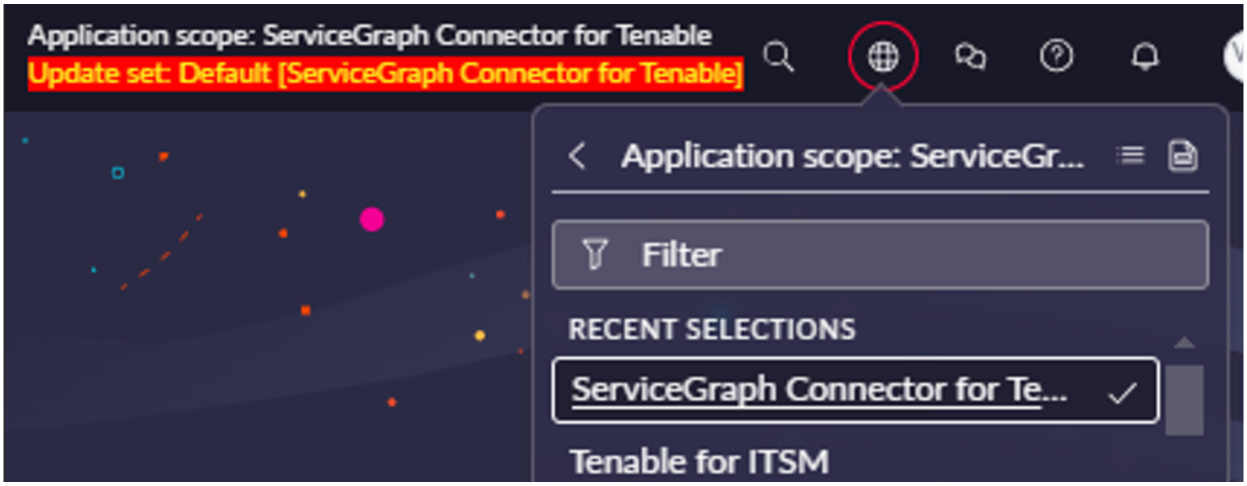
After Cache Flush

Servlet Memory
Max memory: 1980.0
Allocated: 1980.0
In use: 1264.0
Free percentage: 36.0

Why are Jobs not created after executing the scheduled job?

1. Create missing cross scope privilege records manually:

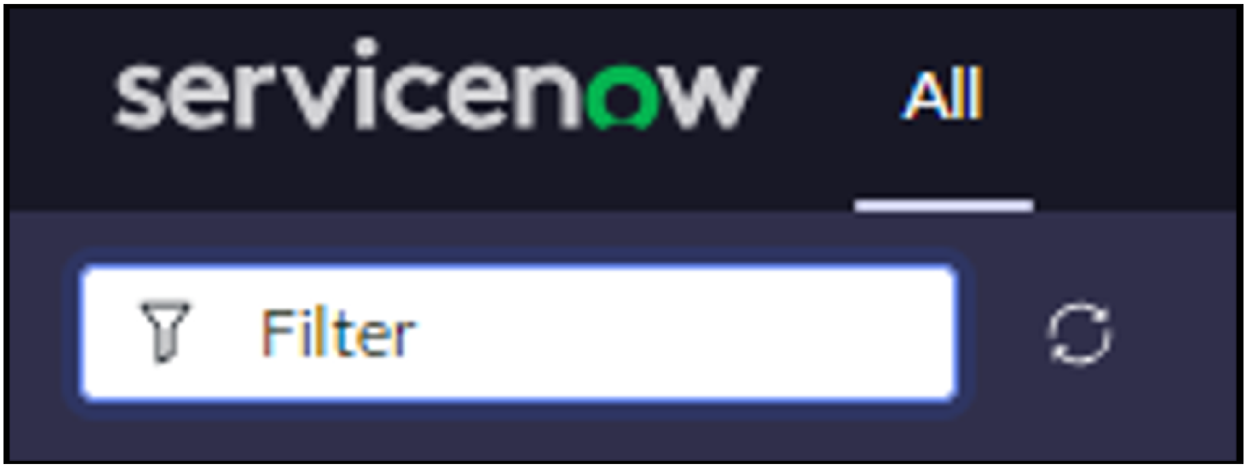
   a. Set Application scope to Service Graph Connector for Tenable from here:



Application scope: ServiceGraph Connector for Tenable
Update set: Default [ServiceGraph Connector for Tenable]

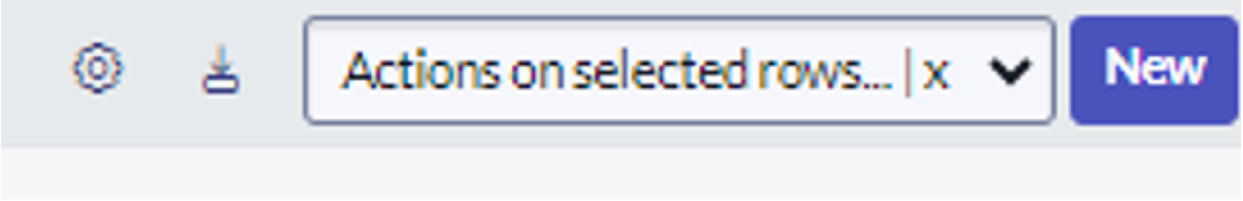
Application scope: ServiceGr...
Filter
RECENT SELECTIONS
ServiceGraph Connector for Te...
Tenable for ITSM

   b. Click **Filter** and type "sys_scope_privilege.list".

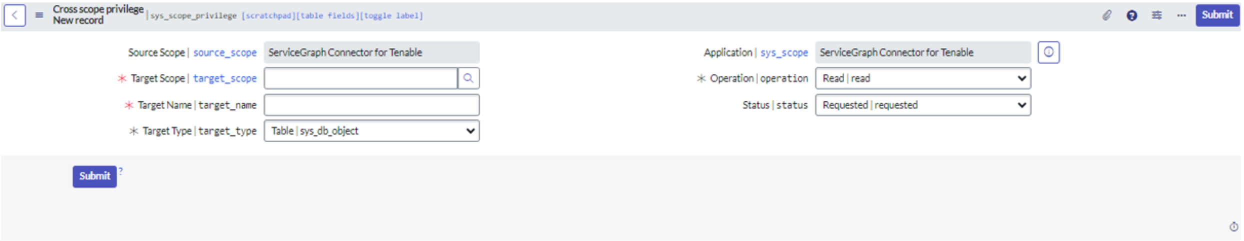


c. Click **Enter**

d. Click the **New** button in the top-right corner.



The form below appears:



Cross scope privilege | sys_scope_privilege [scratchpad][table fields][toggle label]
New record

Source Scope | source_scope	ServiceGraph Connector for Tenable	Application | sys_scope	ServiceGraph Connector for Tenable
* Target Scope | target_scope		* Operation | operation	Read | read
* Target Name | target_name		Status | status	Requested | requested
* Target Type | target_type	Table | sys_db_object		

e. Create six records with following values.

Sr no.	Target Scope	Target Name	Target Type	Operation	Status
1	Tenable for ITSM	x_tsirm_tio_itsm_vulnerability	Table	Read	Allowed

2	Tenable for ITSM	TenableITSMHelper	Script Include	Execute API	Allowed
3	Tenable for ITSM	TenableITSM	Script Include	Execute API	Allowed
4	Tenable for ITSM	TenableITSMScheduleHelper	Script Include	Execute API	Allowed
5	Tenable.ot for VR	TenableVRScheduleHelper	Script Include	Execute API	Allowed
6	Tenable.ot for VR	TenableVRHelper	Script Include	Execute API	Allowed

f. Go to **Schedule Import record** and click **Execute**.

2. Check if all the threads are occupied.

   a. Navigate to the **User Administration** > **All Active transaction**.

   b. Confirm that all threads are occupied. If yes, then remove the unused threads.

   c. Reload the **Scheduled Data** import form.

Why is the integration failing and/or data not being ingested into the table?

1. Check the connector's configuration and make sure it is healthy.

2. Make sure the user has proper roles. Refer to this page to see what role users should have on Tenable platforms.

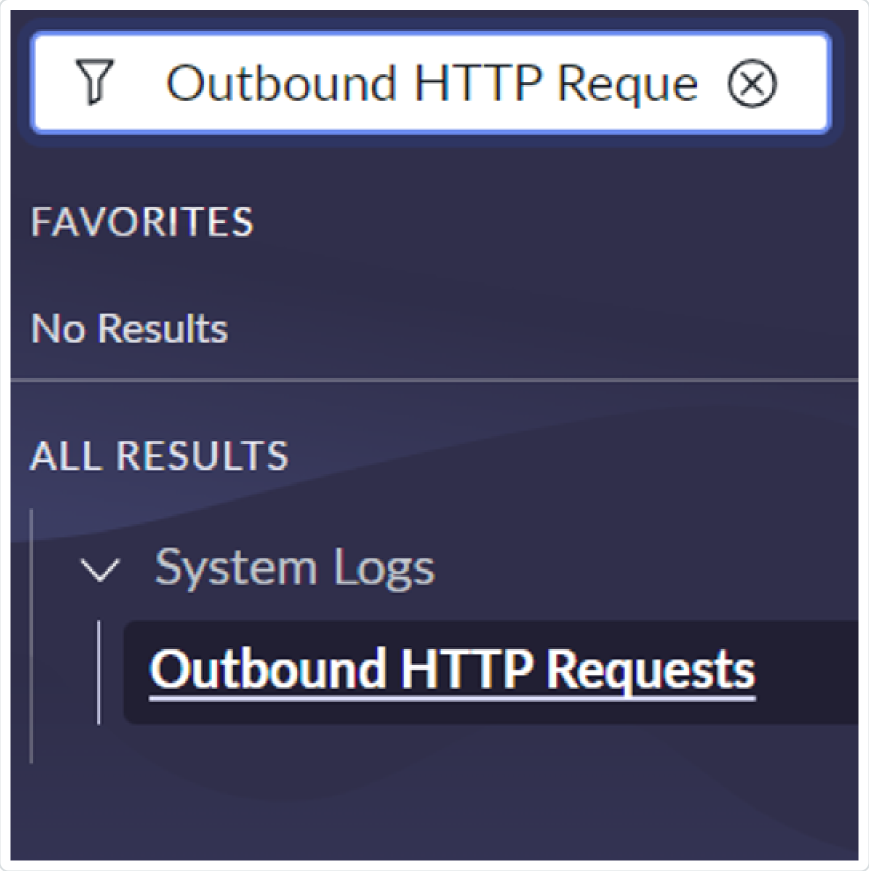
3. Check the **Application Logs**.

4. If the error is related to API calls made, follow these steps:

   a. Enable the following three system properties from the **sys_properties** table (you can type "sys_properties.LIST" in the **Filters** section) and then run the integration again:

- `glide.outbound_http_log.override -> Set value to “true”,`
- `glide.outbound_http_log.override.level -> Set value to “all”`
- `glide.outbound_http.content.max_limit -> Set value to “1000”`

b. Check the HTTP requests in the **Outbound HTTP Requests** module under **System Logs** which contains details of request and response of API calls.



Why am I getting a "Request method or request URL not found from undefined” error?

1. Navigate to the **Flow Designer** > **Actions**.
2. Open the **Rest** step and check the execution. It might be an error from the API.
3. Run scheduled job again.

I got an "Exception: SyntaxError: Empty JSON string” while pulling data using an import job and then increasing the file size. What do I do?

1. Confirm that you have the system administrator (admin) role.
2. Navigate to `sys_properties`.
3. Increase the value of the `com.glide.attachment.max_get_size` and `com.glide.attachment.max_size`. Enter the value in bytes.

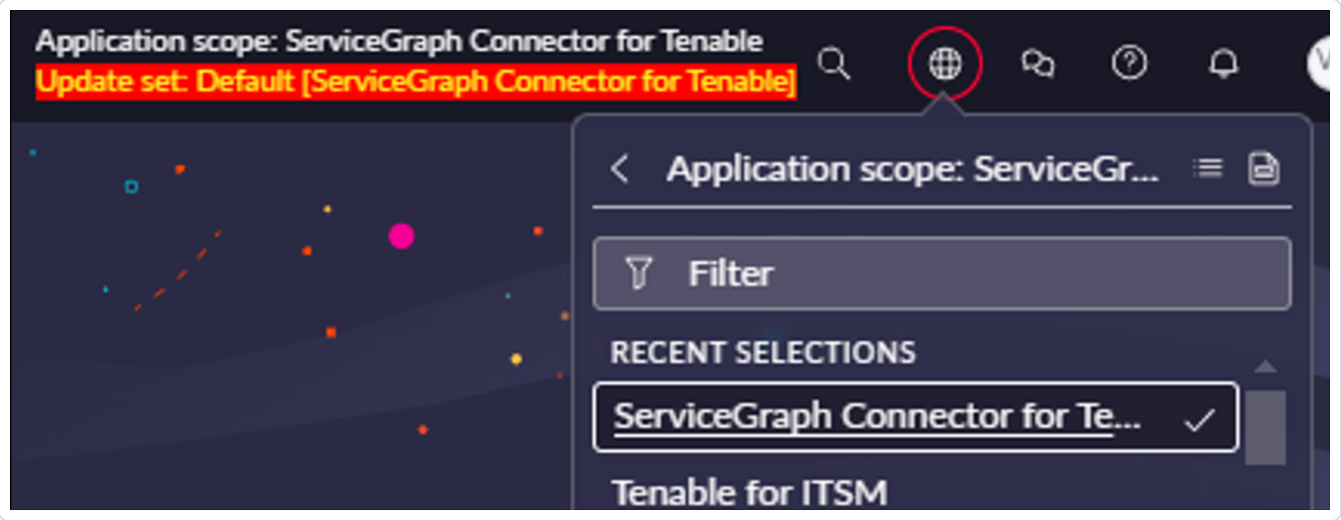
   > **Note:**if the property does not exist then create a new one in Global Scope. (For example, values can be: `com.glide.attachment.max_get_size = 31457280` and `com.glide.attachment.max_size = 4096`)

Why am I unable to validate the MID server?

1. Navigate to **MID Server** > **MID Security Policy**.
2. Open **Intranet and Internet Records** and uncheck **Certificate Chain Check** , **Hostname Check** and **Revocation Check** checkboxes.

How can I activate/deactivate data sources for ITSM or VR?

1. Set the **Application scope to ServiceGraph Connector for Tenable** from here:

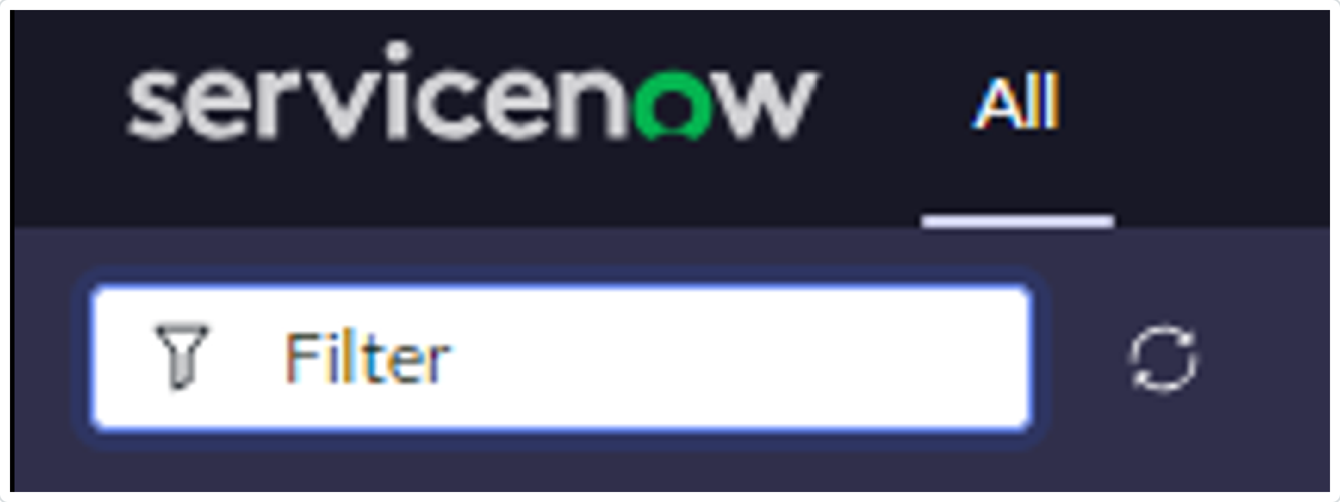


Application scope: ServiceGraph Connector for Tenable

Update set: Default [ServiceGraph Connector for Tenable]

Application scope: ServiceGr...
Filter
RECENT SELECTIONS
ServiceGraph Connector for Te... ✓
Tenable for ITSM

2. Click **Filter**.



3. Type "x_tsirm_tio_now_data_source_registry.list".

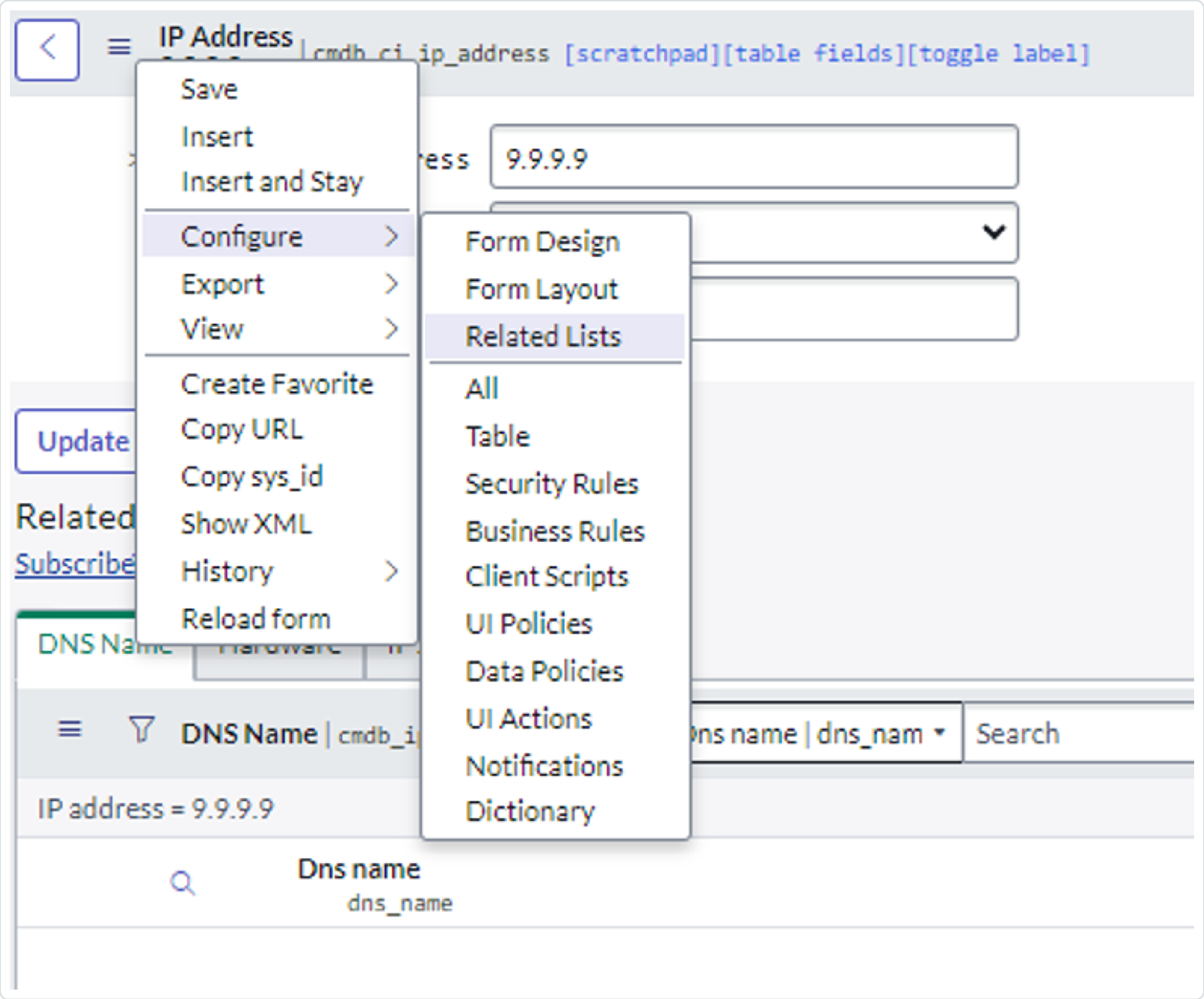
4. Click **Enter**.

5. After applying the appropriate filters, in the **Active** column set the value of that record.

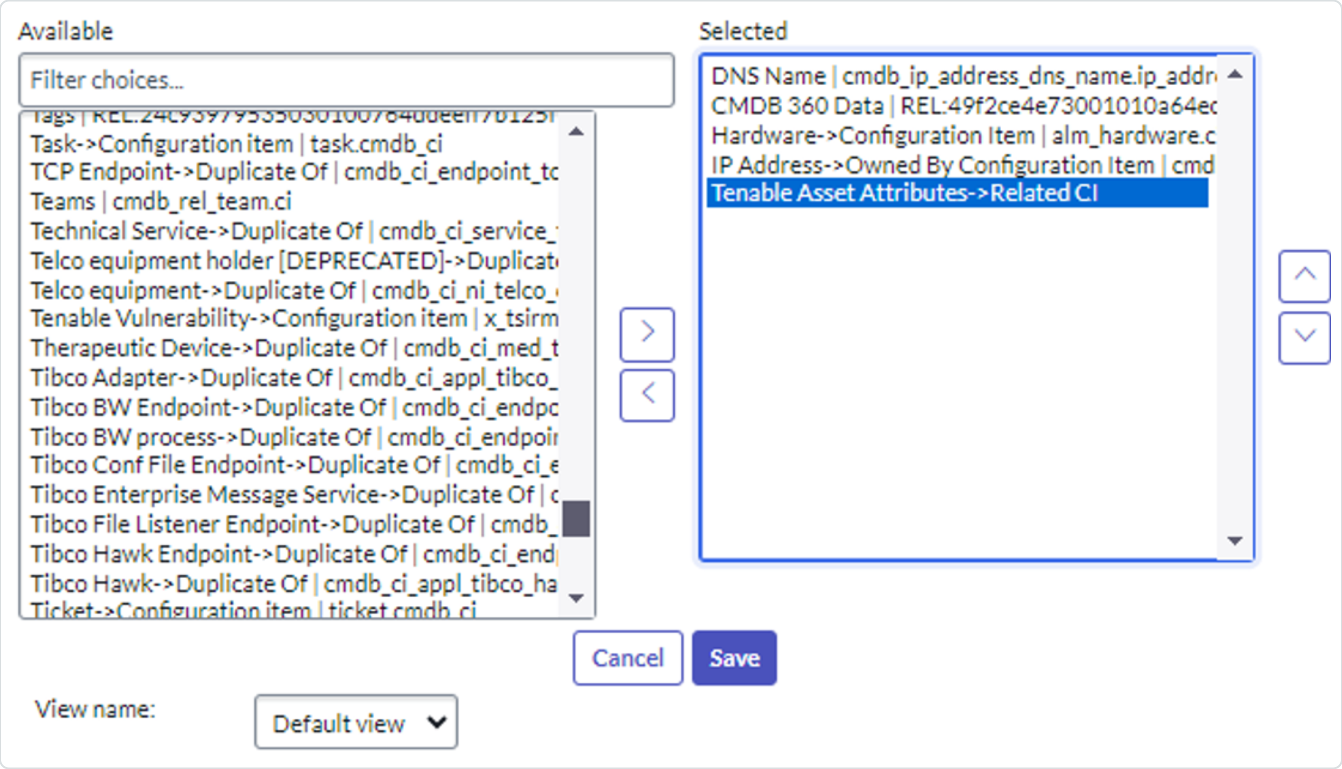
How can I see Tenable Asset Attributes in the related list of Asset records?

1. Click the **Additional Actions** button in the top-left corner of the **Asset** record.

2. Go to **Configure** > **Related Lists**.



3. Select the **Tenable Asset Attributes** option and push it to the **Selected** list.



Available

Filter choices...

Tags | REL:24c93979535030100784dd6ef7b125f
Task->Configuration item | task.cmdb_ci
TCP Endpoint->Duplicate Of | cmdb_ci_endpoint_tc
Teams | cmdb_rel_team.ci
Technical Service->Duplicate Of | cmdb_ci_service_
Telco equipment holder [DEPRECATED]->Duplicat
Telco equipment->Duplicate Of | cmdb_ci_ni_telco_
Tenable Vulnerability->Configuration item | x_tsirm
Therapeutic Device->Duplicate Of | cmdb_ci_med_t
Tibco Adapter->Duplicate Of | cmdb_ci_appl_tibco_
Tibco BW Endpoint->Duplicate Of | cmdb_ci_endpc
Tibco BW process->Duplicate Of | cmdb_ci_endpoi
Tibco Conf File Endpoint->Duplicate Of | cmdb_ci_e
Tibco Enterprise Message Service->Duplicate Of | c
Tibco File Listener Endpoint->Duplicate Of | cmdb_
Tibco Hawk Endpoint->Duplicate Of | cmdb_ci_end
Tibco Hawk->Duplicate Of | cmdb_ci_appl_tibco_ha
Ticket->Configuration item | ticket.cmdb_ci

Selected

DNS Name | cmdb_ip_address_dns_name.ip_addr
CMDB 360 Data | REL:49f2ce4e73001010a64ec
Hardware->Configuration Item | alm_hardware.c
IP Address->Owned By Configuration Item | cmd
Tenable Asset Attributes->Related CI

View name: Default view

4. Click **Save**.

5. Now you can see the **Tenable Asset Attributes** related list in the asset.

In Xanadu, why does the integration redirect to a step of another section when clicking "Mark as Complete" in the guided setup?

- This is currently a known issue in Xanadu. For more details on this issue check the ServiceNow community page.

If the existing connection records do not display on SG Connection Module Table view, after upgrading the application:

1. Navigate to **All** > **Fix Scripts**.

2. Open the fix script record titled **Tenable - Create SG Connections**.

3. Click **Run Fix Script**.

4. After execution, review the records in the **SGC Connection** table.
5. Existing records are now displayed over the **SG Connection Module**.

The Firmware Installation table is displaying duplicate entries for the same Configuration Item (CI):

- This duplication occurred because ServiceNow generates two different Source Native Keys for the same CI record, resulting in the creation of multiple entries.

While configuring a Connection record from the SGC Central module, if the process gets stuck or the page becomes unresponsive:

- Refresh the page and restart the configuration steps from the beginning.

In the Zurich release, once a user completes a Guided Setup, the configuration steps cannot be modified or restarted:

- To address this limitation, ServiceNow introduced SGC Central (post-Zurich) as a replacement for the Guided Setup. With SGC Central Workspace, users can now create and configure new connections more flexibly.
- For detailed instructions on using SGC Central, refer to SGC Central Guided Setup.