Tenable and ServiceNow Integration Guide

Last Revised: April 09, 2025

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.

Application Dependencies

- Platform compatibility:
    - Tenable Vulnerability Management, Tenable Security Center 5.7+, or Tenable OT Security
    - ServiceNow Vancouver, Washington, Xanadu
- Plugins required:
    - ITOM Discovery License - 1.0.0
    - ITOM Licensing - 1.0.0
    - CMDB CI Class Models - 1.54.0
    - Integration Commons for CMDB - 2.14.0
    - (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. Also, you can set the **Application Scope** to Service Graph Connector for Tenable from here

Steps to install the application from the ServiceNow Store:

1. Click the search filter and type "sys_scope_privilege.list."
2. Click **Enter**.
3. Click the **New** button in the top-right corner

   The Cross scope privilege New record form appears.

4. 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

5. 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**.

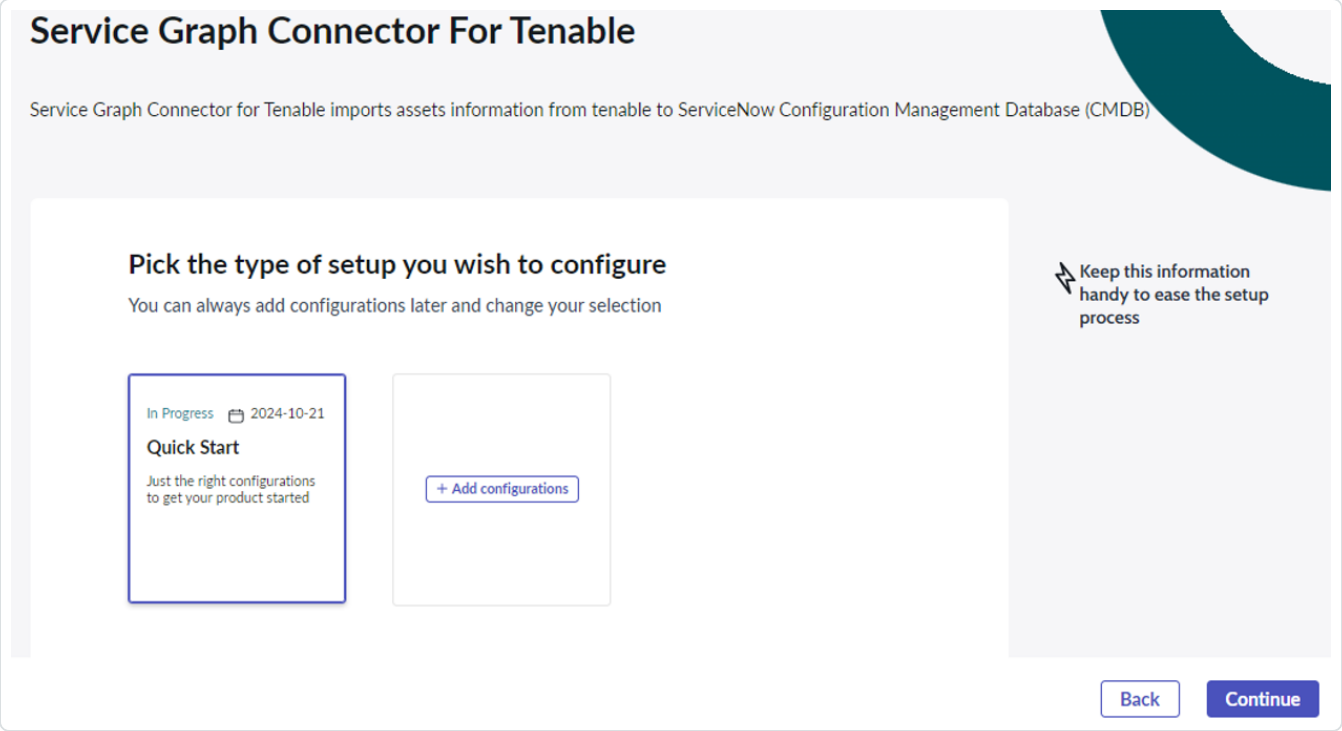
Create a Connection Alias

You can create a connection alias with a guided setup.

Required User Role: Administrator

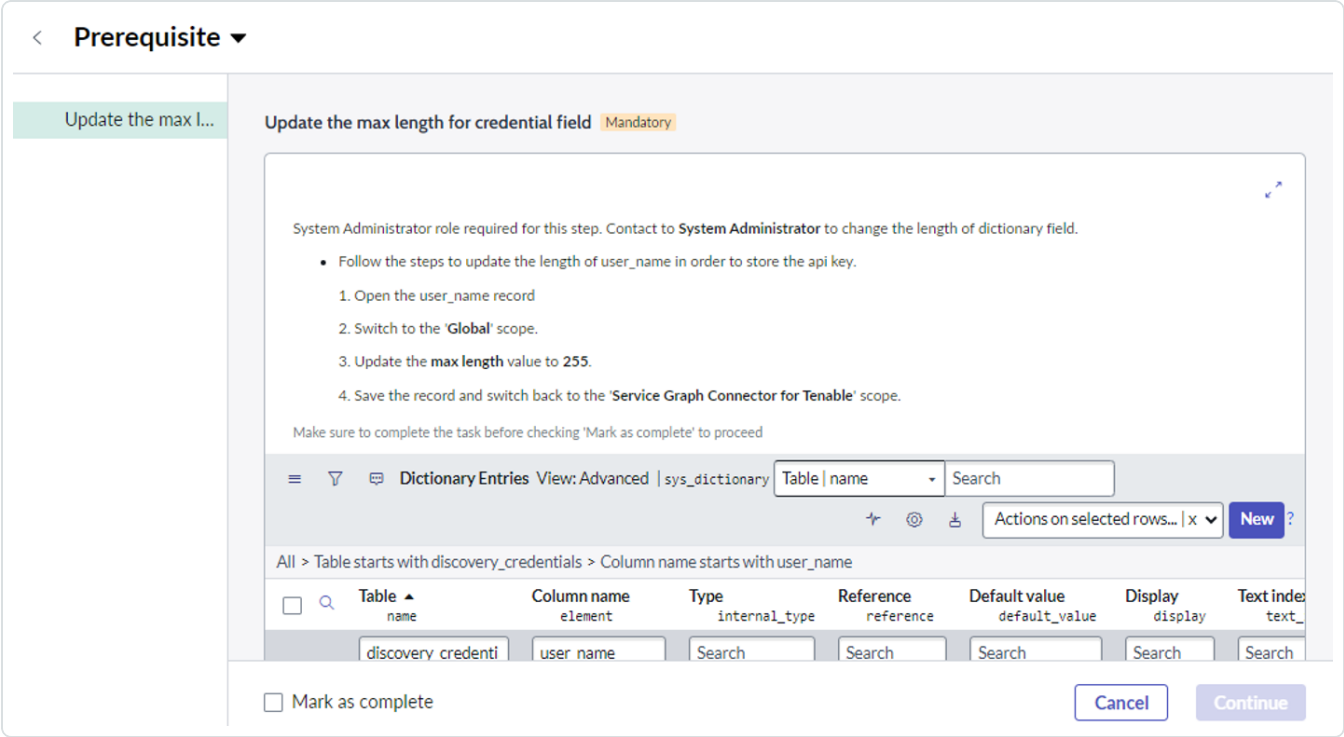
To create a connection alias:

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



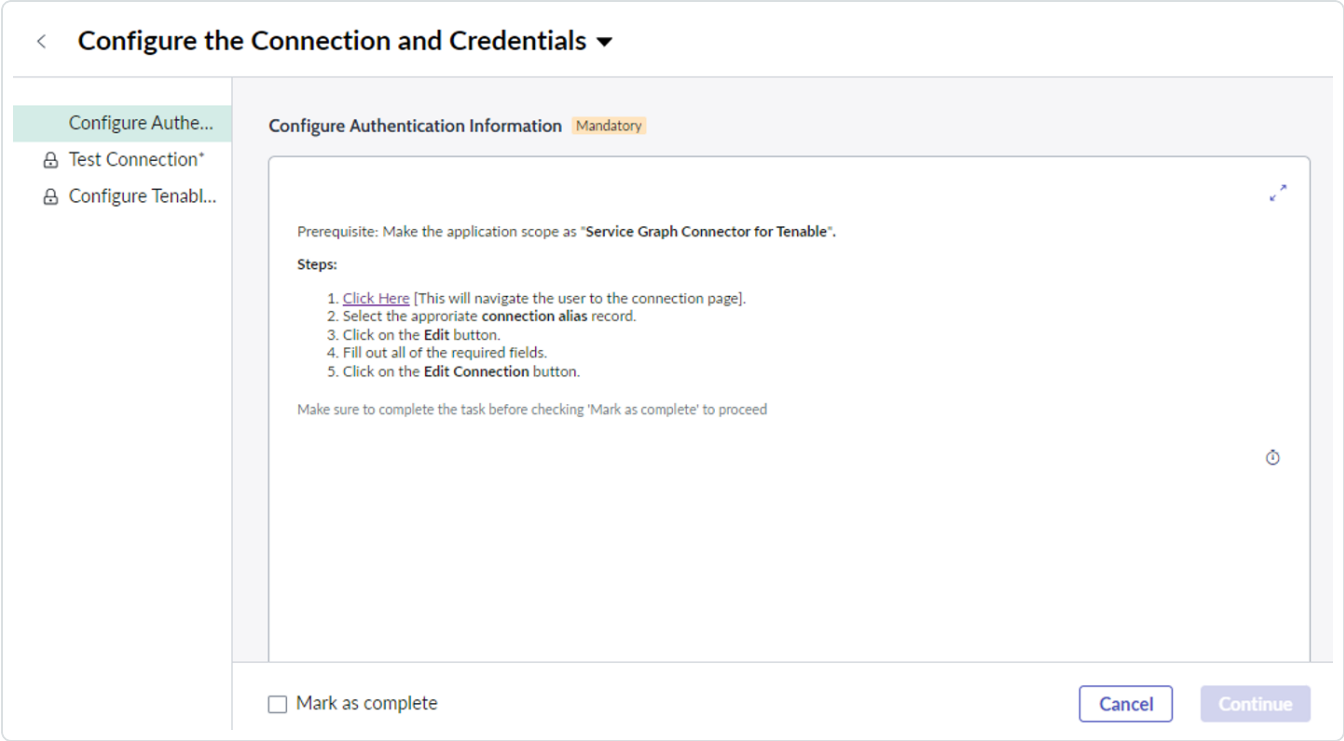
4. Click **Continue**.
5. In the **Prerequisite** page, select the **Update the max length of credential field** tab and follow the steps in the user interface.

   Note: This step of the guided setup type is mandatory.



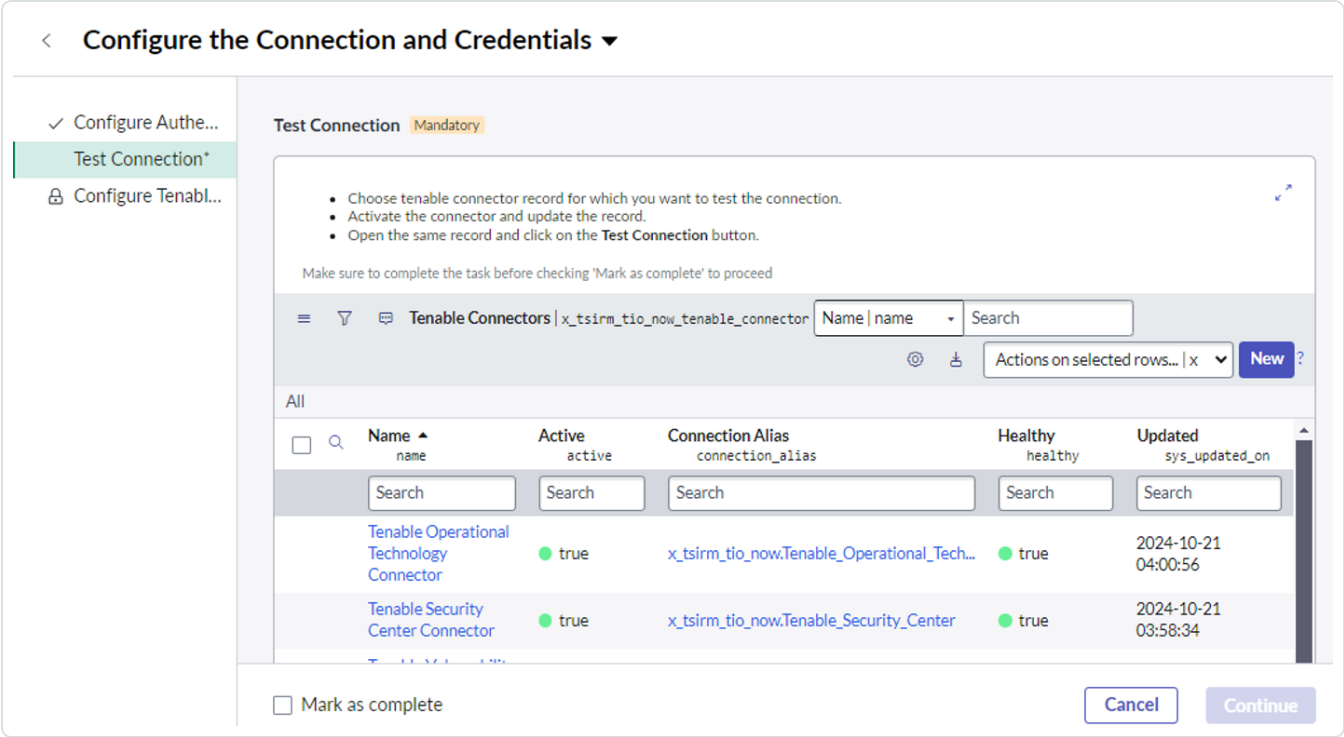
6. Check the **Mark as Complete** checkbox.
7. Click **Continue**.
8. Select the **Configure Authentication Information** tab and follow the steps in the user interface.

> **Note:** This step of the guided setup type is mandatory.

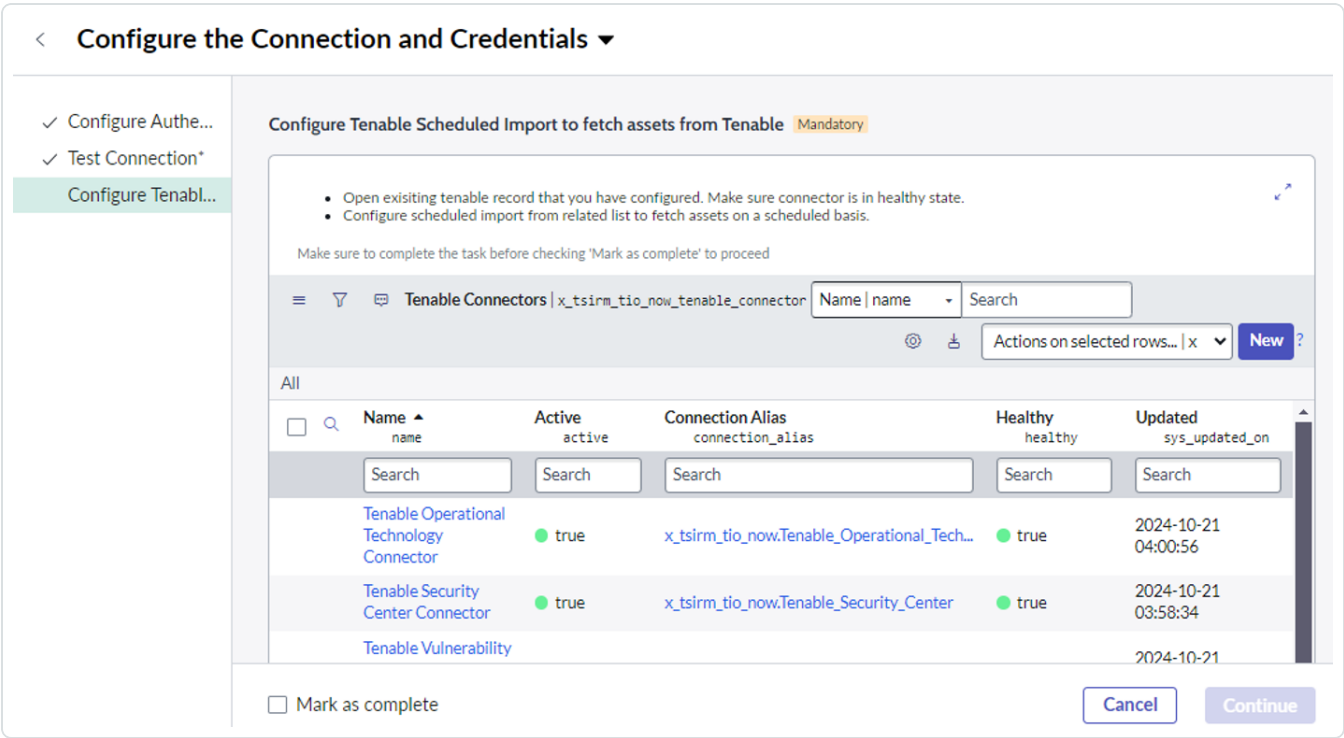


9. Check the **Mark as Complete** checkbox.
10. Click **Continue**.
11. Select the **Test Connection** tab and follow the steps in the user interface.

> **Note:** This step of the guided setup type is mandatory.



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

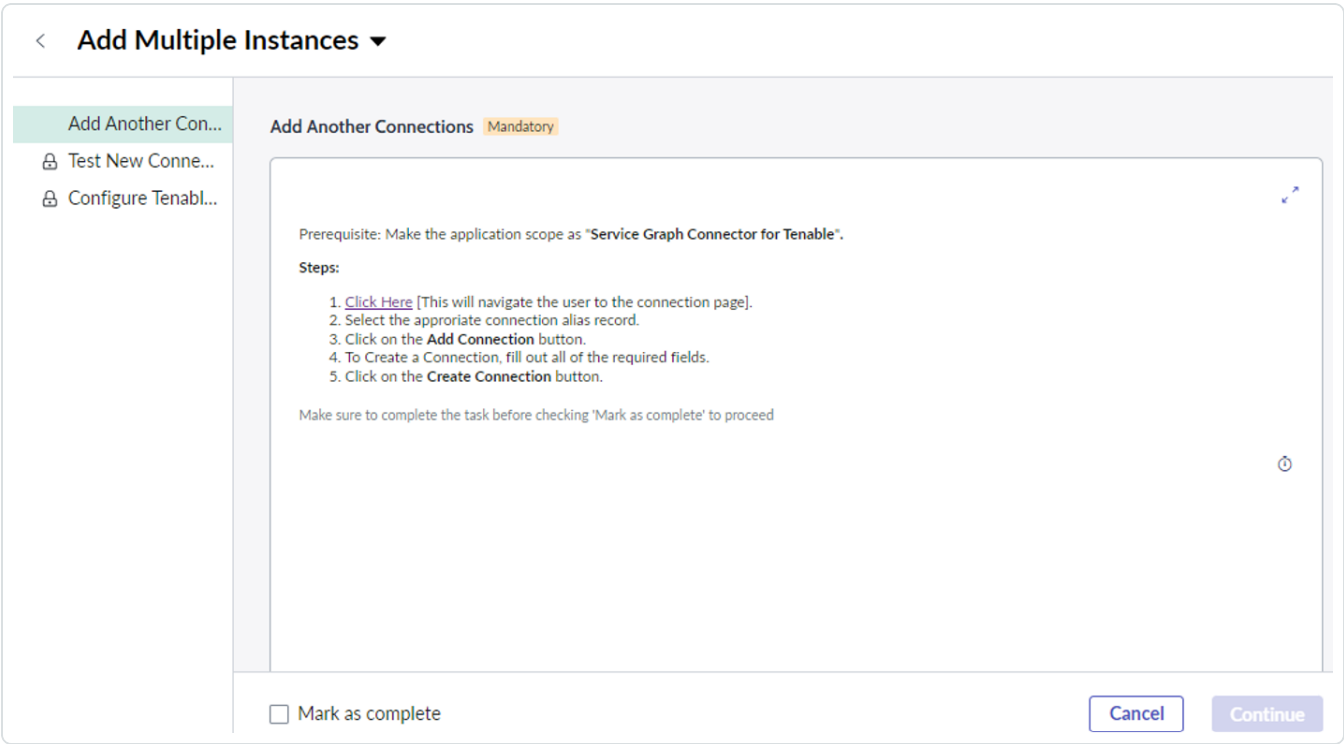


13. Check the **Mark as Complete** checkbox.

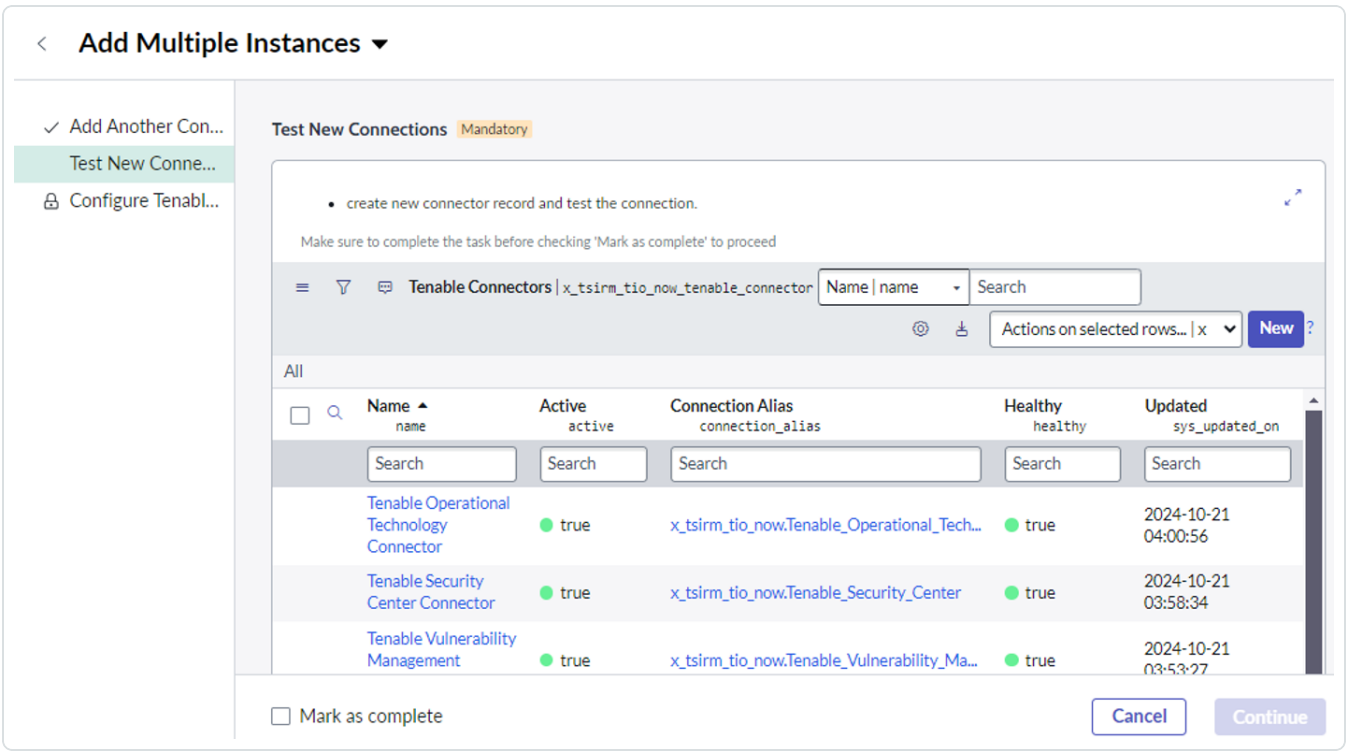
14. Click **Continue**.

Add Multiple Instances (Optional)

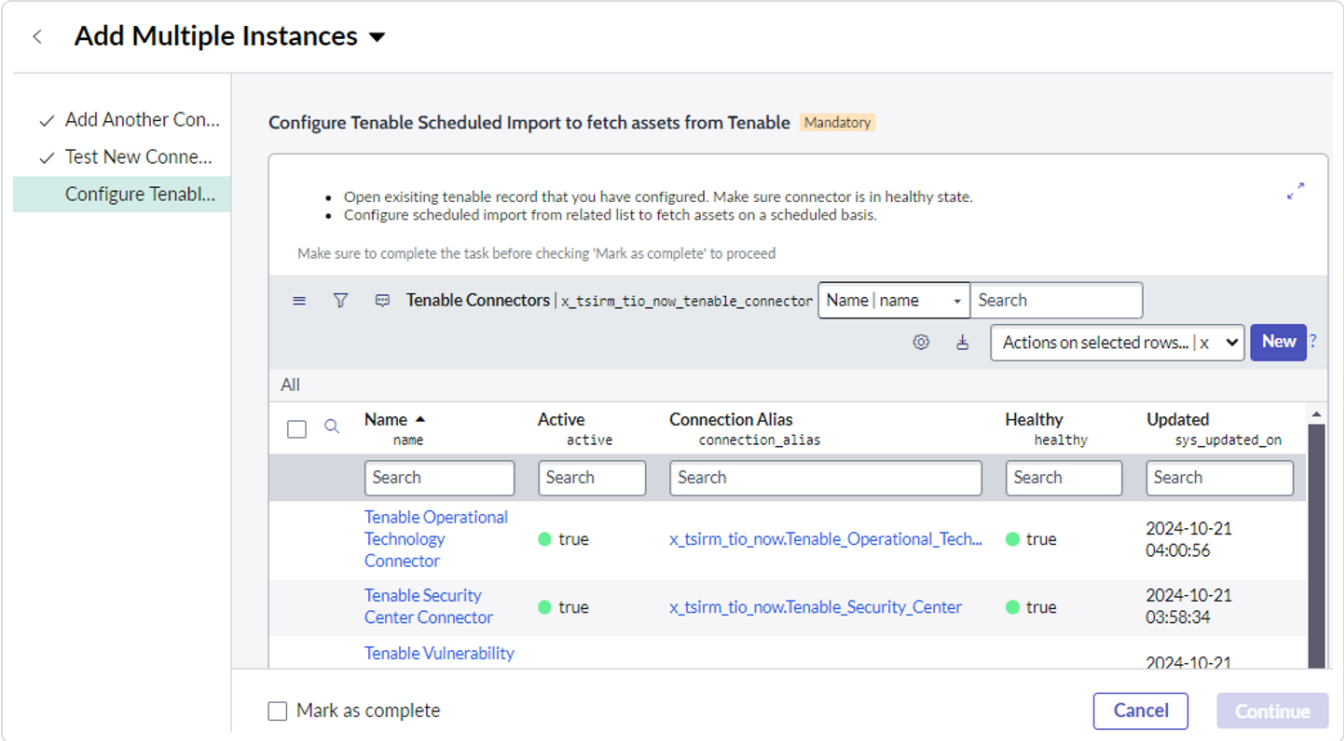
1. Navigate to **Tenable Connector for Assets** > **Add Multiple Instances**?
2. Select the **Add Another Connections** tab and follow the steps in the user interface.



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.



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.



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

10. Click **Continue**.

Create the Connector

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

Required User Role: Administrator

Connector Configuration Options Matrix

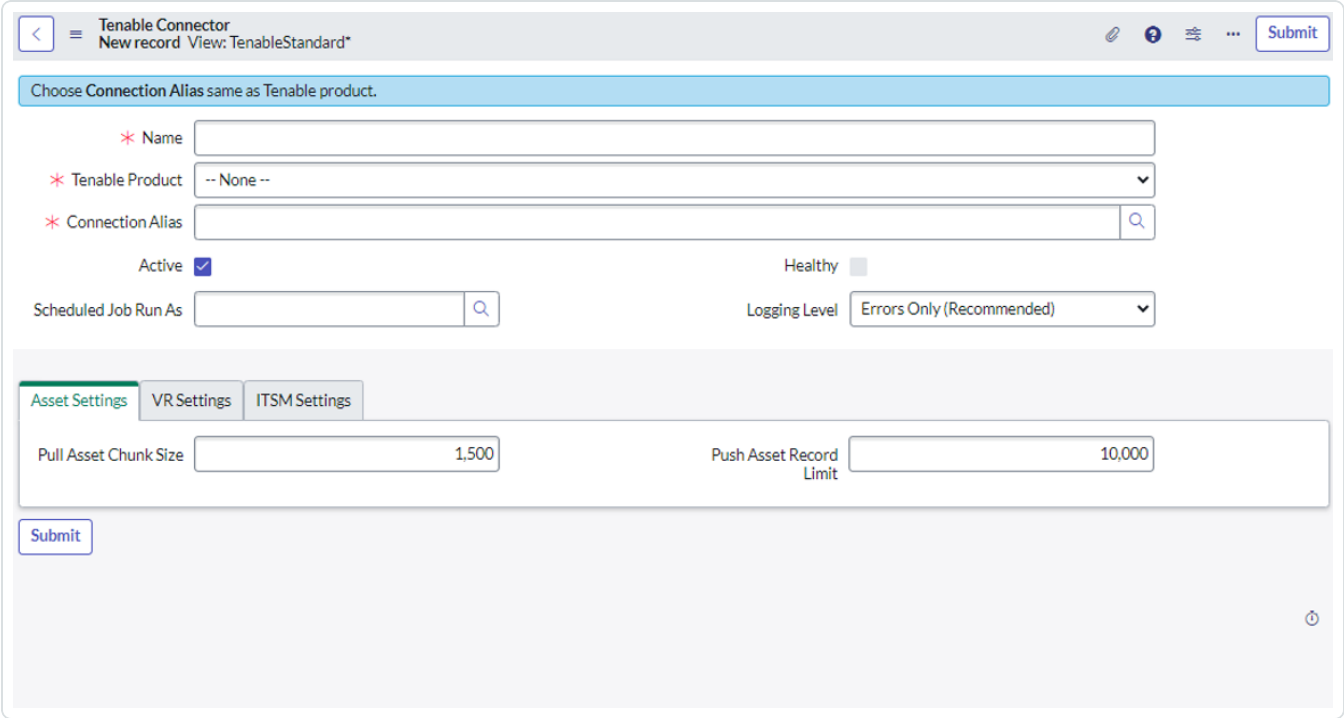
Tenable Product	Module	Job Type
Tenable OT Security (ICP)	Asset	Pull Assets
	VR	Pull Plugins Pull Vulnerabilities
Tenable Security Center	Asset	Pull Assets Push Assets
	ITSM	Pull Vulnerabilities
	SGC for Tenable	Pull Queries
Tenable Vulnerability Management	Asset	Pull Assets Push Assets
	ITSM	Pull Vulnerabilities

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:



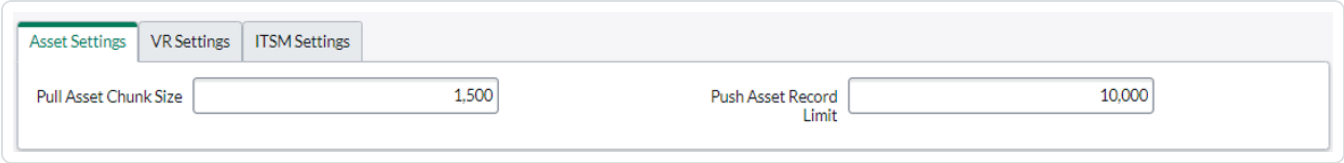
4. In the **Name** field, type the name of the connector.
5. From the **Tenable Product** drop-down box, select **Tenable Vulnerability Management**, **Tenable Security Center**, or **Tenable OT Security (ICP)**.
6. Choose the **Connection Alias** for the selected **Tenable Product**.
7. Continue to 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.

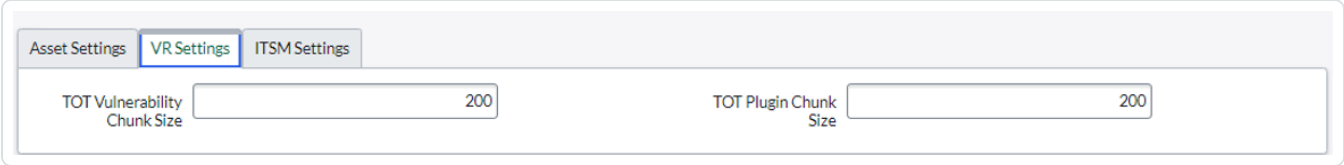
5. (Optional) In the **Asset Settings** tab:



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

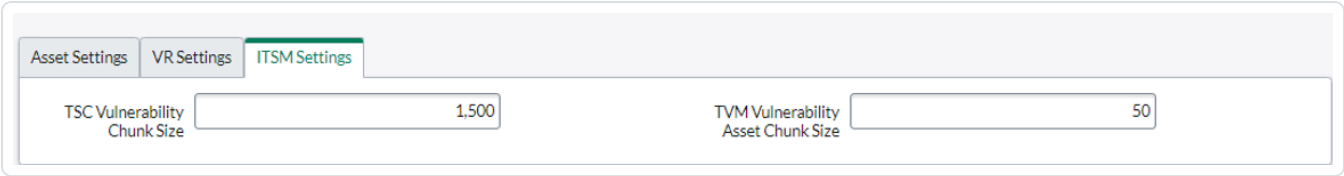
Note: The **VR Settings** and **ITSM Settings** tabs are visible only if plugins are activated.

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



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:



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. In Tenable Vulnerability Management, **Group** is created with the name that you entered when creating the **Schedule Job** task.

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 - Historical	The amount of time (in days) of how far back you want to pull data.	Within the last 365 days

Data		
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.

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 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 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 End. • **Repeat Interval/Time:** Set the time (hh/mm/ss) to run the import. This differs based on the **Run**	If selected, **Daily** is the default value.

	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?

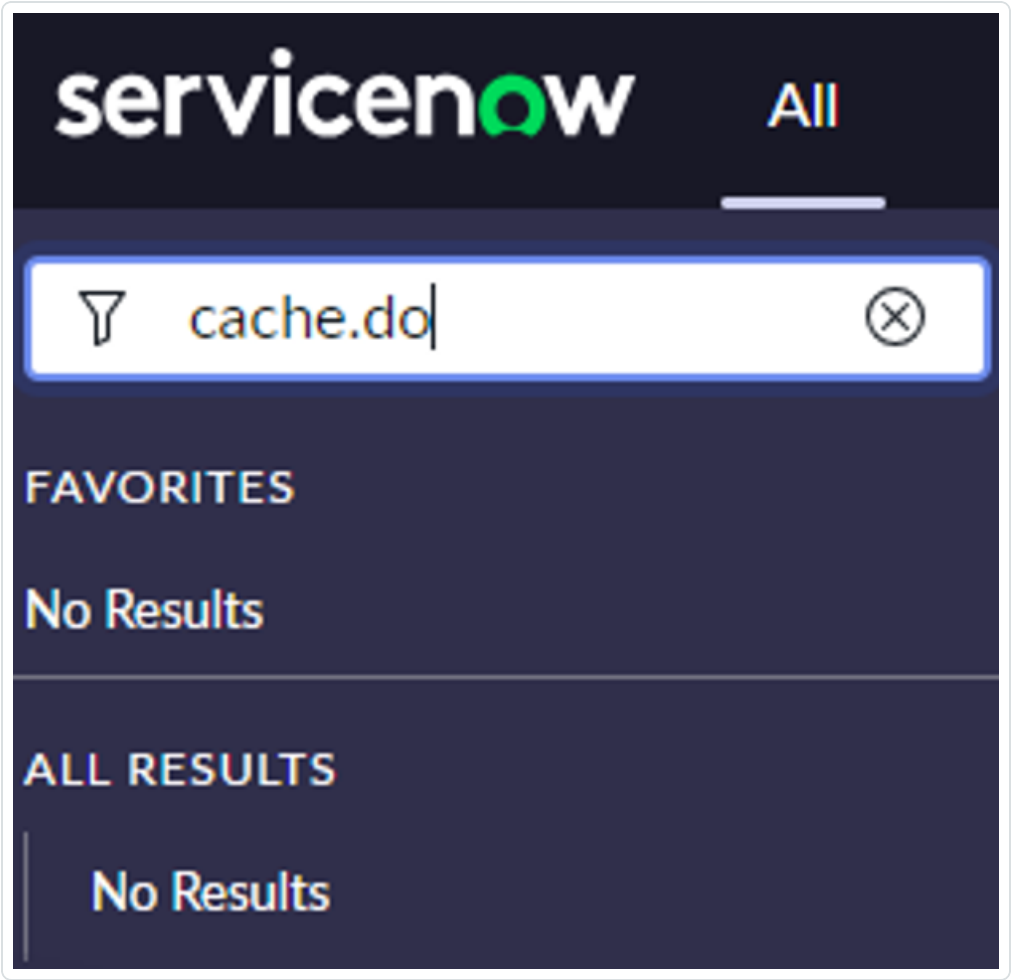
1. Verify you have the system administrator (admin) role or Application Admin role.

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.



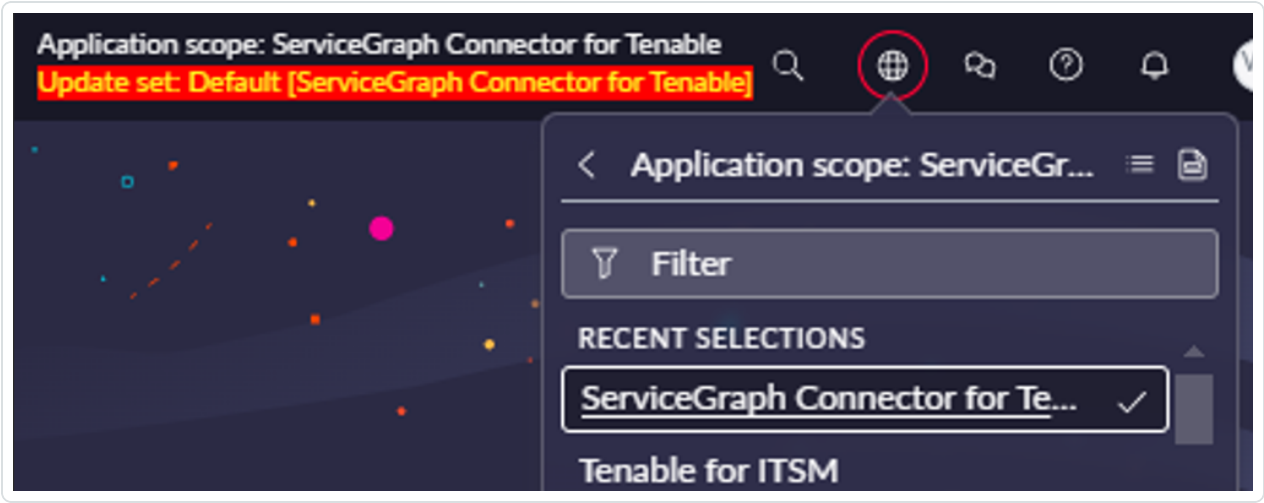
    c. Click **Enter**

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

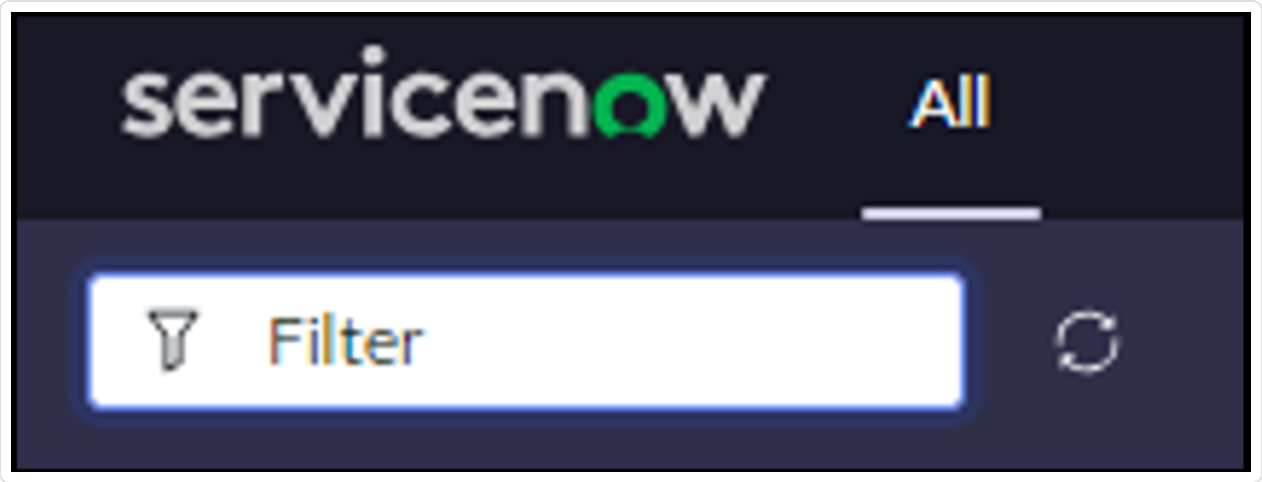
Why are Jobs not created after executing the scheduled job?

1. Create missing cross scope privilege records manually:

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

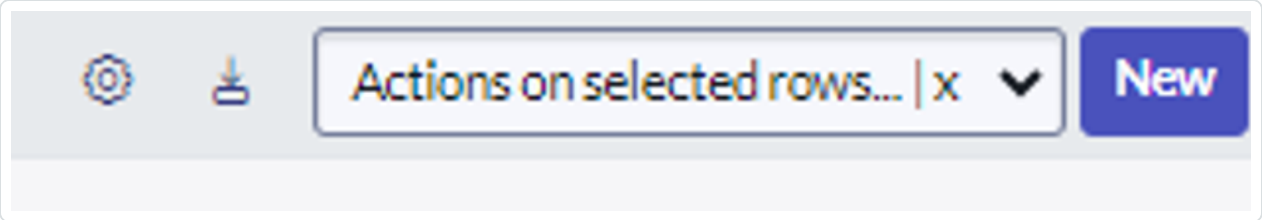


   b. Click **Filter** and type "sys_scope_privilege.list".

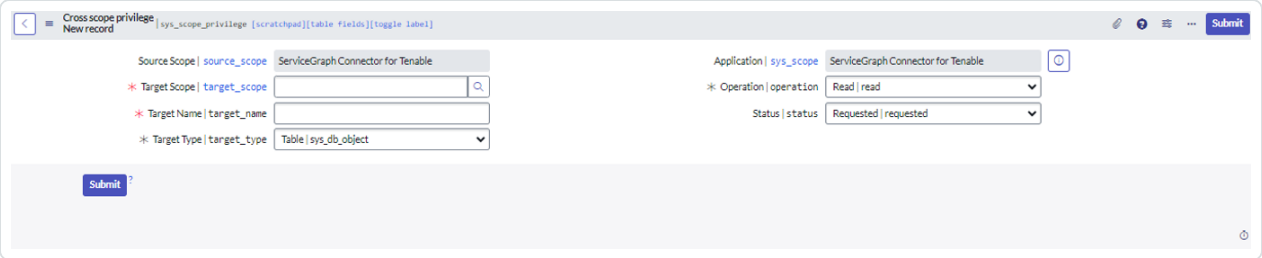


c. Click **Enter**

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



The form below appears:



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.

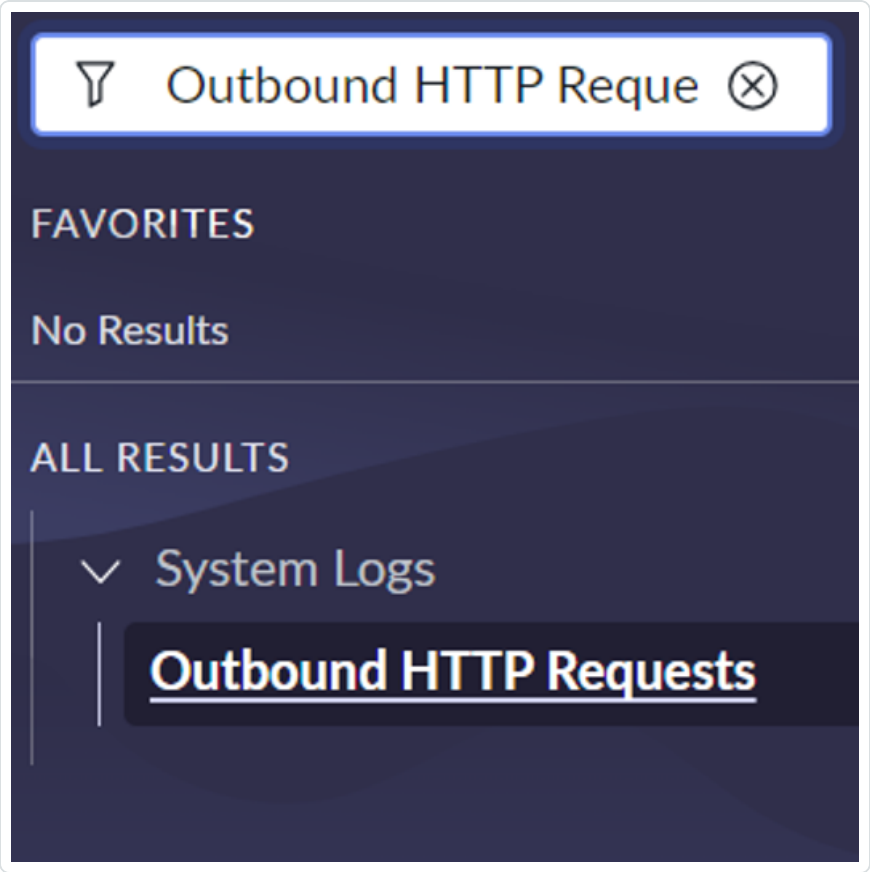
Why is the integration failing and/or data not being ingested into the table?

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.

How can I increase the file size?

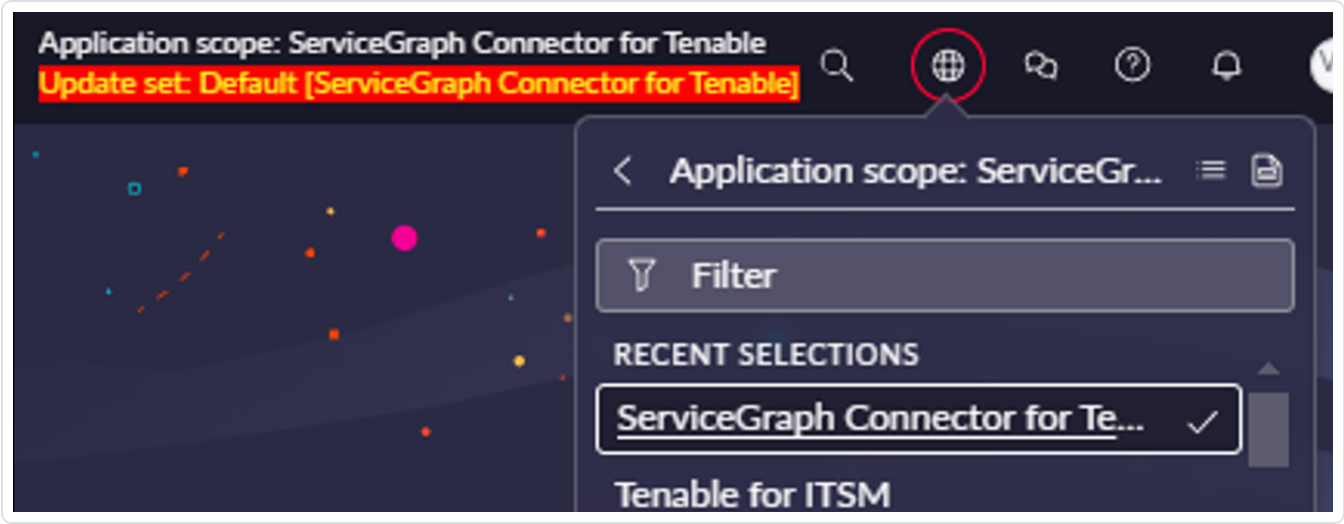
1. Verify you have the system administrator (admin) role.
2. Navigate to **sys_properties**.
3. Increase the value (in bytes) of the `com.glide.attachment.max_get_size` (for example, 31457280) and `com.glide.attachment.max_size` (for example, 4096).

Why am I unable to validate the MID server?

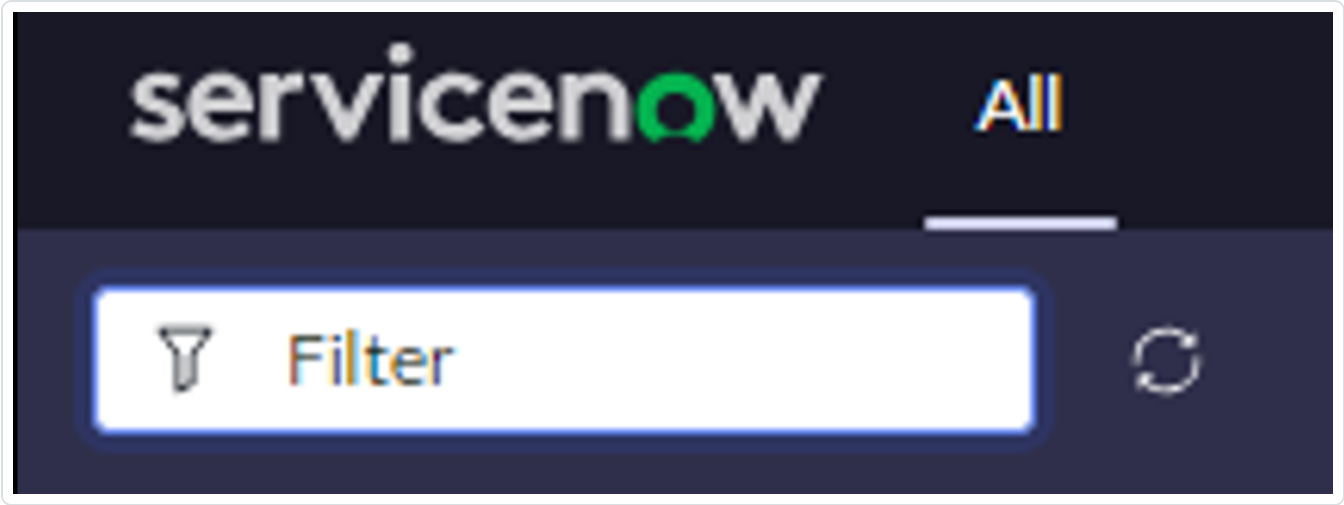
1. Navigate to **MID Server** > **MID Security Policy**.
2. Open **Intranet and Internet Records** and uncheck **Certificate Chain Check** , **Hostname Check** and **Revocation Check** checkboxes.

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

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



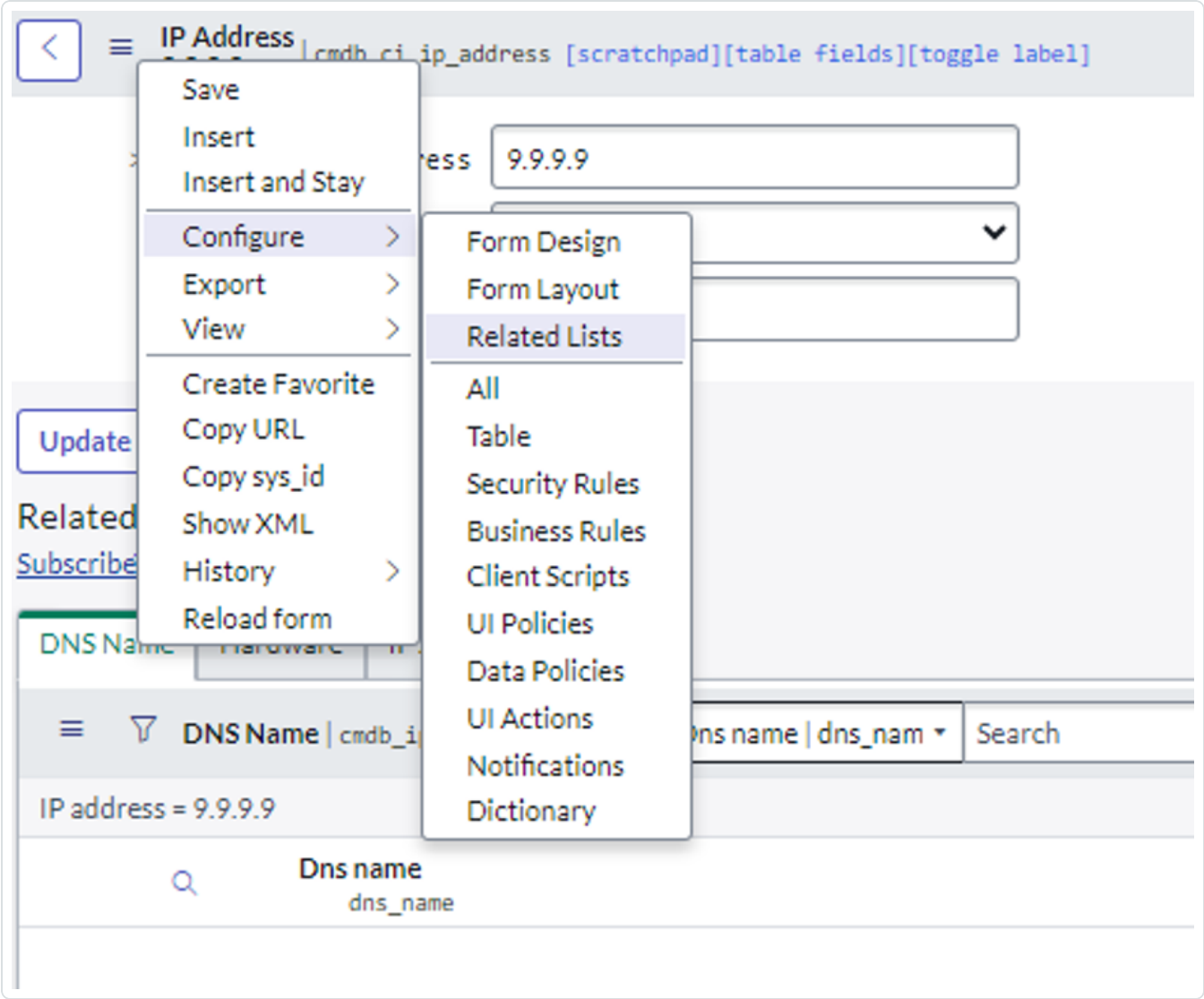
2. Click **Filter**.



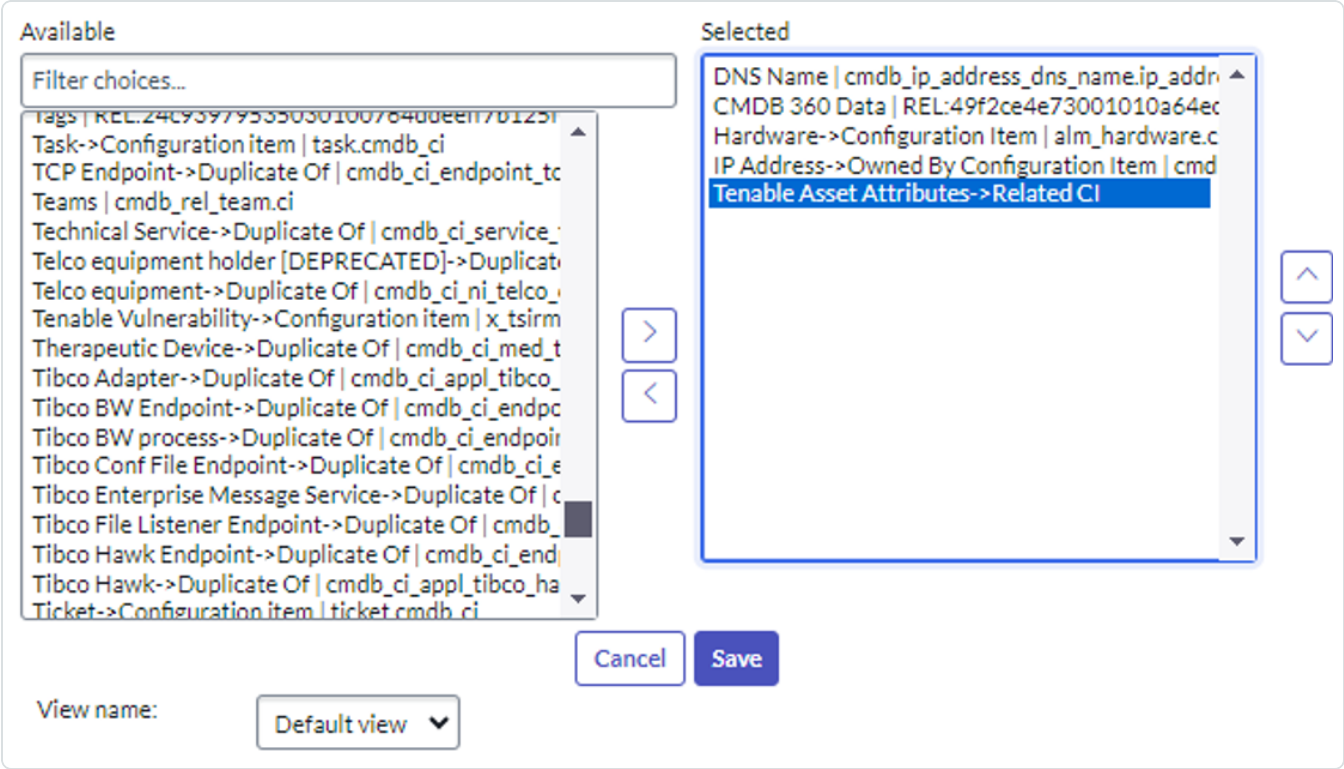
3. Type "x_tsirm_tio_now_data_source_registry.list".
4. Click **Enter**.
5. After applying the appropriate filters, in the **Active** column set the value of that record.

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.



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.