Tenable and ServiceNow Integration Guide

Last Revised: April 09, 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	
Application Dependencies	
Application Installation	
Post-Installation	5
Upgrade from 5.x Version Apps	
User Setup	
User Permissions For Non-Domain Separated Instances	
Create a User	
User Permissions For Non-Domain Separated Instances	
Create a Connection Alias	
Create the Connector	
Connector Configuration Options Matrix	
Configure Tenable Vulnerability Management	
Configure Tenable Security Center	
Configure Tenable OT Security	
Test the Configuration	
FAQ	

- Ø

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

- Ø _____

• (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	TenableITSMScheduleHel per	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 following 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 following 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	canvas_user	Read access of	This user-role is
	Application User	cmdb_inst_admin	configuration	limited to read-
		x_tsirm_tio_itsm.user	Read access to	only
		x_tsirm_tio_now.user	Connectors, scheduled	configurations.
		x_tsirm_tio_vr.user	jobs	These users are
			Support	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

	(<u>_</u>	
			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 <u>User Permissions For Domain</u> 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 Man	agement Database (CMDB)
Pick the type of setup you wish to configure	🔥 Keep this information
You can always add configurations later and change your selection	 handy to ease the setup process
In Progress ## 2024-10-21	
Quick Start	
Just the right configurations to get your product started + Add configurations	
	Back

- 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.



< Prerequisite	↓
Update the max I	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
	→ ③ 占 Actions on selected rows x v New ?
	All > Table starts with discovery credentials > Column name starts with user name
	☐ ☐ Table ▲ Column name Type Reference Default value Display Text index
	name element internal_type reference default_value display text_
	discovery credenti user name Search Search Search Search Search Search
	Mark as complete Continue

ł

- 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.

< Configure the	e Connection and Credentials 👻	
Configure Authe A Test Connection*	Configure Authentication Information Mandatory	
A Configure Tenabl	Prerequisite: Make the application scope as "Service Graph Connector for Tenable". Steps: 1. <u>Click Here</u> [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	2
		0
	Mark as complete Cancel Co	intinue

- 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.

< Configure the	e Connection and Crede	entials 🔻			
✓ Configure Authe	Test Connection Mandatory				
Test Connection*					
요 Configure Tenabl	Choose tenable connector Activate the connector and Open the same record and Make sure to complete the task before	record for which y d update the record click on the Test (re checking 'Mark a ctors x_tsirm_ti	rou want to test the connection. d. Connection button. s complete' to proceed o_now_tenable_connector Name name + Se	earch	~
				Actions on selec	ted rows Ix Y New
	A11		© _	/ caons on serve	
	All ∧ame ▲	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
	T 11 V/1 199				
	Mark as complete				Cancel Continu

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

✓ Configure Authe	Configure	Tenable Scheduled In	nport to fetch a	ssets from Tenable Mandatory			
✓ Test Connection*	compute	Tenuble beneduled in	iport to reterra	Social remarker manadery			
Configure Tenabl	abl 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						
	= 7	👳 Tenable Connec	tors x_tsirm_tic	o_now_tenable_connector Name name - Se	arch		
				 ≥ ± (Actions on selec	cted rows x 🗸 New	
	All			,			
	<u> </u>	Name A	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	

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.

0

< Add Multiple	Instances 🗸	
Add Another Con	Add Another Connections Mandatory	
A Configure Tenabl	Prerequisite: Make the application scope as "Service Graph Connector for Tenable". Steps: 1. <u>Click Here</u> [This will navigate the user to the connection page]. 2. Select the approvate connection alias record. 3. Click on the Add Connection button. 4. To Create a Connection, fill out all of the required fields. 5. Click on the Create Connection button. Make sure to complete the task before checking 'Mark as complete' to proceed	
	•	
	Mark as complete Continu	е

- 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	Instance	s v				
✓ Add Another Con	Test New	Connections Mandatory	1			
Test New Conne						
🔒 Configure Tenabl	• (reate new connector recor	rd and test the conn	ection.		
	Make su	re to complete the task befor	re checking 'Mark as o	complete' to proceed		
	= 77	Tenable Connect	tors x tsirm tio	now tenable connector Name name * S	earch	
				© *	Actions on selec	ted rows x 🗸
	All					
		Name A	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	e true	x tsirm tio nowTenable Vulnerability Ma	e true	2024-10-21

- 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	Configure Ten	able Scheduled In	nport to fetch as	ssets from Tenable Mandatory		
Configure Tenabl	Oper Confi	n exisiting tenable reco igure scheduled impor	ord that you have co	onfigured. Make sure connector is in healthy state. o fetch assets on a scheduled basis.		
	Make sure to	complete the task befo	re checking 'Mark as	complete' to proceed		
		👳 Tenable Connec	tors x_tsirm_tio	_now_tenable_connector Name name -	Search	
				<u></u> لا ھ	Actions on sele	ected rows x 🗸 Ne
	All	2me 🔺	Active	© ±	Actions on sele	Lindated
	All	ame ▲ name	Active active	Connection Alias	Actions on sele	Updated sys_updated_on
	All	ame Aname Search	Active active Search	© definition Alias Connection Alias Connection_alias	Actions on sele Healthy healthy Search	Updated sys_updated_on Search
	All N	ame Aname Search enable Operational echnology onnector	Active active Search • true	© ± Connection Alias connection_alias Search x_tsirm_tio_now.Tenable_Operational_Tech.	Actions on sele Healthy healthy Search	Updated sys_updated_on Search 2024-10-21 04:00:56
		ame Aname Search enable Operational echnology onnector enable Security enter Connector	Active active Search • true • true	Image: Connection Alias connection_alias Connection_alias Search x_tsirm_tio_now.Tenable_Operational_Tech. x_tsirm_tio_now.Tenable_Security_Center	Actions on sele Healthy healthy Search • true • true	Updated sys_updated_on Search 2024-10-21 04:00:56 2024-10-21 03:58:34

1

- 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	Asset	Pull Assets
Security (ICP)	VR	Pull Plugins Pull Vulnerabilities
Tenable Security Center	Asset	Pull Assets Push Assets
	ITSM	Pull Vulnerabilities
	SGC for Tenable	Pull Queries
Tenable Vulnerability	Asset	Pull Assets Push Assets
Management	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 Conn New record \	ector /iew: TenableStandard*	Ø	0	**	··· Sub	bmit
Choose Connection Alia	s same as Tenable product.					
★ Name						
* Tenable Product	None		•			
* Connection Alias		0				
Active	- Healthy					
Scheduled Job Run As	Q Logging Level Errors Only (Recommended)	•	•			
Asset Settings VR Se Pull Asset Chunk Size	ITSM Settings 1,500 Push Asset Record Limit	10,00	0			
Submit						Ō

- 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.
- (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:

		Q	
Asset Settings VR Settings ITSM Settings			
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:

Asset Settings VR Settings ITSM Settings			
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:

Asset Settings VR Settings ITSM Settings			
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.

0

8. Click Submit.

Next steps:

- <u>Configure Tenable Vulnerability Management</u>.
- 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:	If selected, Daily is the default
	Note: Make sure not to set the run frequency too high, as this can result in congested jobs and create performance issues.	value.
	• 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.	

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:	lf enabled, Daily is the default
	Note: Make sure not to set the run frequency too high, as this can result in congested jobs and create performance issues.	value.
	• 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.	

- 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.
- 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

Ø				
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**.

- Ø ------

8. Click **Submit**.

Next steps:

• Go to <u>Test Configuration</u>.

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.

0

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,	lf enabled, Daily is the default value.
	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. 	

 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.

 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.

- 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:	lf selected, Daily is the default
	Note: Make sure not to set the run frequency too high, as this can result in congested jobs and create performance issues.	value.
	• 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.	

ð

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 <u>Test Configuration</u>.

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:	If selected, Daily is the default
	Note: Make sure not to set the run frequency too high, as this can result in congested jobs and create performance issues.	value.
	• 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.	

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.	N/A		
	Note: This field is for the Fixed job mode.			
Run Fixed Query on Initial Run	Run Fixed Pulls fixed vulnerabilities on the first import. Query on Initial Run			
Edit Run Schedule	Select this box if you want to configure the scheduled job run configuration. The following options must be configured:	lf selected, Daily is the default		
	Note: Make sure not to set the run frequency too high, as this can result in congested jobs and create performance issues.	value.		
	• 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.			

O

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.	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:	lf selected, Daily is the default
	Note: Make sure not to set the run frequency too high, as this can result in congested jobs and create performance issues.	value.
	• 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	

- Ø -

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 <u>Test Configuration</u>.

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 <u>MID server</u> section in the ServiceNow documentation.
- Ensure your system meets the MID server system requirements, as described in the <u>MID</u> <u>Server System requirements</u> 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 <u>User Administration.</u>

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?

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

0 -

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.

servicenow	All				
	\otimes				
FAVORITES No Results					
ALL RESULTS No Results					

c. Click Enter

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

	<u>Clear Cache</u>
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:



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



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

© ±		Actions on selected rows x		New

The form below appears:

Cross scope privilege sys_scope_privilege [scr	atchpad][table fields][toggle label]			6	0	**	··· Submit
Source Scope source_scope * Target Scope target_scope * Target Name target_name * Target Nyne target_type	ServiceGraph Connector for Tenable Q Table sys_db_object	Application sys_scope *: Operation operation Status status	ServiceGraph Connector for Tenable Read read Requested requested				
Submit ²							٥

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	oleITSMHelper Script Include		Allowed
3	Tenable for ITSM	TenableITSM	Script Include	Execute API	Allowed
4	Tenable for ITSM	TenableITSMScheduleH elper	Script Include	Execute API	Allowed
5	Tenable.o t for VR	TenableVRScheduleHelp er	Script Include	Execute API	Allowed
6	Tenable.o t 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.
- Make sure the user has proper roles. Refer to <u>this</u> 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"

- Ø _____

- 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.

7	Outbound HTTP Reque ⊗			
FAVORITES				
No Re	sults			
ALL RESULTS				
\sim	System Logs			
Outbound HTTP Requests				

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**.
- 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:

Application scope: ServiceGraph Connector for Tenable Update set: Default [ServiceGraph Connector for Tenable] Q P Q P Q P						
	< Application scope: ServiceGr =					
•	RECENT SELECTIONS					

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**.

< =	IP Address cmdb.ci.	ip_address [scratchpa	ad][table fields][toggle label]
2	Insert Insert and Stay	ess 9.9.9.9	
	Configure >	Form Design	~
	Export >	Form Layout	
	View >	Related Lists	
	Create Favorite	All	
Update	Copy URL	Table	
	Copy sys_id	Security Rules	
Related	Show XML	Business Rules	
<u>Subscribe</u>	History >	Client Scripts	
DNISNIA	Reload form	UI Policies	
DINS Name Haroware II.		Data Policies	
= 7	DNS Name cmdb_i	UI Actions	ons name dns_nam * Search
		Notifications	
IP address	s = 9.9.9.9	Dictionary	
	Q Dns name dns_n	ame	

O

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

vailable	Selected
Filter choices Tags REC.24C9397953503010076400een701251 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]->Duplicate Telco equipment->Duplicate Of cmdb_ci_ni_telco_? Tenable Vulnerability->Configuration item x_tsirm Therapeutic Device->Duplicate Of cmdb_ci_endpc Tibco Adapter->Duplicate Of cmdb_ci_endpc Tibco BW Endpoint->Duplicate Of cmdb_ci_endpc Tibco Conf File Endpoint->Duplicate Of cmdb_ci_endpc Tibco File Listener Endpoint->Duplicate Of cmdb_ci_endpc Tibco File Listener Endpoint->Duplicate Of cmdb_ci_endpc Tibco Hawk Endpoint->Duplicate Of cmdb_ci_endpc Tibco Hawk->Duplicate Of cmdb_ci_appl_tibco_ha Tibco Hawk->Duplicate Of cmdb_ci_appl_tibco_ha Tibco Hawk->Duplicate Of cmdb_ci_endpc Tibco Hawk->Duplicate Of cmdb_ci_appl_tibco_ha Tibco Hawk->Duplicate Of cmdb_ci_appl_tibco_ha	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
Cance	Save

- 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.