

Integrate your Tenable.io and Tenable.sc with ServiceNow Vulnerability Response

Reduce your cyber risk by prioritizing and responding to vulnerabilities fast

What's in this Success Playbook

By installing the Tenable™ for Vulnerability Response application into your ServiceNow® instance, you can import your vulnerability data and act on it directly within ServiceNow to reduce your overall attack surface. This Success Playbook will help you get started on your vulnerability management journey with ServiceNow by:

- Outlining what's required prior to installing the Tenable application into your ServiceNow instance
- Walking you through the steps to integrate Tenable.io and/or Tenable.sc with ServiceNow
- Offering guidance on how to properly configure the Tenable application

Key takeaways

The most important things to know

- When your Tenable product is integrated with your ServiceNow instance, you can pull data from the scanner into Vulnerability Response, publish entries in the ServiceNow third-party vulnerability table, prioritize vulnerable items based on business criticality, and assign tasks to IT workers from one console.
- When items are closed in Vulnerability Response, the workflow can automatically initiate a rescan to ensure the patch was applied successfully and the vulnerability was mitigated.
- Tenable.sc or Tenable.io are needed in order to import vulnerability scan data from your Tenable installation into ServiceNow Vulnerability Response.

The payoff of getting this right

Effectively integrating Tenable.io and Tenable.sc will help you prioritize and respond to vulnerabilities faster.

What you need to get started

Prerequisites

You need [ServiceNow Vulnerability Response](#) (either standalone or as part of [Security Operations Professional or Enterprise](#)) running Madrid Patch 4, Tenable.sc v5.7 or later—or Tenable.io, Tenable for Assets v2.5, and Tenable Connector v2.5.

If you need more information, you can look at the detailed installation and configuration information about [Tenable for Assets and the Tenable Connector](#) or our step-by-step guidance for implementing Vulnerability Response on the [Customer Success Center](#).

Playbook overview

Follow these stages to start prioritizing and responding to vulnerabilities fast:

Stage 1 – Configure MID Server and Tenable (specific to Tenable.sc)

Stage 2 – Download and install the app

Stage 3 – Configure the app

Stage 1 – Configure MID Server and Tenable

Configure your MID Server so Tenable.sc can communicate with ServiceNow.

KEY INSIGHTS

- The MID Server lets on-premises installations of Tenable.sc talk to ServiceNow without firewall rules.
- Create queries to send the most relevant vulnerabilities to Vulnerability Response.
- Configure a query for high- and critical-risk vulnerabilities.

A MID Server is not required if you are using Tenable.io. If you are using Tenable.sc, a MID server allows your ServiceNow cloud instance to execute commands in your enterprise IT environment once it's configured. In this case, it allows your on-premises Tenable.sc to communicate with your ServiceNow instance without having to create special firewall rules.

Take a look at Figure 1 to see how Tenable.sc integrates with ServiceNow.

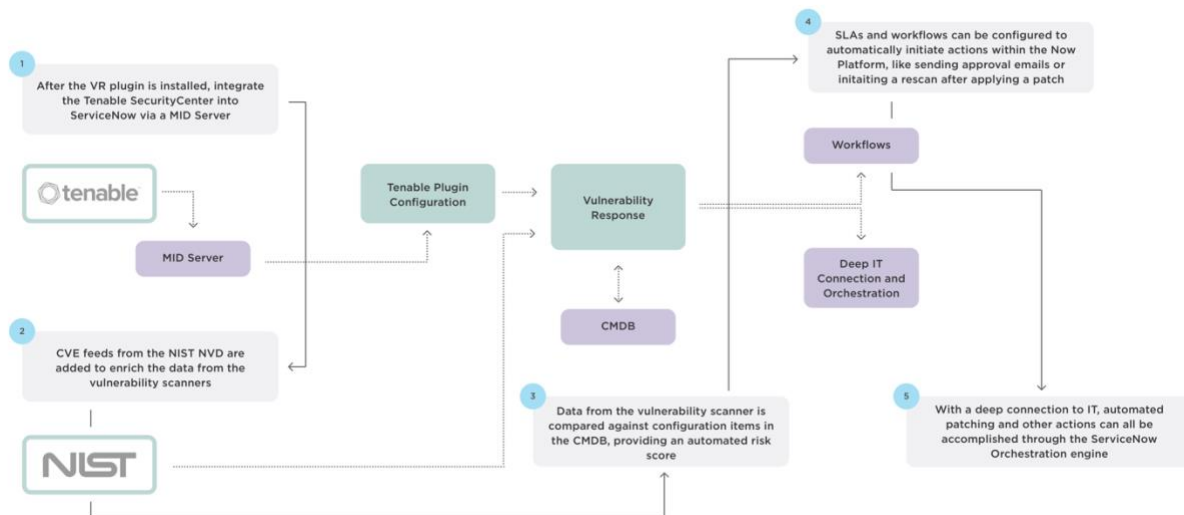
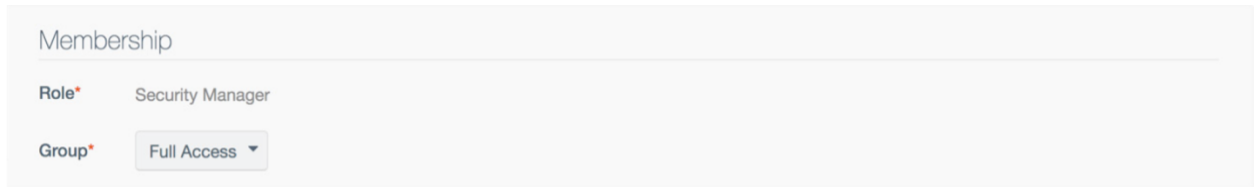


Figure 1: The architecture of the integration of the Tenable.sc with ServiceNow

Step 1: Configure a Tenable.sc account to use with ServiceNow

1. From the **Users** drop-down list, select **New**.
2. Click **+Add** to create a new user account.
3. Fill in the fields with the relevant information.

4. From the **Role** drop-down list under **Membership**, select **Security Manager**.
5. From the **Group** drop-down list, select **Full Access**.



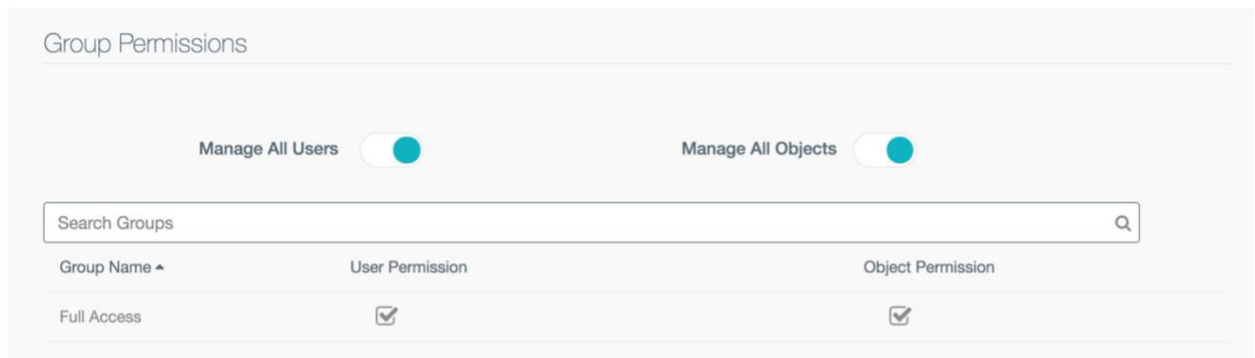
Membership

Role* Security Manager

Group* Full Access

Figure 2: Membership **Role** and **Group** selections

6. Under **Group Permissions**, enable **Manage All Users** and **Manage All Objects** and select the **Full Access** check boxes under **User Permission** and **Object Permission**.



Group Permissions

Manage All Users ☒ Manage All Objects ☒

Search Groups

Group Name ▲	User Permission	Object Permission
Full Access	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 3: Group Permissions selections

7. Click **Submit**.

This creates an account that allows ServiceNow to connect to SecurityCenter to retrieve the vulnerability data via the MID Server.

Step 2: Configure a query

Configure at least one query in Tenable.sc:

1. Add a **name**.
2. Add a **description** and **tag** (optional).
3. From the **Type** drop-down list, select **Vulnerability**.
4. From the **Tool** drop-down list, select **Vulnerability Detail List**.

Figure 4: Configuring a Tenable.sc query

You'll use this query in a later step, when you configure the Tenable.sc for the Vulnerability Response app in your ServiceNow instance.

Configure a filter query for high-risk vulnerabilities

If you want to focus on managing high- to critical-risk vulnerabilities (most organizations do):

1. From within the **query** you're building, click **+Add Filter**.
2. In the **Exploit Available** field, select **Yes**.
3. In the **Severity** field, select **Critical, High**.

Figure 5: Query filter selections for high- and critical-risk vulnerabilities

When you apply these filters, ServiceNow only pulls in the vulnerabilities with existing exploits that have a high or critical severity. You can continue to tune the filter after the initial run with selections like **Patch Published**, **CVE ID**, etc.

Discover the systems impacted by a specific vulnerability

If you are trying to determine which systems are impacted by a specific vulnerability—for example, if a new exploit is making headlines—create a query with the filter **CVE ID**. Yes, you can add multiple CVEs to this query.

When you do this, SecurityCenter sends only the items that match the CVE filters, and you get a prioritized list of configuration items to target for remediation right away.

Stage 2 – Download and install the apps

Use your HI login credentials to log in to the ServiceNow Store.

KEY INSIGHT

- Download the CVE catalog to get a list of all publicly known vulnerabilities.

In this stage, you'll do a little more than just download and install the Tenable applications. You'll also import the Common Vulnerabilities and Exposures (CVE) catalog from the [NIST National Vulnerability Database](#). Finally, you'll make the Tenable app visible in Application Navigator, which you'll need for Stage 3.

Step 1: Request the Tenable applications

Log in to the [ServiceNow Store](#) and make a request to have Tenable for Assets, Tenable Connector, and Tenable for Vulnerability Response installed in your instance. Make sure to install Tenable for Assets and Tenable Connector *before* installing Tenable for Vulnerability Response; otherwise, it won't install correctly. For detailed instructions on how to install and configure each of these, please review the [product documentation](#).

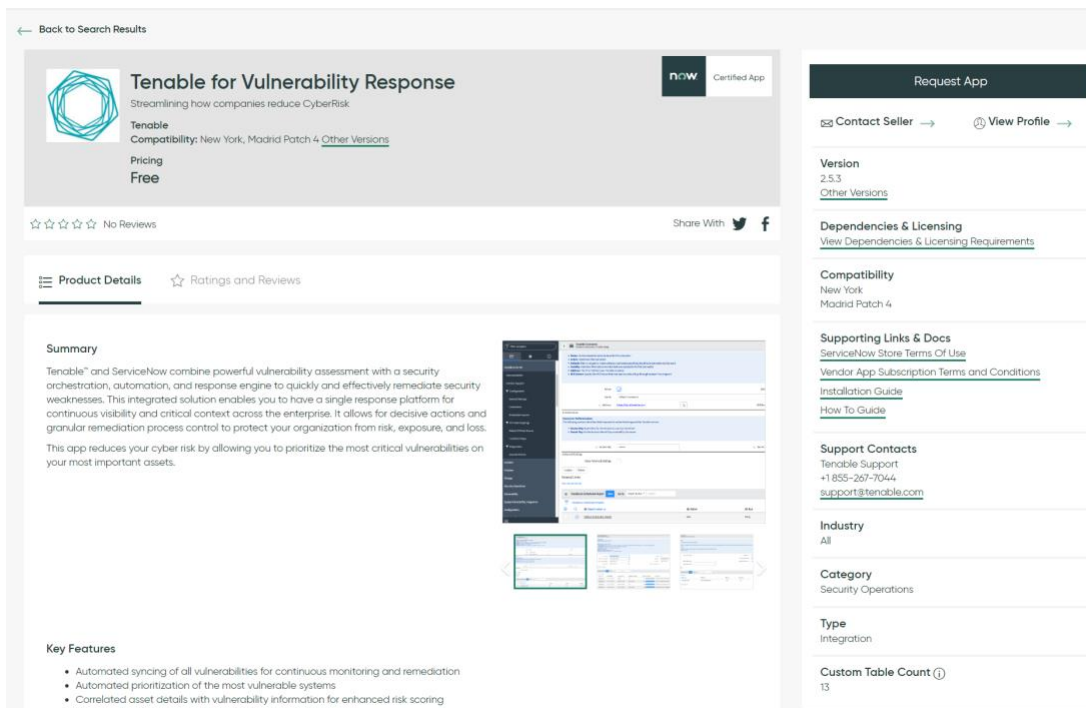


Figure 6: Tenable for Vulnerability Response in the ServiceNow Store

Step 2: Import the CVE catalog

1. Log in to your instance and navigate to **Vulnerability > Administration > On-demand Update**.
2. Select all the check boxes and click **Import**.

National Vulnerability Database					Import
	Name	Total entries	Last refreshed	Last import	Status
<input checked="" type="checkbox"/>	Recent	670	2018-01-15	0	Downloading
<input checked="" type="checkbox"/>	Modified	1085	2018-01-15	20	Downloading
<input checked="" type="checkbox"/>	2018	486	2018-01-22	315	Ready
<input checked="" type="checkbox"/>	2017	11585	2018-01-15	124	Downloading
<input checked="" type="checkbox"/>	2016	9183	2018-01-15	0	Downloading
<input checked="" type="checkbox"/>	2015	7744	2018-01-12	0	Downloading
<input checked="" type="checkbox"/>	2014	8303	2018-01-15	0	Downloading
<input checked="" type="checkbox"/>	2013	6103	2018-01-15	1	Downloading
<input checked="" type="checkbox"/>	2012	5533	2018-01-15	20	Downloading
<input checked="" type="checkbox"/>	2011	4601	2018-01-15	16	Downloading
<input checked="" type="checkbox"/>	2010	5072	2018-01-15	0	Downloading
<input checked="" type="checkbox"/>	2009	4955	2018-01-15	0	Downloading
<input checked="" type="checkbox"/>	2008	7146	2018-01-15	0	Downloading

Figure 7: National Vulnerability Database options

This pulls the CVE list, which is a catalog of all publicly known vulnerabilities, from the NIST National Vulnerability Database.

Step 3: Install the apps

1. From the Filter Navigator, navigate to **System Applications > Applications > All**.
2. Find Tenable and click **Install** next to each item.

It may take a while for the installation to complete—this is normal.

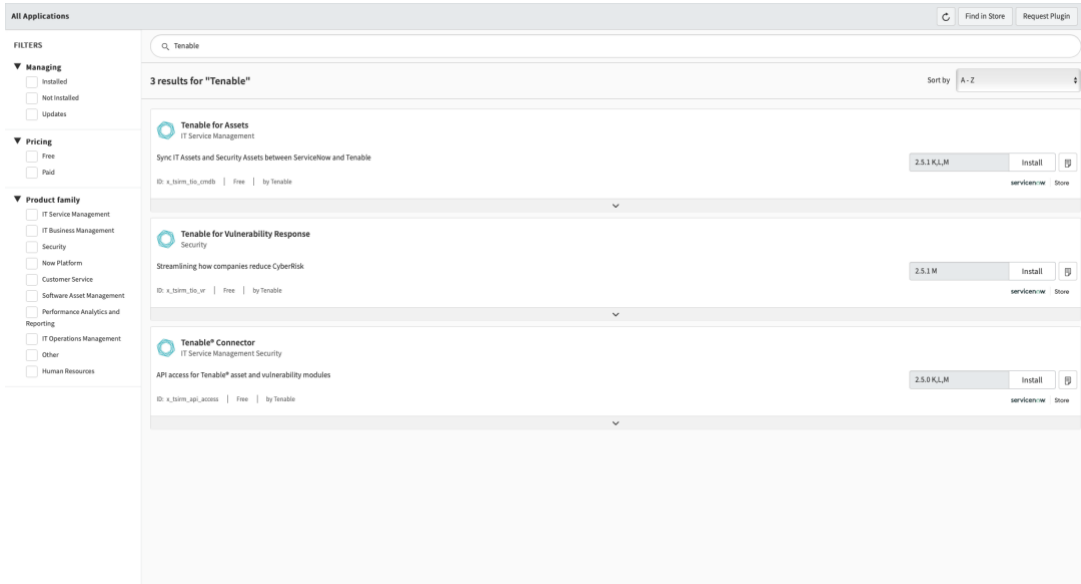


Figure 8: Tenable apps install window

Step 4: Make Tenable show in Application Navigator

Once the installation is complete, refresh the page to make it appear in the Application Navigator (the pane on the left). Search for the word "Tenable" in the Filter Navigator.

If Tenable doesn't appear in the Application Navigator after you refresh the page, log out and back in. That will force the UI to refresh.

Stage 3 – Configure the app

Configure connectors and schedule imports to get Tenable running.

KEY INSIGHTS

- Use queries with Tenable.sc to control the vulnerability types you see in ServiceNow.
- You can run Tenable.io and Tenable.sc simultaneously.

With the application installed into your ServiceNow instance, you're almost ready to start pulling in data from your Tenable.sc or Tenable.io scanners.

In this stage, you'll configure your connectors and schedule your imports.

Step 1: Activate your integration and configure your connectors

1. From your ServiceNow instance, navigate to **Tenable for VR > Connectors** and click on either **Default Tenable.io Connector** or **Default Tenable.sc connector**, depending on which one you'd like to configure.
2. Check the box next to **Active** and click **Update**.

Figure 9: Activation check box

Alternately, instead of clicking **Update**, you can right-click on the gray bar at the top of the page and then click **Save**. This will save the record without closing it; **Update** saves the record and closes it.

3. If you updated your record, in the Application Navigator, navigate to **Tenable for VR > Connectors**.
4. For **Tenable.sc**: configure the connector with your Tenable.sc address, MID Server information, API Username and API Password, and click **Update**. You can add multiple connectors if you have multiple instances of Tenable.sc.

For **Tenable.io**: configure the Access Key, Secret Key, and Outbound Map, and click **Update**.

5. You can test the connector by clicking the **Test the Connector** button.

Tenable Connector
Connection information that allows ServiceNow to talk to the Tenable server

* Tenable Product: Tenable.io Active: ☐ Default: ☒

Name: Default Tenable.io Connector

* Address: <https://cloud.tenable.com>

Authentication
Connector Authentication The following section identifies fields required to authenticate against the Tenable service

* Access Key: ***** * Secret Key: ***** Healthy: ☒

Outbound Configuration (for Tenable.io products only)

Outbound map: [] Outbound trigger fields: name, short_description

Advanced Settings
Show Advanced Settings: ☐

Tenable Plugin Import

Import Plugin Data: ☐ This feature is not available for Tenable.io at this time. Plugin data is downloaded in the same schedule as Vulnerable Items

Latest Modification Timestamp: [] Last Plugin Data Run: [] Plugin Chunk Size: 1,500

Frequency (minutes): 1,440

Update Test the connector Delete

Figure 10: Tenable Connectors form

Step 2a: Schedule an import for Tenable.io

1. In the Application Navigator, navigate to **Tenable > Scheduled Imports**.
2. On the **Tenable Scheduled Imports** (Scheduled Imports) form, choose **Default Tenable.io VR Scheduled Import** or click **New**.
3. In the **Initial Run - Historical Data** field, specify how far back (in days) to import when this scheduled import runs for the first time. For example, if you select **Within 30 days**, vulnerabilities that were observed 12 or 24 days ago are imported into ServiceNow. After the first import, the Security Operations app only requests new data that hasn't yet been imported.
4. Choose the **severities** and **plugin family names** you'd like to include in the import.
5. Under **Schedule**, specify how often you'd like the import to run.
6. Check the box next to **Active**.
7. Click **Update**.

Figure 11: Tenable.io Scheduled Imports form

Step 2b: Schedule an import for Tenable.sc

8. In the Application Navigator, navigate to **Tenable > Scheduled Imports**.
9. On the **Tenable Scheduled Imports** (Scheduled Imports) form, choose **Default Tenable SC Analysis API** or click **New**.
10. In the **Initial Run - Historical Data** field, specify how far back (in days) to import when this scheduled import runs for the first time. For example, if you select **Within 30 days**, vulnerabilities that were observed 12 or 24 days ago are imported into ServiceNow. After the first import, the Security Operations app only requests new data that hasn't yet been imported.
11. In **SC Query**, choose the query you previously created in Tenable.sc.
12. Under **Schedule**, specify how often you'd like the import to run.
13. Check the box next to **Active**.
14. Click **Update**.

Figure 12: Tenable.sc Scheduled Imports form

EXPERT TIP

You can also right-click the top gray bar and click **Save** then **Execute Now**.

Step 3: Confirm your vulnerabilities imported

To ensure your Tenable vulnerabilities imported:

1. Navigate to **Vulnerability > Vulnerable Items**.
2. Select **Vulnerabilities** from the **Go to** drop-down list. In the field to the right, type **TNS** for (Tenable.sc vulnerabilities) or **TEN** (for Tenable.io vulnerabilities) and then press **Enter** or **Return** on your keyboard. These are the prefixes used by all vulnerabilities imported from Tenable.

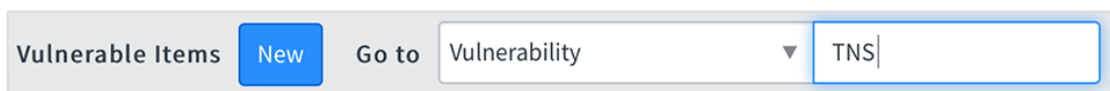


Figure 13: Confirming your vulnerabilities imported

EXPERT TIP

You can also view all imported vulnerabilities at **Vulnerability > Libraries > Third Party**.

For more information on how to work with vulnerable items, check out the [ServiceNow Vulnerability Response](#) page.

The takeaway

After you follow these three stages, your Tenable.sc and/or Tenable.io is integrated with your ServiceNow instance. You can pull data from the scanner into Vulnerability Response, publish entries in the ServiceNow third-party vulnerability table, prioritize vulnerable items based on business criticality, and assign tasks to IT workers from one console. And when items are closed in Vulnerability Response, the workflow can automatically initiate a rescan to ensure the patch was applied successfully and the vulnerability was mitigated.

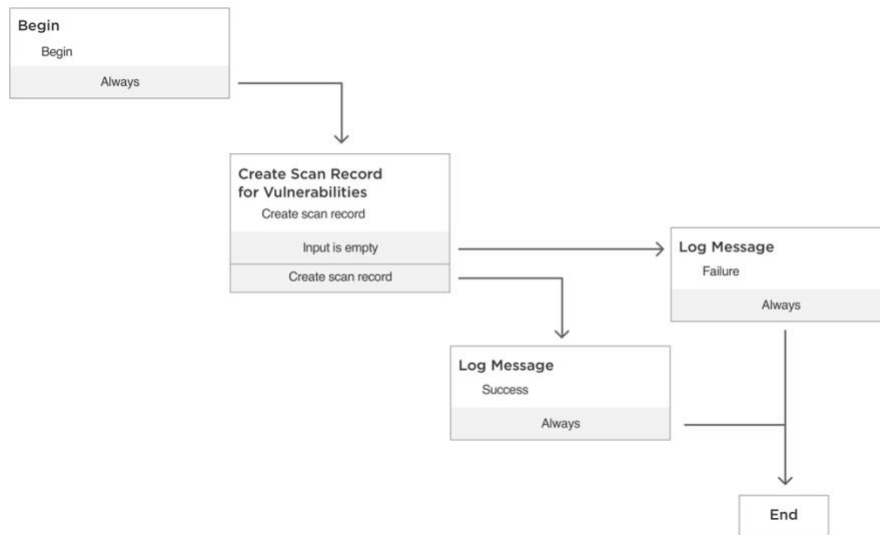


Figure 14: Vulnerability Response workflow

Appendix

Related resources

- [Tenable website](#)
- [Tenable for Assets app request form](#)
- [Tenable Connector app request form](#)
- [Tenable for Vulnerability Response app request form](#)
- [Data Security Playbook – Key elements to consider when securing your instance](#)
- [ServiceNow product documentation site](#)
- [ServiceNow Community](#)