Tenable and Splunk Integration Guide

Last Revised: May 26, 2021
# Table of Contents

**Welcome to Tenable for Splunk** ................................................................. 4

Components ........................................................................................................... 5

Tenable Add-on (TA-tenable) .................................................................................. 6

Source and Source Types ....................................................................................... 7

CIM Mapping ........................................................................................................... 8

Tenable App for Splunk .......................................................................................... 9

Saved Searches ....................................................................................................... 13

Tenable Plugin for Splunk Mission Control .......................................................... 15

**Installation Workflow** ..................................................................................... 17

Upgrade from App v1 to v4 .................................................................................... 18

Splunk Environments ............................................................................................. 19

Installation ............................................................................................................ 21

**Configuration** .................................................................................................. 23

Configure Tenable.io .............................................................................................. 24

Configure Tenable.sc Credentials ......................................................................... 29

Tenable.sc Certificates .......................................................................................... 34

Configure Tenable NNM ......................................................................................... 38

Configure Tenable Plugin for Mission Control ..................................................... 41

Configure Tenable.ot ............................................................................................... 43

**Create an Input** ............................................................................................... 46

**Adaptive Response** .......................................................................................... 50

Alert Action Configuration ..................................................................................... 55
Additional Information .................................................................................................................. 56
Customized Actions ..................................................................................................................... 57
Tenable Macros ............................................................................................................................. 58
Troubleshooting ............................................................................................................................ 59
Welcome to Tenable for Splunk

The Tenable for Splunk applications perform data collection, normalization, and visualization.

The application is divided into two parts:

- **Tenable Add-On for Splunk (TA-tenable)** provides all data collection and normalization functionality.

- **Tenable App for Splunk (TenableAppforSplunk)** provides a dashboard to view the Tenable data in Splunk.

Optional plugins for the Splunk application:

- **Tenable Plugin for Splunk Mission Control** provides vulnerability data and insights to the Splunk Mission Control application.

Tenable Application Topology
Components

The Tenable Add-on has specific purposes for each Splunk component. The components are listed and described below.

Heavy Forwarder

The **Heavy Forwarder** collects and forwards data for all events.

- **Note:** You must configure inputs to run from the heavy forwarder.
- **Note:** You must enable the key value store (KV) on the heavy forwarder.

Indexer

The **Indexer** ensures Tenable data is properly indexed.

- **Note:** You can use a default index or create and set a custom index. This is required.

Search Head

The **Search Head** allows full functionality of the Tenable Add-on adaptive response actions.

- **Note:** You must configure the Search Head with the same configuration details you have on the Heavy Forwarder for the adaptive response actions to work correctly.
- **Note:** If you install the Tenable App for Splunk on the search head, you must also install the Tenable Add-on.
Tenable Add-on (TA-tenable)

The Tenable Add-On for Splunk pulls data from Tenable platforms and normalizes it in Splunk.

The current Tenable Add-On uses the following endpoints.

Tenable.io

- Request Export: /vulns/export
- Vulnerability Export: /vulns/export
- Asset Export: /assets/export

Tenable.sc

- Vulnerability and assets details: /rest/analysis
- Plugin details: /rest/plugins
- Repository details: /rest/repository
# Source and Source Types

The Tenable Add-on for Splunk stores data with the following sources and source types.

## Tenable.sc

<table>
<thead>
<tr>
<th>Source</th>
<th>Sourcetype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;username&gt;</td>
<td>&lt;address&gt;</td>
<td>tenable:sc:vuln</td>
</tr>
<tr>
<td>&lt;username&gt;</td>
<td>&lt;address&gt;</td>
<td>tenable:sc:assets</td>
</tr>
<tr>
<td>&lt;username&gt;</td>
<td>&lt;address&gt;</td>
<td>tenable:sc:plugin</td>
</tr>
</tbody>
</table>

## Tenable.io

<table>
<thead>
<tr>
<th>Source</th>
<th>Sourcetype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tenable_io://&lt;data input name&gt;</td>
<td>tenable:io:vuln</td>
<td>This collects all vulnerability data.</td>
</tr>
<tr>
<td>tenable_io://&lt;data input name&gt;</td>
<td>tenable:io:assets</td>
<td>This collects all asset data.</td>
</tr>
<tr>
<td>tenable_io://&lt;data input name&gt;</td>
<td>tenable:io:plugin</td>
<td>This collects all plugin data.</td>
</tr>
</tbody>
</table>
CIM Mapping

This chart displays how we map Tenable vulnerability findings to Splunk CIM.

<table>
<thead>
<tr>
<th>Field Name from Tenable.io API</th>
<th>Field Name from Tenable.sc API</th>
<th>CIM Field Name</th>
<th>CIM Data Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>asset.fqdn</td>
<td>dnsName</td>
<td>dest_name</td>
<td>vulnerability</td>
</tr>
<tr>
<td>asset.ipv4</td>
<td>ip</td>
<td>dest_ip</td>
<td>vulnerability</td>
</tr>
<tr>
<td>plugin.bid</td>
<td>bid</td>
<td>bugtraq</td>
<td>vulnerability</td>
</tr>
<tr>
<td>plugin.family</td>
<td>family.name</td>
<td>category</td>
<td>vulnerability</td>
</tr>
<tr>
<td>plugin.synopsis</td>
<td>synopsis</td>
<td>signature</td>
<td>vulnerability</td>
</tr>
<tr>
<td>tenable</td>
<td>tenable</td>
<td>vendor</td>
<td>vulnerability</td>
</tr>
<tr>
<td>tenable.io</td>
<td>tenable.sc</td>
<td>product</td>
<td>vulnerability</td>
</tr>
</tbody>
</table>
Tenable App for Splunk

The Tenable App for Splunk provides a single dashboard that displays all of your Tenable data.

To properly display the Tenable App for Splunk:

- [Set up the macro definition](#)
- [Run the All Time saved search](#)

To Setup the Tenable App for Splunk:

Set up the macro definition

1. In Splunk, go to Settings > Advance search > Search Macros.
2. In the App section, select Tenable App for Splunk.
3. Click the search icon.
   
   Results appear.
4. Click `get_tenable_index`.
   
   The `get_tenable_index` macro page appears.
5. In the Definition entry field, update the definition to `index=INDEX_NAME`.
   
   The INDEX_NAME should be the same name entered when you created the data input.
6. Click Save.

Run the All Time saved search

After installation, you must run the All Time saved search specific to your Tenable platform. This is a one-time operation to properly populate indices that the Tenable App for Splunk depends on.

1. Navigate to the Tenable App for Splunk.
2. Click Saved Searches.
3. Select either Tenable IO Vuln Date - All Time or Tenable SC Vuln Data - All Time.
   
   Splunk completes the query.

Displayed Components
- Total Vulnerabilities Today
- Active Vulnerabilities Today
- Fixed Vulnerabilities Today
- Total Vulnerabilities
- Active Vulnerabilities
- Fixed Vulnerabilities
- Top 10 Vulnerabilities
- Most Vulnerable Hosts
- Vulnerabilities by Severity
- New Vulnerabilities
Tenable App Tenable NNM

The Tenable App for Splunk provides a single dashboard showing all of your Tenable NNM data. You must set the following components:

Displayed Components

Dashboard

- Total Real-time events
- Unique Real-time events
• Top 10 Events
• Top Event Trends
• Top Source IP
• Top Event Name

**Traffic Overview**

• Top Destination Port
• Top Source Port
• Top Destination IP
• Top Source IP

**Traffic Map**

• Source IP Map
• Destination IP Map

**Events**

• Top Events
• Events
Saved Searches

The Saved Search option creates lookup tables. The lookup tables contain filtered data that automatically removes duplicate information providing accurate, readable results.

Tenable Saved Searches

Tenable.io vulnerability data: Type the following command to view the KV store collection for Tenable.io vulnerability data.

```bash
io_vuln_data_lookup
```

Tenable.io asset data: Type the following command to view the KV store collection for Tenable.io asset data.

```bash
io_asset_data_lookup
```

Tenable.io plugin data: Type the following command to view the KV store collection for Tenable.io plugin data.

```bash
io_plugin_data_lookup
```

Tenable.sc Saved Searches

Tenable.sc vulnerability data: Type the following command to view the KV store collection for Tenable.sc vulnerability data.

```bash
sc_vuln_data_lookup
```

Tenable.sc asset data: Type the following command to view the KV store collection for Tenable.sc asset data.

```bash
sc_asset_data_lookup
```

Tenable.sc plugin data: Type the following command to view the KV store collection for Tenable.sc plugin data.
sc_plugin_data_lookup

Tenable.NNM Saved Searches

**Tenable.NNM vulnerability data:** Type the following command to view the KV store collection for Tenable.NNM vulnerability data.

nnm_vuln_data_lookup

**NNM events over time, NNM Top 10 Events, NNM Top Destination by Country, NNM Top Source by Country, Top Destination IP, Top Destination Port, Top NNM Plugin ID, Top Source IP, and Top Source Port:** Type the following command to view NNM events.

tenable:nnm:vuln
Tenable Plugin for Splunk Mission Control

Tenable Plugin for Splunk Mission Control is an optional plugin for the Splunk application which provides vulnerability data and insights to the Splunk Mission Control application. Splunk Mission Control is a unified cloud-based security operations platform that provides security incident triage, investigation, collaboration, and response functionality as a Software-as-a-Service (SaaS) solution.

Topology features and workflow:

- Tenable Add-on for Splunk collects Tenable data on your Splunk Enterprise, or Enterprise Cloud, deployment.

- Splunk Enterprise Security generates notable events via correlation searches which are forwarded to Mission Control using Splunk Connect for Mission Control App.

- Splunk Connect for Mission Control is used to establish connection between your on-prem, or cloud, Splunk deployment & Mission Control.

- Tenable Plugin for Splunk Mission Control fetches data from your connected on-prem, or cloud, deployment’s Splunk indexes.
Configuration

To configure Tenable Plugin for Mission Control, refer to Configure Tenable Plugin for Mission Control.
Installation Workflow

Follow the steps below to complete the installation and configuration of the Tenable applications for Splunk.

Before you begin:

- Complete the [Upgrade from App v1 to v4](#) from Splunk V1 to Splunk V2.

Install and Configure

1. Install the Tenable application.
2. Configure the desired Tenable application for Splunk.
   
   **Note:** You need unique credentials for each Splunk environment.

3. [Create an input](#) for the configured Tenable application for Splunk.
4. [Configure adaptive response](#) actions.
Upgrade from App v1 to v4

**Note:** If you are upgrading from App v2 or v3 to v4, install the new version (v4) over your current version.

Complete the following steps to upgrade your application from v1 to v4.

**Before you begin:**

- Backup all current application configurations outside the Splunk install path.

**To upgrade from v1 to v4:**

**Note:** The upgrade process includes uninstalling v1 before you install v4.

1. Delete the app and all app configuration files from all Splunk search heads and heavy forwarders from the command line. For example:
   
   ```
   rm -rf $SPLUNK_HOME/etc/apps/TA-tenable/
   ```

2. **Installation** the v4 app.

3. **Configuration** your account.

4. Create a new index to store your data.
   
   **Note:** You cannot re-use an existing index.

5. **Create an Input**.
   
   **Note:** Use the index that you created in step 4.

**After the upgrade:**

- When you enable the input, v4 imports all of your existing vulnerabilities, including all previously fixed vulnerabilities. This ensures that no data is lost.

- Synchronization of previously fixed vulnerabilities is optional during the input setup and disabled by default. To enable the synchronization, see the **Create an Input** section.

- When the initial import completes, you can run saved searches to create lookup tables and build reports.
Splunk Environments

The installation process for the Tenable App for Splunk and Tenable Add-On for Splunk varies based on your Splunk environment.

Deployment Types

Single server, distributed deployment, and cloud instance options are available.

Single Server Deployment

In a single server deployment, a single instance of Splunk Enterprise works as a data collection node, indexer, and search head. In this instance, install the Tenable Add-On and Tenable App on this node. Complete the setup for the Tenable Add-On to start data collection.

Distributed Deployment

In a distributed deployment, install Splunk on at least two instances. One node works as a search head while the other node works as an indexer for data collection.

The following table displays information on how the Tenable Add-On and Tenable App are installed in the distributed environment.

<table>
<thead>
<tr>
<th>Component</th>
<th>Forwarder</th>
<th>Indexer</th>
<th>Search Head</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenable Add-on for Splunk (TA-Tenable)</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• configure accounts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• configure data input</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tenable-SC App for Splunk (Tenable App)</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Cloud Instance

In Splunk Cloud, the data indexing takes place in a cloud instance.
**Note:** The data collection can take place in an on premise Splunk instance that works as a heavy forwarder.

The application can be installed via a command line or from the Splunk UI.
Installation

For Tenable.io:

**Required User Role:** Administrator

For Tenable.sc:

**Required User Role:** Vulnerability Analyst

Before you begin:

- Complete the [Upgrade from App v1 to v4](#) from Splunk v1 to Splunk v4.
- You must have Splunk downloaded on your system with a Splunk basic login.

**Note:** See the [Splunk Environments](#) section for additional information about the different types of Splunk deployments and their requirements.

**Note:** If you install the Tenable App for Splunk on the search head, you must also install the Tenable Add-on.

Install via the Splunk User Interface

1. Log in to Splunk.
2. Go to **Apps** at the top of the screen.
   - A drop-down appears.
3. Click **Manage App**.
4. In the search bar, type Tenable.
Tenable related options appear.

5. Click **Launch App** for the Tenable application you want to install.

   Follow the Splunk prompts to launch the application.

**Note:** You must restart Splunk after installing the Tenable App or Tenable Add-On.

**Note:** You may need to update the Tenable Macro, `get_tenable_index`, for data to begin populating the application dashboards.

**Note:** Next, configure the Tenable application.
Configuration

Tenable provides three application configuration options for the Tenable Add-On for Splunk. View the corresponding link for steps to configure your application.

Tenable.sc Credentials

Tenable.sc Certificates

Tenable.io
Configure Tenable.io

To complete the installation process, you must complete the setup for the **Tenable Add-on for Splunk**.

**Before you begin:**

**Required User Role:** Administrator

- You must have your Tenable.io API keys.

**Note:** For your Tenable.io integration:
- You must generate an API key in Tenable.io to complete the configuration. See the [Tenable.io user guide](#) for instructions on how to generate an API key. (Do not use this API key for any other third party or custom built application or integration. It must be unique for each installed instance of the integration.)

To setup the **Tenable Add-on for Splunk**:

1. Log in to the heavy forwarder where you installed the Tenable Add-on for Splunk.
2. In the left navigation bar, click **Tenable Add-on for Splunk**.
3. Click the **Configuration** tab.

4. Click the **Add** button.

   A new window appears.
Add Account

Account Name * admin
Enter a unique name for this account.

Tenable Account Type * Tenable.io
Select the App for Tenable

Address *
Enter the FQDN or IP of your server for this account.

Verify SSL Certificate
Should we verify your SSL certificate?

Access Key
Enter the Access Key for this account.

Secret Key
Enter the secret key for this account.

Proxy Enable
Check to enable the proxy.

Add
Cancel
5. Enter the necessary information for each field. The field options are described in the chart below.

<table>
<thead>
<tr>
<th>Input Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Name</td>
<td>(Required) The unique name for each Tenable data input.</td>
</tr>
<tr>
<td>Tenable Account Type</td>
<td>(Required) The type of Tenable account - Tenable.io, Tenable.sc Credentials, or Tenable.sc Certificate</td>
</tr>
<tr>
<td>Address</td>
<td>(Required) The host name or IP address for Tenable.io.</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>If enabled, Splunk verifies the SSL certificate in Tenable.io.</td>
</tr>
<tr>
<td>Access Key</td>
<td>(Required) Tenable.io API access key.</td>
</tr>
<tr>
<td>Secret Key</td>
<td>(Required) Your Tenable.io API secret key.</td>
</tr>
<tr>
<td>Proxy Enable</td>
<td>Enables the plugin to collect Tenable.io data via a proxy server. If you select this option, the plugin prompts you to enter the following:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Proxy Type</strong> - the type of proxy used.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Proxy Host</strong> - the host name or IP address of the proxy server.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Proxy Port</strong> - the port number of the proxy server.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Proxy Username</strong> - the username for an account that has permissions to access and use the proxy server.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Proxy Password</strong> - the password associated</td>
</tr>
</tbody>
</table>
6. To complete the configuration, click **Add**.

**Next steps:**

- [Create an Input](#) for the Tenable Add-On for Splunk.
Configure Tenable.sc Credentials

To complete the **installation** process, you must complete the setup for the **Tenable Add-on for Splunk**.

For Tenable.sc:

**Required User Role:** Security Analyst

To setup the **Tenable Add-on for Splunk**:

1. Log in to your data collection node.
2. In the left navigation bar, click **Tenable Add-on for Splunk**.
3. Click the **Configuration** tab.
4. Click the **Add** button.

A new window appears.
5. In the **Tenable Access Type** field, select **Tenable.sc Credentials**.
6. Enter the necessary information for each field, described in the chart below.

<table>
<thead>
<tr>
<th>Input Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Name</td>
<td>(Required) The unique name for each Tenable data input.</td>
</tr>
<tr>
<td>Tenable Account Type</td>
<td>(Required) The type of Tenable account - Tenable.io, Tenable.sc Credentials, or Tenable.sc Certificate.</td>
</tr>
<tr>
<td>Address</td>
<td>(Required) The host name or IP address for Tenable.sc.</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>If enabled, Splunk verifies the certificate in Tenable.sc.</td>
</tr>
<tr>
<td>Username</td>
<td>(Required) The username in Tenable.sc.</td>
</tr>
<tr>
<td>Password</td>
<td>The password in Tenable.sc.</td>
</tr>
<tr>
<td>Proxy Enable</td>
<td>Enables the plugin to collect Tenable.sc data via a proxy server. If you select this option, the plug-in prompts you to enter the following:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Proxy Type</strong> - the type of proxy used.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Proxy Host</strong> - the host name or IP address of the proxy server.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Proxy Port</strong> - the port number of the proxy server.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Proxy Username</strong> - the username for an account that has permissions to access and use the proxy server.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Proxy Password</strong> - the password associated with the username you provided.</td>
</tr>
</tbody>
</table>

7. Click **Add** to complete the configuration.
Next steps:

- Create an Input for the Tenable Add-On for Splunk.
Tenable.sc Certificates

To complete the installation process, you must complete the setup for the Tenable Add-on for Splunk. For additional information on Tenable.sc Certificates, see SSL Client Certificate Authentication.

To setup the Tenable Add-on for Splunk:

1. Log in to your data collection node.

2. In the left navigation bar, click Tenable Add-on for Splunk.

3. Click the Configuration tab.
4. Click the **Add** button.

The **Add Account** window appears.
5. In the **Tenable Account Type** field, select **Tenable.sc Certificates**.

6. Enter the necessary information for each field, described in the chart below.

---

**Note:** The certificates you upload and configure must be associated to a specific user in Tenable.sc.

<table>
<thead>
<tr>
<th>Input Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Name</td>
<td><em>(Required)</em> The unique name for each Tenable.sc data input.</td>
</tr>
<tr>
<td>Tenable Account Type</td>
<td><em>(Required)</em> The type of Tenable account - Tenable.io, Tenable.sc Credentials, or Tenable.sc Certificate.</td>
</tr>
<tr>
<td>Address</td>
<td><em>(Required)</em> The host name or IP address for Tenable.sc.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>If enabled, Splunk verifies the SSL Certificate in Tenable.sc.</td>
</tr>
<tr>
<td>Certificate Filename</td>
<td>The name of the certificate that you uploaded to $SPLUNK_HOME/etc/apps/TA-tenable/certs/.</td>
</tr>
<tr>
<td>Key Filename</td>
<td>The name of the key that you uploaded to $SPLUNK_HOME/etc/apps/TA-tenable/certs/.</td>
</tr>
<tr>
<td>Key Password</td>
<td>The password for the key file you uploaded.</td>
</tr>
<tr>
<td>Proxy Enable</td>
<td>Enables the plugin to collect Tenable.sc data via a proxy server. If you select this option, the plug-in prompts you to enter the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Proxy Type</strong> - the type of proxy used.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Proxy Host</strong> - the host name or IP address of the proxy server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Proxy Port</strong> - the port number of the proxy server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Proxy Username</strong> - the username for an account that has permissions to access and use the proxy server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Proxy Password</strong> - the password associated with the username you provided.</td>
</tr>
</tbody>
</table>

7. Click **Add** to complete the configuration.

Next steps:

- [Create an Input](#) for the Tenable Add-On for Splunk.
Configure Tenable NNM

You can connect to Tenable Nessus Network Monitor using a syslog input. You must configure a default UDP/TCP data input of Splunk.

<table>
<thead>
<tr>
<th>Source Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tenable:nnm:vuln</td>
<td>This contains all vulnerability data.</td>
</tr>
</tbody>
</table>

To configure Tenable NNM:

Complete the following steps in Splunk.

1. In the top navigation bar, click Settings > Data Inputs.
   
   The Data Inputs page appears.

2. In the Local Inputs section, scroll to TCP or UDP.

3. Click the + Add New option in the TCP or UDP row.
   
   The Add Data page appears with the TCP/UDP option selected.

4. Enter the port configuration information.
5. At the top of the page, click **Next**. The **Input Settings** page appears.

6. For the **Source Type** option, click **New**. Additional options appear.

7. In the **Source Type** field, enter **tenable:nnm:vuln**.

8. In the **Source Type Category** drop-down, select **Tenable**.

9. (Optional) Enter a description in the **Source Type Description** field.

10. Scroll down to the **Index** option.

11. Click on the **Index** drop-down menu.

12. Select an **Index**.
13. At the top of the page, click **Review**.


   **Note:** If your configuration needs edits, click **Back** to update your settings.

15. At the top of the page, click **Done**.

Complete the following steps in NNM:

1. Log in to NNM.
2. Go to  > **Configuration**.
   
   The **Configuration** page appears.
3. In the **Setting Type** drop-down, click **Syslog**.
   
   The **Syslog** options appear.
4. Next to **Realtime Syslog Server List**, click **Add**.
   
   The **+Add Syslog Item** window appears.
5. In the **IP** field, enter the IP address of the Splunk server you configured to accept syslog.
6. In the **Port** field, enter the port number you have Splunk set to listen to when syslog is on.
7. For **Format Type**, select **Standard**.
8. For **Protocol**, select the protocol you have set up to accept the syslog for Splunk.
Configure Tenable Plugin for Mission Control

Before You Begin

- Install and configure the following on Splunk Enterprise (version 8 or higher)
  - Tenable Add-On for Splunk (TA-tenable) provides all data collection and normalization functionality.
  - Tenable App for Splunk (TenableAppforSplunk) provides a dashboard to view the Tenable data in Splunk.
  - Splunk Enterprise Security 6.2.0
  - Splunk Connect for Mission Control 1.6.1
- Access Splunk Mission Control:
  - Ensure you have access to a Splunk Mission Control tenant. If you do not have a tenant set up, contact your Splunk representative.

Configuration

To configure Tenable Plugin for Mission Control:

1. Confirm that you have an active connection in Splunk Connect for Mission Control.
   - In Mission Control, click on the ellipsis icon on the top right corner.
   - From the drop-down menu, navigate to Admin Settings > Product Settings > Splunk Connect for Mission Control.
   - Confirm that the connection status shows Active. Log in and navigate to the Mission Control Home page.

2. In the upper-right corner, click the ellipses icon on the top right corner. A drop-down menu appears.

3. From the drop-down menu, navigate to Product Settings > Splunk Connect for Mission Control. Select the instance configured with Mission Control. Save the deployment ID for future
use. This deployment ID is used as a default instance while populating the Tenable Vulnerability Center dashboard.

4. Navigate to **Product Settings > Plugin**. If you do not see the **Plugin** page, contact your Splunk representative.

5. Select **Tenable Plugin for Mission Control**. The setup page appears.

6. Enable the Tenable Plugin for Mission Control by clicking the toggle.

7. In the **Default Connection ID** box, enter the deployment ID that you previously took note of.

8. If you see, the message **Subscription Successful** - you have enabled the plugin. You will be able to see Tenable Vulnerability Center Dashboard under Managed Dashboards sections in Dashboards drop-down.

9. Configure your notable events label to enable integration between the Tenable Plugin and Mission Control. The notable events label **mcef_tenable_plugin_for_mission_control** must be applied for the integration to work.
   a. In the **Splunk Connect for Mission Control** application, navigate to **Settings > Searches, reports, and alerts on Cloud/on-premise instance**.
   b. To filter the list, in the Owner drop-down box, select **All**.
   c. To configure the saved searches to forward notables with specific label values of plugin Id, in the **Mission Control - Forward Notable Events** box enter the label **mcef_tenable_plugin_for_mission_control**.
   d. Click **Save**. Splunk Mission Control is configured to forward notable events with this label to the Tenable Plugin for Mission Control dashboard.

**Troubleshooting**

If you are experiencing problems with setup or data retrieval with Tenable Plugin for Mission Control, refer to [Troubleshooting](#).
Configure Tenable.ot

You can connect to Tenable.ot using a syslog input. You must configure a default UDP/TCP data input of Splunk.

<table>
<thead>
<tr>
<th>Source Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tenable:ot:alerts</td>
<td>This option configures Splunk to accept Tenable.ot alerts.</td>
</tr>
</tbody>
</table>

To configure Tenable.ot:

Complete the following steps in Splunk.

1. In the top navigation bar, click **Settings > Data Inputs**.
   The **Data Inputs** page appears.

2. In the **Local Inputs** section, scroll to **TCP** or **UDP**.

3. Click the + **Add New** option in the **TCP** or **UDP** row.
   The **Add Data** page appears with the **TCP/UDP** option selected.

4. Enter the port configuration information.
5. At the top of the page, click **Next**.

   The **Input Settings** page appears.

   ![Input Settings page](image)

6. For the **Source Type** option, click **New**.

   Additional options appear.

7. In the **Source Type** field, enter `.tenable:ot:alerts`.

8. In the **Source Type Category** drop-down, select **Tenable**.

9. (Optional) Enter a description in the **Source Type Description** field.

10. Scroll down to the **Index** option.

11. Click on the **Index** drop-down menu.

12. Select an **Index**.
13. At the top of the page, click **Review**.


   **Note:** If your configuration needs edits, click **Back** to update your settings.

15. At the top of the page, click **Done**.

Complete the following steps in Tenable.ot:

1. In the Tenable.ot console, under **Local Settings**, go to the **Servers > Syslog Servers** screen.

2. Click **Add Syslog Server**.

   The **Syslog Server** configuration window is displayed.

3. In the **Server Name** field, enter a name for your Splunk system.

4. In the **Hostname/IP** field, enter the IP address of your Splunk system.

5. In the **Port** field, enter the port number on the Splunk system to which the events will be sent.

6. In the **Transport** field, select from the dropdown list the transport protocol to be used. (Options are **TCP** or **UDP**).

7. Click **Send Test Message** to send a test message to verify that the configuration was successful, and check if the message has arrived. If the message did not arrive, then troubleshoot to discover the cause of the problem and correct it.

8. Click **Save**.
Create an Input

After you complete the configuration for your Tenable Add-On for Splunk, you must create the input.

To create an input:

1. In the Splunk interface, click the Inputs tab.

![Splunk Inputs Interface]

2. Click the Create New Input button.

   A drop-down box appears.

   ![Create New Input Dropdown]

3. Select the appropriate Tenable application.

   The selected Tenable application input options open in a new window.
4. Enter the necessary information for each field, described in the chart below.

**Note:** If you don’t use the default index, you must update the Tenable Macro.

### Tenable.io

<table>
<thead>
<tr>
<th>Input Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>(Required) The unique name for each Tenable data input.</td>
</tr>
<tr>
<td>Interval</td>
<td>(Required) The interval parameter specifies when the input restarts to perform the task again (in seconds). The interval amount must be between 3600 and 86400.</td>
</tr>
<tr>
<td>Index</td>
<td>(Required) The index in which to store Tenable.io data.</td>
</tr>
<tr>
<td>Global Account</td>
<td>(Required) The Tenable account from which data is acquired.</td>
</tr>
<tr>
<td>Start Time</td>
<td>The date and time to start collecting data. If you leave this field blank, all historical data is collected. (Enter in this format - YYYY-MM-DD hh:mm:ss.)</td>
</tr>
<tr>
<td>Lowest Severity Score</td>
<td>(Required) The lowest level of severity that will be stored.</td>
</tr>
<tr>
<td>Historical Fixed Vulnerability</td>
<td>Allows the import of vulnerabilities fixed prior to the current day.</td>
</tr>
<tr>
<td>Tags</td>
<td>Limits vulnerabilities pulled to assets that have tags selected.</td>
</tr>
</tbody>
</table>

### Tenable.sc Vulnerability

<table>
<thead>
<tr>
<th>Input Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>(Required) The unique name for each Tenable data input.</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Interval</strong></td>
<td>(Required) The interval parameter specifies when the input restarts to perform the task again (in seconds). The interval amount must be between 300 and 86400.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If using a Tenable.sc version previous to 5.7, the minimum interval you can select is 24 hours. If using Tenable.sc 5.7 or later, you can specify a minimum interval of an hour.</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td>(Required) The index in which to store Tenable.sc data.</td>
</tr>
<tr>
<td><strong>Global Account</strong></td>
<td>(Required) The Tenable account from which data is acquired.</td>
</tr>
<tr>
<td><strong>Start Time</strong></td>
<td>The date and time to start collecting data. If you leave this field blank, all historical data is collected.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Uses the <code>YYYY-MM-DD hh:mm:ss</code> format.</td>
</tr>
<tr>
<td><strong>Sync Plugin Details</strong></td>
<td>If selected, plugin details are included for the related tags in Tenable assets.</td>
</tr>
<tr>
<td><strong>Historical Fixed Vulnerability</strong></td>
<td>Allows the import of vulnerabilities fixed prior to the current day.</td>
</tr>
<tr>
<td><strong>Query Name</strong></td>
<td>A name for Tenable.sc vulnerability filter.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The interval must be query type - <strong>Vulnerability Detail List</strong>.</td>
</tr>
</tbody>
</table>

Tenable.sc Mobile
<table>
<thead>
<tr>
<th>Input Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>(Required) The unique name for each Tenable data input.</td>
</tr>
<tr>
<td>Interval</td>
<td>(Required) The interval parameter specifies when the input restarts to perform the task again (in seconds).</td>
</tr>
<tr>
<td>Index</td>
<td>(Required) The index in which to store Tenable.sc data.</td>
</tr>
<tr>
<td>Global Account</td>
<td>(Required) The Tenable account from which data is acquired.</td>
</tr>
<tr>
<td>Query Name</td>
<td>A name for Tenable.sc vulnerability filter.</td>
</tr>
</tbody>
</table>

**Note:** The interval must be query type - **Vulnerability Detail List**.

5. Click **Add** to create the input.

6. Run the **All Time** saved search.

7. Schedule an **All Time** saved search.

**Note:** Tenable recommends running the saved search every 24 hours. However, you can adjust as needed.
Adaptive Response

You can create a correlation search and bind it to the adaptive response action when you save it. This allows you to automatically call actions when you run a search.

Before you begin:

You must select an index on the Alert Actions Configuration tab in the Tenable Configuration section to retrieve data.

Configure Saved Actions

Configure adaptive response actions when you create a correlation search.

**Note:** The actions are retrieved automatically when you run the search.

To configure adaptive response actions:

1. In the Splunk navigation bar, click the Apps drop-down menu.

2. Select **Enterprise Security**.

   The **Enterprise Security** page appears.
3. In the **Enterprise Security** top navigation bar, click **Configure**.

   A drop-down menu appears.

4. Click **Content**.
Additional options appear.

5. Click **Content Management**.

   The **Content Management** page appears.

6. In the top right corner, click the **Create New Content** button.

   A drop-down menu appears.

7. Select **Correlation Search**.

8. Enter information for the correlation search. Refer to the **Correlation Search** section in the Splunk user guide for additional information.

9. Scroll to the **Adaptive Response Actions** section.

10. Click the **Add New Response Action** link.

    A list of options appear.
11. Select the appropriate action for your search.

12. The field options for the selected option appears..
13. Enter the required information in the fields of your added response action.

14. Click **Save**.

A confirmation message appears.

15. Run a search.
Alert Action Configuration

1. In the Tenable navigation bar, click **Configuration**.

   The **Configuration** page appears.

2. Click the **Adaptive Actions Configuration** tab.

   The Alert Actions Configuration options appear.

3. Select an index from the **Alert Actions Index** drop-down menu.

4. Click **Save**.
Additional Information

See the following pages for additional information.

Update Macro Definition

Troubleshooting
Customized Actions

The Tenable Add-on for Splunk provides an option that you to manually call a customized action. You can call an action to make a REST API call for a specific action.

To call a customized action:

1. Open the Incident Review and search for events.
   The list of events appears.
2. Do one of the following:
   - Expand the event to view the details.
   - Click drop-down list in the top right corner of the item.
   A list of the configured adaptive response actions appears.

Next steps:

- You can view the Alert Action status in the Adaptive Responses section to verify they were executed successfully.
Tenable Macros

To modify the macro definition:

Tenable Index Macro

1. Go to Settings > Advance search > Search Macros.
2. In the App section, select Tenable App for Splunk.
3. Click the search icon.
   Results appear.
4. Click get_tenable_index.
   The get_tenable_index macro page appears.
5. In the Definition entry field, update the definition to index=INDEX_NAME. The INDEX_NAME should be the same name entered when you created the data input.
6. Click Save.

Tenable Source Types

1. Go to Settings > Advance search > Search Macros.
2. Click get_tenable_sourcetype.

   Note: The default macro definition is sourcetype=(tenable:sc:vuln OR tenable:io:vuln).
Troubleshooting

1. **I am getting a Splunk error.**
   - Check the `$SPLUNK_HOME/var/log/splunk/splunkd.log` for Splunk related errors. If you see errors, contact your Splunk administrator.
   
   **Note:** Your must set your $SPLUNK_HOME environment.

2. **I don’t see data after setting up mod input.**
   - For Tenable.io mod-input, check the `$SPLUNK_HOME/var/log/splunk/ta_tenable_tenable_io.log` file.
   - For Tenable.sc mod-input, check the `$SPLUNK_HOME/var/log/splunk/ta_tenable_tenable_securitycenter.log`.
   - For Tenable.sc mobile mod-input, check the `$SPLUNK_HOME/var/log/splunk/ta_tenable_tenable_securitycenter_mobile.log` file.

3. **Data is not populating in the Tenable App dashboards.**
   - Run an **All Time** saved search for Tenable.io or Tenable.sc. After running the **All Time** saved search, turn on and schedule a saved search.
   - Try expanding the time range from the last 24 hours.
   - Check the Tenable macro *(get_tenable_index)* and ensure the Tenable index is set correctly.
   - The dashboard can take some time to populate when data collection is started. To ensure you are receiving all available data, take the following steps:
     - search `get_tenable_index` | stats count by source type
     - You should see the following source types: `tenable:io:vuln`, `tenable:io:assets`, `tenable:sc:vuln`
     - Check the log file for any errors - `$SPLUNK_HOME/var/log/splunk/splunkd.log`
• Note that the app only imports new information from Tenable.sc. So if you have not scanned recently, there will not be any updates.

4. While running Tenable.io, I get the following error: ERROR pid=106020 tid=MainThread file=io_connect.py:__checkResponse:83 | Tenable Error: response: Duplicate export not allowed. Please modify request or wait until existing export is complete.
   • You must create a new, unique user and API login to use in Splunk.

5. I can't set up a connection with Splunk Mission Control.
   • If you have an issue trying to establish connection with Mission Control, refer to Splunk documentation for Splunk Connect for Mission Control.

6. I can't set up a default Instance.
   • If you are unable to find the Tenable Vulnerability Center dashboard under Managed Dashboards section in the Dashboards drop-down, make sure there are no trailing white-spaces for the connection ID fetched from Admin Settings. Refer to Tenable Plugin for Splunk documentation.

7. Data is not populated on Mission Control.
   • If you are not able to find data on Plugin Dashboards/ AQ tabs/ Investigation tabs:
     1. Verify that you have an active connection between the On-premise instance and Mission Control by navigating to Admin settings > Product Settings > Splunk Connect for Mission Control. Check the connection status against the configured instance.
     2. If the status is Inactive, please refer to Splunk documentation.
     3. If the status is Active, verify that the Tenable application’s look-up has data by referring to Tenable App for Splunk documentation.

8. The Analyst Queue and Investigation tabs are not getting rendered for a particular Notable in Splunk Mission Control.
   • If you are not able to render Tenable Summary Analyst Queue tabs and Tenable Investigation tabs, make sure the label for the given notable is mcef_tenable_plugin_for_
**mission_control.** If not, update the label for that notable manually with the edit option or reconfigure the Notable Events step in the Tenable App for Splunk documentation with the correct label.