# Table of Contents

- Welcome to Tenable for Splunk .......................................................... 4
  - Components ................................................................................. 5
- Tenable Add-on (TA-tenable) .............................................................. 6
  - Source and Source Types .............................................................. 6
  - Splunk Common Information Model Mapping .................................. 7
- **Installation Workflow** ................................................................. 9
  - Splunk Environments .................................................................. 9
  - Installation .................................................................................. 10
- **Configuration** .............................................................................. 16
  - Create an Input ........................................................................... 16
  - Configure Tenable Identity Exposure ........................................... 22
  - Configure Tenable Nessus Network Monitor .................................... 25
  - Configure Tenable OT Security Account and Data Collection ............ 28
  - Configure Tenable Security Center Credentials .............................. 31
  - Configure Tenable Security Center Certificates .............................. 35
  - Configure Tenable Vulnerability Management ............................... 40
- **Tenable Data in Splunk Dashboard** .............................................. 45
  - Vulnerability Center Dashboard .................................................... 47
  - Saved Searches ........................................................................... 49
- **Adaptive Response** ..................................................................... 52
  - Alert Action Configuration ........................................................... 56
- **Additional Information** ............................................................... 58
  - Best Practices ............................................................................ 58
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customized Actions</td>
<td>58</td>
</tr>
<tr>
<td>Tenable Macros</td>
<td>59</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>60</td>
</tr>
</tbody>
</table>
Welcome to Tenable for Splunk

The Tenable for Splunk integration performs data collection, normalization, and visualization. The integration is divided into two parts:

- **Tenable Add-On for Splunk (TA-tenable)** provides all data collection and normalization functionality.
- **Tenable App for Splunk** provides a dashboard to view the Tenable data in Splunk.

**Note:** The Tenable integration with Splunk also supports Splunk "Cloud" versions.

Tenable integration topology:
Components

The Tenable Add-on has specific purposes for each Splunk component. The available components are in the following list:

**Heavy Forwarder**

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

**Note:** Configure inputs to run from the heavy forwarder.

**Note:** Enable the key value store (KV) on the heavy forwarder.

**Search Head**

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

**Note:** 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 API endpoints:

Asset Export

Note: By default, assets/export endpoints fetch both licensed and unlicensed assets.

- POST /assets/export
- GET /assets/export/{export_uuid}/status
- GET /assets/export/{export_uuid}/chunks/{chunk_id}

Vulnerability Export

Note: By default, vulns/export endpoints fetch only licensed vulnerabilities.

- POST /vulns/export
- GET /vulns/export/{export_uuid}/status
- GET /vulns/export/{export_uuid}/chunks/{export_uuid}

Plugins

- GET /plugins/plugin

Source and Source Types

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

Tenable Security Center

<table>
<thead>
<tr>
<th>Source</th>
<th>Source type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;username&gt;</td>
<td>&lt;address&gt;</td>
<td>tenable:sc:vuln</td>
</tr>
</tbody>
</table>
and agent scans.

<table>
<thead>
<tr>
<th>Source</th>
<th>Source type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 Vulnerability Management

<table>
<thead>
<tr>
<th>Source</th>
<th>Source type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tenable_io://&lt;data input name&gt;</td>
<td>tenable:io:vuln</td>
<td>Collects cumulative vulnerability data from active, agent and frictionless assessment scans from licensed assets.</td>
</tr>
<tr>
<td>tenable_io://&lt;data input name&gt;</td>
<td>tenable:io:assets</td>
<td>Collects all assets data.</td>
</tr>
<tr>
<td>tenable_io://&lt;data input name&gt;</td>
<td>tenable:io:plugin</td>
<td>Collects all plugin detail data.</td>
</tr>
</tbody>
</table>

### Tenable OT Security

<table>
<thead>
<tr>
<th>Source</th>
<th>Source type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tenable_ot://&lt;data input name&gt;</td>
<td>tenable:ot:vuln</td>
<td>Collects cumulative vulnerability data from active, agent and frictionless assessment scans from licensed assets.</td>
</tr>
<tr>
<td>tenable_ot://&lt;data input name&gt;</td>
<td>tenable:ot:assets</td>
<td>Collects all assets data.</td>
</tr>
<tr>
<td>tenable_ot://&lt;data input name&gt;</td>
<td>tenable:ot:plugin</td>
<td>Collects all plugin detail data.</td>
</tr>
</tbody>
</table>

### Splunk Common Information Model Mapping

This chart displays mapping for Tenable vulnerability findings to Splunk Common Information Model (CIM).
<table>
<thead>
<tr>
<th>Field Name from Tenable Vulnerability Management API</th>
<th>Field Name from Tenable Security Center API</th>
<th>CIM Field Name</th>
<th>CIM Data Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>asset_fqdn</td>
<td>dnsName</td>
<td>dns_name</td>
<td>vulnerability</td>
</tr>
<tr>
<td>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>
Installation Workflow

Use the following workflow to complete the installation and configuration of the Tenable applications for Splunk.

**Note:** The Tenable Splunk integration app versions 6.0.3 and later do not support web application findings, host audits, or cloud findings. Refer to one of Tenable's other integration applications with Splunk (e.g., Tenable Web App Scanning Add-on for Splunk). For a list of available Splunk applications, see Splunk's Discover Apps page.

Before you begin:

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

To install and configure Tenable applications for Splunk:

1. [Install](#) the Tenable application.
2. Configure the required Tenable application for Splunk: [Tenable Vulnerability Management](#), [Tenable Security Center Credentials](#), [Tenable Security Center Certificates](#), [Tenable Nessus Network Monitor](#), [Tenable Identity Exposure](#), or [OT Security](#).

   **Note:** You need unique credentials for each Splunk environment.

3. [Create an input](#) for the configured Tenable application for Splunk.
4. [Configure](#) your Tenable App for Splunk dashboard.
5. [Configure adaptive response](#) actions.

Splunk Environments

The installation process 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. Use this instance to install the Tenable Add-on and Tenable App on this node. Complete the setup 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 Tenable Add-On and Tenable App installation information 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></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-premises Splunk instance that works as a heavy forwarder.

You can install the application via a command line or from the Splunk user interface.

**Installation**

For Tenable Vulnerability Management:

*Minimum Required User Role:* Basic User

*Note:* The Tenable integration with Splunk works with a **Basic User** if that user is assigned **Can View** permissions on the assets they are to export, along with **Can Use** permissions on tags the assets are
assigned. Without the **Can Use** tag permissions, the assets return undefined or the integration fails to export vulnerabilities if a tag filter is used. For more information on Tenable Vulnerability Management permissions and user roles, refer to [Permissions](#) in the *Tenable Developer Portal*.

For Tenable Security Center:

**Minimum Required User Role:** Vulnerability Analyst

**Before you begin:**

- 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.

**To install Tenable Add-on for Splunk and Tenable App for Splunk for the first time:**

1. Log in to Splunk.
2. Go to **Apps** at the top of the screen.

   A drop-down menu appears:
3. Click **Find More Apps**.

4. On the **Browse More Apps** page, type Tenable in the search bar.

   Tenable-related options appear:

5. Click the **Install** button next to **Tenable Add-on for Splunk**.
6. Restart Splunk if a **Restart Required** prompt displays.

To upgrade Tenable Add-on for Splunk and Tenable App for Splunk:

1. Log in to Splunk.
2. Go to **Apps** at the top of the screen.
   
   A drop-down menu appears:

3. Click **Manage Apps**.
4. In the search bar, type Tenable.
   
   Tenable-related options appear:
5. In the **Version** column, click **Update to x.y.z** version link for Tenable Add-On for Splunk:

6. Restart Splunk if a **Restart Required** prompt appears.

**Note:** You can set `useMillisecondsForScVulns` = True in the configuration under `TA-Tenable/default/ta_tenable_settings.conf` to enable millisecond based time fields in Tenable Security Center vulnerability data. Add the following lines under `local/ta_tenable_settings.conf` if you do not want the change to be reset after a plugin update: `[sc_configuration] and useMillisecondsForScVulns` = True

**Note:** You can optionally update the default chunk size for Tenable Vulnerability Management export host vulnerabilities and export host assets sync calls. To update the default setting, open the `$SPLUNK_HOME/etc/apps/TA-tenable/default/inputs.conf` file, and update the value of `vuln_num_assets` (number of assets used to chunk the vulnerabilities) and `assets_chunk_size` (number of assets per exported chunk) in `tenable_io` stanza as per requirement. Save the file changes and restart Splunk.

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

**Note:** If SSL Verification is not needed for a particular product, you can set it to 'False' by navigating to `$SPLUNK_HOME/etc/apps/TA-tenable/bin/tenable_consts.py` and disable it for that particular product. The list of product flags:
Next, configure the Tenable application.

- verify_ssl_for_ot = True
- verify_ssl_for_sc_cert = True
- verify_ssl_for_sc_api_key = True
- verify_ssl_for_sc_creds = True
Configuration

Tenable provides multiple application configuration options for the Tenable Add-On for Splunk.

View the corresponding pages for steps to configure your application:

- Tenable Identity Exposure
- Tenable Vulnerability Management
- Tenable Tenable Nessus Network Monitor
- Tenable OT Security
- Tenable Security Center Credentials
- Tenable Security Center Certificates

**Note:** Splunk versions 6.0.3 and later do not support web application findings, host audits, or cloud findings.

Create an Input

After you complete the configuration for your Tenable Add-On for Splunk, you must create the input. The following process outlines input creation if you have a deployment with Tenable Add-On for Splunk or Tenable App for Splunk.

**To create an input:**

1. In the left navigation bar, click Tenable Add-On for Splunk, Tenable App for Splunk.
2. Click the Inputs tab.
3. Click **Create New Input**.

A new configuration window appears.

4. Provide the following information.

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

**Tenable Vulnerability Management**

<table>
<thead>
<tr>
<th>Input Parameters</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The unique name for each Tenable data input.</td>
<td>Yes</td>
</tr>
<tr>
<td>Interval</td>
<td>The interval parameter specifies when the input restarts to perform the task again. This supports seconds</td>
<td>Yes</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td>The index in which to store Tenable Vulnerability Management data.</td>
<td></td>
</tr>
<tr>
<td><strong>Global Account</strong></td>
<td>Splunk pulls data from this Tenable account.</td>
<td></td>
</tr>
<tr>
<td><strong>Sync Plugin Details</strong></td>
<td>If selected, the related tags in Tenable assets include plugin details.</td>
<td></td>
</tr>
<tr>
<td><strong>Host Vulnerability</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Start Time</strong></td>
<td>The date and time to start collecting host data. If you leave this field blank, the integration collects all historical data. (Enter in this format - YYYY-MM-DD hh:mm:ss.)</td>
<td>No</td>
</tr>
<tr>
<td><strong>Lowest Severity Score</strong></td>
<td>The lowest level of severity stored.</td>
<td>No</td>
</tr>
<tr>
<td><strong>Historical Fixed Vulnerability</strong></td>
<td>Allows the import of host vulnerabilities fixed before the current day.</td>
<td>No</td>
</tr>
</tbody>
</table>
### Tags

| Tags | Limits host vulnerabilities pulled to host assets that have tags selected. | No |

### Tenable Security Center Vulnerability

<table>
<thead>
<tr>
<th>Input Parameters</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The unique name for each Tenable data input.</td>
<td>Yes</td>
</tr>
<tr>
<td>Interval</td>
<td>The interval parameter specifies when the input restarts to perform the task again. This supports seconds (between 300 and 86400) or a cron schedule.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Note:** Restricting the input to collect data during inactive scan periods with a cron schedule is recommended, especially for large Security Center deployments. For smaller deployments, a minimum interval of one hour (3600) can be used.

<table>
<thead>
<tr>
<th>Index</th>
<th>The index in which to store Tenable Security Center data.</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Account</td>
<td>Splunk pulls data from this Tenable account.</td>
<td>Yes</td>
</tr>
<tr>
<td>Start Time</td>
<td>The date and time to start collecting data. If you leave this field blank, the integration collects all historical data.</td>
<td>No</td>
</tr>
</tbody>
</table>

**Note:** Uses the YYYY-MM-DD hh:mm:ss format.

| Sync Plugin Details | If selected, the related tags in Tenable assets | Yes |
include plugin details.

**Historical Fixed Vulnerability**
Allows the import of vulnerabilities fixed before the current day.

<table>
<thead>
<tr>
<th>Input Parameters</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The unique name for each Tenable data input.</td>
<td>Yes</td>
</tr>
<tr>
<td>Interval</td>
<td>The interval parameter specifies when the input restarts to perform the task again (in seconds).</td>
<td>Yes</td>
</tr>
<tr>
<td>Index</td>
<td>The index in which to store Tenable Security Center data.</td>
<td>Yes</td>
</tr>
<tr>
<td>Global Account</td>
<td>Splunk pulls data from this Tenable account.</td>
<td>Yes</td>
</tr>
<tr>
<td>Query Name</td>
<td>A name for Tenable Security Center vulnerability filter.</td>
<td>No</td>
</tr>
</tbody>
</table>

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

**Tenable Security Center Mobile**

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.
Note: Asset and vulnerabilities in Splunk might differ from individual scan results since the Splunk integration synchronizes cumulative vulnerability and asset data from the Tenable API endpoints.

To create the Tenable OT Security input:

1. Navigate to the Tenable Add-on for Splunk > Inputs.
2. Click Create New Input > Tenable OT Security (ICP).

3. Enter a unique name for the data input in the Name field
4. Enter the time interval of input. (Measured in seconds, after which data gets collected again. min value = 86400 secs. max value = 604800 secs)
5. Select the index in which you want to collect the data.
7. Select the lowest level of vulnerability in the Lowest Severity to Store field that you want to collect.
8. Click **Add** to save the input.

**Configure Tenable Identity Exposure**

You can connect to Tenable Identity Exposure using a syslog input. Configure a default UDP/TCP data input of Splunk with the following steps.

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

**To configure Tenable Identity Exposure with Splunk:**

**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**. More options appear.

7. In the **Source Type** box, enter `tenable:ad: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 Identity Exposure**

1. In the Tenable Identity Exposure console, under **Local Settings**, go to the **Servers > Syslog Servers** screen.
2. Click **+ Add Syslog Server**.
   
   The **Syslog Server** configuration window appears.
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 drop-down list the transport protocol in use. (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**.

---

**Configure Tenable Nessus Network Monitor**

You can connect to Tenable Nessus Network Monitor using a syslog input. Configure a default UDP/TCP data input of Splunk with the following steps.

<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 with Splunk:

**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.

   ![Add Data Page Screenshot]

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**. More 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**.

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.
   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 OT Security Account and Data Collection

Connect to OT Security by creating the account configuration.

Note: The OT Security integration is available for Splunk add-on version 6.3.0 and later.

Account Creation

Complete the following steps to configure your account:
1. Navigate to the **Tenable Add-on for Splunk > Configuration**.

2. Under the **Account** tab click **Add**.

3. Select **Tenable OT Security (ICP)** in the **Tenable Account Type** drop-down.

4. Enter a name in the **Account Name** field.

5. Enter the FQDN or IP of your server for this account without scheme (http:// or https://) in the **Address** field.

6. Enter your API secret in the **API Secret** field.

**Note:** For more information on API keys, see [Generate an API Key](#).
7. (Optional) If you are using a proxy, click the **Proxy Enable** checkbox and complete the proxy fields.

8. Click **Add** to save the configuration.

**Data Collection**

Three types of data are collected for OT Security:

- **Assets data.** Stored in the `tenable:ot:assets` sourcetype:

- **Vulnerability data.** Stored in the `tenable:ot:vuln` sourcetype:
Plugins data. Stored in `tenable:ot:plugin` sourcetype:

For more information, see [Source and Source Types](#).

**Configure Tenable Security Center Credentials**

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

For Tenable Security Center:

**Required User Role:** Security Analyst

To set up 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.

   An **Add Account** window appears:
5. In the **Tenable Access Type** drop-down box, select **Tenable Security Center Credentials**.

6. Enter the necessary information for each field. The following table describes the available options.

<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</td>
</tr>
<tr>
<td>Input</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Tenable Account Type</strong></td>
<td>(Required) The type of Tenable account - Tenable Vulnerability Management, Tenable Security Center API Keys, or Tenable Security Center Certificate.</td>
</tr>
<tr>
<td><strong>Address</strong></td>
<td>(Required) The hostname or IP address for Tenable Security Center.</td>
</tr>
</tbody>
</table>
| **Verify SSL Certificate** | Enabled by default, Splunk verifies the certificate in Tenable Security Center. To disable, set one or more of the following to ‘False’ based upon your use case:  
- verify_ssl_for_sc_cert = True  
- verify_ssl_for_sc_api_key = True  
- verify_ssl_for_sccreds = True |
| **Username** | (Required) The username in Tenable Security Center. |
| **Password** | The password in Tenable Security Center. |
| **Proxy Enable** | Enables the plugin to collect Tenable Security Center data via a proxy server. If you select this option, the plug- in prompts you to enter the following:  
- **Proxy Type** - the type of proxy used.  
- **Proxy Host** - the hostname or IP address of the proxy server.  
- **Proxy Port** - the port number of the proxy server. |
7. Click **Add** to complete the configuration.

Next steps

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

Configure Tenable Security Center Certificates

To complete the [installation](#) process, you must complete the setup for the Tenable Add-on for Splunk. For additional information on Tenable Security Center Certificates, see [SSL Client Certificate Authentication](#).

To set up 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** box, select **Tenable Security Center Certificates**.
6. Enter the necessary information for each field. The following table describes the available options.

**Note:** The certificates you upload and configure must be associated with a specific user in Tenable Security Center.

<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 Security Center data input.</td>
</tr>
<tr>
<td>Tenable Account Type</td>
<td>(Required) The type of Tenable account - Tenable Vulnerability Management, Tenable Security Center API Keys, or Tenable Security Center Certificate.</td>
</tr>
<tr>
<td>Address</td>
<td>(Required) The hostname or IP address for Tenable Security Center.</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>Enabled by default, Splunk verifies the certificate in Tenable Security Center. To disable, set one or more of the following to 'False' based upon your use case:</td>
</tr>
<tr>
<td></td>
<td>• verify_ssl_for_sc_cert = True</td>
</tr>
<tr>
<td></td>
<td>• verify_ssl_for_sc_api_key = True</td>
</tr>
<tr>
<td></td>
<td>• verify_ssl_for_sccreds = True</td>
</tr>
<tr>
<td>T.sc Access Key</td>
<td>(Required) Tenable Security Center API access key.</td>
</tr>
<tr>
<td>T.sc Secret Key</td>
<td>(Required) Your Tenable Security Center API secret key.</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>
</tbody>
</table>
7. Click **Add** to complete the configuration.

**Install certificate authority:**

1. Run the following command to make a backup of the cacert.pem file.

   ```bash
   # cp $SPLUNK_HOME/etc/apps/TA-tenable/bin/ta_tenable/certifi/cacert.pem /tmp/cacert.pem
   ```

2. Run the following command to append the PEM-encoded root certificate authority that signed the Tenable Security Center SSL certificate to the cacert.pem.

   ```bash
   # cat <path_to_root_ca.pem> >> $SPLUNK_HOME/etc/apps/TA-tenable/bin/ta_tenable/certifi/cacert.pem
   ```
3. Run the following command to restart Splunk.

   # /opt/splunk/bin/splunk restart

Splunk installs the self-signed certificate to trust in your configuration.

Next steps

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

**Configure Tenable Vulnerability Management**

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

**Required User Role:** Administrator

**Before you begin:**

- Generate an API key in Tenable Vulnerability Management to complete the configuration. See the [Tenable Vulnerability Management 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.

**Note:** Asset and vulnerabilities in Splunk might differ from individual scan results since the Splunk integration synchronizes cumulative vulnerability and asset data from the [Tenable API endpoints](#).

**To set up 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

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Name *</td>
<td>admin</td>
</tr>
<tr>
<td>Tenable Account Type *</td>
<td>Tenable.io</td>
</tr>
<tr>
<td>Address *</td>
<td></td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>Yes</td>
</tr>
<tr>
<td>Access Key</td>
<td>.........</td>
</tr>
<tr>
<td>Secret Key</td>
<td></td>
</tr>
<tr>
<td>Proxy Enable</td>
<td>No</td>
</tr>
</tbody>
</table>

* Enter a unique name for this account.
* Select the App for Tenable.
* Enter the FQDN or IP of your server for this account.
* Should we verify your SSL certificate?
* Enter the Access Key for this account.
* Enter the secret key for this account.
* Check to enable the proxy.

[Add]
5. Enter the necessary information for each field. The following table describes the available options.

<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 Vulnerability Management, Tenable Security Center API Keys, or Tenable Security Center Certificate</td>
</tr>
<tr>
<td>Address</td>
<td>(Required) The hostname or IP address for Tenable Vulnerability Management.</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>Enabled by default, Splunk verifies the certificate in Tenable Vulnerability Management. To disable, set one or more of the following to ‘False’ based upon your use case:</td>
</tr>
<tr>
<td></td>
<td>• verify_ssl_for_sc_cert = True</td>
</tr>
<tr>
<td></td>
<td>• verify_ssl_for_sc_api_key = True</td>
</tr>
<tr>
<td></td>
<td>• verify_ssl_for_sc_creds = True</td>
</tr>
<tr>
<td>Access Key</td>
<td>(Required) Tenable Vulnerability Management API access key.</td>
</tr>
<tr>
<td>Secret Key</td>
<td>(Required) Your Tenable Vulnerability Management API secret key.</td>
</tr>
<tr>
<td>Proxy Enable</td>
<td>Enables the plugin to collect Tenable Vulnerability Management data via a proxy server. If you select this option, the plugin prompts you to enter the following:</td>
</tr>
<tr>
<td></td>
<td>• Proxy Type - the type of proxy used.</td>
</tr>
<tr>
<td>Proxy Host</td>
<td>the hostname or IP address of the proxy server.</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Proxy Port</td>
<td>the port number of the proxy server.</td>
</tr>
<tr>
<td>Proxy Username</td>
<td>the username for an account that has permissions to access and use the proxy server.</td>
</tr>
<tr>
<td>Proxy Password</td>
<td>the password associated with the username you provided.</td>
</tr>
</tbody>
</table>

6. To complete the configuration, click **Add**.

**Next steps**

- [Create an Input](#) for the Tenable Add-On for Splunk.
Tenable Data in Splunk Dashboard

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

To set up 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 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 populate indices that the Tenable App for Splunk depends on.

1. Navigate to the Tenable App for Splunk.
2. Click Saved Searches.
3. Select Tenable IO Plugin Data - All Time.
   Splunk completes the query.
4. Repeat steps 2 and 3 for other All Time saved searches:
   a. Tenable IO Vuln Data - All Time
   b. Tenable SC Vuln Data - All Time

Displayed Components
- Total Vulnerabilities Found Today
- Active Vulnerabilities Found Today
- Fixed Vulnerabilities Found Today
- Total Vulnerabilities
- Active Vulnerabilities
- Fixed Vulnerabilities
- Top 10 Vulnerabilities
- Top 10 Vulnerable Assets
- Vulnerabilities by Severity
- Top 10 Latest Plugins

Tenable Nessus Network Monitor Data in Splunk Dashboard

The Tenable App for Splunk provides a single dashboard showing all of your Tenable Nessus Network Monitor data. 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

Vulnerability Center Dashboard

Clicking the value in any panel of the Vulnerability Center dashboard results in a drill-down table.

Drill-down tables
Splunk application lookup and drill-down fields for Tenable Vulnerability Management and Tenable Security Center.

<table>
<thead>
<tr>
<th>Tenable Security Center drill-down field</th>
<th>Tenable Security Center lookup field</th>
<th>Tenable Vulnerability Management-Host drill-down field</th>
<th>Tenable Vulnerability Management-Host lookup field</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>SC_address</td>
<td>-</td>
<td>asset_uuid</td>
</tr>
<tr>
<td>DNS Name</td>
<td>dns_name</td>
<td>Data Source</td>
<td>data_source</td>
</tr>
<tr>
<td>First Found</td>
<td>first_found</td>
<td>Asset Name</td>
<td>dns_name</td>
</tr>
<tr>
<td>-</td>
<td>ip</td>
<td>First Found</td>
<td>first_found</td>
</tr>
<tr>
<td>-</td>
<td>last_fixed</td>
<td>-</td>
<td>last_fixed</td>
</tr>
<tr>
<td>Last Found</td>
<td>last_found</td>
<td>Last Found</td>
<td>last_found</td>
</tr>
<tr>
<td>Plugin ID</td>
<td>plugin_id</td>
<td>Plugin ID</td>
<td>plugin_id</td>
</tr>
<tr>
<td>Port</td>
<td>port</td>
<td>Port</td>
<td>port</td>
</tr>
<tr>
<td>Protocol</td>
<td>protocol</td>
<td>Protocol</td>
<td>protocol</td>
</tr>
<tr>
<td>-</td>
<td>repository_id</td>
<td>Severity</td>
<td>severity</td>
</tr>
<tr>
<td>Severity</td>
<td>severity</td>
<td>Solution</td>
<td>solution</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>Solution</td>
<td>solution</td>
<td>State</td>
<td>state</td>
</tr>
<tr>
<td>State</td>
<td>state</td>
<td>Signature</td>
<td>synopsis</td>
</tr>
<tr>
<td>Signature</td>
<td>synopsis</td>
<td>-</td>
<td>vpr_score</td>
</tr>
</tbody>
</table>

**Tenable Vulnerability Management-Plugin drill-down field**

<table>
<thead>
<tr>
<th>Tenable Vulnerability Management-plugin lookup field</th>
<th>Tenable Security Center-Plugin drill-down field</th>
<th>Tenable Security Center-plugin lookup field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plugin ID</td>
<td>Plugin ID</td>
<td>plugin_id</td>
</tr>
<tr>
<td>Plugin Name</td>
<td>Plugin Name</td>
<td>plugin_name</td>
</tr>
<tr>
<td>-</td>
<td>plugin_version</td>
<td>plugin_family_id</td>
</tr>
<tr>
<td>Severity</td>
<td>risk_factor</td>
<td>-</td>
</tr>
<tr>
<td>Solution</td>
<td>plugin_solution</td>
<td>plugin_version</td>
</tr>
<tr>
<td>Signature</td>
<td>plugin_synopsis</td>
<td>Severity</td>
</tr>
<tr>
<td>Publication Date</td>
<td>plugin_publication_date</td>
<td>plugin_synopsis</td>
</tr>
<tr>
<td>-</td>
<td>plugin_modification_date</td>
<td>Solution</td>
</tr>
<tr>
<td>-</td>
<td>vpr_score</td>
<td>Publication Date</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>plugin_modification_date</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>vpr_score</td>
</tr>
</tbody>
</table>

**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 Search Types**

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

```
io_vuln_data_lookup
```

**Tenable Vulnerability Management asset data:** Type the following command to view the KV store collection for Tenable Vulnerability Management host asset data.

```
io_asset_data_lookup
```

**Tenable Vulnerability Management plugin data:** Type the following command to view the KV store collection for Tenable Vulnerability Management plugin data.

```
io_plugin_data_lookup
```

**Tenable Security Center Saved Searches**

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

```
sc_vuln_data_lookup
```

**Tenable Security Center asset data:** Type the following command to view the KV store collection for Tenable Security Center asset data.

```
sc_asset_data_lookup
```

**Tenable Security Center plugin data:** Type the following command to view the KV store collection for Tenable Security Center plugin data.

```
sc_plugin_data_lookup
```
Tenable Nessus Network Monitor Saved Search Types

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

```bash
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 Tenable Nessus Network Monitor events.

```bash
tenable:nnm:vuln
```
Adaptive Response

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

Before you begin:

Select an index on the Alert Actions Configuration tab in the Tenable Configuration section to retrieve data.

To configure saved actions:

Configure adaptive response actions when you create a correlation search.

Note: When you run the search, the actions are retrieved automatically

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


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

A drop-down menu appears:

4. Click **Content**.

More 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 appears:
11. Select the appropriate action for your search.

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

14. Click **Save**.

A confirmation message appears.

15. Run a search.

---

**Adaptive Response Actions**

**Add New Response Action**

- **Request Scan for Tenable IO**
  - **Scan Name**: Enter the Scan Name.
  - **Host Name**: Supports hostname and token both. e.g: 'ipvm.biz' or $result.dest$
  - **IP Address**: Supports ip and token both. e.g: 'some.example.com'/'215.2.1' or $result.dest_ip$ or $result.dest$

- **Scan Machine for Tenable SC**

---

**Adaptive Responses**

<table>
<thead>
<tr>
<th>Response</th>
<th>Mode</th>
<th>Time</th>
<th>User</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get Vulnerability Summary</td>
<td>adhoc</td>
<td>2018-04-12T17:22:35+0530</td>
<td>system</td>
<td>✓ success</td>
</tr>
<tr>
<td>Notable</td>
<td>saved</td>
<td>2018-04-11T14:09:07+0530</td>
<td>nobody</td>
<td>✓ success</td>
</tr>
</tbody>
</table>

View Adaptive Response Invocations

**Alert Action Configuration**

To configure alert actions:
1. In the Tenable navigation bar, click **Configuration**.

   The **Configuration** page appears:

   ![Configuration page screenshot](image)

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:

- [Customized Actions](#)
- [Update Macro Definition](#)
- [Troubleshooting](#)

Best Practices

The Splunk 6.1.1 Tenable Add-on fix can cause a small amount of duplicate data to be synced to the Splunk index. To address this, Tenable recommends using deduplication in queries when searching for Tenable Vulnerability Management data in Splunk. Tenable dashboard in Splunk takes care of showing only the unique vulnerabilities.

Customized Actions

The Tenable Add-on for Splunk provides an option that allows you to call a customized action manually. 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.
3. Select **Run Adaptive Response Action**.
   - 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.
   - Set your $SPLUNK_HOME environment.

2. I don’t see data after setting up mod input.
   - For Tenable Security Center mod-input, check the $SPLUNK_HOME/var/log/splunk/ta_tenable_tenable_securitycenter.log.
   - For Tenable Security Center mobile mod-input, check the $SPLUNK_HOME/var/log/splunk/ta_tenable_tenable_securitycenter_mobile.log file.
   - For Tenable OT Security mod-input, check the $SPLUNK_HOME/var/log/splunk/ta_tenable_tenable_ot_security_icp.log file.

3. Data is not populating the Tenable App dashboards.
   - Run an All Time saved search for Tenable Vulnerability Management or Tenable Security Center. 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 set the Tenable index correctly.
   - The dashboard can take some time to populate when data collection starts. To ensure you are receiving all available data, take the following steps:
     - search `get_tenable_index` | stats count by source type
• Check the log file for any errors - $SPLUNK_HOME/var/log/splunk/splunkd.log

• The app only imports new information from Tenable Security Center. So if you have not scanned recently, there may not be any updates.

4. **While running Tenable Vulnerability Management, 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.
```

• Create a new, unique user and API login to use in Splunk.

5. **I can't set up a default Instance.**

• If you are unable to find the Tenable Vulnerability Center dashboard under the 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.

6. **I am getting an error when applying internal self-signed SSL certificates to Tenable Security Center.**

• You may get the following error if your Tenable Security Center self-signed certificate is not installed to Splunk and the optional Verify SSL Certificate setting is enabled. Completing this installation allows Splunk to trust the designated SSL client certificate you installed.
You need to install the CA for the Splunk integration to trust. For more information, see Configure Tenable Certificates.

7. Connection aborted due to "Remote end closed connection without response" error in Splunk logs.

   If the “Remote end closed connection without response” error shows in either the ta_tenable_tenable_io.log, ta_tenable_tenable_securitycenter.log, or ta_tenable_tenable_securitycenter_mobile.log files at location $SPLUNK_HOME/var/log/splunk, make sure that there is no ongoing data collection process in Splunk while stopping the
Splunk service or upgrading the Tenable Application for Splunk or Splunk Add-on. Whenever this type of error occurs, Splunk tries again to process the failed request by using the same checkpoint values after coming back online.

8. **Fields are not getting displayed on the “Inputs > Add Tenable.io” / “Inputs > Update Tenable.io” page.**

   - If you are not able to see a few fields on the Inputs > Add Tenable.io and Inputs > Update Tenable.io pages after upgrading the Tenable Application for Splunk, reload cached content in the browser.

9. **Input is created successfully but data is not getting collected for OT Security.**

   - Check the data by expanding the time range in Splunk search.

   - Make sure that you are entering the correct search query. For example, if you want to search OT Security assets data, the search query should be `index = your_index sourcetype = tenable:ot:assets`.

   - Check the log messages for any errors:

     - For logs related to OT Security data collection: You can view the logs in the `ta_tenable_tenable_ot_security_icp.log` log file by navigating to `$_SPLUNK_HOME/var/log/splunk/`.

     - For logs related to OT Security account creation: You can view the logs in the `ta_tenable_account_validation.log` log file by navigating to `$_SPLUNK_HOME/var/log/splunk/`.

     - Error log messages regarding OT Security data collection and account creation can also be seen from Splunk search in the _internal index.

       - Data collection: `index = _internal source = *ta_tenable_tenable_ ot_security_icp* ERROR`

       - Account creation: `index = _internal source = *ta_tenable_account_ validation* ERROR`

**Note:** `$SPLUNK_HOME` is the path where Splunk is installed.