



Tenable and Splunk Integration Guide

Last Revised: July 10, 2023



Table of Contents

Welcome to Tenable for Splunk	4
Components	6
Tenable Add-on (TA-tenable)	7
Source and Source Types	8
Splunk Common Information Model Mapping	9
Installation Workflow	10
Upgrade the App from v1 to v4	11
Splunk Environments	13
Installation	15
Configuration	19
Configure Tenable Identity Exposure	20
Configure Tenable Vulnerability Management	23
Configure Tenable Nessus Network Monitor	28
Configure Tenable OT Security	31
Configure Tenable Security Center Credentials	34
Configure Tenable Security Center Certificates	39
Create an Input	44
Tenable Data in Splunk Dashboard	51
Vulnerability Center Dashboard	54
Saved Searches	57
Adaptive Response	59
Alert Action Configuration	64
Additional Information	65



Best Practices	66
Customized Actions	67
Tenable Macros	68
Troubleshooting	69
Known Issues	73
Splunk Integration v6.2 (BETA) Content	74
Source and Source Types	75
Create an Input	76
Tenable Data in Splunk Dashboard	81
Vulnerability Center Dashboard	84
Saved Searches	87
Troubleshooting	89
Known Issues	93



Welcome to Tenable for Splunk

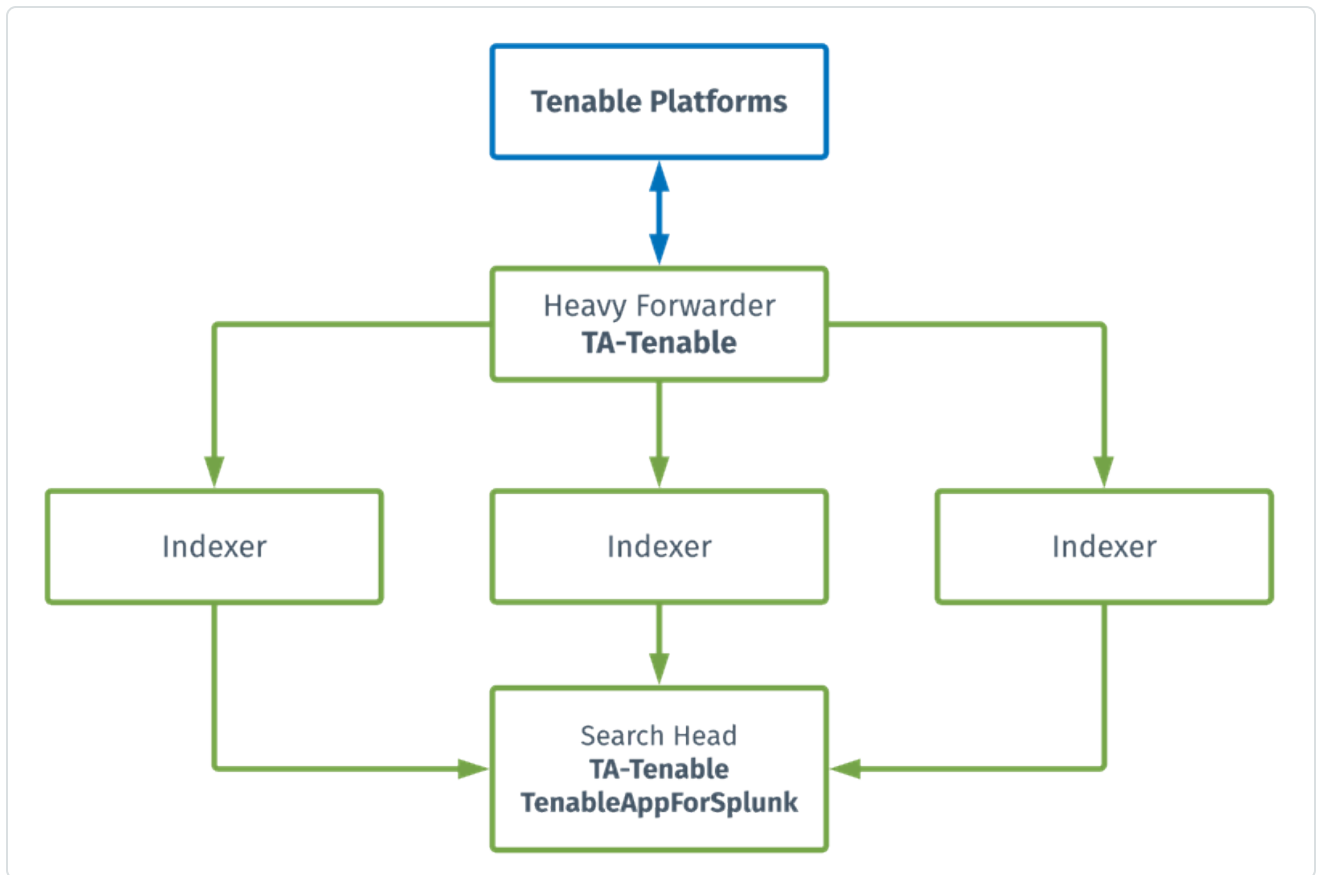
The Tenable for Splunk application performs data collection, normalization, and visualization. The application is divided into two parts:

- [Tenable Add-On for Splunk \(TA-tenable\)](#) provides all data collection and normalization functionality.
- [Tenable Web App Scanning Add-on for Splunk](#) provides all data collection and normalization functionality.
- [Tenable App for Splunk](#) provides a dashboard to view the Tenable data in Splunk.

Tenable Application Topology



The Tenable Web App Scanning Add-On for Splunk pulls data from Tenable platforms and normalizes it in Splunk. The current Tenable Web App Scanning Add-on uses the following pyTenable SDK to retrieve all data.





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.

Indexer

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

Note: Use a default index or create and set a custom index. (Required)

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.

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

Tenable Web App Scanning

Source	Source type	Description
<username> <address>	tenable:io:vuln:was	This collects all vulnerability data.

Tenable Security Center

Source	Source type	Description
<username> <address>	tenable:sc:vuln	Collects cumulative vulnerability and compliance data from active and agent scans.
<username> <address>	tenable:sc:assets	Collects all assets data.
<username> <address>	tenable:sc:plugin	Collects all plugin detail data.

Tenable Vulnerability Management

Source	Source type	Description
tenable_io://<data input name>	tenable:io:vuln	Collects cumulative vulnerability data from active, agent and frictionless assessment scans from licensed assets.
tenable_io://<data input name>	tenable:io:assets	Collects all assets data.
tenable_io://<data input name>	tenable:io:plugin	Collects all plugin detail data.



Splunk Common Information Model Mapping

This chart displays mapping for Tenable vulnerability findings to Splunk Common Information Model (CIM).

Field Name from Tenable Vulnerability Management API	Field Name from Tenable Security Center API	CIM Field Name	CIM Data Model
asset_fqdn	dnsName	dns_name	vulnerability
ipv4	ip	dest_ip	vulnerability
plugin.bid	bid	bugtraq	vulnerability
plugin.family	family.name	category	vulnerability
plugin.synopsis	synopsis	signature	vulnerability
Tenable	Tenable	vendor	vulnerability
Tenable.io	Tenable.sc	product	vulnerability



Installation Workflow

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

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

Before you begin:

- Complete the [Upgrade the App from v1 to v4](#) 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 [Tenable 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.



Upgrade the App from 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:

- Back up 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. Doing this ensures that you lose no data.
- 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 Web App Scanning 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. Use this instance to install the Tenable Web App Scanning Add-On, 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.

Component	Forwarder	Indexer	Search Head
Tenable Add-on for Splunk (TA-Tenable)	Yes <ul style="list-style-type: none">• configure accounts• configure data input	No	Yes <ul style="list-style-type: none">• configure accounts
Tenable-SC App for Splunk (Tenable App)	No	No	Yes

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:

Required User Role: Administrator

For Tenable Security Center:

Required User Role: Security Manager, Security Analyst, or Vulnerability Analyst

Complete the installation and configuration of the Tenable applications for Splunk according to the following workflow.

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.

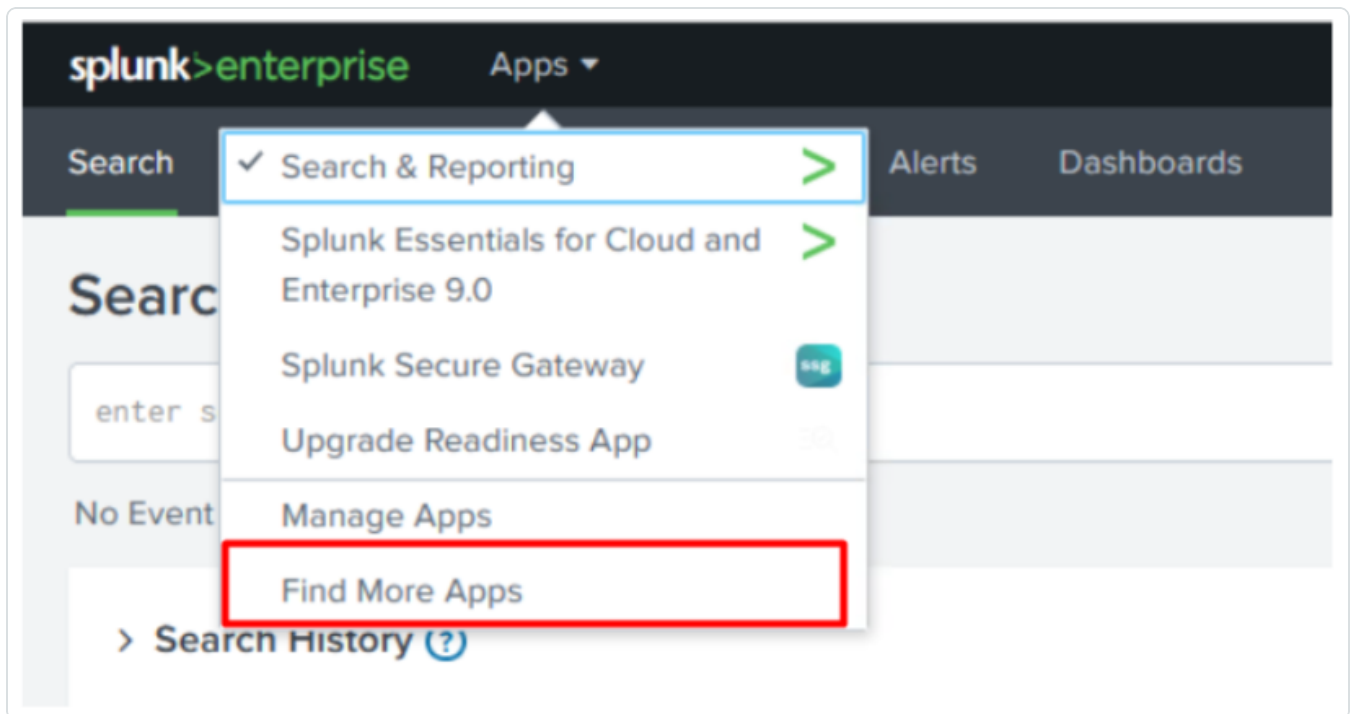
Note: If you install the Tenable App for Splunk on the search head, you must also install the Tenable Add-on.

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

To install Tenable Web App Scanning Add-on for Splunk for the first time:

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

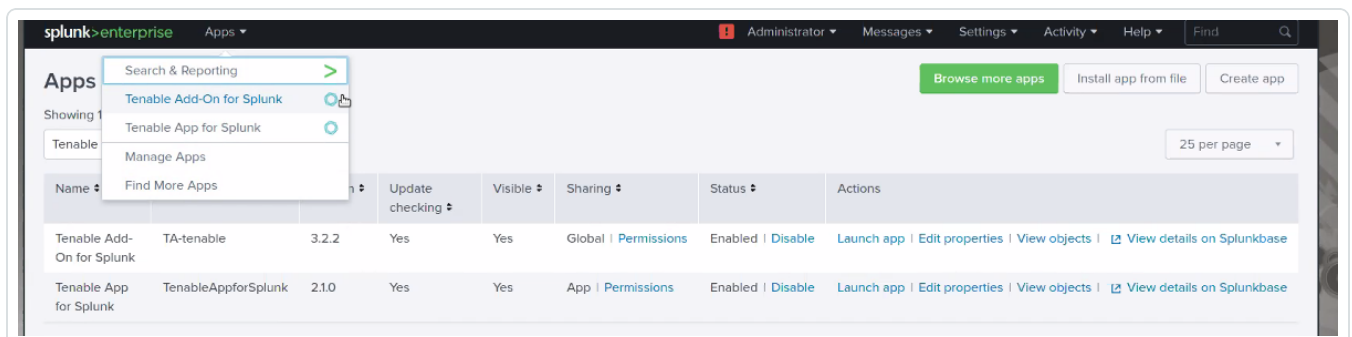
A drop-down menu appears:



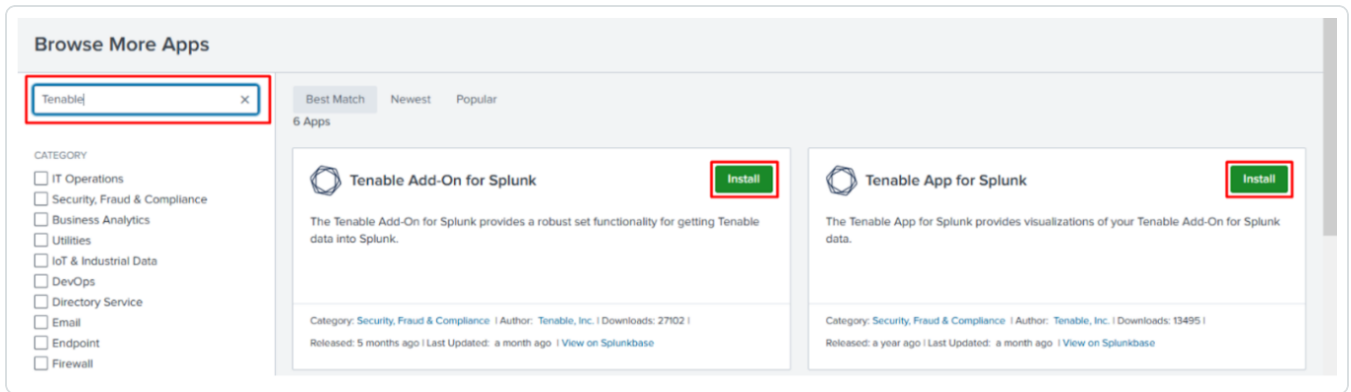
3. Click **Find More Apps**.

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. Click the **Install** button next to **Tenable Tenable Web App Scanning Add-on for Splunk**.
7. Restart Splunk if a **Restart Required** prompt displays.

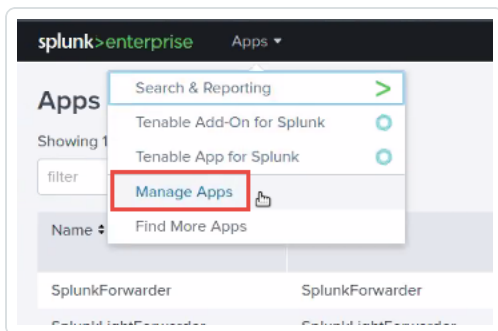
Note: Follow steps 1 to 6 to install the **Tenable App for Splunk**.

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

To upgrade Tenable Web App Scanning Add-on for Splunk:

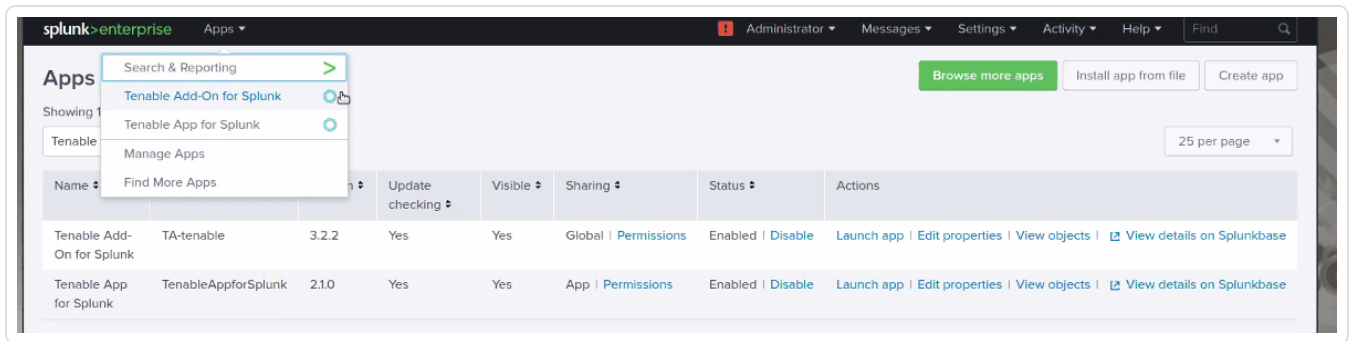
1. Log in to Splunk.
2. Go to **Apps** at the top of the screen.

A drop-down menu appears:

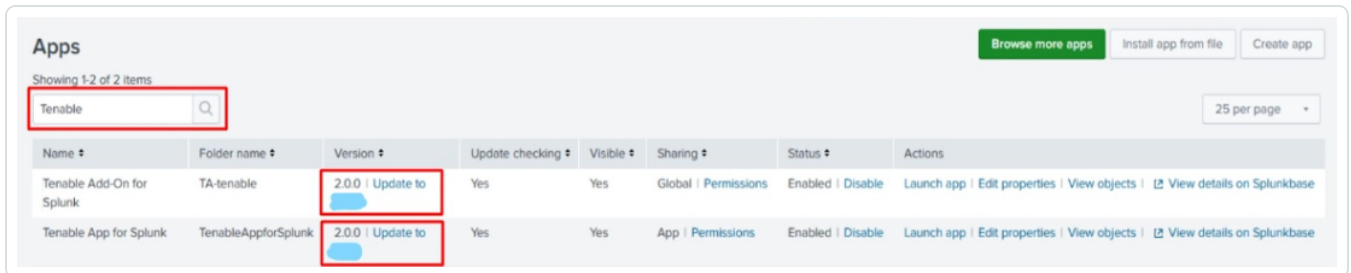


3. Click **Manage Apps**.
4. In the search bar, type Tenable.

Tenable-related options appear:



5. In the **Version** column, click **Update to** x.y.z version link for Tenable Add-On for Splunk:



6. In the **Version** column, click **Update to** x.y.z version link for Tenable Web App Scanning Add-On for Splunk:

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

Note: Follow steps 1 to 6 to upgrade the **Tenable App for Splunk**.

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 value of `vuIn_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.

Next, [configure](#) the Tenable application.



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](#)
- [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.



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.

Source Type	Description
tenable:ad:alerts	This option configures Splunk to accept Tenable Identity Exposure alerts.

To configure Tenable Identity Exposure with Splunk:

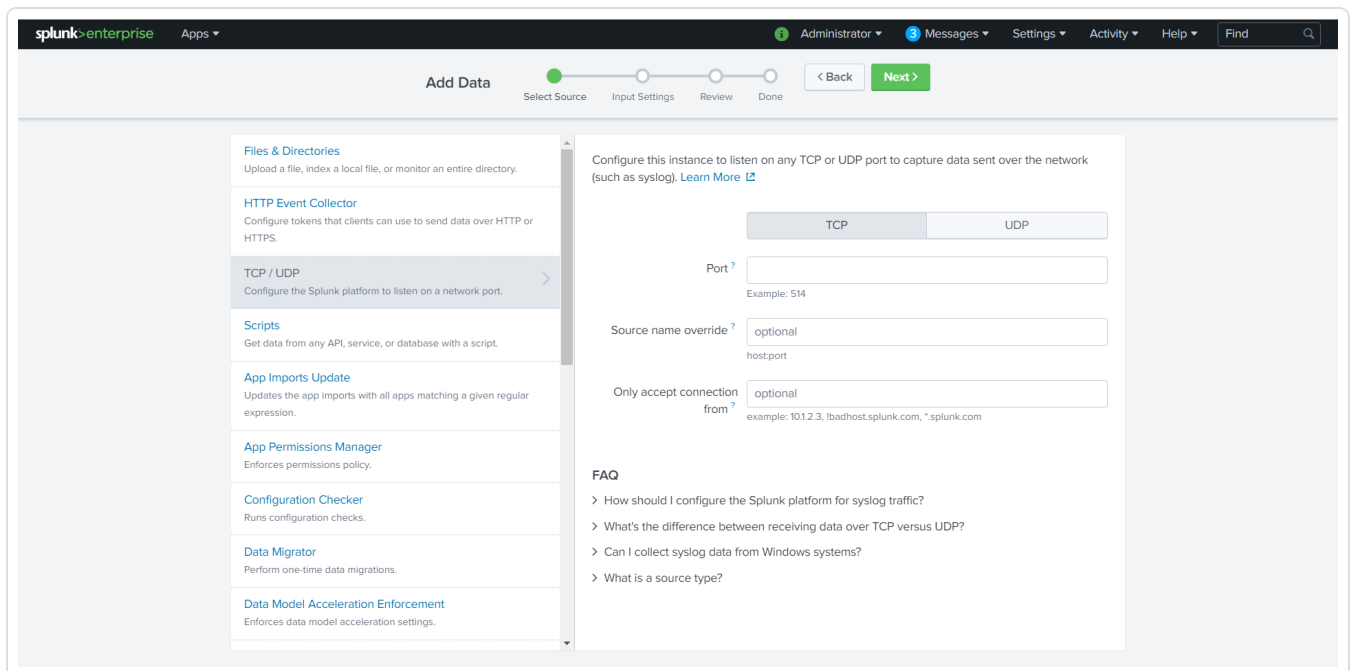
Complete the following steps in Splunk

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.

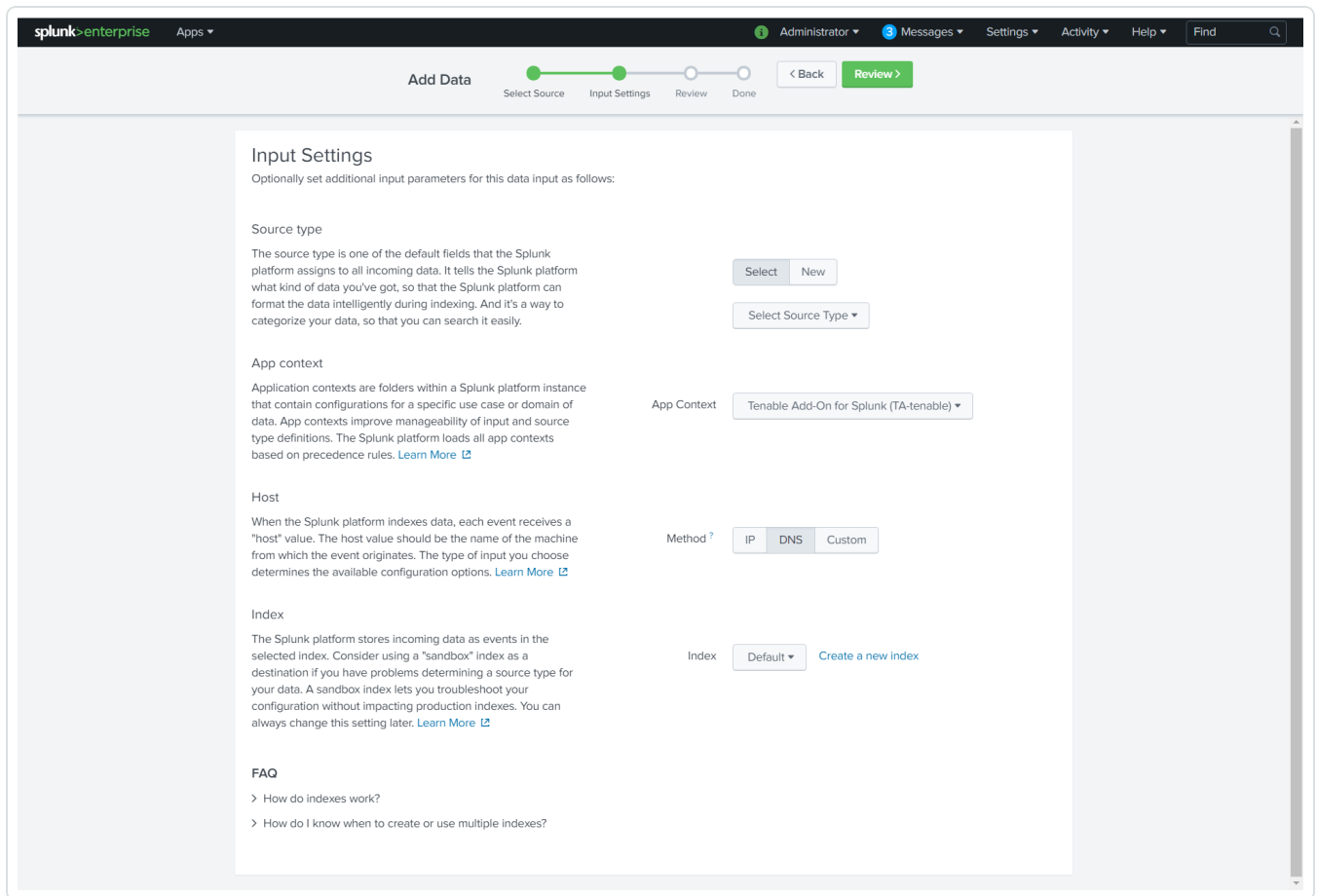


4. Enter the port configuration information.



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**.
14. Review your configuration settings.

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 Vulnerability Management

To complete the [installation](#) process, you must complete the setup for the Tenable Add-on for Splunk.

Required User Role: Administrator

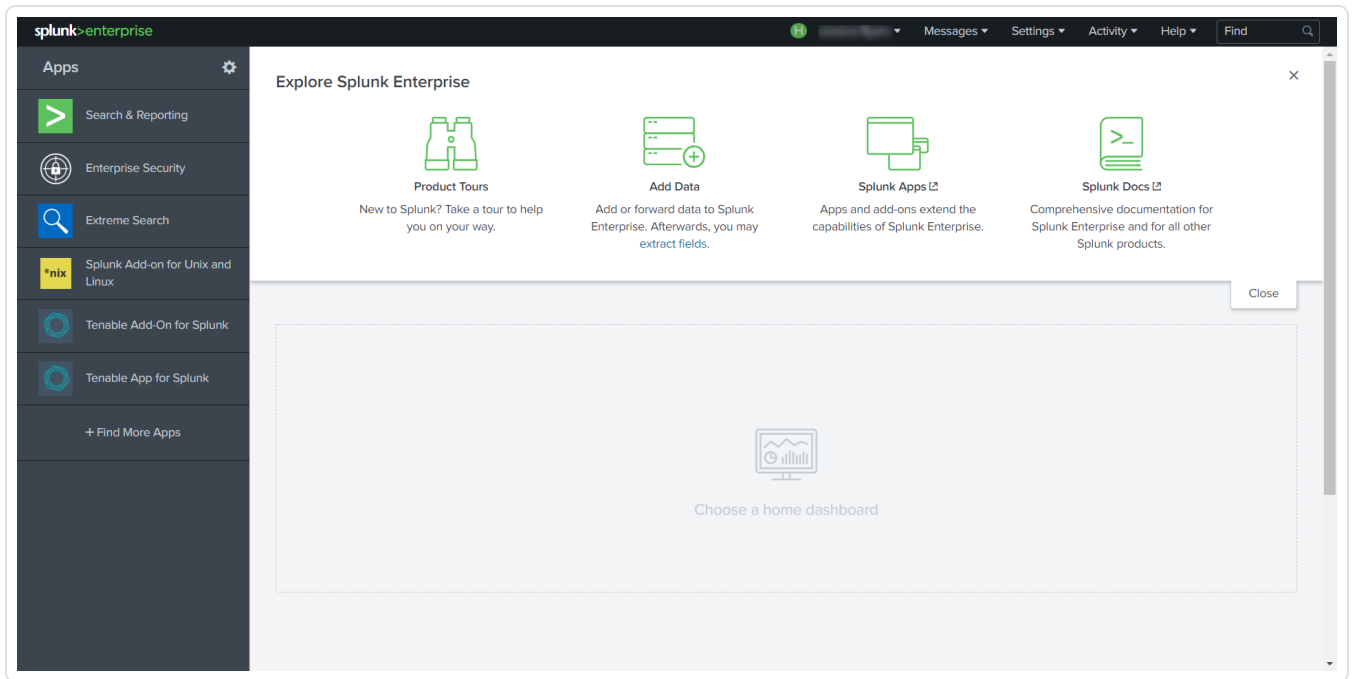
Before you begin:

- 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.

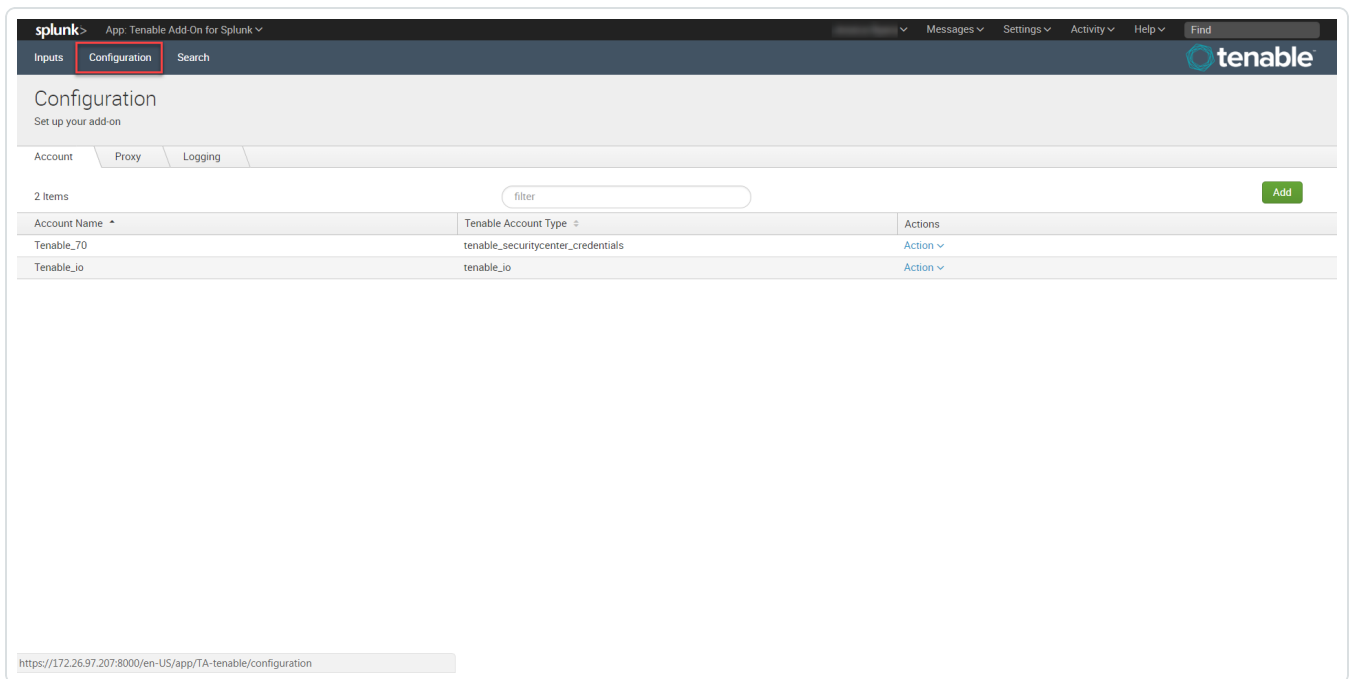
Note: Asset and vulnerabilities in Splunk might differ from individual scan results since the Splunk integration synchronizes cumulative vulnerability and asset data from the [Tenable API endpoints](#).

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 ✕

Account Name *
Enter a unique name for this account.

Tenable Account Type *
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.



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

Input Parameters	Description
Account Name	(Required) The unique name for each Tenable data input.
Tenable Account Type	(Required) The type of Tenable account - Tenable Vulnerability Management, Tenable Security Center API Keys, or Tenable Security Center Certificate
Address	(Required) The hostname or IP address for Tenable Vulnerability Management.
Verify SSL Certificate	If enabled, Splunk verifies the SSL certificate in Tenable Vulnerability Management.
Access Key	(Required) Tenable Vulnerability Management API access key.
Secret Key	(Required) Your Tenable Vulnerability Management API secret key.
Proxy Enable	Enables the plugin to collect Tenable Vulnerability Management data via a proxy server. If you select this option, the plug- in prompts you to enter the following: <ul style="list-style-type: none">• 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.• Proxy Username - the username for an account that has permissions to access and



use the proxy server.

- **Proxy Password** - the password associated with the username you provided.

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

Next steps

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



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.

Source Type	Description
tenable:nm:vuln	This contains all vulnerability data.

To configure Tenable NNM with Splunk:

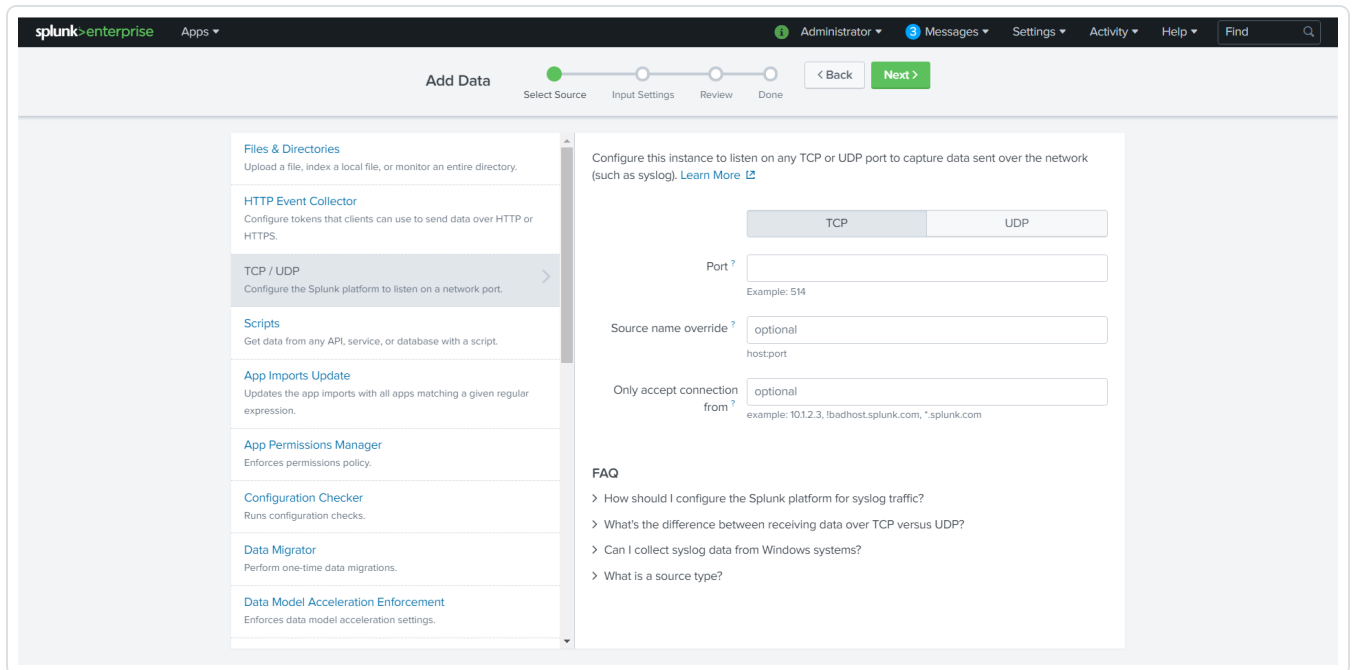
Complete the following steps in Splunk

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.

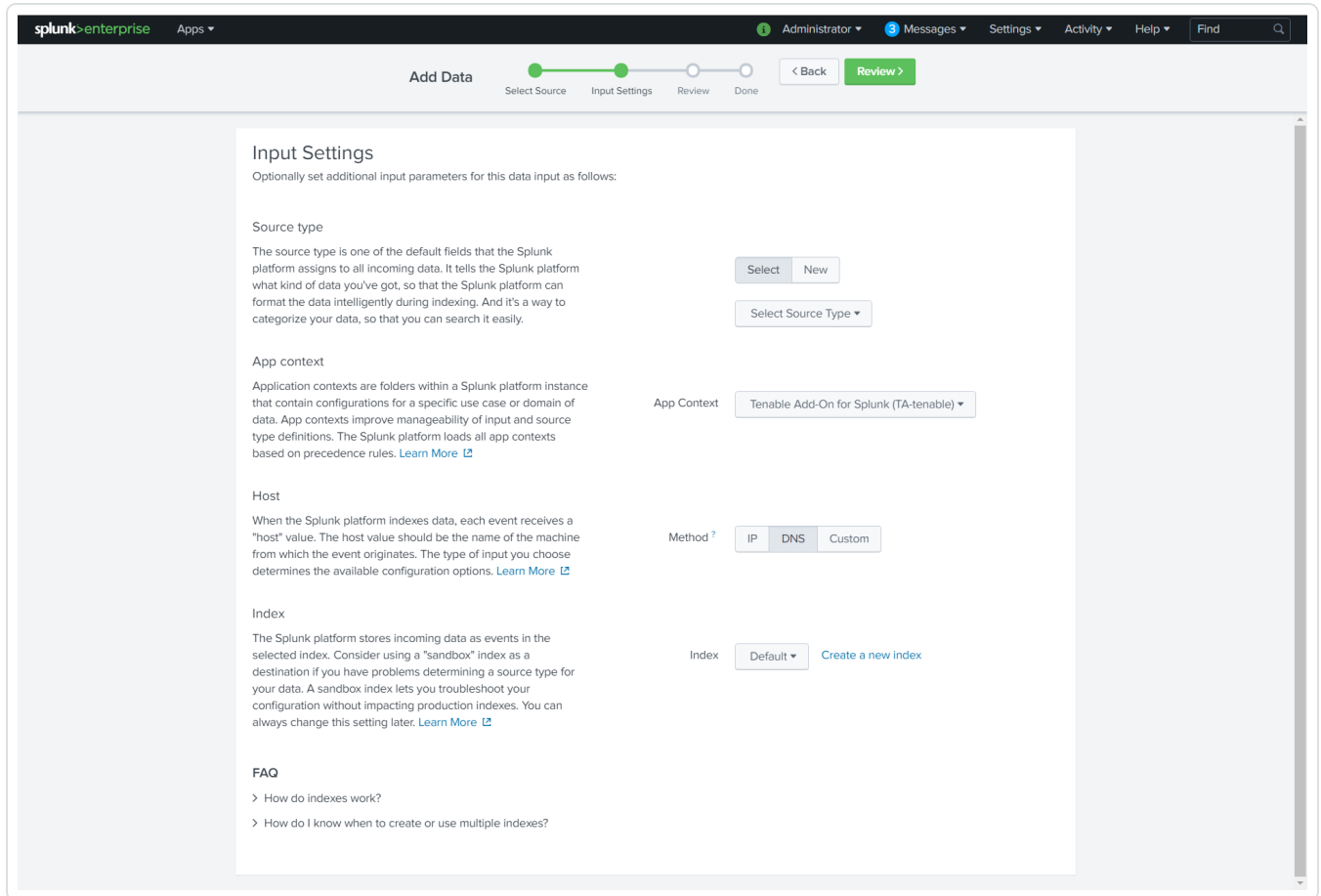


4. Enter the port configuration information.



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:nm: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**.
14. Review your configuration settings.

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 OT Security

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

Source Type	Description
tenable:ot:alerts	This option configures Splunk to accept Tenable OT Security alerts.

To configure Tenable OT Security with Splunk:

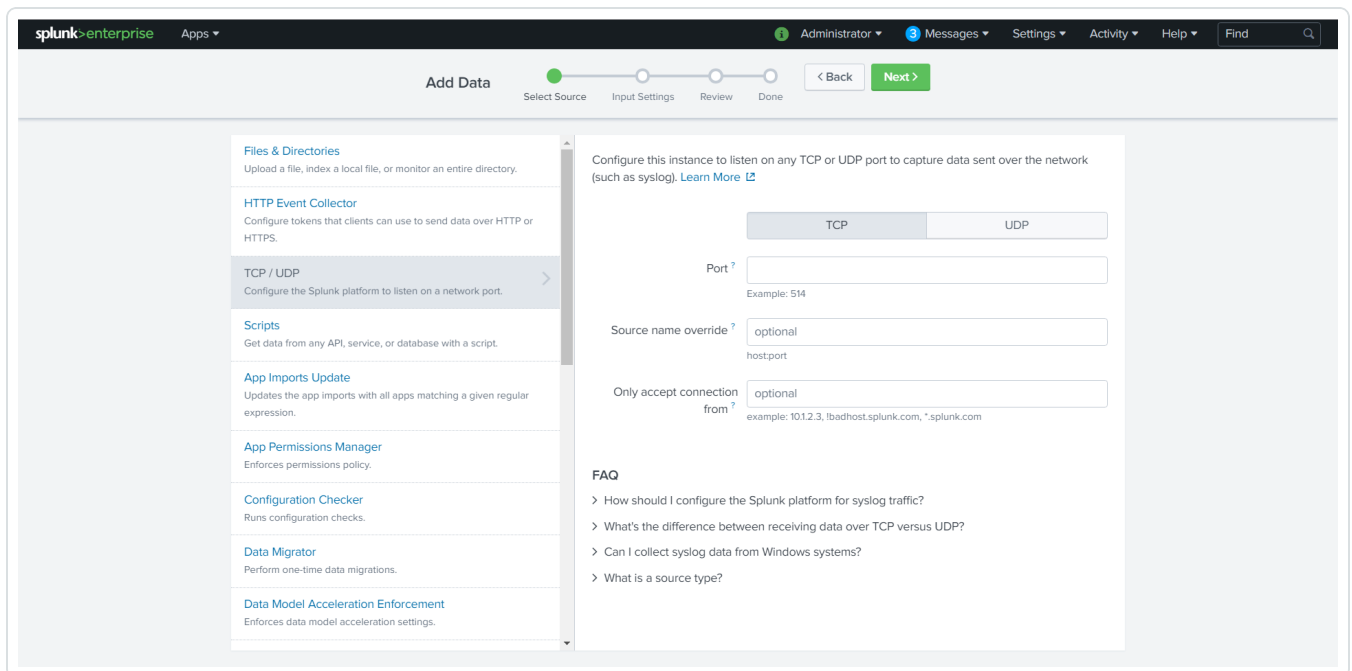
Complete the following steps in Splunk

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:

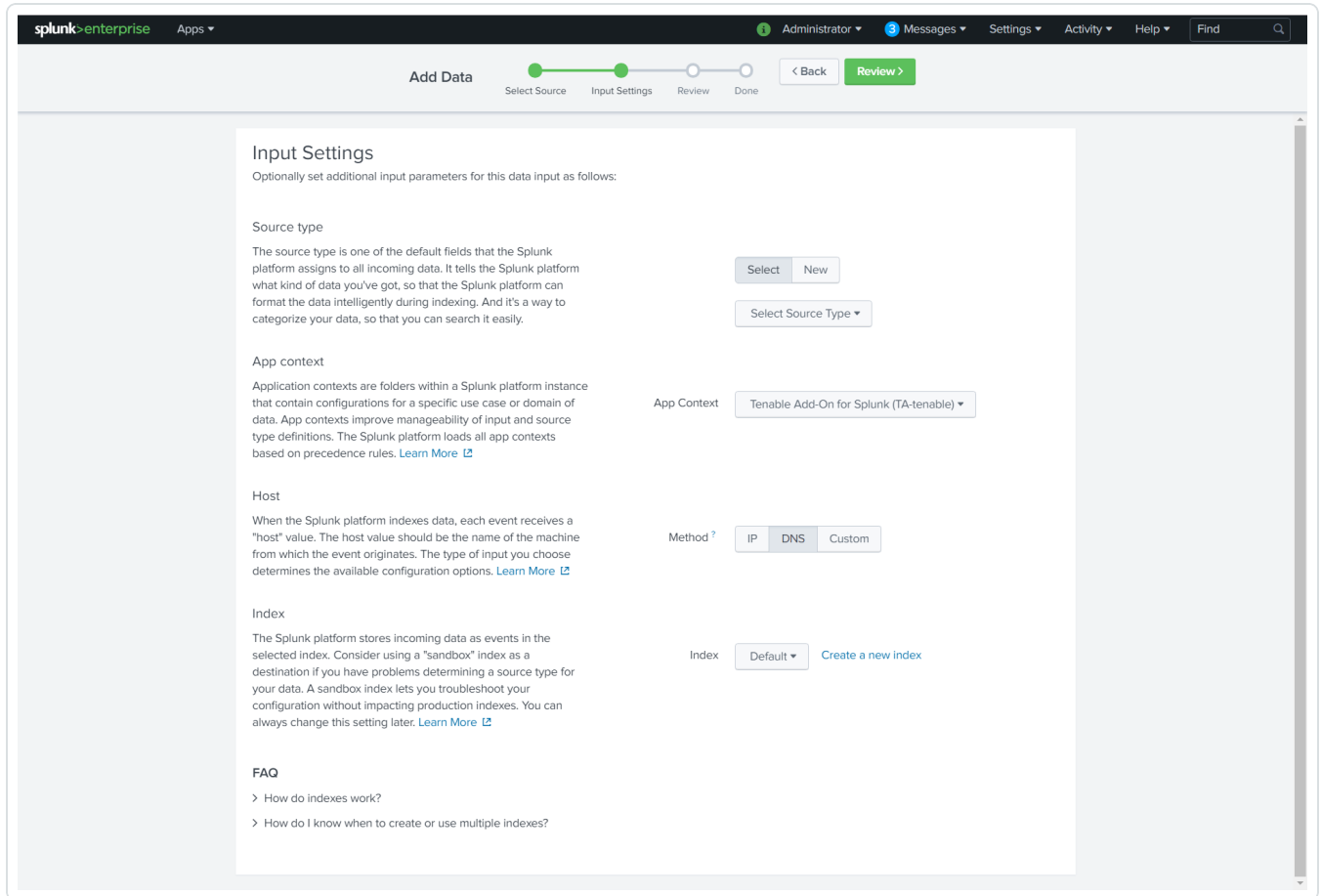


4. Enter the port configuration information.



- At the top of the page, click **Next**.

The **Input Settings** page appears:



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

More options appear.

- In the **Source Type** field, enter `tenable:ot:alerts`.
- In the **Source Type Category** drop-down, select **Tenable**.
- (Optional) Enter a description in the **Source Type Description** field.
- Scroll down to the **Index** option.
- Click on the **Index** drop-down menu.
- Select an **Index**.



13. At the top of the page, click **Review**.
14. Review your configuration settings.

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 Security

1. In the Tenable OT Security 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 Security Center Credentials

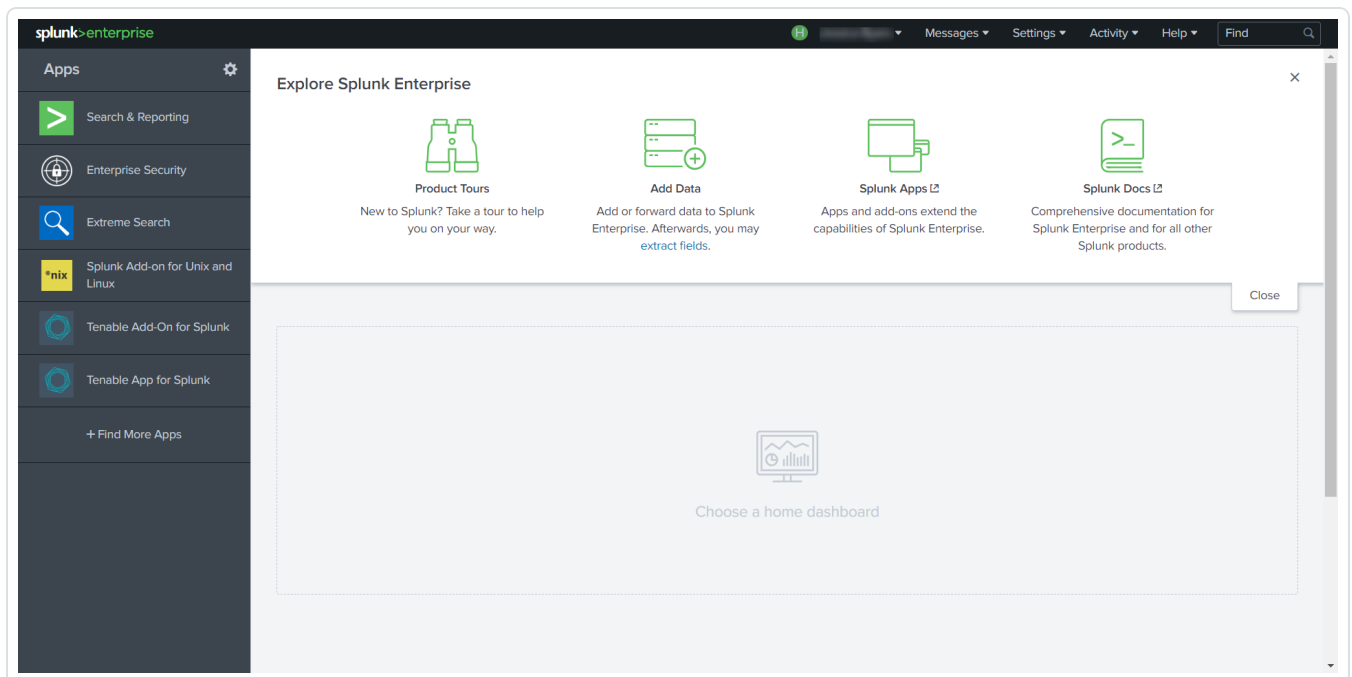
To complete the [installation](#) process, you must complete the setup for the Tenable Add-on for Splunk.

For Tenable Security Center:

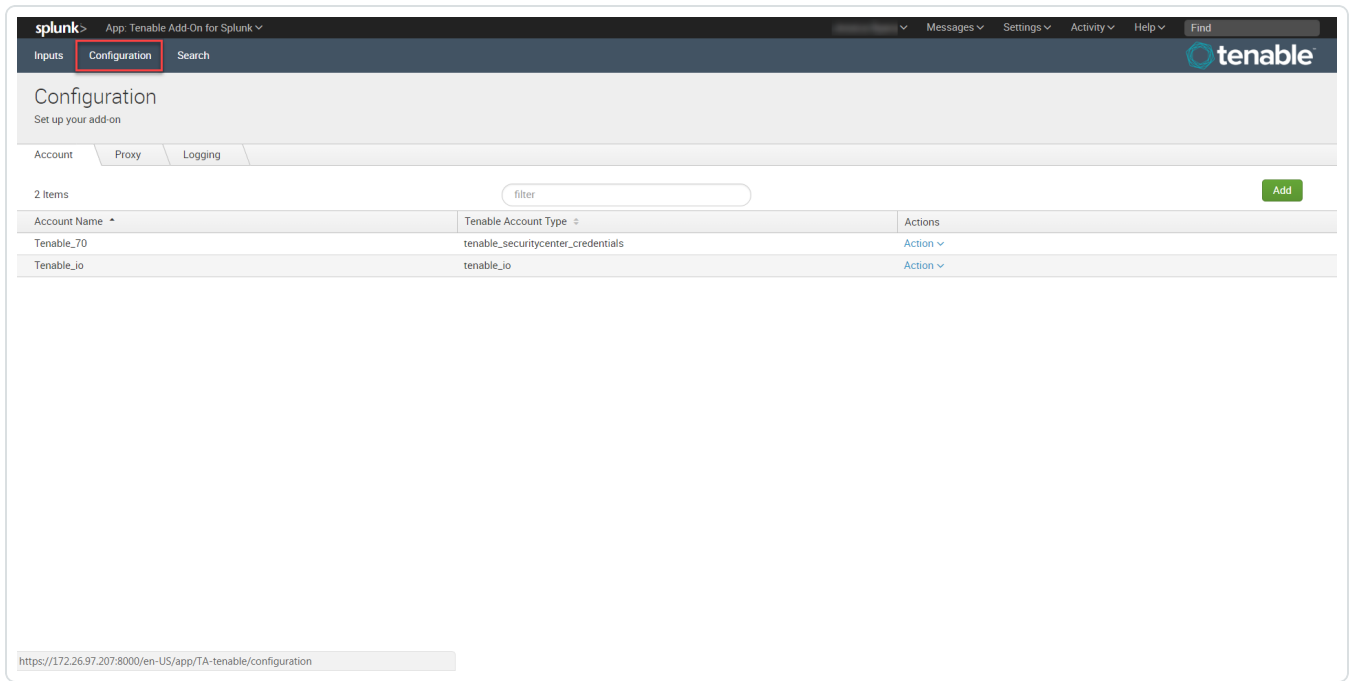
Required User Role: Security Analyst

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:



Add Account ✕

Account Name
Enter a unique name for this account.

Tenable Account Type Tenable.sc Credentials(Deprecated) ✕

Address Tenable.io
✓ Tenable.sc Credentials(Deprecated)
Tenable.sc Certificate
Tenable.sc API Keys

Verify SSL Certificate Should we verify your SSL certificate?

Username
Enter the username for this account.

Password
Enter the password for this account.

Proxy Enable
Check to enable the proxy.

Cancel Add

Note: Tenable Security Center standard credential use is deprecated. Use Tenable Security Center API keys for account authentication. For more information on Tenable Security Center API keys, see [Generate API Keys](#).

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.

Input Parameters	Description
Account Name	(Required) The unique name for each Tenable data input.
Tenable Account Type	(Required) The type of Tenable account - Tenable Vulnerability Management, Tenable Security Center API Keys, or Tenable Security Center Certificate.
Address	(Required) The hostname or IP address for Tenable Security Center.
Verify SSL Certificate	If enabled, Splunk verifies the certificate in Tenable Security Center.
Username	(Required) The username in Tenable Security Center.
Password	The password in Tenable Security Center.
Proxy Enable	<p>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:</p> <ul style="list-style-type: none">• 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.• Proxy Username - the username for an account that has permissions to access and use the proxy server.



- **Proxy Password** - the password associated with the username you provided.

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

Next steps

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

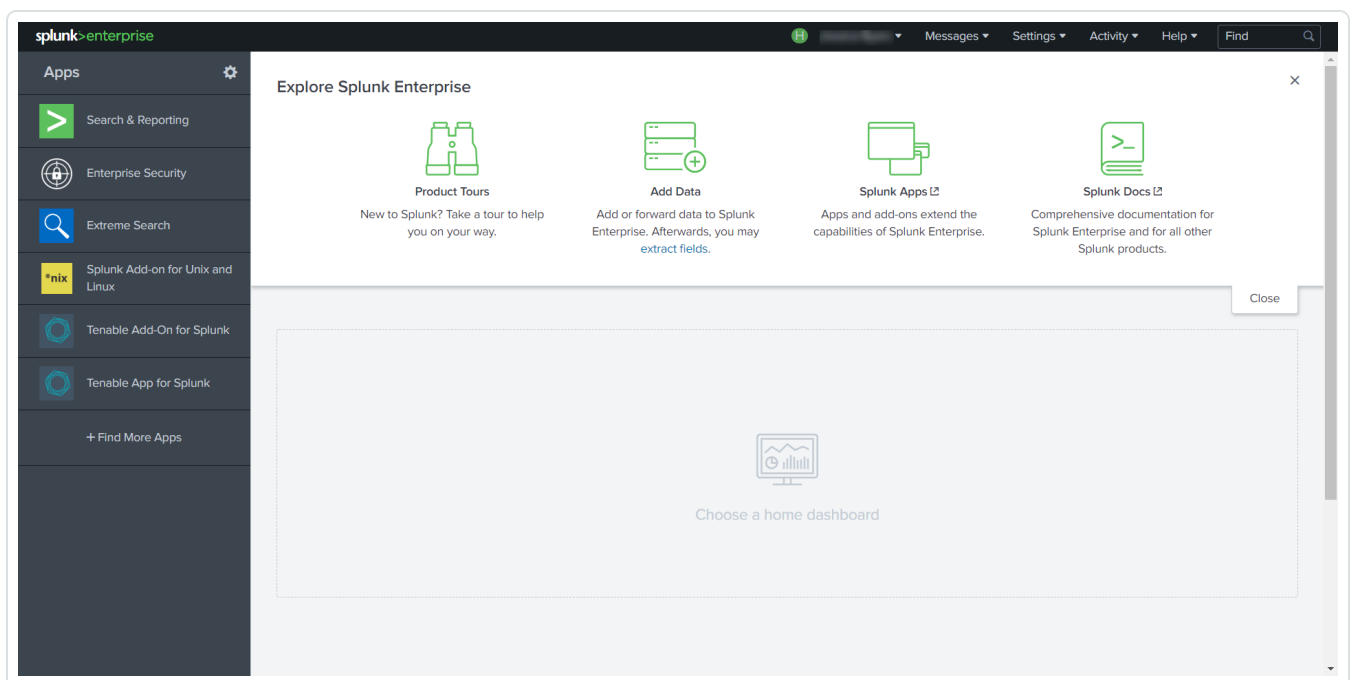


Configure Tenable Security Center Certificates

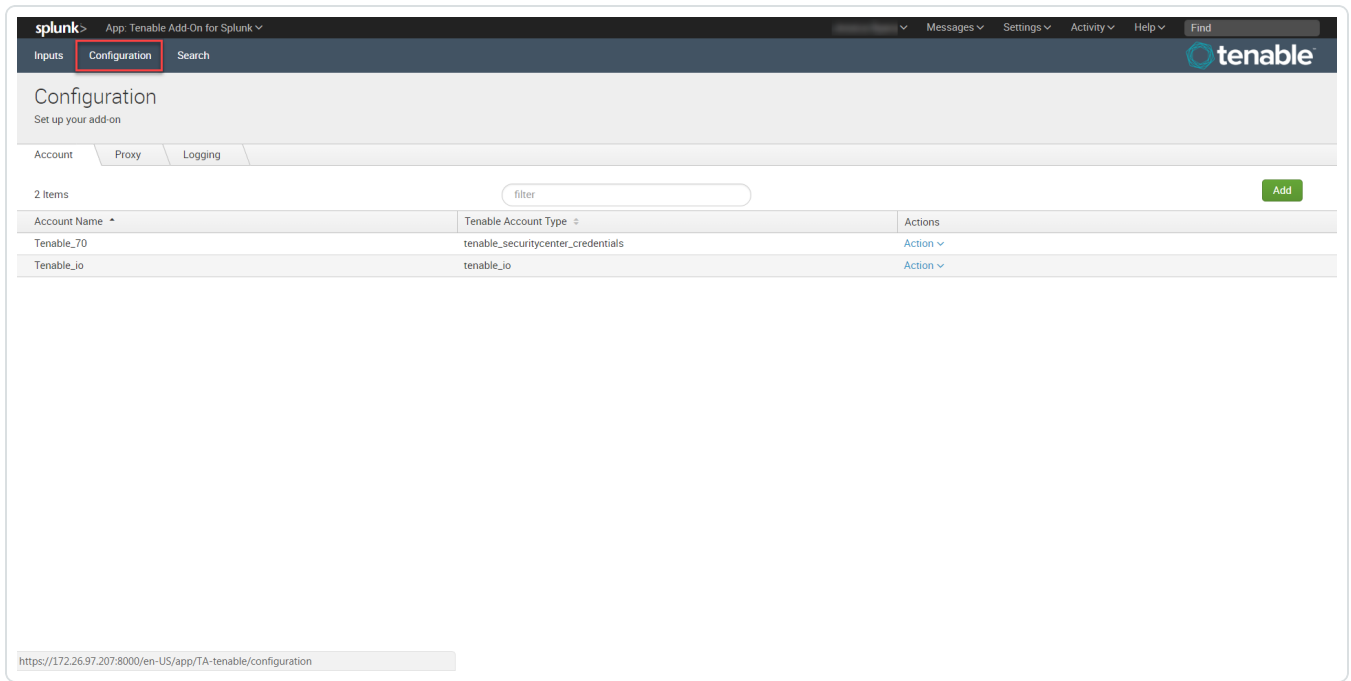
To complete the [installation](#) process, you must complete the setup for the Tenable Add-on for Splunk. For additional information on Tenable Security Center Certificates, see [SSL Client Certificate Authentication](#).

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:



Add Account ✕

Account Name
Enter a unique name for this account.

Tenable Account Type Tenable.sc Certificate ▼ ✕
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?

T.sc Access Key
Enter the Access Key for this account.

T.sc Secret Key
Enter the secret key for this account.

Certificate Filename
Enter the filename of the certificate you stored in
\$SPLUNK_HOME/etc/apps/TA-tenable/certs/

Key Filename
Enter the filename of the key you stored in
\$SPLUNK_HOME/etc/apps/TA-tenable/certs/

Key Password
Enter the key password for this account.

Proxy Enable
Check to enable the proxy.

Cancel Add

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.

Input Parameters	Description
Account Name	(Required) The unique name for each Tenable Security Center data input.
Tenable Account Type	(Required) The type of Tenable account - Tenable Vulnerability Management, Tenable Security Center API Keys, or Tenable Security Center Certificate.
Address	(Required) The hostname or IP address for Tenable Security Center.
Verify SSL Certificate	If enabled, Splunk verifies the SSL Certificate in Tenable Security Center.
T.sc Access Key	(Required) Tenable Security Center API access key.
T.sc Secret Key	(Required) Your Tenable Security Center API secret key.
Certificate Filename	The name of the certificate that you uploaded to <code>\$SPLUNK_HOME/etc/apps/TA-tenable/certs/</code> .
Key Filename	The name of the key that you uploaded to <code>\$SPLUNK_HOME/etc/apps/TA-tenable/certs/</code> .
Key Password	The password for the key file you uploaded.
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:



	<ul style="list-style-type: none">• 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.• Proxy Username - the username for an account that has permissions to access and use the proxy server.• Proxy Password - the password associated with the username you provided.
--	---

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

Install certificate authority:

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

```
# 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.

```
# 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.

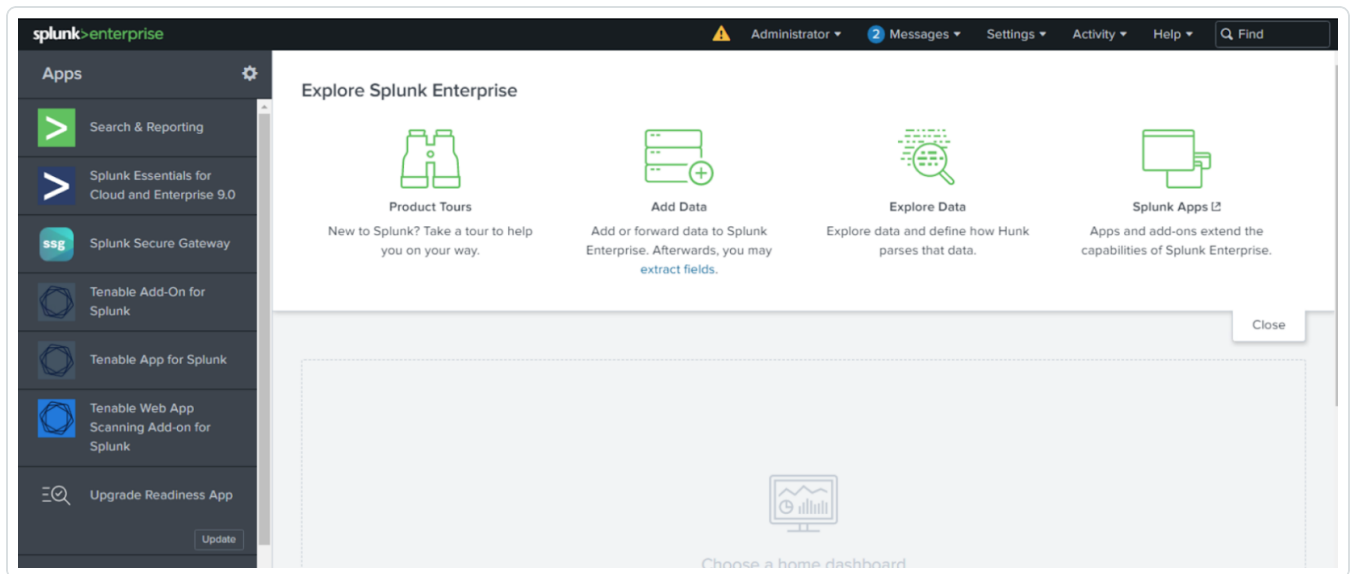


Create an Input

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, Tenable Web App Scanning Add-on for Splunk.

To create an input:

1. In the left navigation bar, click **Tenable Add-On for Splunk**, **Tenable App for Splunk**, or **Tenable Web App Scanning Add-on for Splunk**.



2. Click the **Inputs** tab.



splunk> App: Tenable Add-On for Splunk

Inputs Configuration Search tenable

Inputs Create New Input

Manage your data inputs

2 Inputs Services: All

i	Name	Interval	Index	Status	Actions
>	Tenable_io	3600	default	Enabled	Action
>	tenable_70	86400	default	Enabled	Action

splunk>enterprise Administrator Messages Settings Activity Help Find

Inputs Configuration Search tenable

Inputs Create New Input

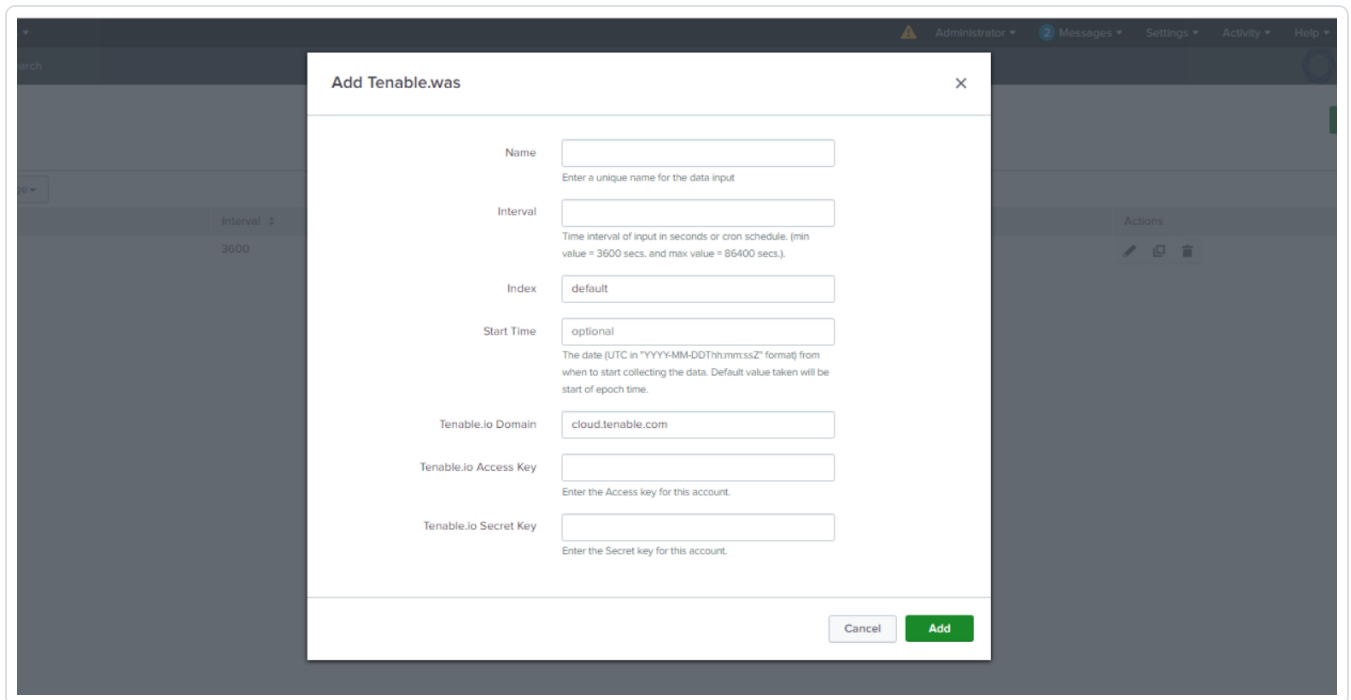
Manage your data inputs

1 Input 10 Per Page

i	Name	Interval	Index	Status	Actions
>	webscanning	3600	default	Enabled	

3. Click **Create New Input**.

The **Add Tenable Web App Scanning Add-on for Splunk** window appears:



4. Click **Create New Input**.

A new configuration window appears.

5. Provide the following information.

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

Tenable Web App Scanning

Input Parameters	Description	Required
Name	The unique name for each Tenable data input.	Yes
Interval	The interval parameter specifies when the input restarts to perform the task again (in seconds). The interval amount must be between 300 and 86400.	Yes
Index	The index in which to store Tenable Vulnerability Management data.	Yes



Start Time	The date and time to start collecting data. If you leave this field blank, the integration collects all historical data. Note: Uses the <i>YYYY-MM-DD hh:mm:ss</i> format.	No
Tenable Vulnerability Management Domain	Splunk pulls data from this Tenable account.	Yes
Tenable Vulnerability Management Access Key	Tenable Vulnerability Management API access key.	Yes
Tenable Vulnerability Management Secret Key	Your Tenable Vulnerability Management API secret key	Yes

Tenable Vulnerability Management

Input Parameters	Description	Required
Name	The unique name for each Tenable data input.	Yes
Interval	The interval parameter specifies when the input restarts to perform the task again (in seconds). The interval amount must be between 3600 and 86400.	Yes
Index	The index in which to store Tenable Vulnerability Management	Yes



		data.	
Global Account		Splunk pulls data from this Tenable account.	Yes
Sync Plugin Details		If selected, the related tags in Tenable assets include plugin details.	Yes
Host Vulnerability	Start Time	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.)	No
	Lowest Severity Score	The lowest level of severity stored.	No
	Historical Fixed Vulnerability	Allows the import of host vulnerabilities fixed before the current day.	No
	Tags	Limits host vulnerabilities pulled to host assets that have tags selected.	No

Tenable Security Center Vulnerability

Input Parameters	Description	Required
Name	The unique name for each Tenable data input.	Yes
Interval	The interval parameter specifies when the	Yes



	<p>input restarts to perform the task again (in seconds). The interval amount must be between 300 and 86400.</p> <p>Note: If using a Tenable Security Center version previous to 5.7, the minimum interval you can select is 24 hours. If using Tenable Security Center 5.7 or later, you can specify a minimum interval of an hour.</p>	
Index	The index in which to store Tenable Security Center data.	Yes
Global Account	Splunk pulls data from this Tenable account.	Yes
Start Time	The date and time to start collecting data. If you leave this field blank, the integration collects all historical data.	No
	<p>Note: Uses the <i>YYYY-MM-DD hh:mm:ss</i> format.</p>	
Sync Plugin Details	If selected, the related tags in Tenable assets include plugin details.	Yes
Historical Fixed Vulnerability	Allows the import of vulnerabilities fixed before the current day.	No
Query Name	A name for Tenable Security Center vulnerability filter.	No
	<p>Note: The interval must be query type Vulnerability Detail List.</p>	
Max Event Size	Maximum allowed size for an event.	No
Page Size	Number of events to be fetched in one page.	No

Tenable Security Center Mobile



Input Parameters	Description	Required
Name	The unique name for each Tenable data input.	Yes
Interval	The interval parameter specifies when the input restarts to perform the task again (in seconds).	Yes
Index	The index in which to store Tenable Security Center data.	Yes
Global Account	Splunk pulls data from this Tenable account.	Yes
Query Name	A name for Tenable Security Center vulnerability filter. <div style="border: 1px solid blue; padding: 5px; margin-top: 10px;">Note: The interval must be query type - Vulnerability Detail List.</div>	No

6. Click **Add** to create the input.
7. Run the **All Time** saved search.
8. 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](#).



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

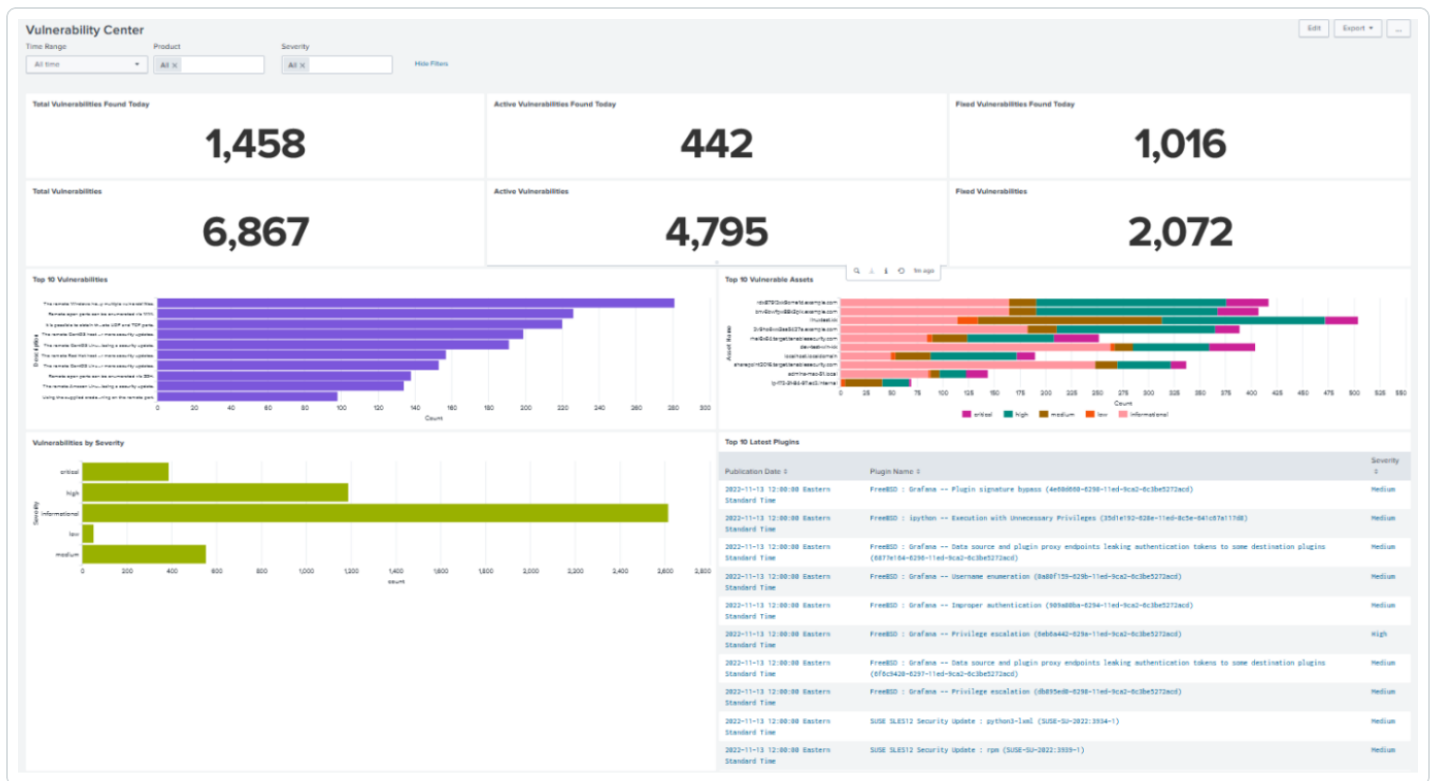
After installation, you must run the **All Time** saved search specific to your Tenable platform. This is a one-time operation to populate indices that the Tenable App for Splunk depends on.

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

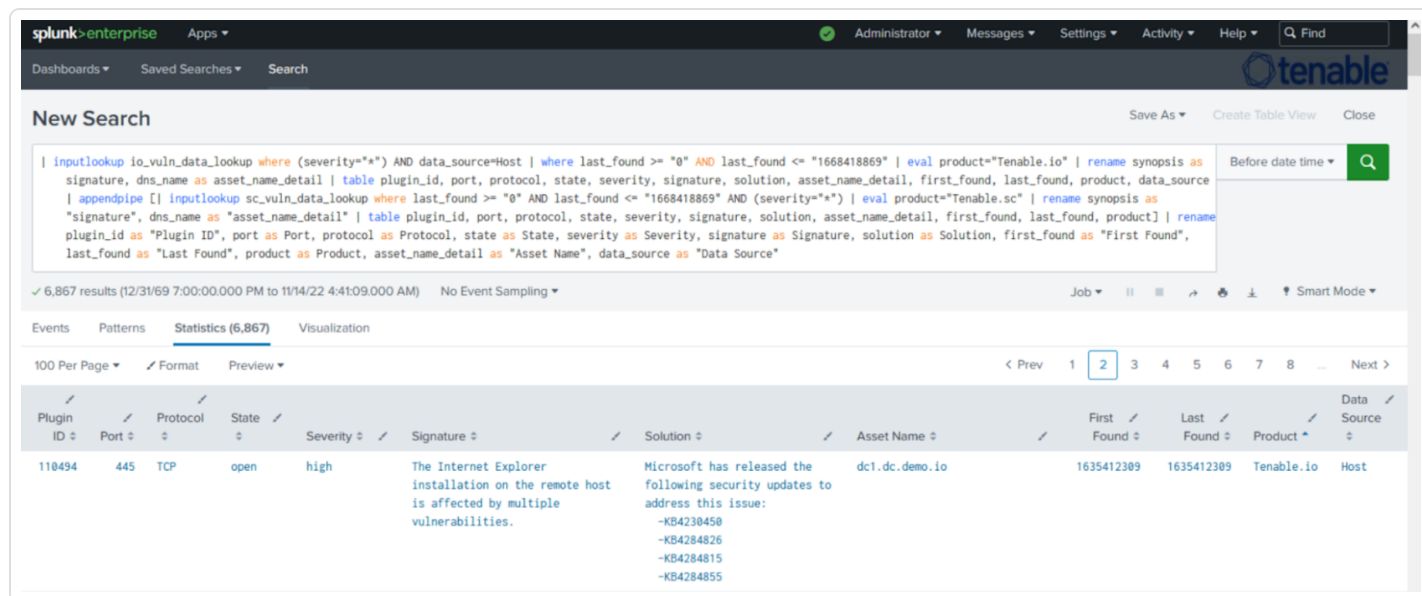
Events

- 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.

Tenable Security Center drill-down field	Tenable Security Center lookup field	Tenable Vulnerability Management-Host drill-down field	Tenable Vulnerability Management-Host lookup field
-	SC_address	-	asset_uuid
DNS Name	dns_name	Data Source	data_source
First Found	first_found	Asset Name	dns_name
-	ip	First Found	first_found
-	last_fixed	-	last_fixed
Last Found	last_found	Last Found	last_found



Plugin ID	plugin_id	Plugin ID	plugin_id
Port	port	Port	port
Protocol	protocol	Protocol	protocol
-	repository_id	Severity	severity
Severity	severity	Solution	solution
Solution	solution	State	state
State	state	Signature	synopsis
Signature	synopsis	-	vpr_score
-	vpr_score	-	-

Tenable Vulnerability Management-Plugin drill-down field	Tenable Vulnerability Management-plugin lookup field	Tenable Security Center-Plugin drill-down field	Tenable Security Center-plugin lookup field
Plugin ID	plugin_id	Plugin ID	plugin_id
Plugin Name	plugin_name	Plugin Name	plugin_name
-	plugin_version	-	plugin_family_id
Severity	risk_factor	-	plugin_family
Solution	plugin_solution	-	plugin_version
Signature	plugin_synopsis	Severity	risk_factor
Publication Date	plugin_publication_date	Signature	plugin_synopsis
-	plugin_modification_date	Solution	plugin_solution
-	vpr_score	Publication Date	plugin_publication_date
-	-	-	plugin_modi-



			fication_date
-	-	-	vpr_score



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.

```
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.

```
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:

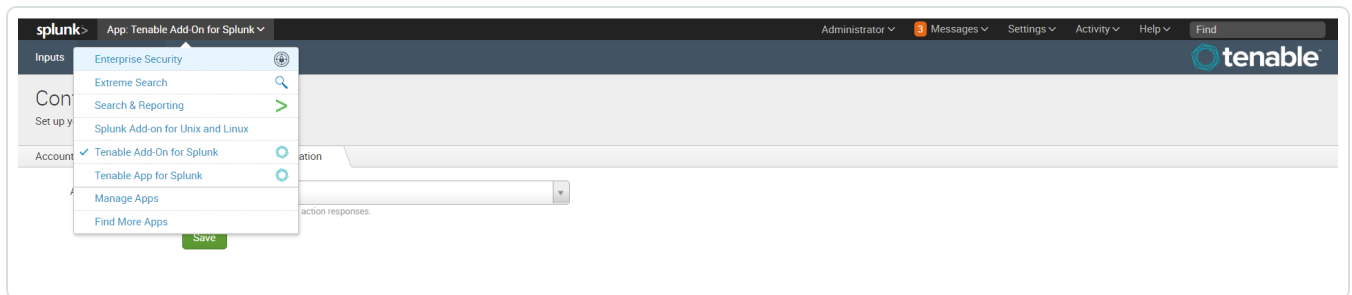
Select an index on the [Alert Actions Configuration](#) tab in the Tenable Configuration section to retrieve data.

To configure saved actions:

Configure adaptive response actions when you create a correlation search.

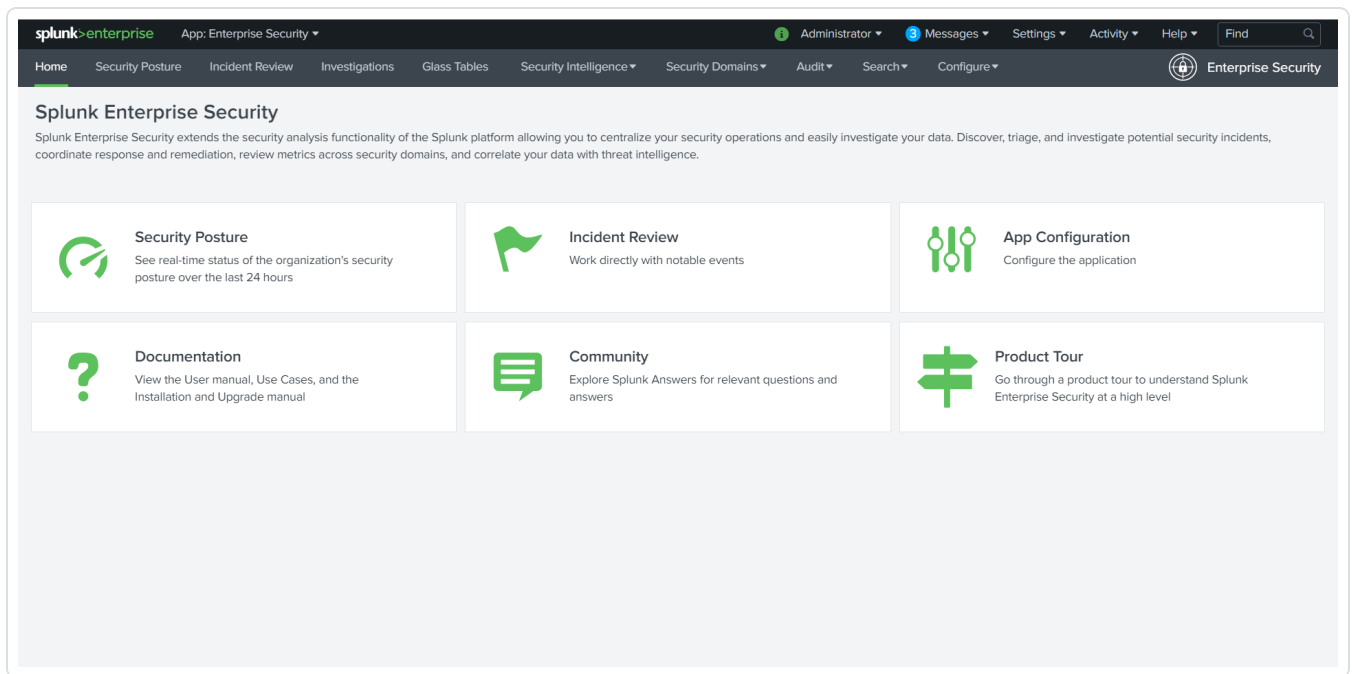
Note: When you run the search, the actions are retrieved automatically

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



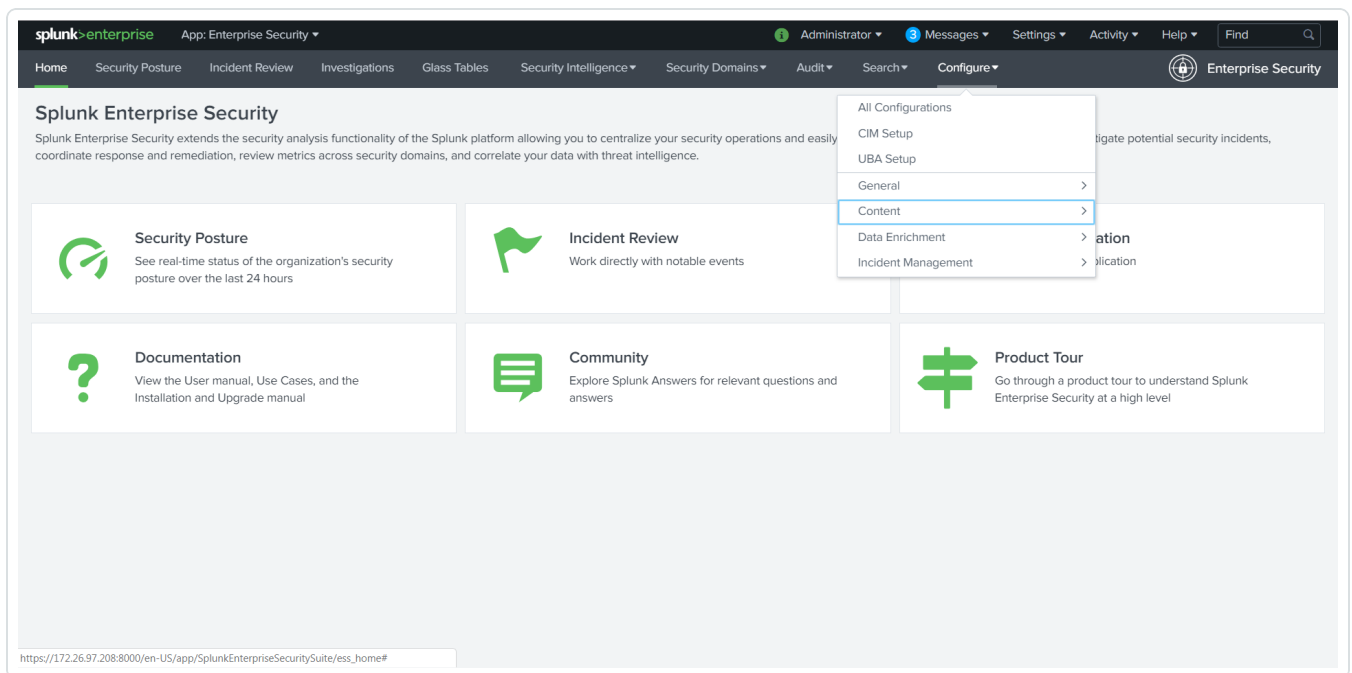
2. Select **Enterprise Security**.

The **Enterprise Security** page appears:



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

A drop-down menu appears:



4. Click **Content**.

More options appear.

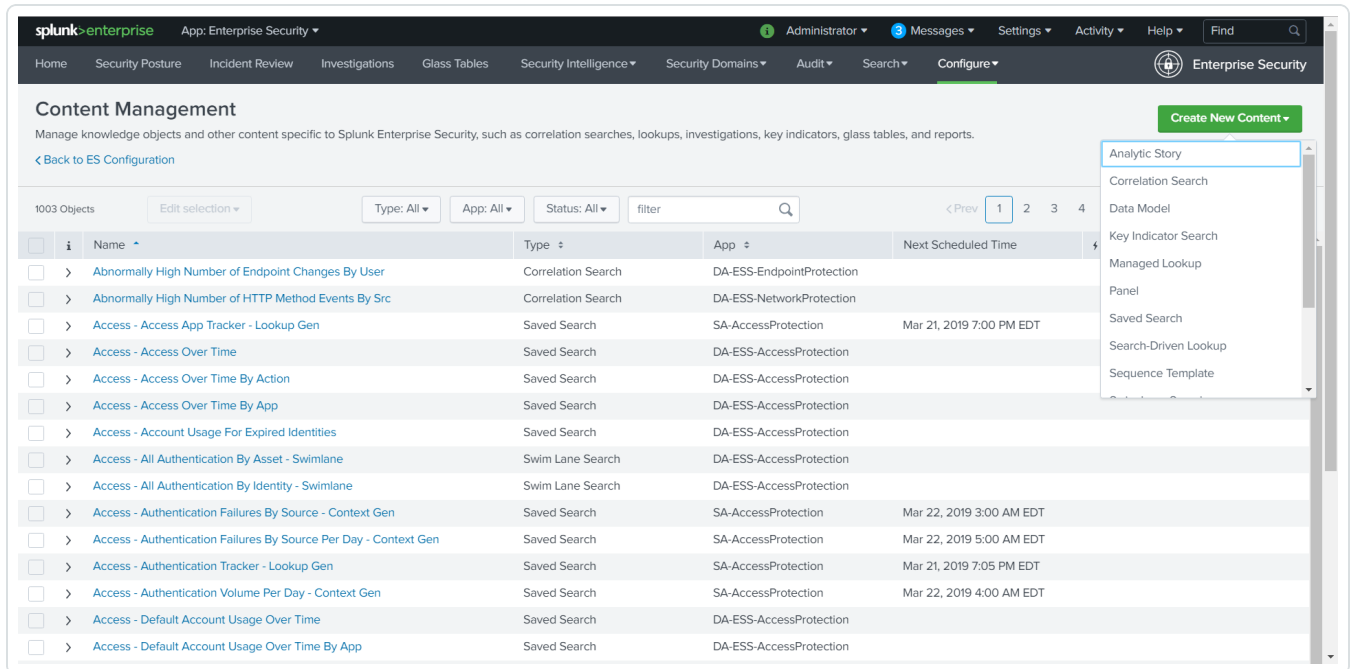


5. Click **Content Management**.

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:

The screenshot displays the 'Adaptive Response Actions' section. At the top, there is a '+ Add New Response Action' button. Below it, a 'Category' dropdown is set to 'All', and a 'Search' input field is present. A list of four actions is shown, each with a gear icon, a title, a description, and a metadata string:

- Scan Machine for Tenable SC**
Start a scan for machine on Tenable SC server.
Category: [Add Active Scan](#) | Task: [update](#) | Subject: [endpoint](#) | Vendor: [Tenable](#)
- Get Vulnerability Summary from Tenable IO**
Get Current Vulnerability from Tenable IO.
Category: [Information Gathering](#) | Task: [retrieve](#) | Subject: [endpoint](#) | Vendor: [Tenable](#)
- Request Scan for Tenable IO**
Request a scan for Tenable IO asset.
Category: [Add Active Scan](#) | Task: [update](#) | Subject: [endpoint](#) | Vendor: [Tenable](#)
- Launch Remediation Scan for Tenable SC**
Launch a remediation scan on Tenable SC server.

11. Select the appropriate action for your search.

12. The field options for the selected option appear:

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 ✕

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 Responses: 🔄

Response	Mode	Time	User	Status
Get Vulnerability Summary	adhoc	2018-04-12T17:22:35+0530	system	✓ success
Notable	saved	2018-04-11T14:09:07+0530	nobody	✓ success

[View Adaptive Response Invocations](#)

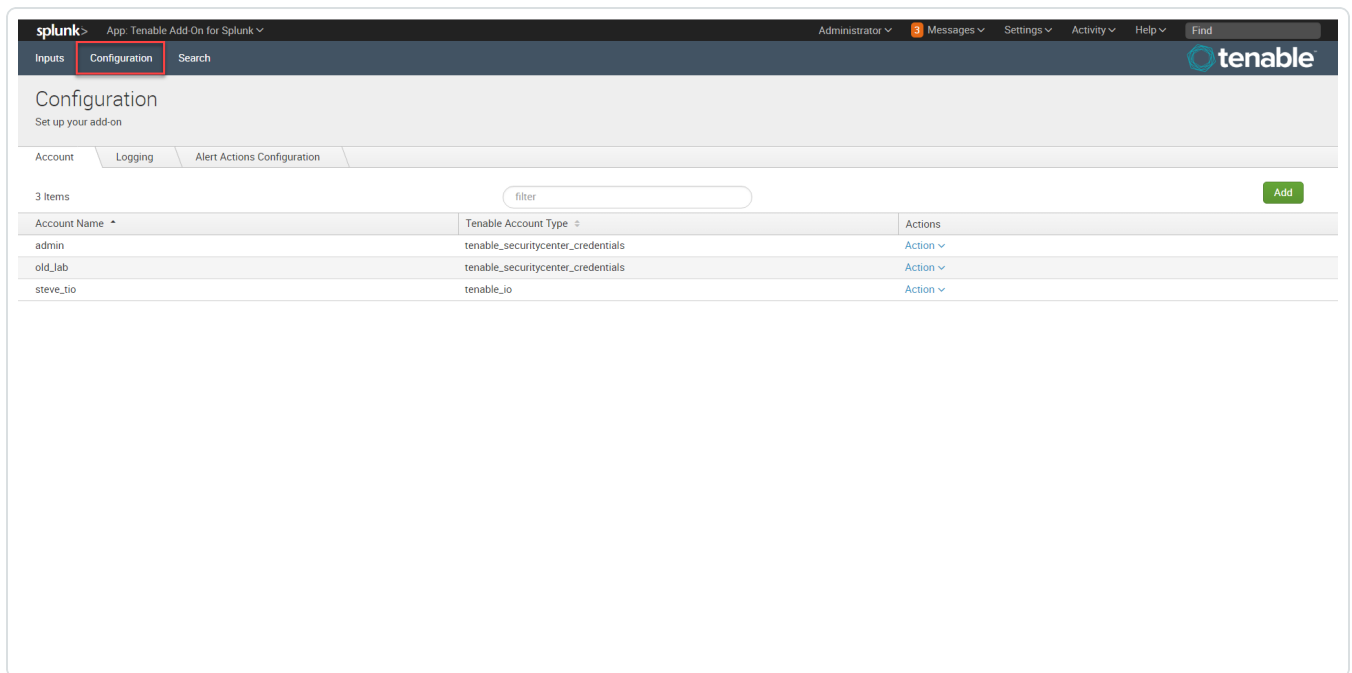


Alert Action Configuration

To configure alert actions:

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:

- [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 Vulnerability Management mod-input, check the `$SPLUNK_HOME/var/log/splunk/ta_tenable_tenable_io.log` file.
- For Tenable Security Center mod-input, check the `$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.

3. Data is not populating in 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`
 - You should see the following source types: `tenable:io:vuln`, `tenable:io:assets`, `tenable:io:plugin`, `tenable:sc:vuln`, `tenable:sc:plugin`, `tenable:sc:assets`, `tenable:sc:mobile:vuln`, `tenable:sc:mobile:assets`, `tenable:nm:vuln`.
 - 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.



Update Account ✕

! Please enter valid Address, SC Access key and SC Secret key or configure valid proxy settings or verify SSL certificate.

Account Name	<input type="text" value="scanman"/>
	<small>Enter a unique name for this account.</small>
Tenable Account Type	<input type="text" value="Tenable.sc API Keys"/> ✕
	<small>Select the App for Tenable</small>
Address	<input type="text" value="sc.integrations.lab"/>
	<small>Enter the FQDN or IP of your server for this account.</small>
Verify SSL Certificate	<input checked="" type="checkbox"/>
	<small>Should we verify your SSL certificate?</small>
T.sc Access Key	<input type="password" value="....."/>
	<small>Enter the Access Key for this account.</small>
T.sc Secret Key	<input type="password" value="....."/>
	<small>Enter the secret key for this account.</small>
Proxy Enable	<input type="checkbox"/>
	<small>Check to enable the proxy.</small>

- 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.



Known Issues

1. User is able to see the **Host Audit**, **Cloud Findings**, and **Web Application findings** parameters in the **Settings > Data Inputs** Splunk user interface while creating the IO input from there, but these do not fetch the **Host Audit**, **Cloud Findings**, and **Web Application findings** data.
2. User is able to see the **Host Audit**, **Cloud Findings**, and **Web Application findings** parameters in the `inputs.conf($SPLUNK_HOME/etc/apps/TA-tenable/local/inputs.conf)` while upgrading the add-on from 6.0.1 to 6.0.3, for the existing inputs, but these do not fetch the **Host Audit**, **Cloud Findings**, and **Web Application findings** data.



Splunk Integration v6.2 (BETA) Content

Tenable integration for Splunk version 6.2 (BETA) content is available for selected users. This section has topics and functionality exclusive to the BETA content. All standard functionality can be found in the standard Tenable and Splunk integration content pages in this guide.

Note: BETA content is subject to change in future releases. Contact your Tenable representative for more information.



Source and Source Types

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

Tenable Security Center

Source	Sourcetype	Description
<username> <address>	tenable:sc:vuln	This collects all vulnerability data.
<username> <address>	tenable:sc:assets	This collects pull assets data.
<username> <address>	tenable:sc:plugin	This collects all plugin data.

Tenable Vulnerability Management

Source	Sourcetype	Description
tenable_io://<data input name>	tenable:io:vuln	This collects all host vulnerability data.
tenable_io://<data input name>	tenable:io:assets	This collects all host asset data.
tenable_io://<data input name>	tenable:io:plugin	This collects all plugin data.

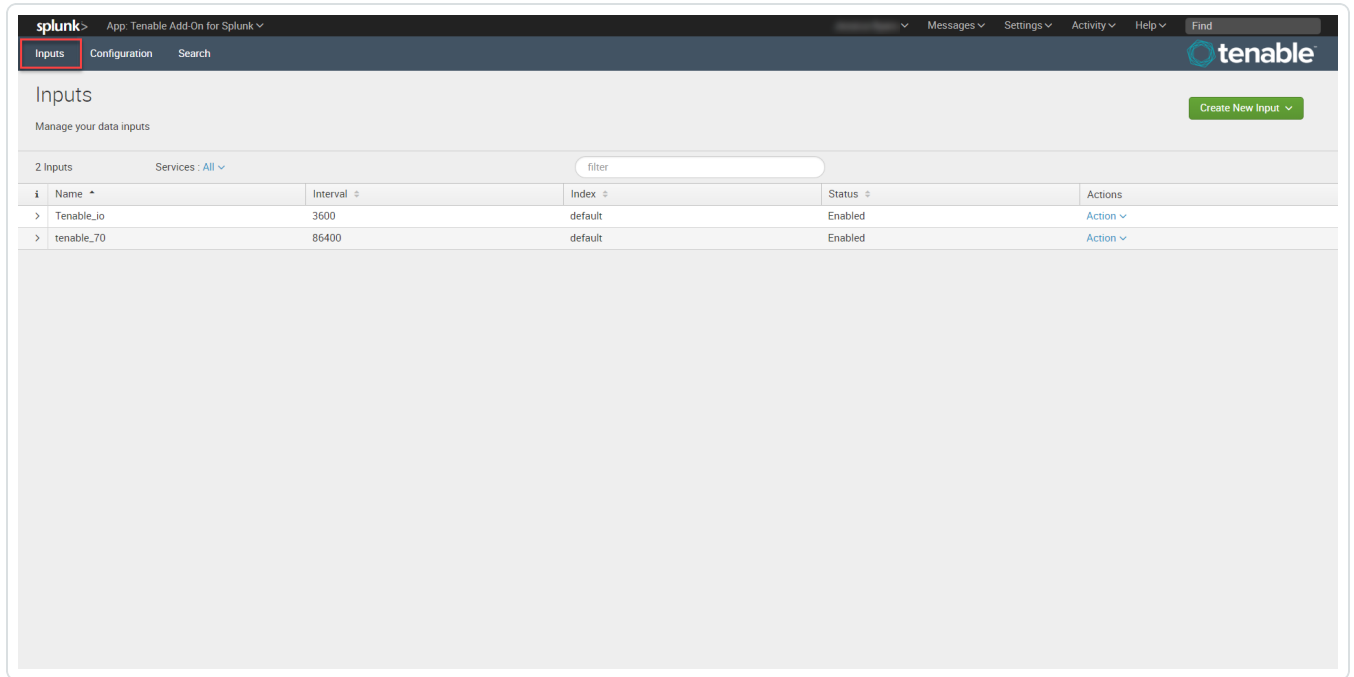


Create an Input

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

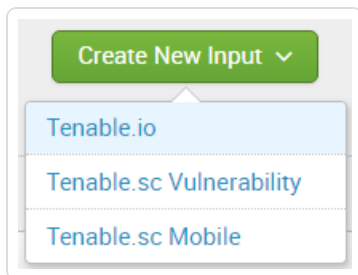
To create an input:

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



2. Click the **Create New Input** button.

A drop-down box appears:



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. The following table describes the available options.

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

Tenable Vulnerability Management

Input Parameters		Description	Required
Name		The unique name for each Tenable data input.	Yes
Interval		The interval parameter specifies when the input restarts to perform the task again (in seconds). The interval amount must be between 3600 and 86400.	Yes
Index		The index in which to store Tenable Vulnerability Management data.	Yes
Global Account		Splunk pulls data from this Tenable account.	Yes
Sync Plugin Details		If selected, the related tags in Tenable assets include plugin details.	Yes
Host Vulnerability	Enable Host Vulnerability	Enable to collect host assets and host vulnerabilities.	Yes; for at least one data source.



	Start Time	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.)	No
	Lowest Severity Score	The lowest level of severity stored.	No
	Historical Fixed Vulnerability	Allows the import of host vulnerabilities fixed before the current day.	No
	Tags	Limits host vulnerabilities pulled to host assets that have tags selected.	No

Tenable Security Center Vulnerability

Input Parameters	Description	Required
Name	The unique name for each Tenable data input.	Yes
Interval	The interval parameter specifies when the input restarts to perform the task again (in seconds). The interval amount must be between 300 and 86400. Note: If using a Tenable Security Center version previous to 5.7, the minimum interval you can select is 24 hours. If using Tenable Security Center 5.7 or later, you can specify a minimum interval of an hour.	Yes



Index	The index in which to store Tenable Security Center data.	Yes
Global Account	Splunk pulls data from this Tenable account.	Yes
Start Time	The date and time to start collecting data. If you leave this field blank, the integration collects all historical data. Note: Uses the <code>YYYY-MM-DD hh:mm:ss</code> format.	No
Sync Plugin Details	If selected, the related tags in Tenable assets include plugin details.	Yes
Historical Fixed Vulnerability	Allows the import of vulnerabilities fixed before the current day.	No
Query Name	A name for Tenable Security Center vulnerability filter. Note: The interval must be query type Vulnerability Detail List .	No

Tenable Security Center Mobile

Input Parameters	Description	Required
Name	The unique name for each Tenable data input.	Yes
Interval	The interval parameter specifies when the input restarts to perform the task again (in seconds).	Yes
Index	The index in which to store Tenable Security Center data.	Yes
Global Account	Splunk pulls data from this Tenable account.	Yes



Query Name	A name for Tenable Security Center vulnerability filter. Note: The interval must be query type - Vulnerability Detail List.	No
------------	--	----

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.



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

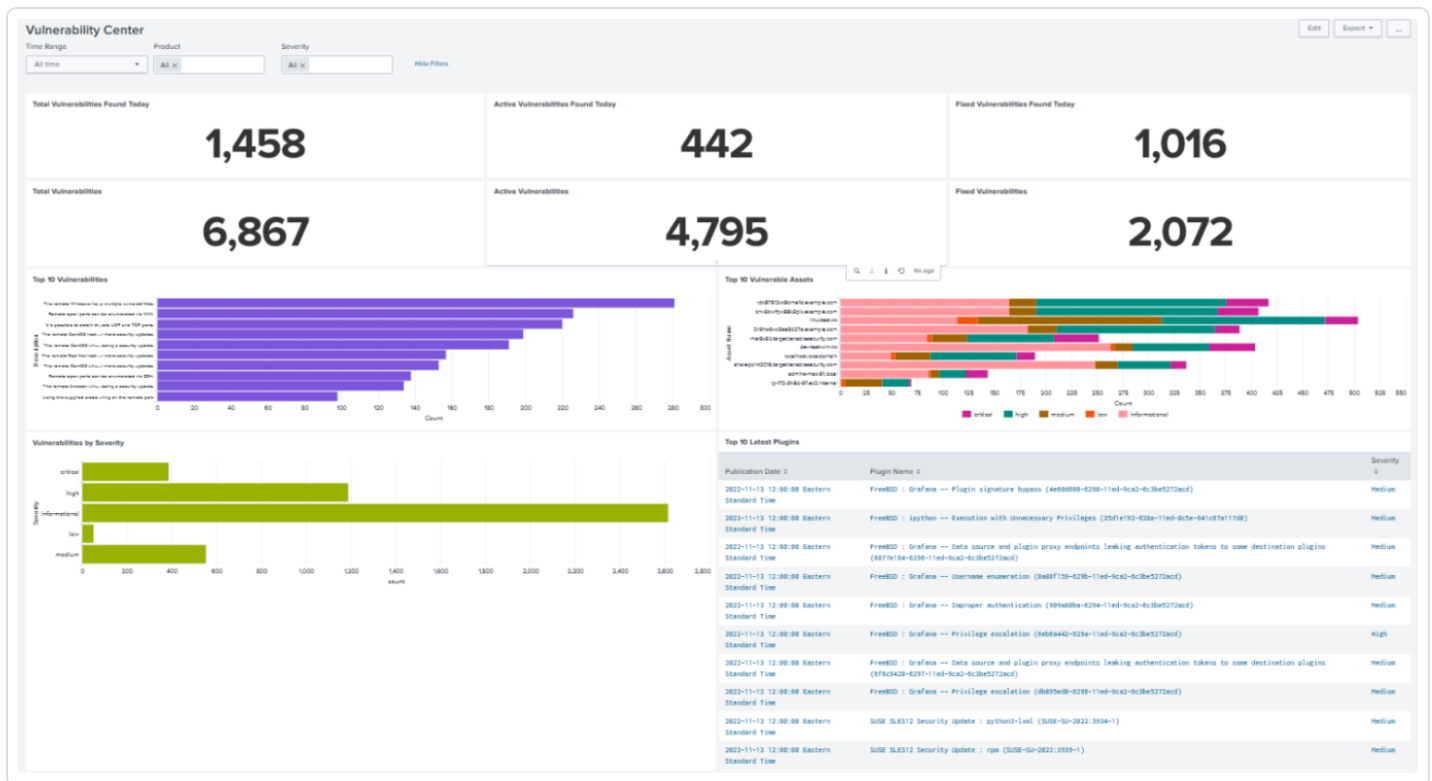
After installation, you must run the **All Time** saved search specific to your Tenable platform. This is a one-time operation to populate indices that the Tenable App for Splunk depends on.

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

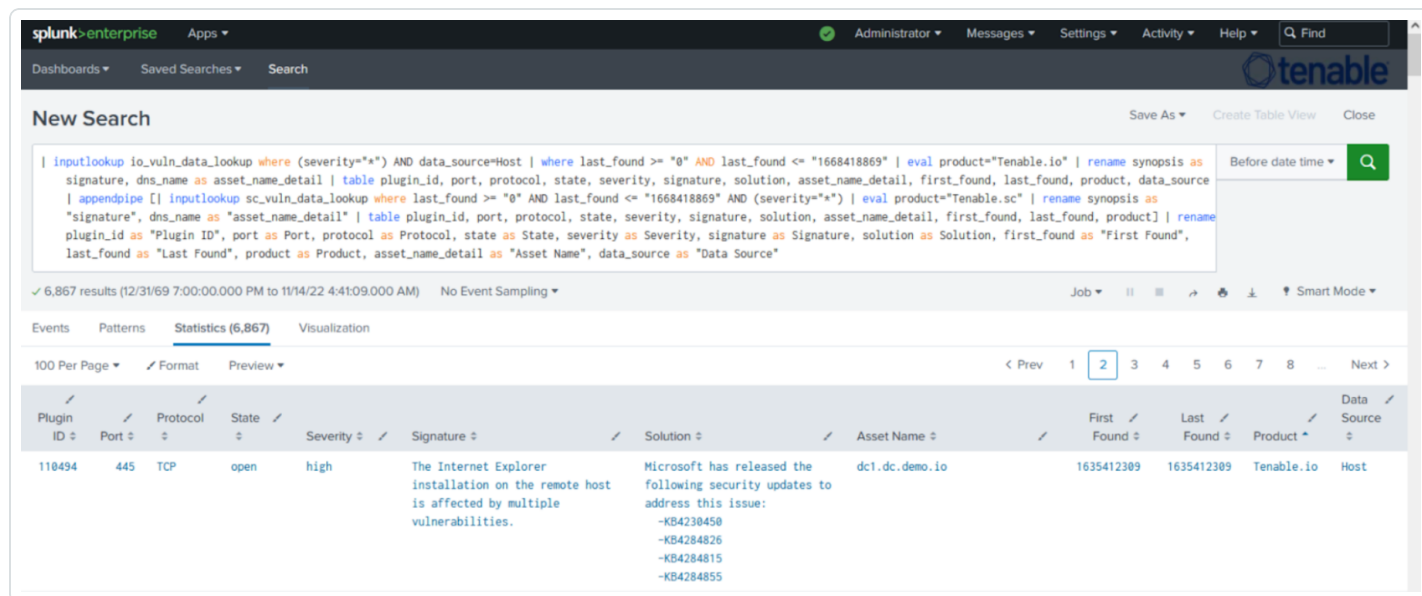
Events

- 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.

Tenable Security Center drill-down field	Tenable Security Center lookup field	Tenable Vulnerability Management-Host drill-down field	Tenable Vulnerability Management-Host lookup field
-	SC_address	-	asset_uuid
DNS Name	dns_name	Data Source	data_source
First Found	first_found	Asset Name	dns_name
-	ip	First Found	first_found
-	last_fixed	-	last_fixed
Last Found	last_found	Last Found	last_found



Plugin ID	plugin_id	Plugin ID	plugin_id
Port	port	Port	port
Protocol	protocol	Protocol	protocol
-	repository_id	Severity	severity
Severity	severity	Solution	solution
Solution	solution	State	state
State	state	Signature	synopsis
Signature	synopsis	-	vpr_score
-	vpr_score	-	-

Tenable Vulnerability Management-Plugin drill-down field	Tenable Vulnerability Management-plugin lookup field	Tenable Security Center-Plugin drill-down field	Tenable Security Center-plugin lookup field
Plugin ID	plugin_id	Plugin ID	plugin_id
Plugin Name	plugin_name	Plugin Name	plugin_name
-	plugin_version	-	plugin_family_id
Severity	risk_factor	-	plugin_family
Solution	plugin_solution	-	plugin_version
Signature	plugin_synopsis	Severity	risk_factor
Publication Date	plugin_publication_date	Signature	plugin_synopsis
-	plugin_modification_date	Solution	plugin_solution
-	vpr_score	Publication Date	plugin_publication_date
-	-	-	plugin_modi-



			fication_date
-	-	-	vpr_score



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.

```
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.

```
tenable:nnm: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 Vulnerability Management mod-input, check the `$(SPLUNK_HOME)/var/log/splunk/ta_tenable_tenable_io.log` file.
- For Tenable Security Center mod-input, check the `$(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.

3. Data is not populating in 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`
 - You should see the following source types: `tenable:io:vuln`, `tenable:io:assets`, `tenable:io:plugin`, `tenable:sc:vuln`, `tenable:sc:plugin`, `tenable:sc:assets`, `tenable:sc:mobile:vuln`, `tenable:sc:mobile:assets`, `tenable:nm:vuln`.
 - 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.



Update Account ✕

! Please enter valid Address, SC Access key and SC Secret key or configure valid proxy settings or verify SSL certificate.

Account Name	<input type="text" value="scanman"/>
	<small>Enter a unique name for this account.</small>
Tenable Account Type	<input type="text" value="Tenable.sc API Keys"/> ✕
	<small>Select the App for Tenable</small>
Address	<input type="text" value="sc.integrations.lab"/>
	<small>Enter the FQDN or IP of your server for this account.</small>
Verify SSL Certificate	<input checked="" type="checkbox"/>
	<small>Should we verify your SSL certificate?</small>
T.sc Access Key	<input type="password" value="....."/>
	<small>Enter the Access Key for this account.</small>
T.sc Secret Key	<input type="password" value="....."/>
	<small>Enter the secret key for this account.</small>
Proxy Enable	<input type="checkbox"/>
	<small>Check to enable the proxy.</small>

- 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.



Known Issues

1. User is able to see the **Host Audit**, **Cloud Findings**, and **Web Application findings** parameters in the **Settings > Data Inputs** Splunk user interface while creating the IO input from there, but these do not fetch the **Host Audit**, **Cloud Findings**, and **Web Application findings** data.
2. User is able to see the **Host Audit**, **Cloud Findings**, and **Web Application findings** parameters in the `inputs.conf($SPLUNK_HOME/etc/apps/TA-tenable/local/inputs.conf)` while upgrading the add-on from 6.0.1 to 6.0.3, for the existing inputs, but these do not fetch the **Host Audit**, **Cloud Findings**, and **Web Application findings** data.