Tenable and Splunk Integration Guide

Last Revised: July 15, 2025

Table of Contents

Welcome to Tenable for Splunk

The Tenable for Splunk integration performs data collection, normalization, and visualization.

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

Changes in Tenable App for Splunk v6.1.0

- Added "Assets Dashboard" for visualizing asset details of the following products: IO, SC, OT, WAS, and ASM
- Added support for "WAS" and "OT" products in the "Vulnerability Center" dashboard.

Tenable App for Splunk Compatibility Matrix

- Browser: Google Chrome, Mozilla Firefox
- OS: Platform independent
- Splunk Enterprise version: 9.4.x and 9.3.x
- Supported Splunk Deployment: Splunk Cloud, Splunk Standalone, and Distributed Deployment

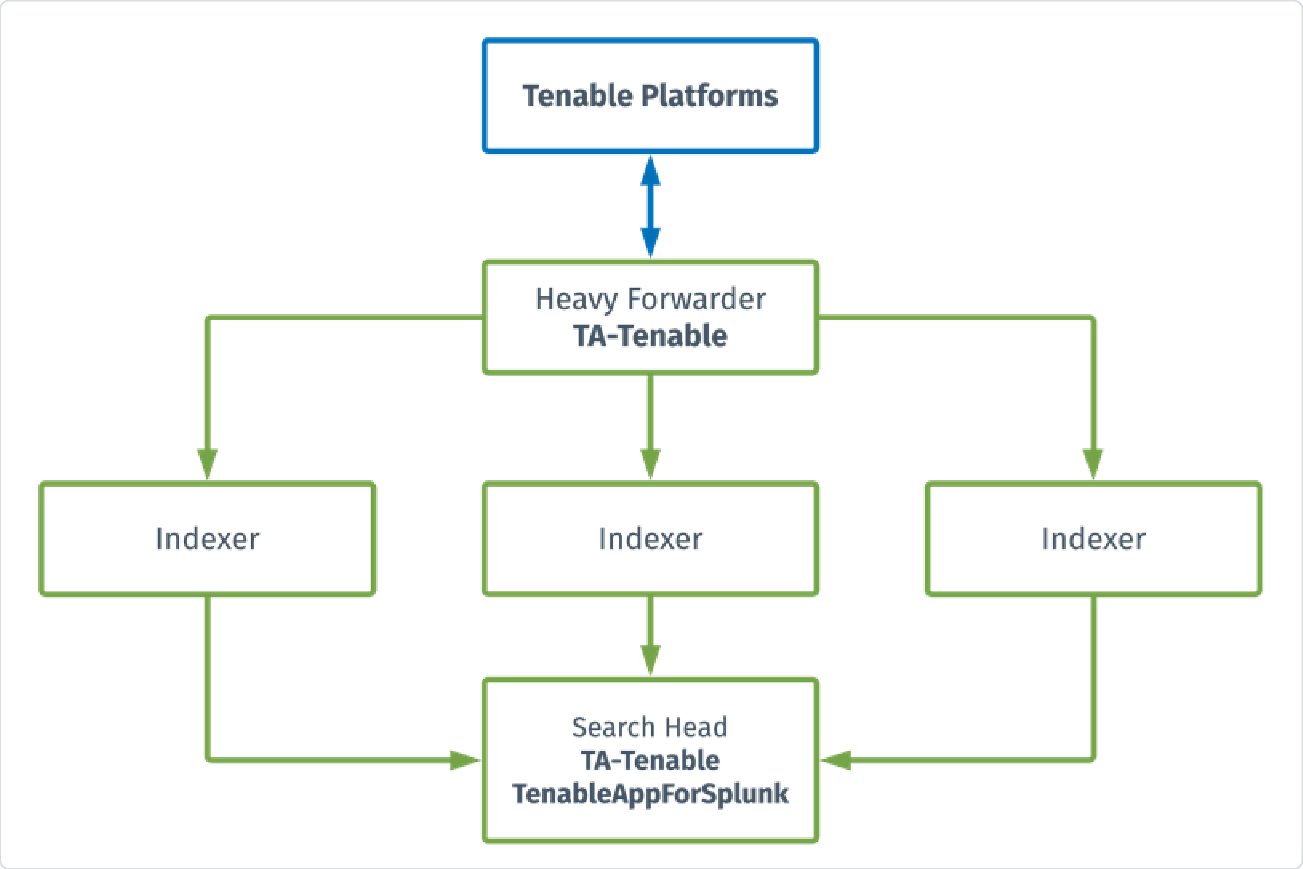
Changes in Tenable Add-On for Splunk v8.0.0

- Added new input to collect TWAS data.
- Added new input to collect TASM data.
- Added support for providing the custom SSL certificate on the Account configuration page.
- Updated the alert actions by adding an option to select Tenable account that user wants to use.
- Updated the PyTenable to v1.6.2

Tenable Add-On for Splunk Compatibility Matrix

- Browser: Google Chrome, Mozilla Firefox
- OS: Platform independent
- Splunk Enterprise version: 9.4.x and 9.3.x
- Supported Splunk Deployment: Splunk Cloud, Splunk Standalone, and Distributed Deployment

Tenable integration topology:



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.

Tenable Attack Surface Management (TASM) is a web-based inventory tool that you can use to identify internet-accessible assets that your organization may or may not know about. TASM identifies assets using DNS records, IP addresses, and ASN, and includes more than 180 columns of metadata to help you organize and inventorize your assets. TASM performs data collection and normalization.

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}
- /analysis (Security Center only)

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}
- /analysis (Security Center only)

Plugins

- GET /plugins/plugin
- /plugin (Security Center only)

Source and Source Types

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

TOT (ICP)

Source	Source type	Description
tenable_ot://<data input name>	tenable:ot:vuln	Collects cumulative vulnerability data from active and agent scans from licensed assets.
tenable_ot://<data input name>	tenable:ot:assets	Collects all assets data.
tenable_ot://<data input name>	tenable:ot:plugin	Collects all plugin detail data.

TSC

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.

TVM

Source	Source type	Description
tenable_io://<data input name>	tenable:io:vuln	Collects cumulative vulnerability data from active and agent 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.

TVM Audit Logs

Source	Source type	Description
tenable_io://<data input name>	tenable:io:audit_logs	Collects all audit logs

TVM Compliance Module

Source	Source type	Description
tenable_io://<data input name>	tenable:io:compliance	Collects all compliance data.

Tenable Attack Surface Management

Source	Source type	Description
<username>|<address>	tenable:asm:assets	This collects all assets data.

Tenable Web App Scanning

Source	Source type	Description

<username>|<address>	tenable:was:assets	This collects all asset data.
<username>|<address>	tenable:was:vuln	This collects all vulnerability 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

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.

Component	Forwarder	Indexer	Search Head
Tenable Add-on for Splunk (TA-Tenable)	Yes • configure accounts • configure data input	No	Yes • 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.

Tenable Add-On for Splunk 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:

Minumum Required User Role: 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 for the first time:

1. Log in to Splunk.
2. Go to **Apps > Manage Apps > Browse more apps** at the top of the screen.
3. Search for “Tenable” and from the list select “Tenable Add-on for Splunk."
4. Download the Add-on from Splunkbase.
5. Go to **Apps > Manage Apps > Install app from file**.

6. Upload the Tenable Add-on for Splunk v8.0.0 file by extracting the compressed file (.tar.gz) into the $SPLUNK_HOME$/etc/apps folder.

To upgrade Tenable Add-on for Splunk:

1. Log in to Splunk.
2. Disable the existing inputs of Tenable Add-on for Splunk by navigating to **Tenable Add-On for Splunk > Inputs**.
3. Click the toggle button under **Status** column.
4. Navigate to **Apps > Manage Apps**.
5. Click **Install app from file**.
6. Click **Choose file**.
7. Select the **Tenable Add-on for Splunk v8.0.0** installation file.
8. Check the **Upgrade** checkbox.
9. Click **Upload**.
10. Restart Splunk if prompted.

Note: You can set `use_milliseconds_for_sc_vulns = 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 `use_milliseconds_for_sc_vulns = 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: (For Tenable OT Security or Tenable Security Center) 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:

- `verify_ssl_for_ot = True`
- `verify_ssl_for_sc_cert = True`
- `verify_ssl_for_sc_api_key = True`
- `verify_ssl_for_sc_creds = True`

Next, create an input.

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 Attack Surface Management
- Tenable Tenable Network Monitor
- Tenable OT Security (ICP)
- Tenable Security Center Certificates
- Tenable Security Center API Keys
- Tenable Vulnerability Management

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

Configure Tenable Attack Surface Management

Required User Role: Administrator

Connect to Tenable Attack Surface Management by creating the account configuration.

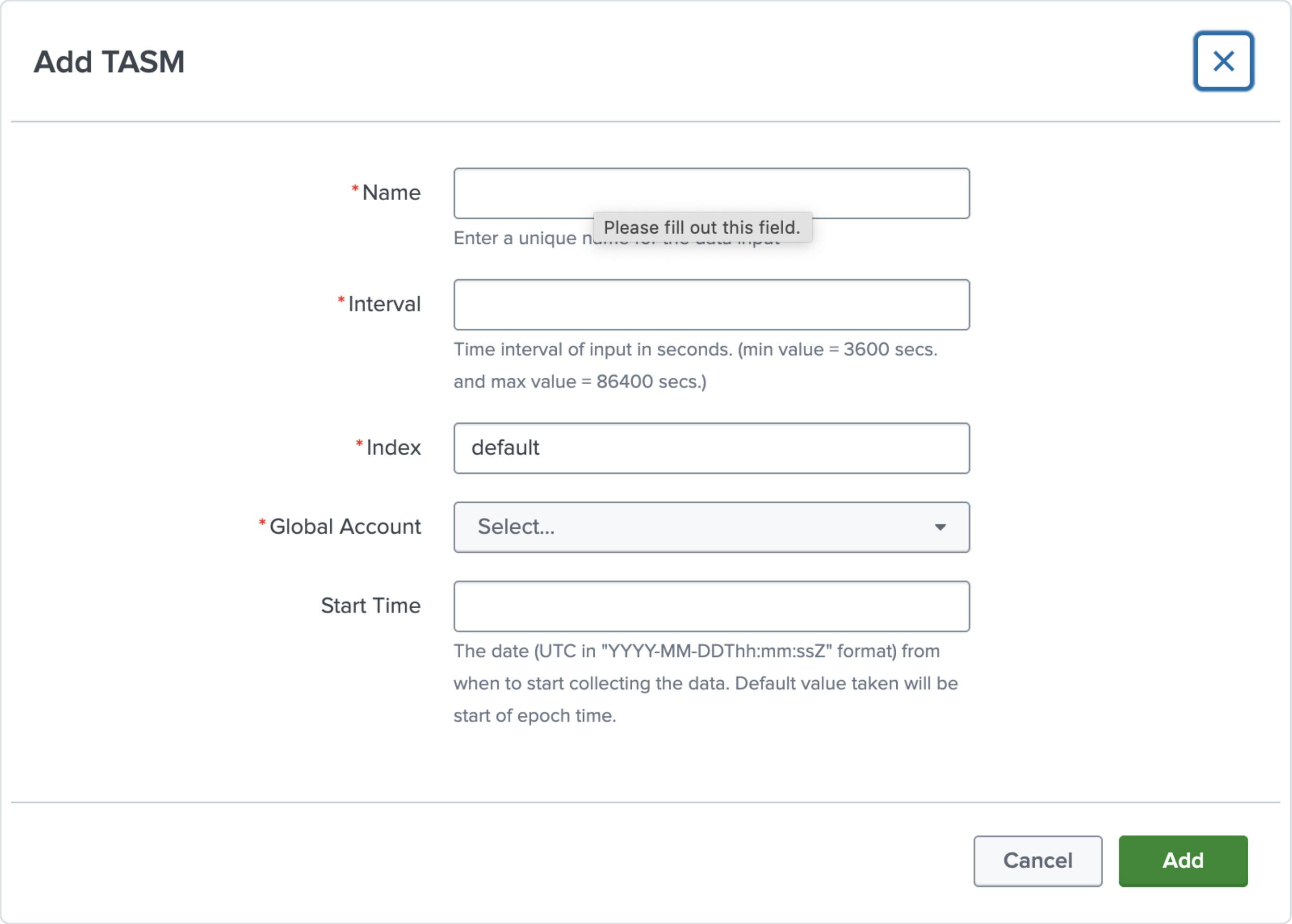
Before you begin:

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

To configure your account for Tenable Attack Surface Management:

1. Navigate to **Tenable Add-on for Splunk > Configuration**
2. Under the **Account** tab click on **Add**.
3. In the **Tenable Account Type** dropdown, select **TASM**.

The **Add TASM** window appears:



Add TASM

*Name

Enter a unique name for the data input

Please fill out this field.

*Interval

Time interval of input in seconds. (min value = 3600 secs. and max value = 86400 secs.)

*Index: default

*Global Account: Select...

Start Time

The date (UTC in "YYYY-MM-DDThh:mm:ssZ" format) from when to start collecting the data. Default value taken will be start of epoch time.

4. Provide any desired name in **Account Name** field.
5. Enter the FQDN, or IP, of your server for this account without scheme (i.e., http:// or https://) in the **TASM** field.
6. Enter your **TASM API Key**.
7. If using a proxy server, click the **Proxy Enable** checkbox and provide proxy fields.
8. To complete the configuration, click **Add**.

Parameters Reference Table

Input Parameters	Description
Account Name	(Required) The unique name for each Tenable data input.

Tenable Account Type	(Required) The type of Tenable account. Select **TASM**.
TASM Domain	(Required) The FQDN, or IP, of your server for this account without scheme (i.e., http:// or https://) in the **TASM** field. (e.g., asm.cloud.tenable.com)
TASM API Key	(Required) Tenable Attack Surface Management API access key.
Proxy Enable	Enables the plugin to collect Tenable Attack Surface Management 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. • **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.

Next steps

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

Configure Tenable Identity Exposure

Connect to Tenable Identity Exposure by creating the account configuration. 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 your account for Tenable Identity Exposure:

Complete the following steps in Splunk:

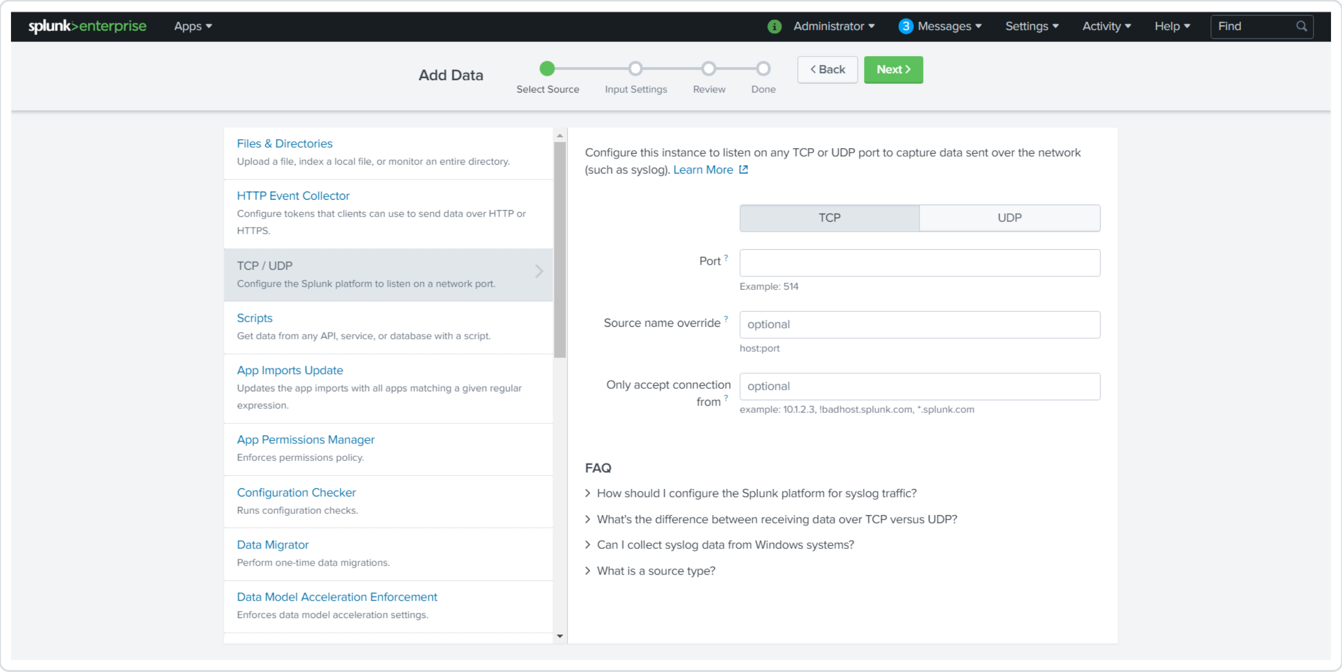
1. In the top navigation bar, click **Settings** > **Data Inputs**.

   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.



Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Scripts
Get data from any API, service, or database with a script.

App Imports Update
Updates the app imports with all apps matching a given regular expression.

App Permissions Manager
Enforces permissions policy.

Configuration Checker
Runs configuration checks.

Data Migrator
Perform one-time data migrations.

Data Model Acceleration Enforcement
Enforces data model acceleration settings.

Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). Learn More

Port ?
Example: 514

Source name override ? optional
host:port

Only accept connection from ? optional
example: 10.1.2.3, !badhost.splunk.com, *.splunk.com

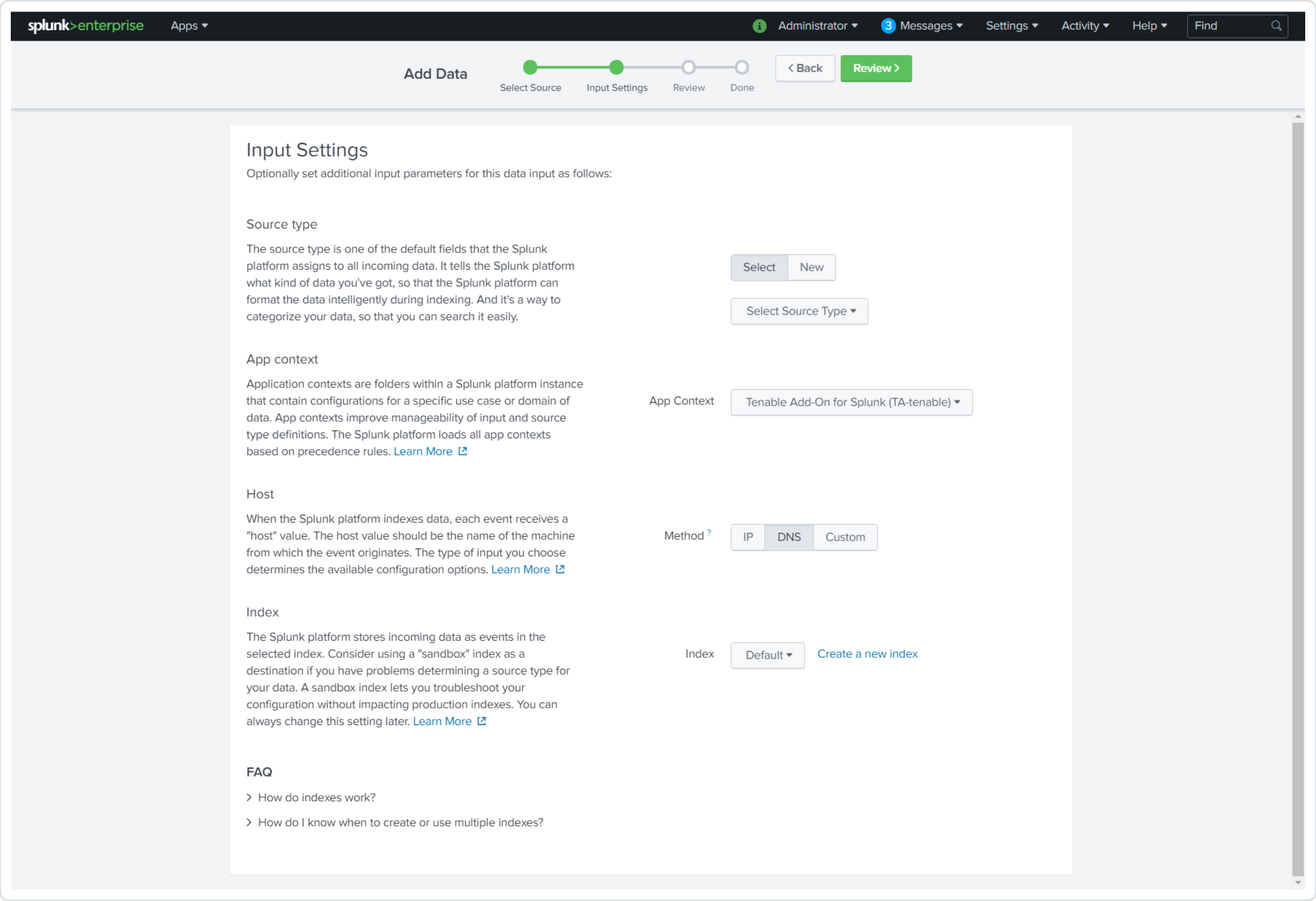
FAQ

- How should I configure the Splunk platform for syslog traffic?
- What's the difference between receiving data over TCP versus UDP?
- Can I collect syslog data from Windows systems?
- What is a source type?

4. Enter the port configuration information.

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

   The **Input Settings** page appears:



Input Settings

Optionally set additional input parameters for this data input as follows:

Source type

The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

App context

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. Learn More

App Context: Tenable Add-On for Splunk (TA-tenable) ▾

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More

Method: IP | DNS | Custom

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More

Index: Default ▾

FAQ

› How do indexes work?

› How do I know when to create or use multiple indexes?

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 Network Monitor

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

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

To configure your account for Tenable Network Monitor:

Complete the following steps in Splunk

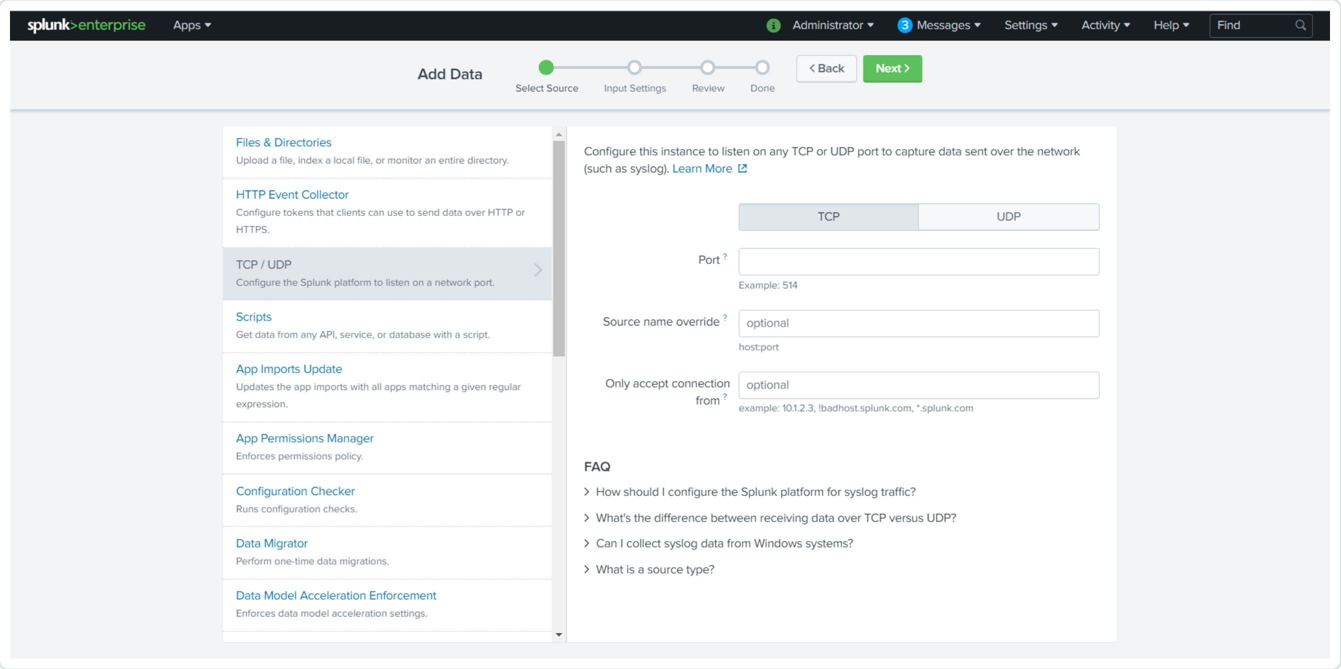
1. In the top navigation bar, click **Settings** > **Data Inputs**.

   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.



Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Scripts
Get data from any API, service, or database with a script.

App Imports Update
Updates the app imports with all apps matching a given regular expression.

App Permissions Manager
Enforces permissions policy.

Configuration Checker
Runs configuration checks.

Data Migrator
Perform one-time data migrations.

Data Model Acceleration Enforcement
Enforces data model acceleration settings.

Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). Learn More

TCP | UDP

Port ?
Example: 514

Source name override ? optional
host:port

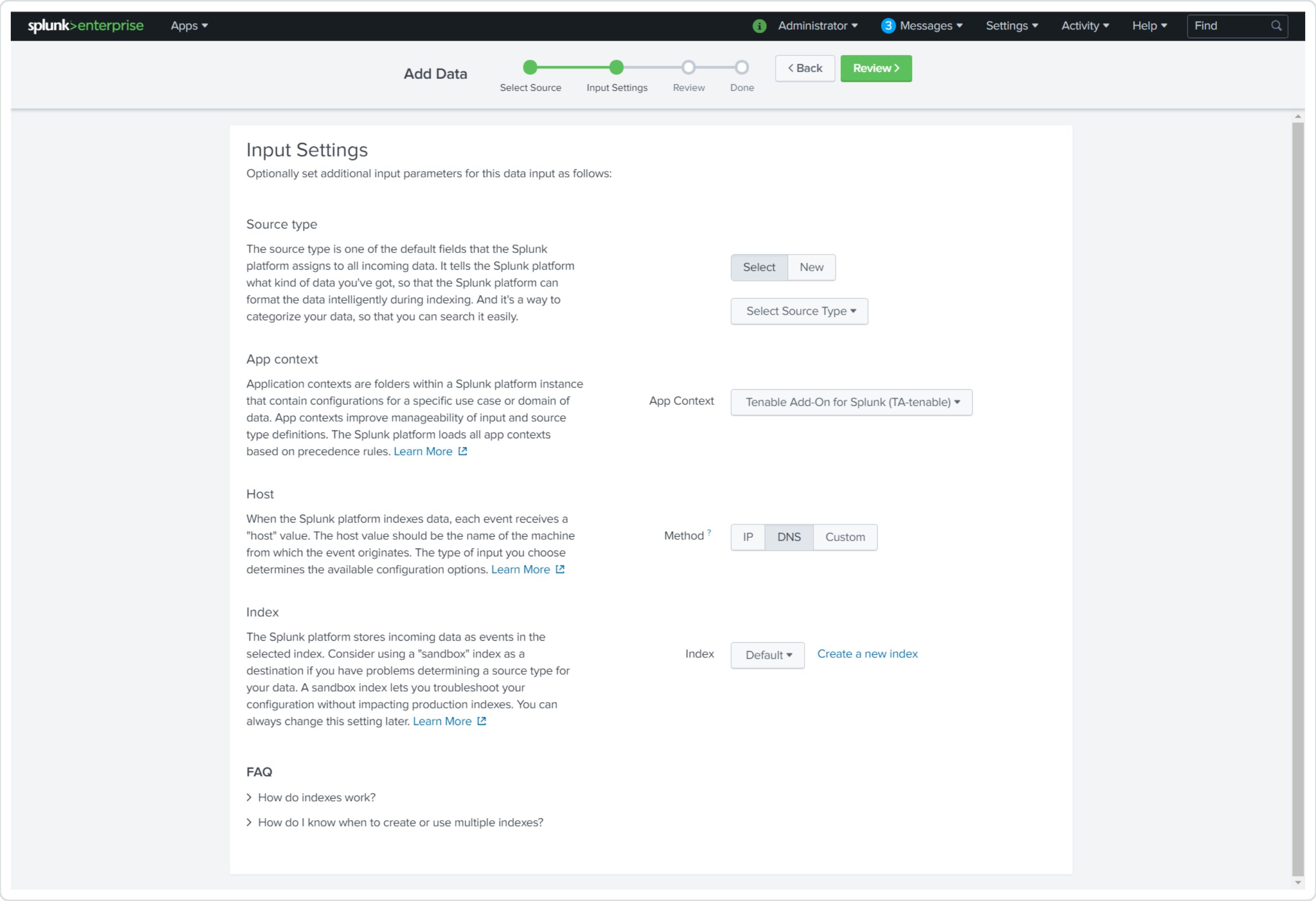
Only accept connection from ? optional
example: 10.1.2.3, !badhost.splunk.com, *.splunk.com

FAQ
- How should I configure the Splunk platform for syslog traffic?
- What's the difference between receiving data over TCP versus UDP?
- Can I collect syslog data from Windows systems?
- What is a source type?

4. Enter the port configuration information.

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

   The **Input Settings** page appears:



Input Settings

Optionally set additional input parameters for this data input as follows:

Source type

The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Select | New

Select Source Type ▾

App context

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. Learn More

App Context: Tenable Add-On for Splunk (TA-tenable) ▾

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More

Method ? IP | DNS | Custom

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More

Index: Default ▾ Create a new index

FAQ

› How do indexes work?

› How do I know when to create or use multiple indexes?

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**.

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 (ICP)

Connect to OT Security (ICP) by creating the account configuration.

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

To configure your account for Tenable OT Security (ICP):

1. Navigate to the **Tenable Add-on for Splunk** > **Configuration**.

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

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

4. 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.
Address	(Required) The FQDN, or IP, of your server for this account without scheme (i.e., http:// or https://) in the **TOT** field.
API Secret	(Required) Tenable OT Security API access key. **Note**: For more information on API keys, see Generate an API Key. **Note:** SSL Verification - Splunk requires all connections to verify SSL by default and not be configurable via the UI. To configure your TSC connection to not verify SSL certificate you will need to modify `{SPLUNK_HOME}/etc/apps/TA-tenable/bin/tenable_consts.py` and set to `verify_ssl_for_ot = False`.
Use Custom CA Certificate	Check this box if you are using a Custom CA Certificate.
Custom CA Certificate	Enter the Custom CA Certificate for this account.
Proxy Enable	(Optional) Enables the plugin to collect Tenable OT Security 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. • **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.

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

Next steps

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

Configure Tenable Security Center API Keys

Required User Role: Security Analyst

Connect to Tenable Security Center API Keys by creating the account configuration.

Note: SSL Verification - Splunk requires all connections to verify SSL by default and not be configurable via the UI. To configure your TSC connection to not verify SSL certificate you will need to modify `{SPLUNK_HOME}/etc/apps/TA-tenable/bin/tenable_consts.py` and set to `verify_ssl_for_sc_api_key = False`.

To configure your account for Tenable Security Center API Keys:

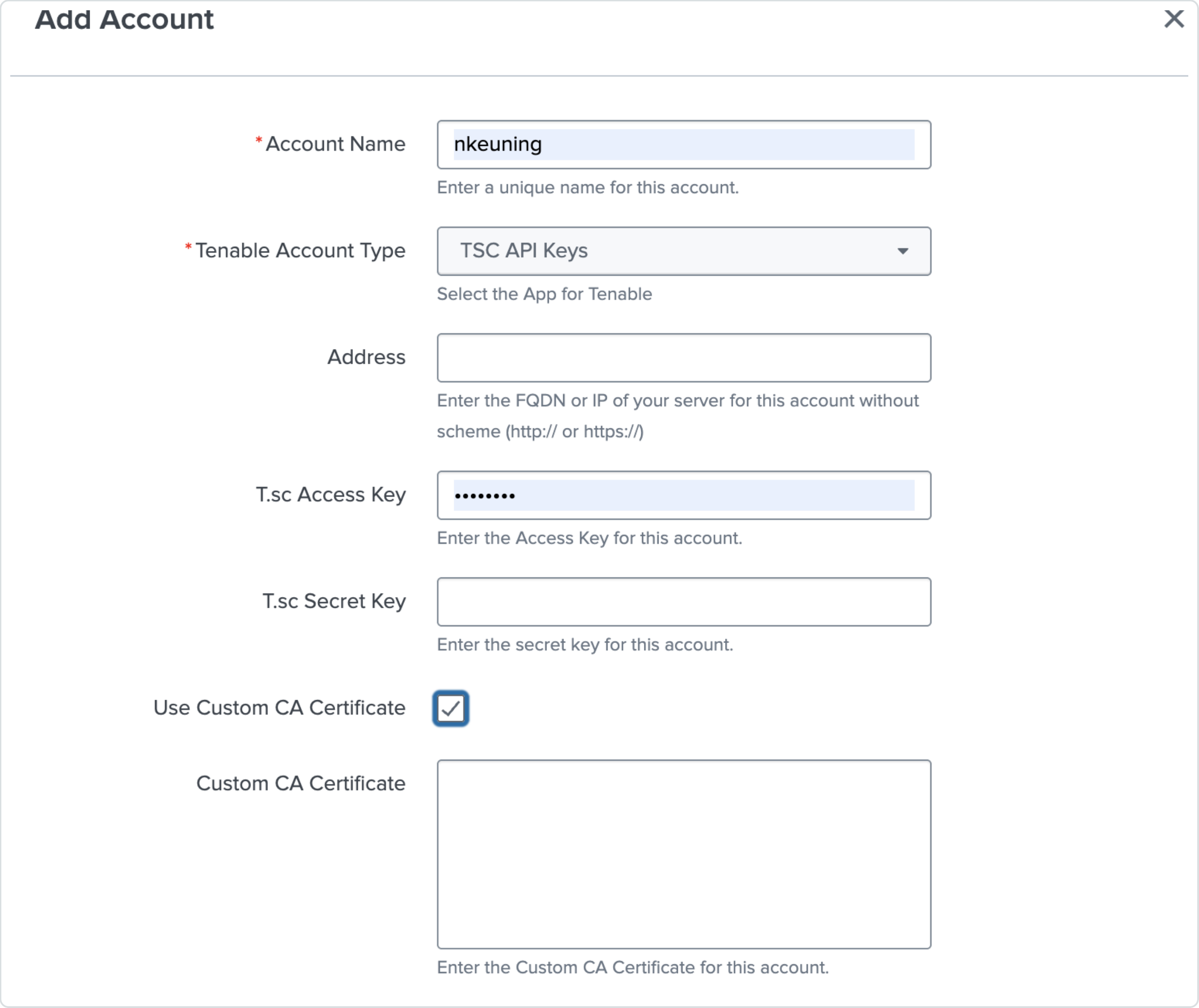
1. Log in to your data collection node.

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: nkeuning

Enter a unique name for this account.

*Tenable Account Type: TSC API Keys

Select the App for Tenable

Address:

Enter the FQDN or IP of your server for this account without scheme (http:// or https://)

T.sc Access Key: ••••••••

Enter the Access Key for this account.

T.sc Secret Key:

Enter the secret key for this account.

Use Custom CA Certificate ☑

Custom CA Certificate:

Enter the Custom CA Certificate for this account.

> **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 **TSC API Keys**.

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. Select **TSC API Keys**.
Address	(Required) The hostname or IP address for Tenable Security Center.
T.sc Access Key	(Required) API Access Key
T.sc Secret Key	(Required) API Secret Key
Use Custom CA Certificate	Check this box if you are using a Custom CA Certificate.
Custom CA Certificate	Enter the Custom CA Certificate for this account.
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. • **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.

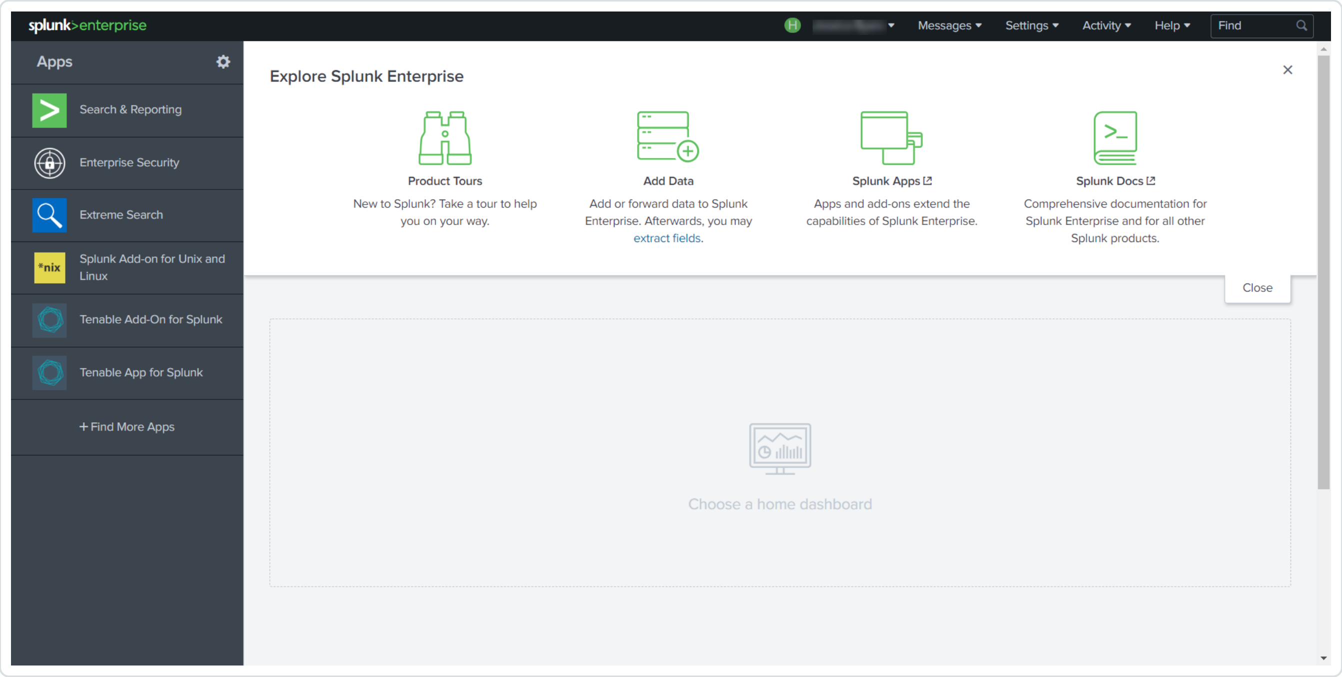
Configure Tenable Security Center Certificates

Connect to Tenable Security Center Certificates by creating the account configuration.

> **Note:** SSL Verification - Splunk requires all connections to verify SSL by default and not be configurable via the UI. To configure your TSC connection to not verify SSL certificate you will need to modify `{SPLUNK_HOME}/etc/apps/TA-tenable/bin/tenable_consts.py` and set to `verify_ssl_for_sc_cert = False`. For additional information on Tenable Security Center Certificates, see SSL Client Certificate Authentication.

To configure your account for Tenable Security Center Certificates:

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



Explore Splunk Enterprise

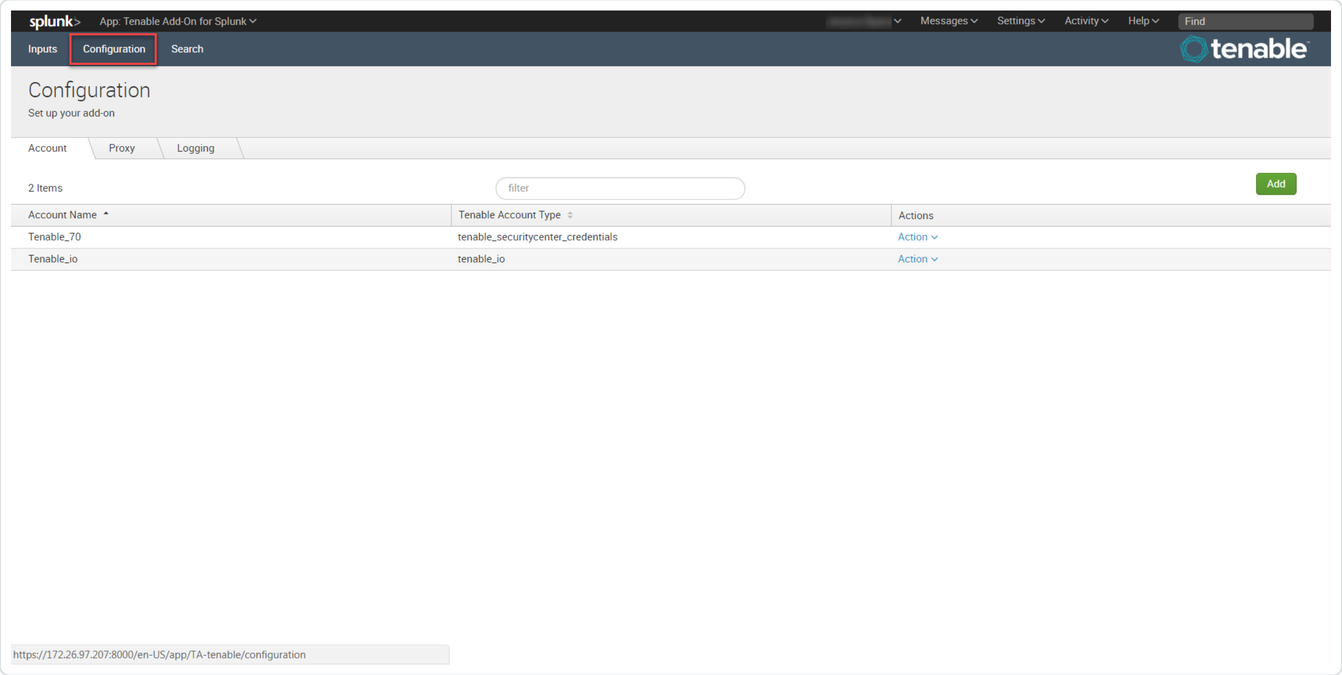
Product Tours
New to Splunk? Take a tour to help you on your way.

Add Data
Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Splunk Apps
Apps and add-ons extend the capabilities of Splunk Enterprise.

Splunk Docs
Comprehensive documentation for Splunk Enterprise and for all other Splunk products.

3. Click the **Configuration** tab.



Configuration

Set up your add-on

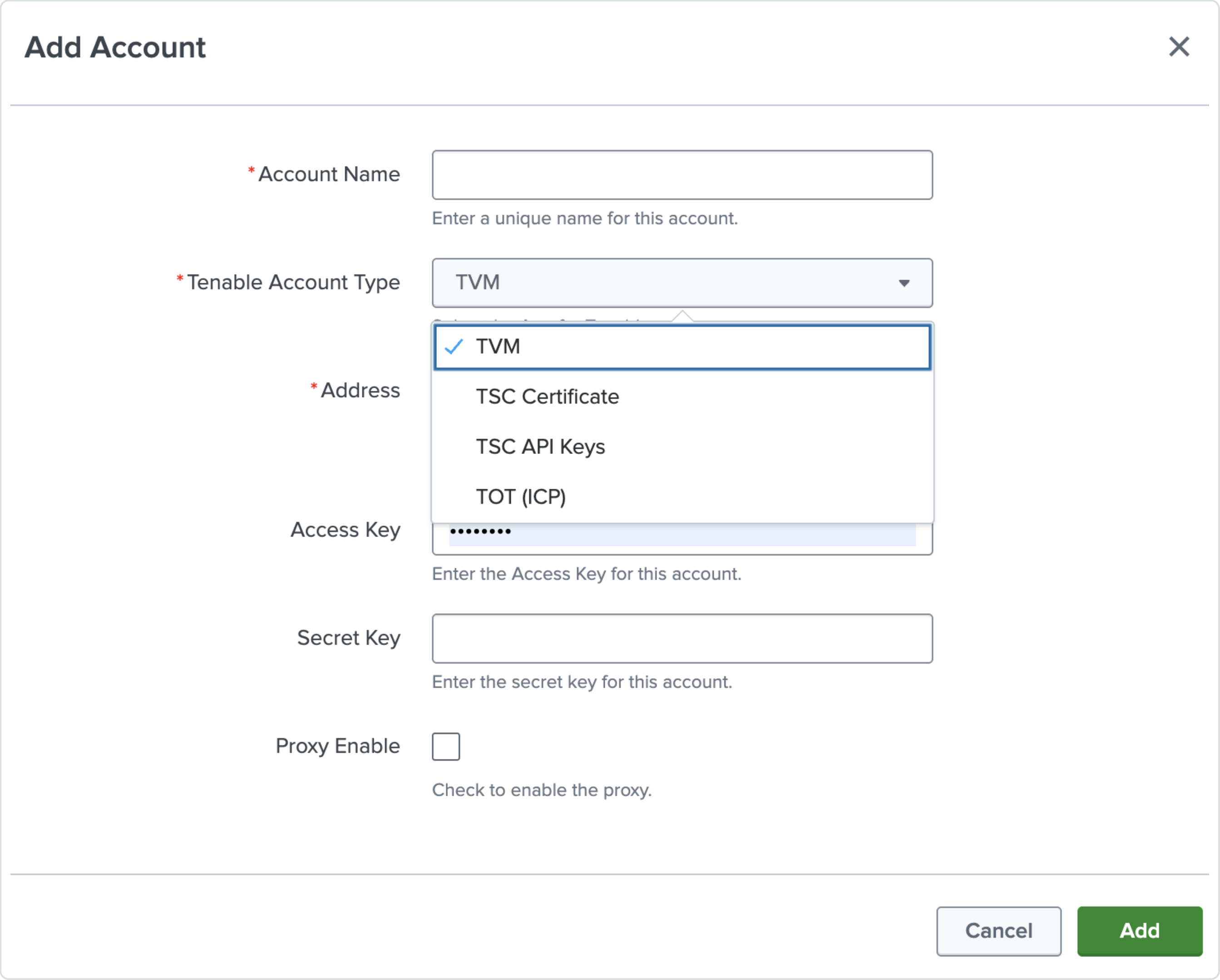
2 Items

Account Name	Tenable Account Type	Actions
Tenable_70	tenable_securitycenter_credentials	Action
Tenable_io	tenable_io	Action

https://172.26.97.207:8000/en-US/app/TA-tenable/configuration

4. Click the **Add** button.

   The **Add Account** window appears.



Add Account

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

*Tenable Account Type: TVM
- ✓ TVM
- TSC Certificate
- TSC API Keys
- TOT (ICP)

*Address

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. In the **Tenable Account Type** box, select **TSC 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	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_sc_creds = True
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 `$SPLUNK_HOME/etc/apps/TA-tenable/certs/`.
Key Filename	The name of the key that you uploaded to `$SPLUNK_HOME/etc/apps/TA-tenable/certs/`.
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: • **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.

Configure Tenable Vulnerability Management or Tenable Web App Scanning

Required User Role: Administrator

Connect to Tenable Vulnerability Management or Tenable Web App Scanning by creating the account configuration.

Before you begin:

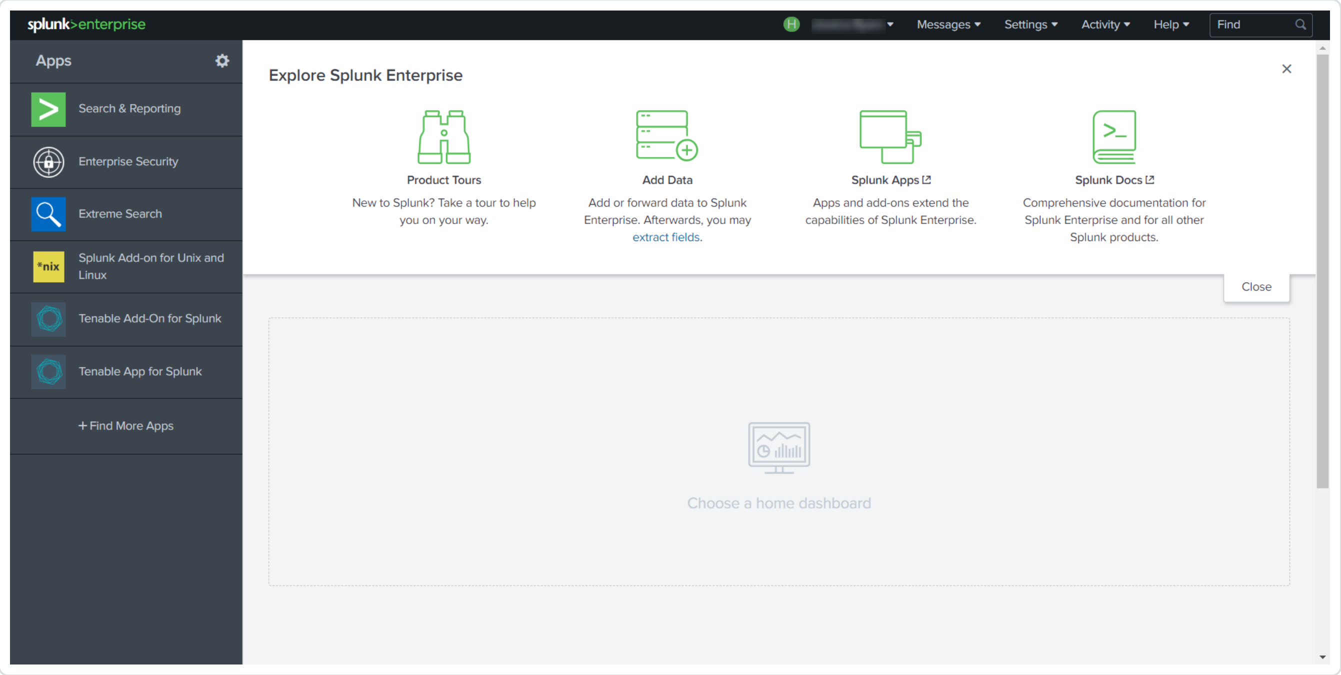
- Generate an API key in Tenable Vulnerability Management to complete the configuration. See the Tenable Vulnerability Management user guide for instructions on how to generate an API key. Do not use this API key for any other third-party or custom-built application or integration. It must be unique 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 configure your account for Tenable Vulnerability Management(**TVM**) or Tenable Web App Scanning(**TWAS**):

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**.



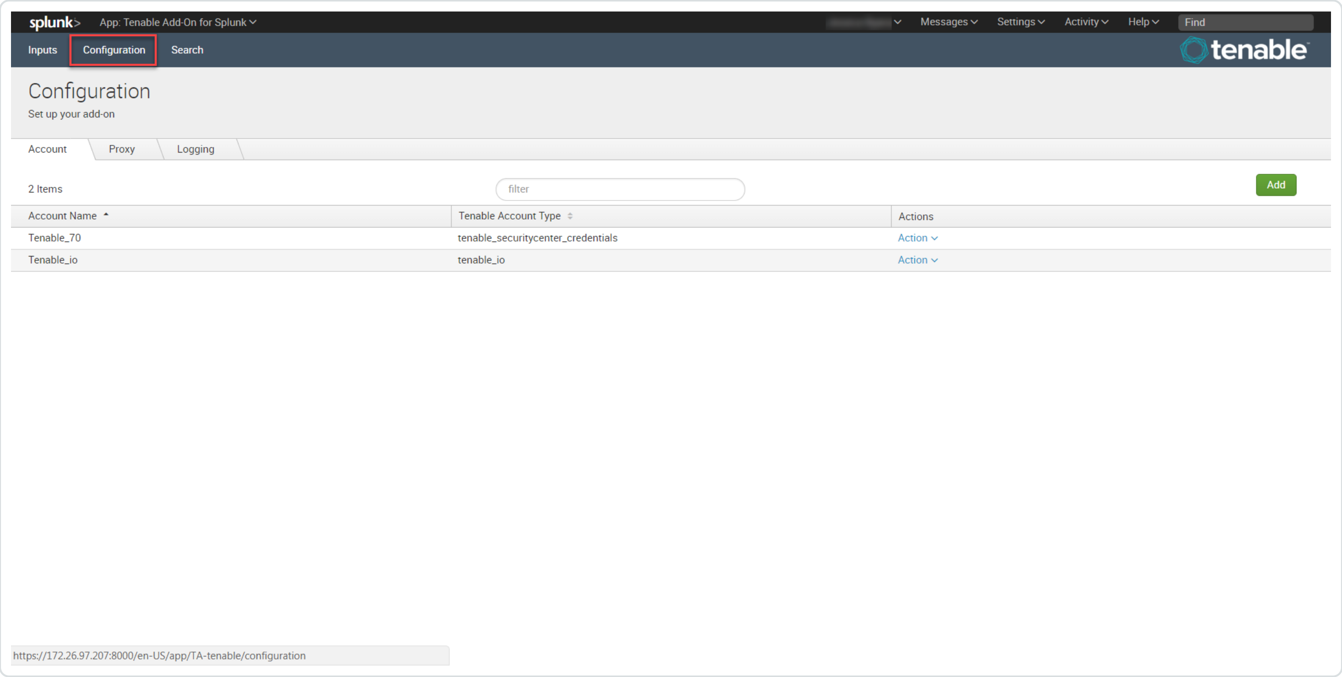
New to Splunk? Take a tour to help you on your way.

Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Apps and add-ons extend the capabilities of Splunk Enterprise.

Comprehensive documentation for Splunk Enterprise and for all other Splunk products.

3. Click the **Configuration** tab.



Configuration

Set up your add-on

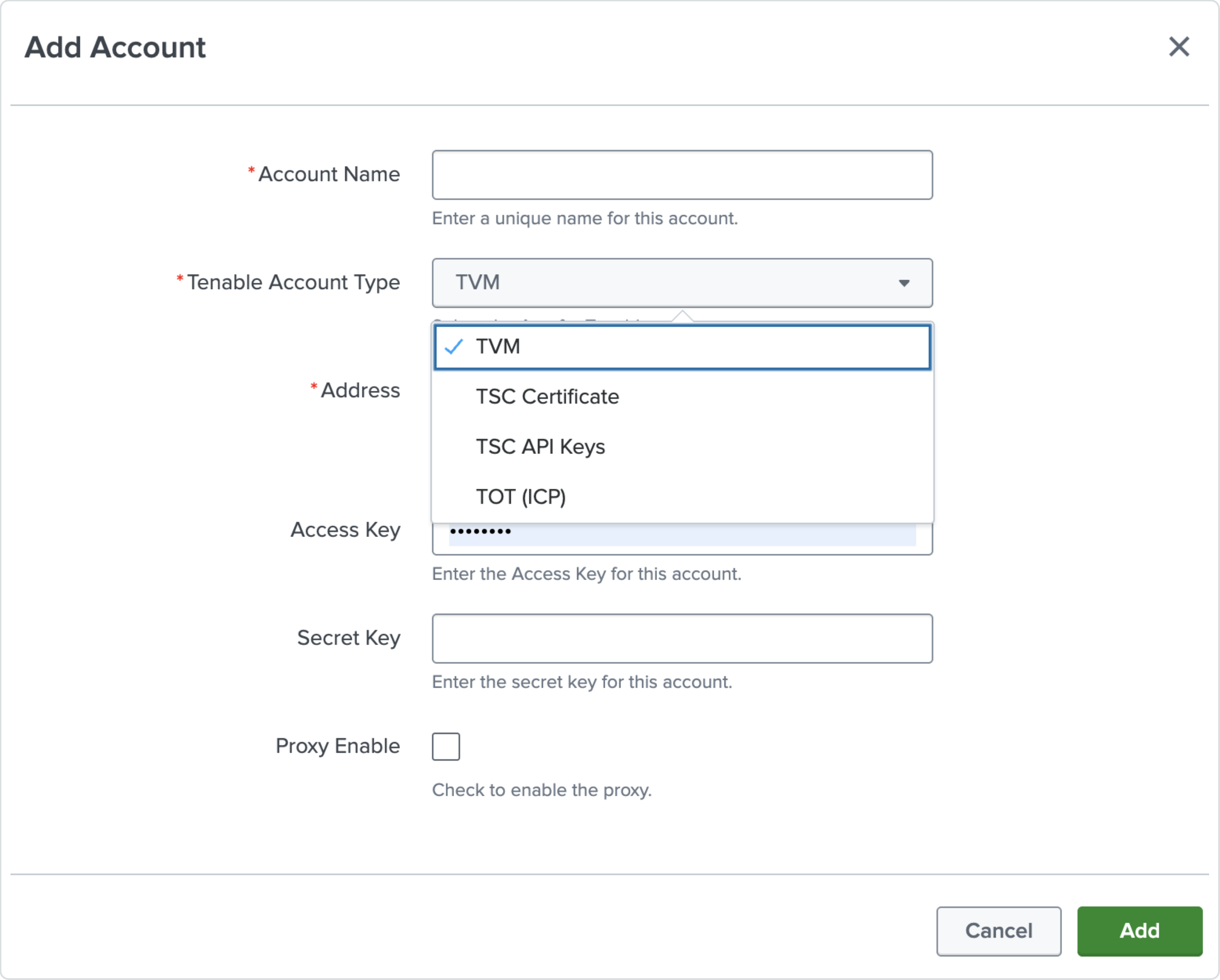
2 Items

Account Name	Tenable Account Type	Actions
Tenable_70	tenable_securitycenter_credentials	Action
Tenable_io	tenable_io	Action

https://172.26.97.207:8000/en-US/app/TA-tenable/configuration

4. Click the **Add** button.

   The **Add Account** window appears:



* Account Name

Enter a unique name for this account.

* Tenable Account Type: TVM ✓

* Address

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. In the **Tenable Account Type** box, select **TVM**.

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. Select **TVM** or **TWAS**.
Address	(Required) The hostname or IP address for Tenable

	Vulnerability Management or Tenable Web App Scanning. (For example, `cloud.tenable.com` or `fedcloud.tenable.com`)
Verify SSL Certificate	Enabled by default, Splunk verifies the certificate in Tenable Vulnerability Management or Tenable Web App Scanning. 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_sc_creds = True
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 or Tenable Web App Scanning 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. • **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. To complete the configuration, click **Add**.

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 for the deployment type you have. The following process outlines input creation if you have a deployment with Tenable Add-On for Splunk.

To create an input:

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

The input drop-down list appears:

4. Select your input type.

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 3600 and 86400.	Yes
Index	The index in which to store Tenable Vulnerability Management data.	Yes
Global Account	Use one of the accounts from the Create an Account page for the matching Tenable product.	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 *YYYY-MM-DD hh:mm:ss* format.	No
Lowest Severity to Store	Select the lowest level of severity to store. Can be **Info**, **Low**, **Medium**, **High**, or **Critical**.	Yes
Historical Fixed Vulnerability	Allows the import of vulnerabilities fixed before the current day.	No

TOT (ICP)

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. This supports seconds (between 3600 and 86400) or a cron schedule.	Yes
Index	The index in which to store Tenable OT Security data.	Yes
Global Account	Use one of the accounts from the Create an Account page for the matching Tenable product.	Yes

TSC Vulnerability

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

	input restarts to perform the task again. This supports seconds (between 300 and 86400) or a cron schedule. **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.	
Index	The index in which to store Tenable Security Center data.	Yes
Global Account	Use one of the accounts from the Create an Account page for the matching Tenable product.	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 *YYYY-MM-DD hh:mm:ss* 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

TSC 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	Use one of the accounts from the Create an Account page for the matching Tenable product.	Yes
Query Name	A name for Tenable Security Center vulnerability filter. **Note:** The interval must be query type - **Vulnerability Detail List**.	No

TVM

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. This supports seconds (between 3600 and	Yes

		86400) or a cron schedule.	
Index		The index in which to store Tenable Vulnerability Management data.	Yes
Global Account		Use one of the accounts from the [Create an Account]() page for the matching Tenable product.	Yes
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
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

TVM Audit Logs

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. This supports seconds (between 3600 and 86400) or a cron schedule.	Yes
Index	The index in which to store Tenable Vulnerability Management data.	Yes

Global Account	Use one of the accounts from the Create an Account page for the matching Tenable product.	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 *YYYY-MM-DD hh:mm:ss* format.	No

TVM Compliance

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. This supports seconds (between 3600 and 86400) or a cron schedule.	Yes

Index	The index in which to store Tenable Vulnerability Management data.	Yes
Global Account	Use one of the accounts from the Create an Account page for the matching Tenable product.	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 *YYYY-MM-DD hh:mm:ss* format.	No

Tenable Attack Surface 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.	
Global Account	Use one of the accounts from the Create an Account page for the matching Tenable product.	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 *YYYY-MM-DD hh:mm:ss* format.	

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

> **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.

Next, configure your application.

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**.

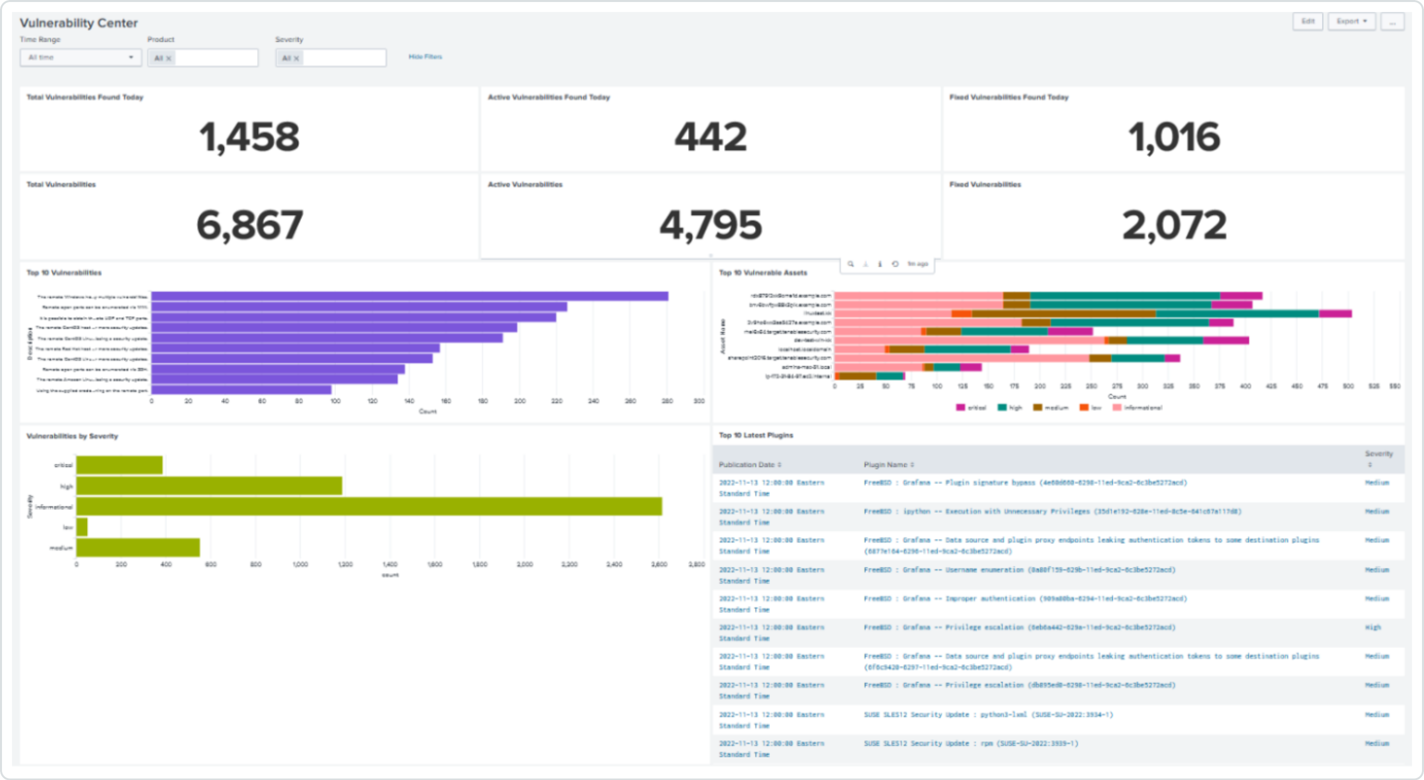
Run the **All Time** saved search

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



Vulnerability Center

Time Range: All time
Product: All ×
Severity: All ×

Total Vulnerabilities Found Today: 1,458

Active Vulnerabilities Found Today: 442

Fixed Vulnerabilities Found Today: 1,016

Total Vulnerabilities: 6,867

Active Vulnerabilities: 4,795

Fixed Vulnerabilities: 2,072

Top 10 Latest Plugins

Publication Date ⇕	Plugin Name ⇕	Severity ⇕
2022-11-13 12:00:00 Eastern Standard Time	FreeBSD : Grafana -- Plugin signature bypass (4e60d660-6298-11ed-9ca2-6c3be5272acd)	Medium
2022-11-13 12:00:00 Eastern Standard Time	FreeBSD : ipython -- Execution with Unnecessary Privileges (35d1e192-628e-11ed-8c5e-641c67a117d8)	Medium
2022-11-13 12:00:00 Eastern Standard Time	FreeBSD : Grafana -- Data source and plugin proxy endpoints leaking authentication tokens to some destination plugins (6877e164-6298-11ed-9ca2-6c3be5272acd)	Medium
2022-11-13 12:00:00 Eastern Standard Time	FreeBSD : Grafana -- Username enumeration (0a80f159-629b-11ed-9ca2-6c3be5272acd)	Medium
2022-11-13 12:00:00 Eastern Standard Time	FreeBSD : Grafana -- Improper authentication (909a80ba-6294-11ed-9ca2-6c3be5272acd)	Medium
2022-11-13 12:00:00 Eastern Standard Time	FreeBSD : Grafana -- Privilege escalation (6eb6a442-629a-11ed-9ca2-6c3be5272acd)	High
2022-11-13 12:00:00 Eastern Standard Time	FreeBSD : Grafana -- Data source and plugin proxy endpoints leaking authentication tokens to some destination plugins (6f6c9420-6297-11ed-9ca2-6c3be5272acd)	Medium
2022-11-13 12:00:00 Eastern Standard Time	FreeBSD : Grafana -- Privilege escalation (db895ed0-6298-11ed-9ca2-6c3be5272acd)	Medium
2022-11-13 12:00:00 Eastern Standard Time	SUSE SLES12 Security Update : python3-lxml (SUSE-SU-2022:3934-1)	Medium
2022-11-13 12:00:00 Eastern Standard Time	SUSE SLES12 Security Update : rpm (SUSE-SU-2022:3939-1)	Medium

Tenable Network Monitor Data in Splunk Dashboard

The Tenable App for Splunk provides a single dashboard showing all of your Tenable 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

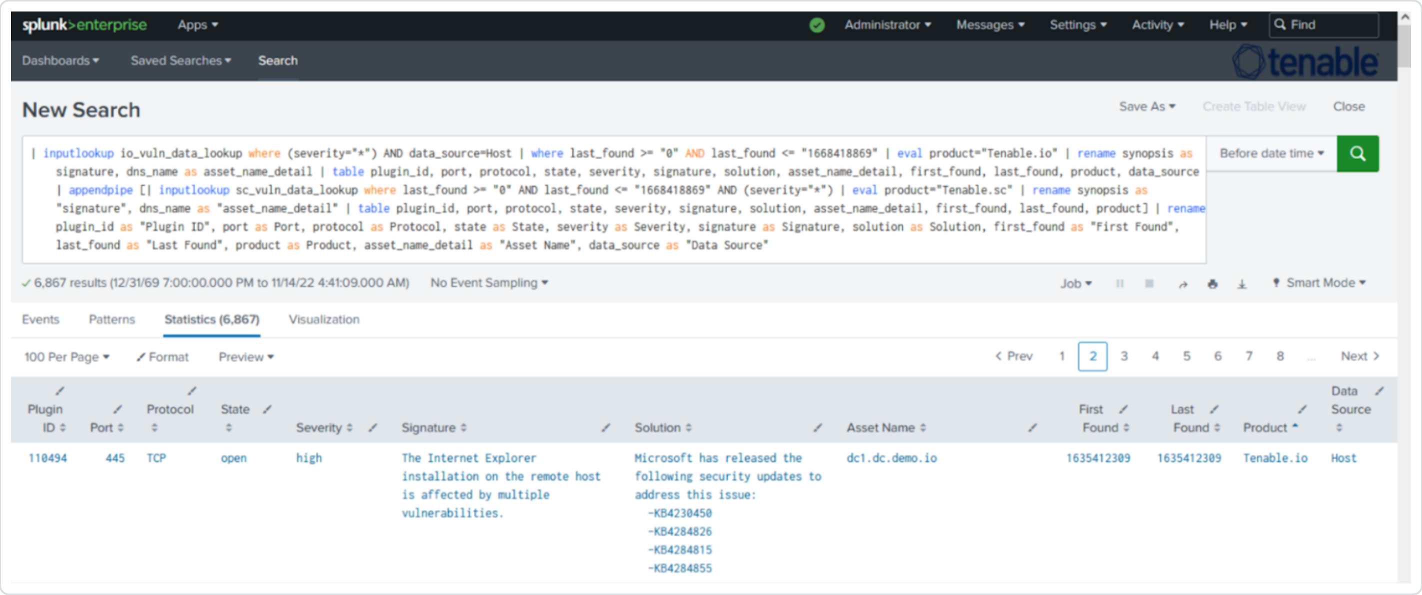
Events

- 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



```
| inputlookup io_vuln_data_lookup where (severity="*") AND data_source=Host | where last_found >= "0" AND last_found <= "1668418869" | eval product="Tenable.io" | rename synopsis as
    signature, dns_name as asset_name_detail | table plugin_id, port, protocol, state, severity, signature, solution, asset_name_detail, first_found, last_found, product, data_source
    | appendpipe [| inputlookup sc_vuln_data_lookup where last_found >= "0" AND last_found <= "1668418869" AND (severity="*") | eval product="Tenable.sc" | rename synopsis as
    "signature", dns_name as "asset_name_detail" | table plugin_id, port, protocol, state, severity, signature, solution, asset_name_detail, first_found, last_found, product] | rename
    plugin_id as "Plugin ID", port as Port, protocol as Protocol, state as State, severity as Severity, signature as Signature, solution as Solution, first_found as "First Found",
    last_found as "Last Found", product as Product, asset_name_detail as "Asset Name", data_source as "Data Source"
```

✓ 6,867 results (12/31/69 7:00:00.000 PM to 11/14/22 4:41:09.000 AM)   No Event Sampling ▾

Plugin ID	Port	Protocol	State	Severity	Signature	Solution	Asset Name	First Found	Last Found	Product	Data Source
110494	445	TCP	open	high	The Internet Explorer installation on the remote host is affected by multiple vulnerabilities.	Microsoft has released the following security updates to address this issue: -KB4230450 -KB4284826 -KB4284815 -KB4284855	dc1.dc.demo.io	1635412309	1635412309	Tenable.io	Host

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_modification_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.

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

> **Note:** Some search commands need an additional key to use KV store lookups. (For example, use `inputlookup` to get search results from a KV Store collection: `inputlookup sc_vuln_data_lookup`)

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 Network Monitor Saved Search Types

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

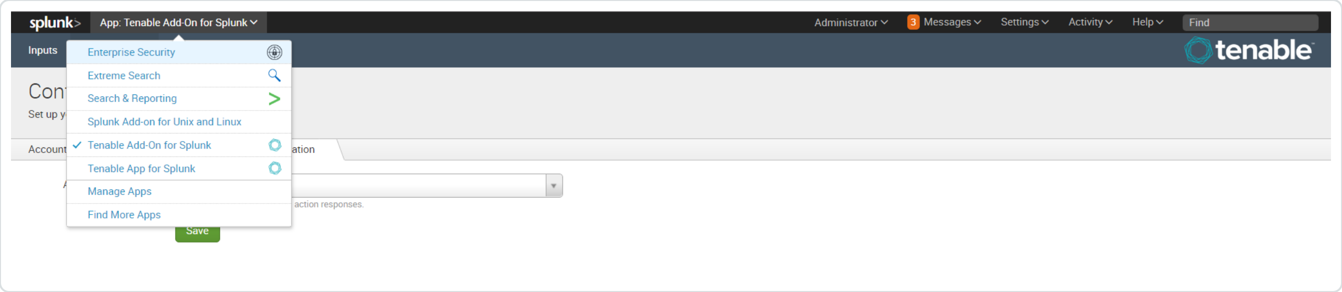
Select an index on the Alert Actions Configuration tab in the Tenable Configuration section to retrieve data.

To configure saved actions:

Configure adaptive response actions when you create a correlation search.

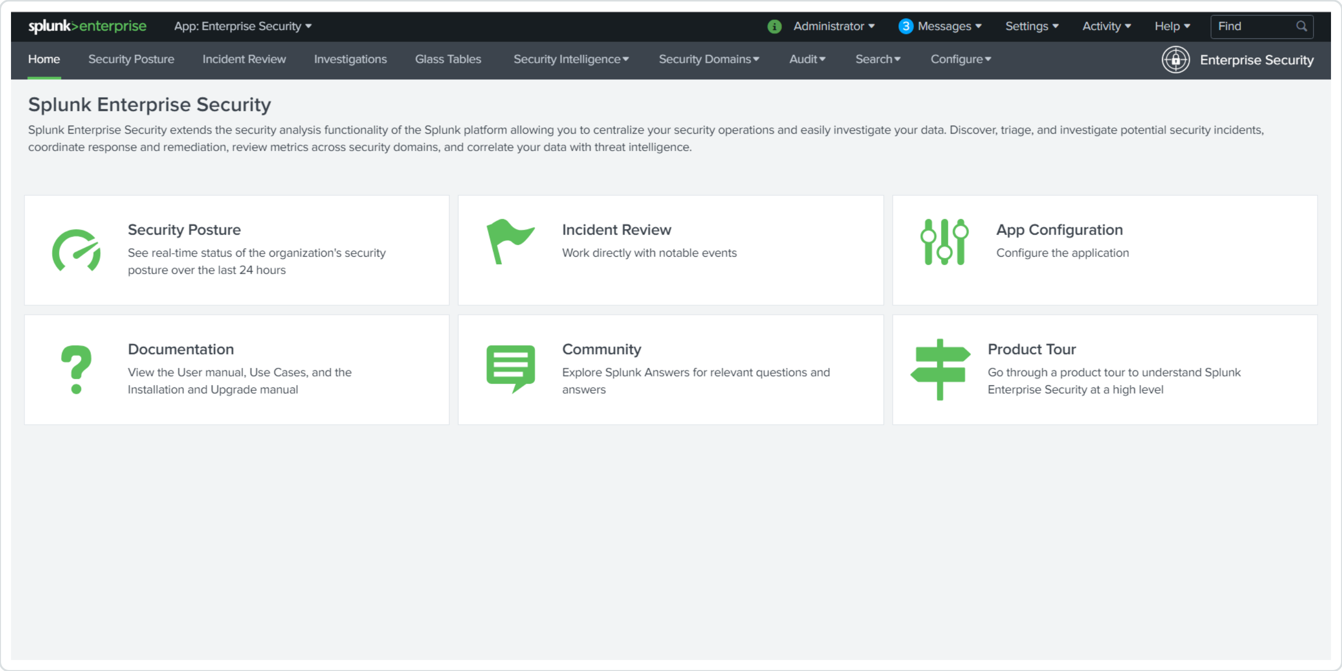
> **Note:** When you run the search, the actions are retrieved automatically

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



2. Select **Enterprise Security**.

   The **Enterprise Security** page appears:



Splunk Enterprise Security

Splunk Enterprise Security extends the security analysis functionality of the Splunk platform allowing you to centralize your security operations and easily investigate your data. Discover, triage, and investigate potential security incidents, coordinate response and remediation, review metrics across security domains, and correlate your data with threat intelligence.

Security Posture
See real-time status of the organization's security posture over the last 24 hours

Incident Review
Work directly with notable events

App Configuration
Configure the application

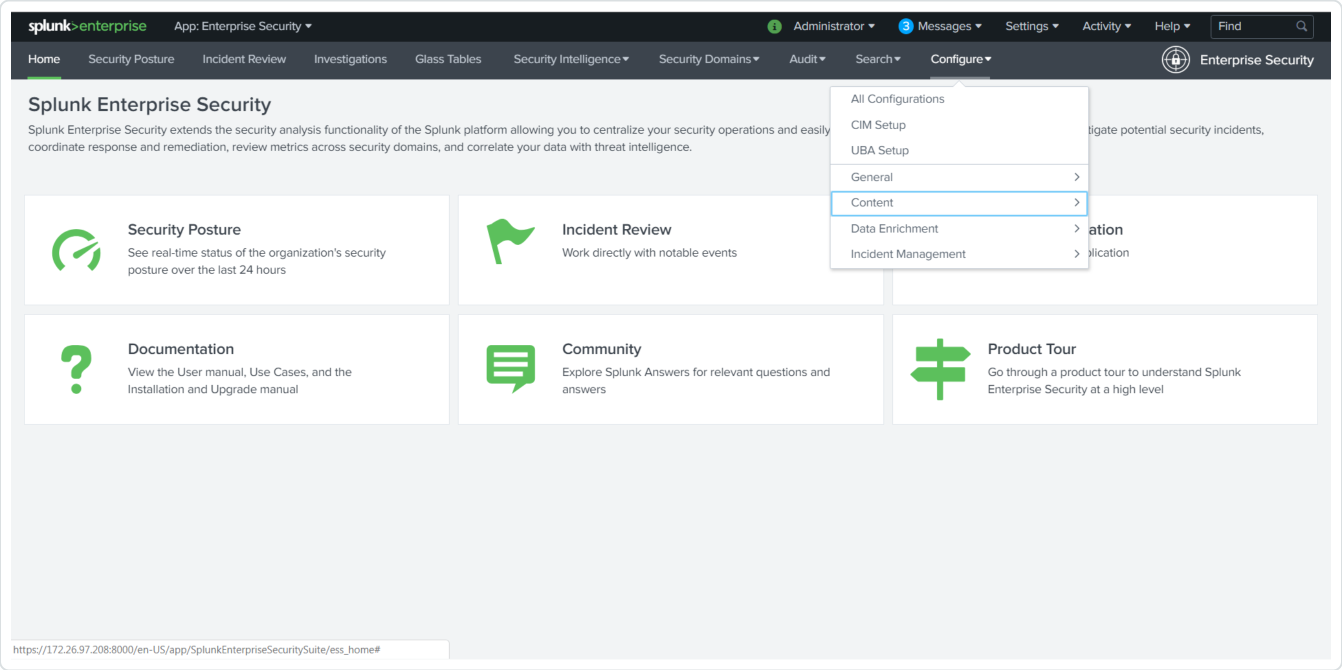
Documentation
View the User manual, Use Cases, and the Installation and Upgrade manual

Community
Explore Splunk Answers for relevant questions and answers

Product Tour
Go through a product tour to understand Splunk Enterprise Security at a high level

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

   A drop-down menu appears:



Splunk Enterprise Security

Splunk Enterprise Security extends the security analysis functionality of the Splunk platform allowing you to centralize your security operations and easily tigate potential security incidents, coordinate response and remediation, review metrics across security domains, and correlate your data with threat intelligence.

Security Posture
See real-time status of the organization's security posture over the last 24 hours

Incident Review
Work directly with notable events

Documentation
View the User manual, Use Cases, and the Installation and Upgrade manual

Community
Explore Splunk Answers for relevant questions and answers

Product Tour
Go through a product tour to understand Splunk Enterprise Security at a high level

https://172.26.97.208:8000/en-US/app/SplunkEnterpriseSecuritySuite/ess_home#

4. Click **Content**.

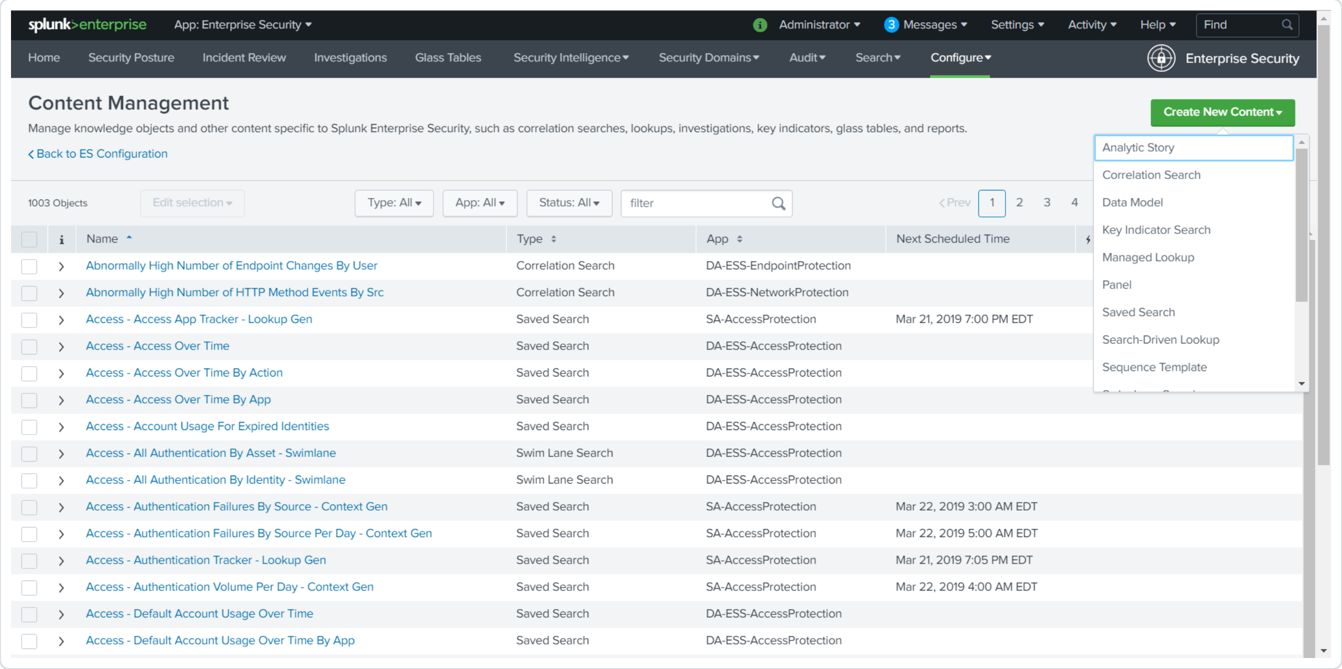
   More options appear.

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:



Content Management

Manage knowledge objects and other content specific to Splunk Enterprise Security, such as correlation searches, lookups, investigations, key indicators, glass tables, and reports.

‹ Back to ES Configuration

1003 Objects

Name	Type	App	Next Scheduled Time
Abnormally High Number of Endpoint Changes By User	Correlation Search	DA-ESS-EndpointProtection	
Abnormally High Number of HTTP Method Events By Src	Correlation Search	DA-ESS-NetworkProtection	
Access - Access App Tracker - Lookup Gen	Saved Search	SA-AccessProtection	Mar 21, 2019 7:00 PM EDT
Access - Access Over Time	Saved Search	DA-ESS-AccessProtection	
Access - Access Over Time By Action	Saved Search	DA-ESS-AccessProtection	
Access - Access Over Time By App	Saved Search	DA-ESS-AccessProtection	
Access - Account Usage For Expired Identities	Saved Search	DA-ESS-AccessProtection	
Access - All Authentication By Asset - Swimlane	Swim Lane Search	DA-ESS-AccessProtection	
Access - All Authentication By Identity - Swimlane	Swim Lane Search	DA-ESS-AccessProtection	
Access - Authentication Failures By Source - Context Gen	Saved Search	SA-AccessProtection	Mar 22, 2019 3:00 AM EDT
Access - Authentication Failures By Source Per Day - Context Gen	Saved Search	SA-AccessProtection	Mar 22, 2019 5:00 AM EDT
Access - Authentication Tracker - Lookup Gen	Saved Search	SA-AccessProtection	Mar 21, 2019 7:05 PM EDT
Access - Authentication Volume Per Day - Context Gen	Saved Search	SA-AccessProtection	Mar 22, 2019 4:00 AM EDT
Access - Default Account Usage Over Time	Saved Search	DA-ESS-AccessProtection	
Access - Default Account Usage Over Time By App	Saved Search	DA-ESS-AccessProtection	

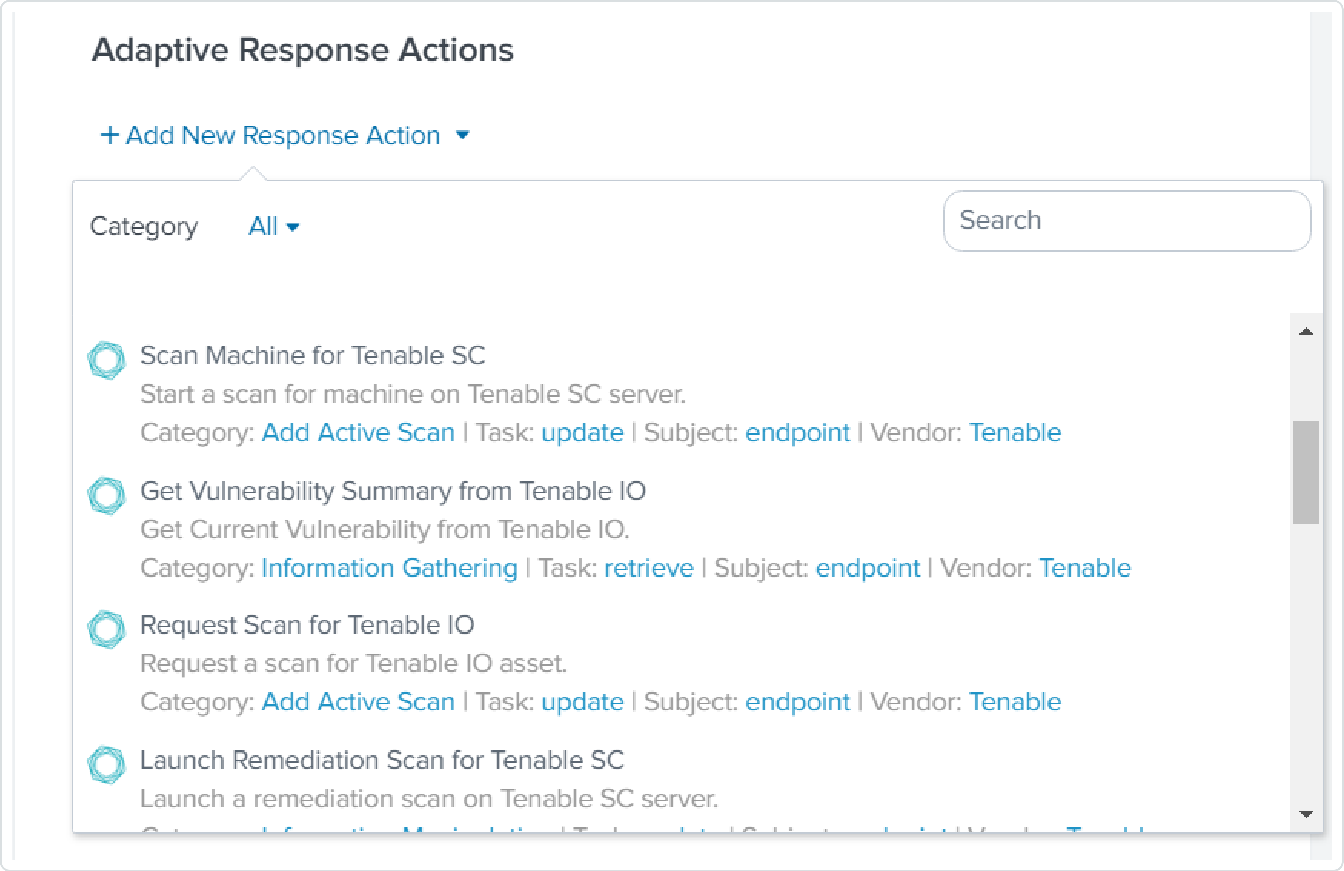
7. Select **Correlation Search**.

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:



Adaptive Response Actions

Scan Machine for Tenable SC
Start a scan for machine on Tenable SC server.
Category: Add Active Scan | Task: update | Subject: endpoint | Vendor: Tenable

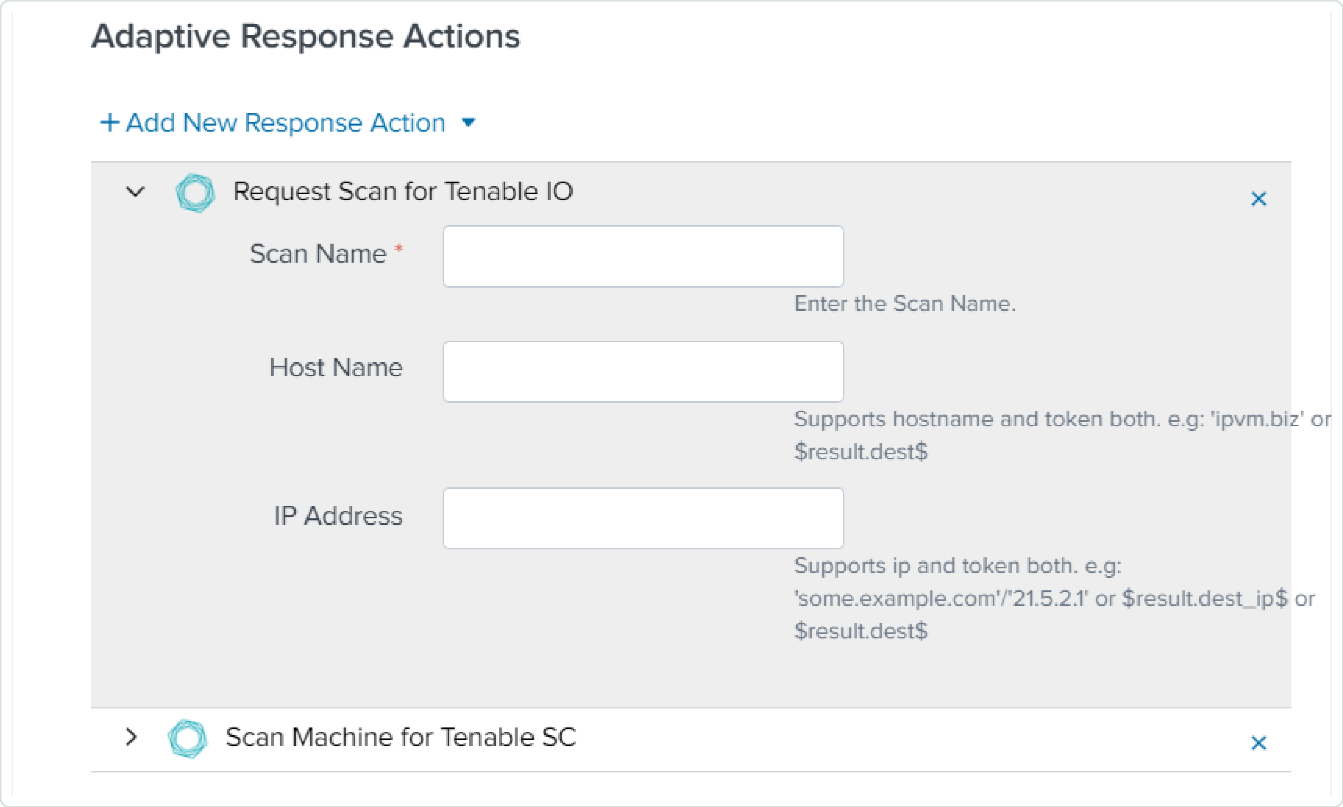
Get Vulnerability Summary from Tenable IO
Get Current Vulnerability from Tenable IO.
Category: Information Gathering | Task: retrieve | Subject: endpoint | Vendor: Tenable

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

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'/'21.5.2.1' or $result.dest_ip$ or $result.dest$

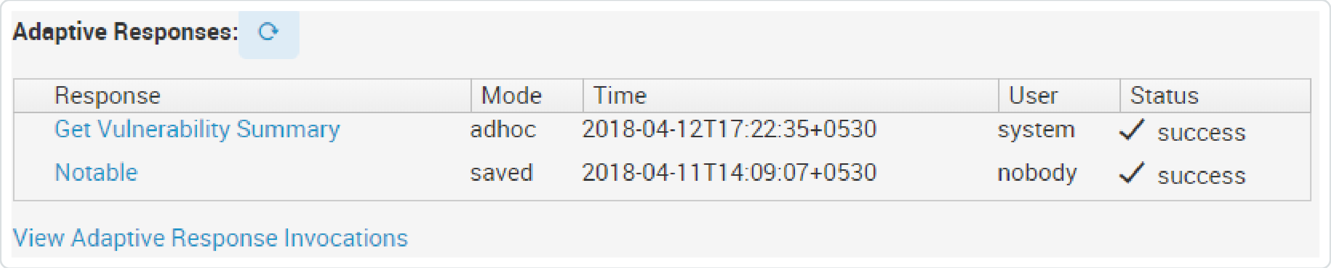
Scan Machine for Tenable SC

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

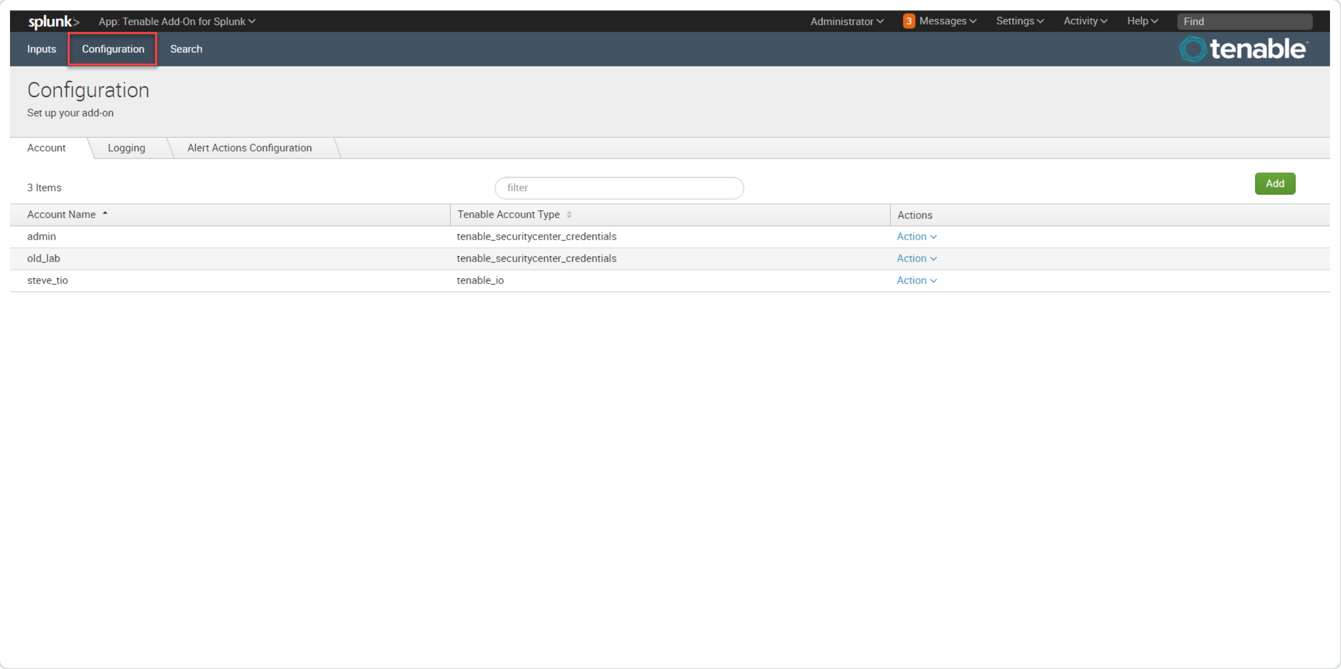
View Adaptive Response Invocations

Alert Action Configuration

To configure alert actions:

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

   The **Configuration** page appears:



Configuration

Set up your add-on

3 Items

Account Name	Tenable Account Type	Actions
admin	tenable_securitycenter_credentials	Action
old_lab	tenable_securitycenter_credentials	Action
steve_tio	tenable_io	Action

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)`.

Frequently Asked Questions

1. **I am unable to save the account for TASM.**
   - Check the **Domain** and **API Key**. Make sure each one is valid.
   - If using a proxy, check the proxy configuration.
2. **I am unable to save the account for TSC and TOT.**
   - Custom Certificate option has been added in v8.0.0, Make sure that SSL Certificate is valid if provided.
3. **Input is created successfully but data is not getting collected.**
   - Check the data by expanding the time range in Splunk search.
   - If using a proxy, check the proxy configuration.Make sure that you are entering correct search query. For example, if you want to search TASM data the search query will be: `index = your_index sourcetype = tenable:asm:assets`
   - Check the log messages for errors:
     - For logs related to TASM data collection: You can view the logs in the `ta_tenable_tenable_asm.log` log file by navigating to `$SPLUNK_HOME/var/log/splunk/`.
     - For logs related to TWAS Assets & Vulns: You can view the logs in the `ta_tenable_tenable_was.log` log file by navigating to `$SPLUNK_HOME/var/log/splunk/`.
     - Error log messages regarding TASM data collection can also be seen from Splunk search in “_internal” index: `index = _internal source = *ta_tenable_tenable_asm.log* ERROR`
     - Error log messages regarding TWAS Assets & Vulns data collection can also be seen from Splunk search in “_internal” index: `index = _internal source = *ta_tenable_tenable_was.log* ERROR`

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