

# **Tenable and Splunk Integration Guide**

Last Revised: July 10, 2023

# Table of Contents

Welcome to Tenable for Splunk	
Components	
Tenable Add-on (TA-tenable)	
Source and Source Types	
Splunk Common Information Model Mapping	
Installation Workflow	
Upgrade the App from v1 to v4	11
Splunk Environments	
Installation	
Configuration	
Configure Tenable Identity Exposure	
Configure Tenable Vulnerability Management	23
Configure Tenable Nessus Network Monitor	
Configure Tenable OT Security	
Configure Tenable Security Center Credentials	
Configure Tenable Security Center Certificates	
Create an Input	
Tenable Data in Splunk Dashboard	
Vulnerability Center Dashboard	
Saved Searches	
Adaptive Response	
Alert Action Configuration	64
Additional Information	

- Ø

	Best Practices	66
	Customized Actions	67
	Tenable Macros	68
	Troubleshooting	69
	Known Issues	73
S	plunk 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

- Ø -

## Welcome to Tenable for Splunk

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

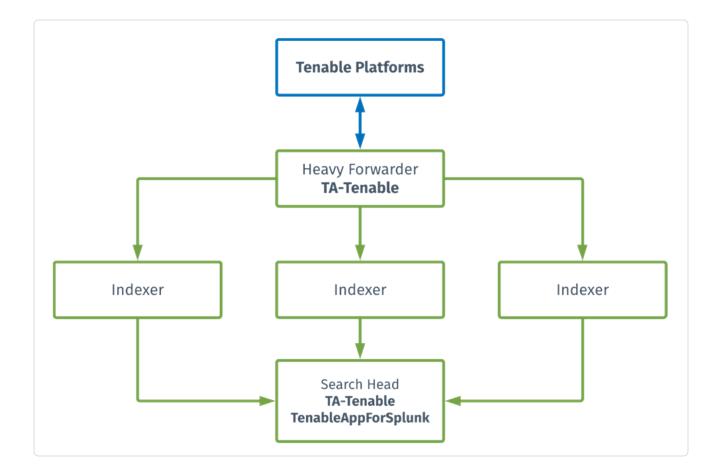
O

- <u>Tenable Add-On for Splunk (TA-tenable)</u> provides all data collection and normalization functionality.
- <u>Tenable Web App Scanning Add-on for Splunk</u> provides all data collection and normalization functionality.
- <u>Tenable App for Splunk</u> 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.

 $\bigcirc$ 



## 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 Addon.

## **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
- <u>GET /assets/export/{export\_uuid}/status</u>
- 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
- <u>GET /vulns/export/{export\_uuid}/chunks/{export\_uuid}</u>

#### **Plugins**

• <u>GET / plugins / plugin</u>

## 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></address></username>	tenable:io:vuln:was	This collects all vulnerability data.

O

### **Tenable Security Center**

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

### **Tenable Vulnerability Management**

Source	Source type	Description
tenable_io:// <data input<br="">name&gt;</data>	tenable:io:vuln	Collects cumulative vulnerability data from active, agent and fric- tionless assessment scans from licensed assets.
tenable_io:// <data input<br="">name&gt;</data>	tenable:io:assets	Collects all assets data.
tenable_io:// <data input<br="">name&gt;</data>	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).

Ø

Field Name from Tenable Vulnerability Man- agement API	Field Name from Ten- able Security Center API	CIM Field Name	CIM Data Model
asset_fqdn	dnsName	dns_name	vulnerability
ipv4	ір	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. <u>Install</u> the Tenable application.
- Configure the required Tenable application for Splunk: <u>Tenable Vulnerability Management</u>, <u>Tenable Security Center Credentials</u>, <u>Tenable Security Center Certificates</u>, <u>Tenable Nessus Net-</u> work Monitor, Tenable Identity Exposure, or <u>Tenable OT Security</u>.

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

- 3. <u>Create an input</u> for the configured Tenable application for Splunk.
- 4. <u>Configure</u> your Tenable App for Splunk dashboard.
- 5. <u>Configure adaptive response</u> 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.

 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. <u>Configuration</u> 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 <u>Create an Input</u> section.

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

0 -

\_\_\_\_\_

# **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-OnTenable 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.

\_

Ø \_\_\_\_\_

## 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 <u>Splunk Environments</u> 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 Addon.

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:

Search	<ul> <li>Search &amp; Reporting</li> </ul>	>	Alerts	Dashboards
Searc	Splunk Essentials for Cloud and Enterprise 9.0	>		
	Splunk Secure Gateway	ssg	_	
enter s	Upgrade Readiness App			
No Event	Manage Apps			
	Find More Apps			

- 3. Click Find More Apps.
- 4. On the **Browse More Apps** page, type Tenable in the search bar.

Tenable-related options appear:

Apps _	Search & Reporting	>					Browse more apps Install app from file Create app
howing 1	Tenable Add-On for Splunk	<u>о</u> њ					
	Tenable App for Splunk	0					
Tenable	Manage Apps						25 per page 🔻
Name 🕯	Find More Apps	n \$	Update checking \$	Visible \$	Sharing \$	Status 🕏	Actions
Tenable A On for Spl		3.2.2	Yes	Yes	Global   Permissions	Enabled   Disable	Launch app   Edit properties   View objects   12 View details on Splunkbase
Tenable A		2.1.0	Yes	Yes	App   Permissions	Enabled   Disable	Launch app   Edit properties   View objects   🛛 View details on Splunkbase

5. Click the **Install** button next to **Tenable Add-on for Splunk**.

	Q	
Browse More Apps		
Tenablej ×	Best Match Newest Popular 6 Apps	
CATEGORY  IT Operations Security, Fraud & Compliance Business Analytics Utilities I of & Industrial Data DevOps	Tenable Add-On for Splunk  Install  The Tenable Add-On for Splunk provides a robust set functionality for getting Tenable data into Splunk.	Tenable App for Splunk Install
Directory Service Email Endpoint Firewall	Category: Security, Fraud & Compliance   Author: Tenable, Inc.   Downloads: 27102   Released: 5 months ago   Last Updated: a month ago   View on Splunkbase	Category: Security, Fraud & Compliance   Author: Tenable, Inc.   Downloads: 13495   Released: a year ago   Last Updated: a month ago   View on Splunkbase

- 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.

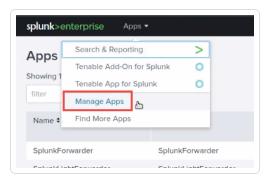
Note: Follow steps 1 to 6 to install the Tenable App for Splunk.

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

To upgrade Tenable Web App ScanningAdd-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:

splunk>e						Administrator	r ▼ Messages ▼ Settings ▼ Activity ▼ Help ▼ Find Q
Apps	Search & Reporting	>					Browse more apps Install app from file Create app
	Tenable Add-On for Splunk	<u>o</u> £-					
Showing 1	Tenable App for Splunk	0					
Tenable	Manage Apps						25 per page 👻
Name 🕯	Find More Apps	n •	Update checking \$	Visible \$	Sharing 🕈	Status 🕈	Actions
Tenable A On for Sp		3.2.2	Yes	Yes	Global   Permissions	Enabled   Disable	Launch app   Edit properties   View objects   12 View details on Splunkbase
Tenable A		2.1.0	Yes	Yes	App   Permissions	Enabled   Disable	Launch app   Edit properties   View objects   Z View details on Splunkbase

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

Apps							Browse more apps Install app from file Create a
howing 1-2 of 2 items Tenable	٩						25 per page
Name \$	Folder name \$	Version \$	Update checking \$	Visible *	Sharing *	Status +	Actions
Tenable Add-On for Splunk	TA-tenable	2.0.0   Update to	Yes	Yes	Global   Permissions	Enabled   Disable	Launch app   Edit properties   View objects   12 View details on Splunkbe
Tenable App for Splunk	TenableAppforSplunk	2.0.0   Update to	Yes	Yes	App   Permissions	Enabled   Disable	Launch app   Edit properties   View objects   🛽 View details on Splunkberger

- 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 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 <u>update the Tenable Macro</u>, **get\_tenable\_index**, for data to begin populating the application dashboards.

Next, <u>configure</u> the Tenable application.

# Configuration

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

O

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.

<b>splunk</b> ≻enterprise Apps <del>•</del>			<ul> <li>Administrator ▼</li> </ul>	3 Messages ▼ Settings ▼	<ul> <li>Activity ▼</li> </ul>	Help - Find	٩
	Add Data Select Soc	urce Input Settings Review	Done Kack	ext >			
	Files & Directories Upload a file, index a local file, or monitor an entire directory.	Configure this instance to list (such as syslog). Learn More		o capture data sent over the net	work		
	HTTP Event Collector Configure tokens that clients can use to send data over HTTP or HTTPS.		TCP	UDP			
	TCP / UDP > Configure the Splunk platform to listen on a network port.	Port ?	Example: 514				
	Scripts Get data from any API, service, or database with a script.	Source name override ?	optional host:port				
	App Imports Update Updates the app imports with all apps matching a given regular expression.	Only accept connection from ?	optional example: 10.1.2.3, !badhost.splunl	.com, *.splunk.com			
	App Permissions Manager Enforces permissions policy.	FAQ					
	Configuration Checker Runs configuration checks.	<ul> <li>How should I configure the</li> <li>What's the difference betw</li> </ul>					
	Data Migrator Perform one-time data migrations.	<ul> <li>Can I collect syslog data fr</li> <li>What is a source type?</li> </ul>	om Windows systems?				
	Data Model Acceleration Enforcement Enforces data model acceleration settings.						
	, v						

4. Enter the port configuration information.

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

The **Input Settings** page appears:

splunk>enterprise Apps <del>•</del>		🚯 Administrator 🕶 🥹 Messages 💌 Settings 🕶 Activity 👻 Help 👻 Find 🔍
	Add Data Select Source Input Settings Review	Done Review >
	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 [2]	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 [2]	IP DNS Custom
	Index The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a location 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 [2]	Default   Create a new index
	FAQ > How do indexes work? > How do I know when to create or use multiple indexes?	

 $\bigcirc$ 

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

- 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 <u>installation</u> 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 <u>Tenable Vulnerability Management user guide</u> 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 <u>Tenable API endpoints</u>.

### 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**.

		- Ø			
splunk>enterprise			H ✓ Messages ✓	Settings ▼ Activity ▼ Help ▼	Find Q,
Apps 🌣	Explore Splunk Enterprise	[] []		>_	×
Enterprise Security	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	Splunk Apps I2 Apps and add-ons extend the capabilities of Splunk Enterprise.	Splunk Docs L <sup>2</sup> Comprehensive documentation for Splunk Enterprise and for all other	
*nix Splunk Add-on for Unix and Linux	you vii youi wey.	extract fields.	саралниез от Эрилік сперизе.	Splunk products.	Close
Tenable Add-On for Splunk					
+ Find More Apps					

3. Click the **Configuration** tab.

splunk > App: Tenable Add-On for Splunk ~	inter la	✓ Messages ✓ Settings ✓ Activity ✓ Help ✓ Find
Inputs Configuration Search		🔘 tenable <sup>:</sup>
Configuration Set up your add on		
Account Proxy Logging		
2 Items	filter	Add
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.

A new window appears:

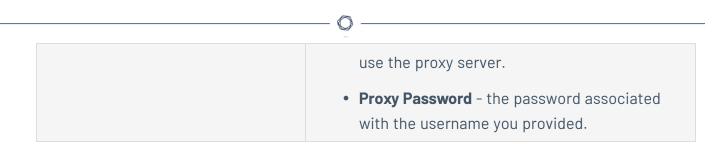
Add Account		×
Account Name *	admin Enter a unique name for this account.	
Tenable Account Type *	Tenable.io       Select the App for Tenable	
Address *	Enter the FQDN or IP of your server for this account.	
Verify SSL Certificate	Should we verify your SSL certificate?	
Access Key	Enter the Access Key for this account.	
Secret Key	Enter the secret key for this account.	
Proxy Enable	Check to enable the proxy.	
Cancel		Add

O

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

0 \_\_\_\_\_

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:
	• <b>Proxy Type</b> - the type of proxy used.
	<ul> <li>Proxy Host - the hostname or IP address of the proxy server.</li> </ul>
	• <b>Proxy Port</b> - the port number of the proxy server.
	• <b>Proxy Username</b> - the username for an account that has permissions to access and



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

### Next steps

• <u>Create an Input</u> 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:nnm: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.

<b>splunk</b> >enterprise Apps <del>v</del>	Add Data Select Soc	arce Input Settings Review	Administrator      3     Administrator      3     Administrator      Admininterrator      Adminintereeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee	Messages ▼ Settings ▼ ,	Activity ▼ Help ▼ Find Q
	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 this instance to list (such as syslog). Learn More	en on any TCP or UDP port to capt	ture data sent over the network	
	Configure the Splunk platform to listen on a network port.  Scripts Get data from any API, service, or database with a script.		Example: 514 optional host.port		
	App Imports Uddate Updates the app imports with all apps matching a given regular expression. App Permissions Manager Enforces permissions policy.	Only accept connection from <sup>7</sup>	optional example: 10.1.2.3, !badhost.splunk.com,	*.splunk.com	
	Configuration Checker Runs configuration checks. Data Migrator Perform one-time data migrations.	<ul> <li>How should I configure the</li> <li>What's the difference betw</li> <li>Can I collect syslog data fr</li> </ul>	e Splunk platform for syslog traffic? reen receiving data over TCP versu om Windows systems?		
	Perform one-time data migrations. Data Model Acceleration Enforcement Enforces data model acceleration settings.	> 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:

<b>splunk</b> >enterprise Apps <del>•</del>	6 Administrator • 3 Messages • Settings • Activity • Help • Find	٩
	Add Data Concernation of the second s	
	Input Settings Optionally set additional input parameters for this data input as follows:	Â
	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 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 12	l
	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 12	l
	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 (2)	
	FAQ > How do indexes work? > How do I know when to create or use multiple indexes?	

 $\bigcirc$ 

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  $\bigcirc$  > 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:

<b>splunk</b> ≻enterprise Apps <del>•</del>			<ul> <li>Administrator ▼</li> </ul>	3 Messages ▼ Settings ▼	<ul> <li>Activity ▼</li> </ul>	Help - Find	٩
	Add Data Select Soc	urce Input Settings Review	Done Kack	ext >			
	Files & Directories Upload a file, index a local file, or monitor an entire directory.	Configure this instance to list (such as syslog). Learn More		o capture data sent over the net	work		
	HTTP Event Collector Configure tokens that clients can use to send data over HTTP or HTTPS.		TCP	UDP			
	TCP / UDP > Configure the Splunk platform to listen on a network port.	Port ?	Example: 514				
	Scripts Get data from any API, service, or database with a script.	Source name override ?	optional host:port				
	App Imports Update Updates the app imports with all apps matching a given regular expression.	Only accept connection from ?	optional example: 10.1.2.3, !badhost.splunl	.com, *.splunk.com			
	App Permissions Manager Enforces permissions policy.	FAQ					
	Configuration Checker Runs configuration checks.	<ul> <li>How should I configure the</li> <li>What's the difference betw</li> </ul>					
	Data Migrator Perform one-time data migrations.	<ul> <li>Can I collect syslog data fr</li> <li>What is a source type?</li> </ul>	om Windows systems?				
	Data Model Acceleration Enforcement Enforces data model acceleration settings.						
	, v						

4. Enter the port configuration information.

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

The **Input Settings** page appears:

<b>splunk</b> ≻enterprise Apps <del>•</del>	👔 Administrator 🔹 3 Messages 🔹 Settings 🔹 Activity 💌 Help 👻 Find 🔍	
	Add Data Select Source Input Settings Review Done Review >	
	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 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 12	
	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 12	
	Index The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a Index destination if you have problems determining a source type for your data. As andbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More 12	
	FAQ > How do indexes work? > How do I know when to create or use multiple indexes?	•

 $\bigcirc$ 

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

More options appear.

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

- 13. At the top of the page, click **Review**.
- 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

- 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 <u>installation</u> 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**.

splunk	Senterprise			H • Messages •	Settings - Activity - Help -	Find Q
Apps	¢	Explore Splunk Enterprise				×
>	Search & Reporting	「「「」			>_	
۲	Enterprise Security	Product Tours	Add Data	Splunk Apps 🖉	Splunk Docs 🖄	
Q	Extreme Search	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.	
*nix	Splunk Add-on for Unix and Linux					Close
Ø	Tenable Add-On for Splunk					
Ø	Tenable App for Splunk					
	+ Find More Apps					
						•

3. Click the **Configuration** tab.

	(A		
splunk> App: Tenable Add-On for Splunk ~		✓ Messages ✓ Settings ✓ Activity ✓ Help ✓ Find	_
Inputs Configuration Search		tenab	
Configuration Set up your add-on			
Account Proxy Logging			
2 Items	filter	Add	
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.

An **Add Account** window appears:

Add Account		×
Account Name		]
Tenable Account Type	Enter a unique name for this account. Tenable.sc Credentials(Deprecated)	×
	Tenable.io	
Address	<ul> <li>Tenable.sc Credentials(Deprecated)</li> <li>Tenable.sc Certificate</li> </ul>	
Verify SSL Certificate	Tenable.sc API Keys Should we verify your SSL certificate?	
Username		]
Password	Enter the username for this account.	7
Password	Enter the password for this account.	J
Proxy Enable	Check to enable the proxy.	
		Cancel Add

O

**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 <u>Generate API Keys</u>.

### 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.

0 -

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	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 fol- lowing:
	• <b>Proxy Type</b> - the type of proxy used.
	• <b>Proxy Host</b> - the hostname or IP address of the proxy server.
	• <b>Proxy Port</b> - the port number of the proxy server.
	• <b>Proxy Username</b> - 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

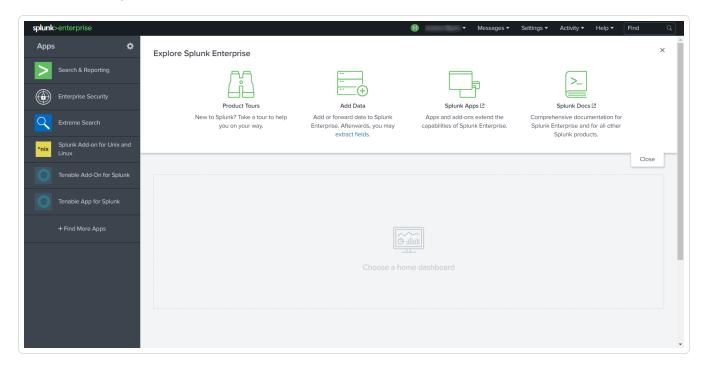
• <u>Create an Input</u> for the Tenable Add-On for Splunk.

# **Configure Tenable Security Center Certificates**

To complete the <u>installation</u> process, you must complete the setup for the Tenable Add-on for Splunk. For additional information on Tenable Security Center Certificates, see <u>SSL Client Cer</u>-tificate 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.

	<u> </u>	
splunk> App: Tenable Add-On for Splunk ~		✓ Messages ✓ Settings ✓ Activity ✓ Help ✓ Find
Inputs Configuration Search		
Configuration		
Set up your add-on		
Account Proxy Logging		
2 Items	filter	Add
Account Name A	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	Tenable.sc Certificate	• ×	
	Select the App for Tenable		
Address			
	Enter the FQDN or IP of your server for this account.		
Verify SSL Certificate	$\checkmark$		
	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.		

O

\_\_\_\_\_

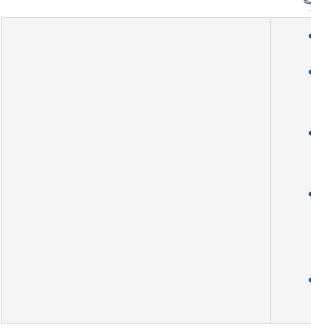
5. In the **Tenable Account Type** box, select **Tenable Security Center Certificates**.

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

 $\bigcirc$ 

**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 Secur- ity 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 \$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 fol- lowing:



- **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_ten-
able/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

• <u>Create an Input</u> 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 orTenable 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**.

<b>splunk</b> >ente	erprise		🚹 Administ	trator ▼ 🝳 Messages ▼ Settings ▼	Activity • Help • Q Find
Apps	¢	Explore Splunk Enterprise			
> Searc	▲ Ch & Reporting	<u>ا</u> ب			
	nk Essentials for d and Enterprise 9.0	Product Tours	Add Data	Explore Data	Splunk Apps 🗠
ssg Splun	nk Secure Gateway	New to Splunk? Take a tour to help you on your way.	Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.	Explore data and define how Hunk parses that data.	Apps and add-ons extend the capabilities of Splunk Enterprise.
Tenab Splun	ble Add-On for nk				Close
Tenab	ble App for Splunk				
	ble Web App ning Add-on for nk				
ΞQ Upgra	ade Readiness App Update				
	Opulae		Choose a hor	me dashboard	

2. Click the **Inputs** tab.

	able Add-On for Splunk 🗸		^		✓ Messages ✓	Settings v Activity v Help	
nputs Configuration	n Search						🔘 tenabl
nputs							Create New Input 🗸
Aanage your data inputs	\$						
Inputs	Services : All 🗸		filter				
Name *		Interval ¢	Index ¢	Stat		Actions	
Tenable_io tenable_70		3600 86400	default default	Enal		Action ~ Action ~	
				▲ Administrator •	Messages • Sc	ttlings ▼ Activity ▼ He	Ip • Find
nputs Configu Nputs	ration Search			Administrator 🕶	2 Messages * Sc	ttlings ▼ Activity ▼ He	tenabl
nputs Configu NPUTS flanage your data i	ration Search			Administrator •	2 Messages • Sc Q	ettings ▼ Activity ▼ He	tenabl
nputs Configu Nputs Manage your data i	ration Search nputs	Interval \$	Index \$			rttings • Activity • He	Ip  Find Tenabl Create New Input
nputs <sup>Manage</sup> your data i Input	ration Search nputs 10 Per Page •	Interval ÷ 3600		filter	Q,	ţ	tenabl

3. Click **Create New Input**.

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

			A	Administrator 👻	2 Messages • Settings •	Activity •	Help 🔻
arch	Add Tenable.was			×			0
	Name						
e -	Interval	Enter a unique name for the data input					
Interval ¢	11021941	Time interval of input in seconds or cron schedule. (min					
3600		value = 3600 secs. and max value = 86400 secs.).			/ 🛛 🔒		
	Index	default					
	Start Time	optional					
		The date (UTC in "YYYY-MM-DDThh:mm:ss2" format) from when to start collecting the data. Default value taken will be start of epoch time.					
	Tenable.io Domain	cloud.tenable.com					
	Tenable.io Access Key						
		Enter the Access key for this account.					
	Tenable.io Secret Key	Entrative Council on Contributions					
		Enter the Secret key for this account.					
			Cancel	Add			

#### 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 Vul- nerability Management data.	Yes

	Ø	
Start Time	The date and time to start collecting data. If you leave this field blank, the integration col- lects all historical data.	No
	<b>Note:</b> Uses the YYYY-MM-DD hh:mm:ss format.	
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 Vul- nerability Management	Yes

	Ø -		
		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 integ- ration collects all his- torical data. (Enter in this format - YYYY-MM-DD hh:mm:ss.)	No
	Lowest Severity Score	The lowest level of sever- ity stored.	No
	Historical Fixed Vulnerability	Allows the import of host vulnerabilities fixed before the current day.	No
	Tags	Limits host vul- nerabilities 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

	O	
	input restarts to perform the task again (in seconds). The interval amount must be between 300 and 86400.	
	<b>Note:</b> 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.	
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 col- lects all historical data.	No
	<b>Note:</b> Uses the YYYY-MM-DD hh:mm:ss format.	
Sync Plugin Details	If selected, the related tags in Tenable assets include plugin details.	Yes
Historical Fixed Vul- nerability	Allows the import of vulnerabilities fixed before the current day.	No
Query Name	A name for Tenable Security Center vul- nerability filter.	No
	<b>Note:</b> The interval must be query type <b>Vul-</b> <b>nerability Detail List</b> .	
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 vul- nerability filter.	No
	<b>Note:</b> The interval must be query type - <b>Vul-</b> <b>nerability Detail List</b> .	

- 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 <u>Tenable API endpoints</u>.

## **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.
- 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

rability Center ge Prod. *		Flore				68	Export
inerabilities Found Today	1,458	Active Vulnerabilities Found Today	44	2	Fixed Vulnerabilities P	<b>1,016</b>	
nerabilities	6,867	Active Vulnerabilities	4,7	95	Fixed Vulnerabilities	2,072	
na Carrill 3 Yand room annu rhy updaten nin Carrill 3 Urus, haring a senarthy updaten na Rael Halt had room annu rhy updaten nin Darill 3 Vicus annu rhy undaten				neiürültergetienebiesecurity.com devidebichick localitedi.ocaldomin	_		
na spor park son to survey with a 15 Str. and Jonese Units being a searchy special anapplate and survey of the servey period	20 40 80 80 90 90 90 G	148 180 200 228 340 380 hvrt	280 900	Top 10 Latest Plugins	28 80 75 100 128 180 178	200 208 200 218 000 208 080 218 400 408 480 47 Cont ■ nation ■ to: ■ informational	5 500
na agus para an sa nu nu nu nu na 220. ana dinasar Unu laring a sanufu paras nu nginal andaing ar the terms part O				to 10 Latest Plugins Publication Date 1 2022-11-13 12:00:00 Eastern		Covet # redux	
repropriet and an overveen of the second sec				arma-resilicat Inf5344441atShee 0 Top 10 Latest Plugins	Plagin Namo 1 Freedoo 1 Grafana Plagin signature bysa	Covet # redux	
And the set of the set			•	serve-resolution prifold-lifetilities 0 Top 10 Latest Plugins Publication Date 1 2022-11-13 12:00-08 Eastern Standard Trior	■ orier ■ kgb Plage Name 1 FreeED : Grafens Flagin signature kge FreeED : gythm Execution with Decer	Court	
And the second s			3,600 3,800	Top 10 Latest Plugins Publication Date 1 2022-11-13 12:00-00 Eastern 2022-11-13 12:00-00 Eastern 2022-11-13 12:00-00 Eastern 2022-11-13 12:00-00 Eastern	Pugn Nanc 1 Frottill : Grafan Flagin signatur hys Frottill : Igrafan Flagin signatur hys Frottill : Igrafan Gats source and plagi	Cont resion for finitesteri a (eth888-028-11e1-ics)-icsbe272eci) sary Privileges (251e120-028-11e1-icsb-641e72e172eci) sary privileges (251e120-028-11e1-icsb-641e72e172eci) s row endpoints leaking authentication takes to save detination plaging	
And the set of the set			1,600 1,800	The Point State of Control State of	Puge Name 1 Preeding 1: Grafies Flagin signature hype Preeding 1: Grafies Execution with Unexec Preeding 1: Grafies Data sources and plagi (0071016-001-11-11-11-02-02100117204)	Correl restor for the biometrical is (etablish-0554-11ei-4cs0-4cs145573ard)) sary Privileges (Sofiel30-0584-11ei-6cs4-66145713110) is proy endpoints lesking suffectiontin taken to same destination plugine Isalaf(Sof-0594-11ei-6cs3-4cs1645273ard))	
An one part to an a constraint of the in- magnetic data and a grant of the in- engence data and a gran			1,600 3,800	The second	■ orier ■ by Pluge Name 1 Freetto : Gorfees Flagts signature bys Freetto : inythes Execution with Unexer Freetto : Gorfees Data source and plug (0171016-0216-1106-1020-0106127200) Freetto : Gorfees Data source exuertion	Correl exercise Correlation (Correlation (C	
And the set of the set			1400 1.800	The 74 Latest Physics         1           The 74 Latest Physics         1           Relation Date 1         1           Statistics Date 2         1	■ oran ■ by Pugn Name 1 FreeDD : Confers Plagin signature hope FreeDD : Confers Cate source and plagi (077/056-0236-104-1042-014217300) FreeDD : Confers Cate source endersite (077/056-0236-104-1042-014217300) FreeDD : Confers Darmare endersite FreeDD : Confers Darmare endersite FreeDD : Confers Normare endersite	Correl exercise Correlation (Correlation (C	
And the set of the set			1,400 3,400	Comparison of the second	Pugo Hamo 1     Pogo Hamo 2     Pogo Hamo 2     PrestD : Grafma Flogin signature hype     PrestD : Grafma Data source and allog     Correct :- Grafma Data source and allog     Correct :- Grafma Data source and allog     Correct :- Grafma Data source and allog     PrestD :- Grafma Data source and allog     PrestD :- Grafma Data source and allog	Con     C	
ere prote no en			2800 2,800	Comparison of the second	Person in program and an an an and an an an and an	Cont	

# 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

O

# **Vulnerability Center Dashboard**

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

O

# Drill-down tables

ashboards 🔻	Saved Search	nes 🔻 Sear												<b>Ler</b>	apie
ew Sear	ch										Sav	e As 🔻			Close
signature,   appendpi "signature plugin_id	dns_name as a pe [  inputlo ", dns_name a: as "Plugin ID	asset_name_d okup sc_vuln s "asset_nam ", port as Pe	etail   tabl _data_lookup e_detail"   ort, protoco	e plu where table l as f	ND data_source=Host   where las in_id, port, protocol, state, a last_found >= "0° AND last_fc plugin_id, port, protocol, sta Protocol, state as State, seven t_name_detail as "Asset Name",	severi ound <= ate, se rity as	ity, signature, solution, asset = "1668418869" AND (severity=", everity, signature, solution, a s Severity, signature as Signat	t_nam *")   asset	ne_detail, first_found   eval product="Tenabl t_name_detail, first_f	d, last_fou le.sc"   re found, last	nd, product, da name synopsis a _found, product	ata_sour as t]   ren	name	efore date time '	, Q
,867 results (12	2/31/69 7:00:00	0.000 PM to 11	/14/22 4:41:09	0.000 A	M) No Event Sampling -						Job 🕶 🛛 🕅	• •	» 👼	± ¶ Smart	Mode 🔻
ents Patter	ns Statisti	cs (6,867)	Visualization	1											
0 Per Page 🔻	Format	Preview •								< Prev	1 2 3	4	5 6	7 8	Next 3
ugin / ID \$ Port \$	Protocol ¢	State 🖌	Severity \$	,	Signature \$	,	Solution \$		Asset Name 🗘	/	First 🖌 Found 🗘		ast 🖌	Product *	Data Source
10494 44	5 TCP	open	high		The Internet Explorer installation on the remote ho is affected by multiple vulnerabilities.	st	Microsoft has released the following security updates to address this issue: -KB4230450 -KB42848256		dc1.dc.demo.io		1635412309	1635	412309	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 Secur- ity Center lookup field	Tenable Vulnerability Man- agement-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
-	ір	First Found	first_found
-	last_fixed	-	last_fixed
Last Found	last_found	Last Found	last_found

		Ø	
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_pub- lication_date
_	-	-	plugin_modi-

_		Ø		
				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 <u>Alert Actions Configuration</u> tab in the Tenable Configuration section to retrieve data.

# To configure saved actions:

Configure adaptive response actions when you create a correlation search.

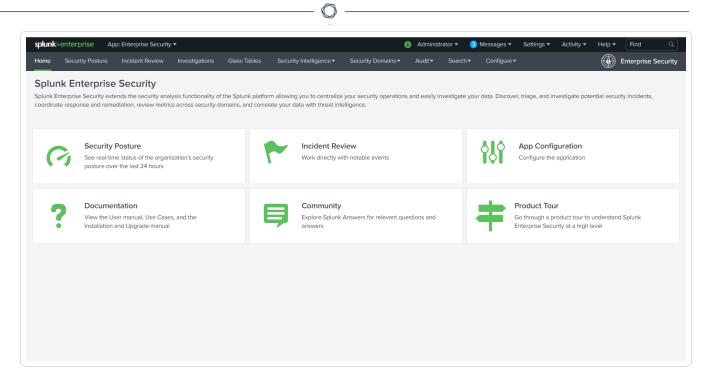
Note: When you run the search, the actions are retrieved automatically

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

Inputs Enterprise Security Extreme Search Search & Reporting Set up y Splunk Add-on for Unix and Lin Accoum  Tenable Add-On for Splunk Tenable App for Splunk			🔘 tenak
Search & Reporting           Set up y         Splunk Add-on for Unix and Lin           Account         ✓ Tenable Add-On for Splunk	9		
Set up y Splunk Add-on for Unix and Lin Account ✓ Tenable Add-On for Splunk			
Account	>		
Account	inux		
Tenable App for Splunk	ation		
	0		
Manage Apps	v		
Find More Apps	action responses.		

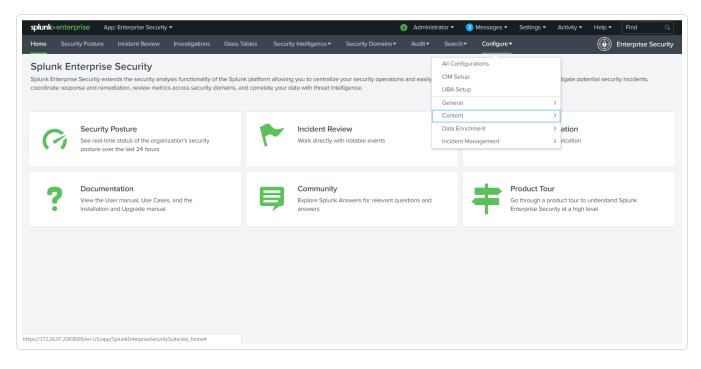
2. Select Enterprise Security.

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:

<b>plunk</b> >ente	арпзе Арр.	Enterprise Security					<ol> <li>Administra</li> </ol>		essages 👻 Settings	ACU	vity ▼ Help ▼	Find Q
lome Sec	urity Posture	Incident Review	Investigations	Glass Tables	Security Intelligence	<ul> <li>Securi</li> </ul>	ity Domains ▼ Audit ▼	Search -	Configure <b>▼</b>		ı 💮 ا	Enterprise Security
Content	Manageme	ent										ite New Content -
	•		ific to Splunk Enter	prise Security, such	as correlation searche	s, lookups, inv	estigations, key indicators,	, glass tables, ar	nd reports.		Crea	
Back to ES Co	onfiguration										Analytic Story	
											Correlation Sear	ch
003 Objects		tion <del>v</del>	Type:	All 🔻 App: All	▼ Status: All ▼	filter	Q,		<prev 1="" 2<="" td=""><td>3 4</td><td>Data Model</td><td></td></prev>	3 4	Data Model	
i Nan	ne 📩				Type ‡		App ¢	Ne	kt Scheduled Time	5	Key Indicator Se	arch
> Abn	ormally High Num	per of Endpoint Ch	anges By User		Correlation Search		DA-ESS-EndpointProtec	tion			Managed Looku	ρ
> Abn	ormally High Num	per of HTTP Metho	od Events By Src		Correlation Search		DA-ESS-NetworkProtect	tion			Panel	
> Acc	ess - Access App 1	racker - Lookup G	en		Saved Search		SA-AccessProtection	Ma	21, 2019 7:00 PM EDT		Saved Search	
> Acc	ess - Access Over	Time			Saved Search		DA-ESS-AccessProtection	on			Search-Driven Lo	ookup
> Acc	ess - Access Over	Time By Action			Saved Search		DA-ESS-AccessProtection	on			Sequence Temp	late
> Acc	ess - Access Over	Time By App			Saved Search		DA-ESS-AccessProtection	on				
> Acc	ess - Account Usag	ge For Expired Ide	ntities		Saved Search		DA-ESS-AccessProtection	on				
> Acc	ess - All Authentica	ation By Asset - Sv	vimlane		Swim Lane Search		DA-ESS-AccessProtection	on				
> Acc	ess - All Authentica	ation By Identity - S	Swimlane		Swim Lane Search		DA-ESS-AccessProtection	on				
> Acce	ess - Authenticatio	n Failures By Sour	ce - Context Gen		Saved Search		SA-AccessProtection	Ma	22, 2019 3:00 AM EDT			
> Acc	ess - Authenticatio	n Failures By Sour	ce Per Day - Conte	kt Gen	Saved Search		SA-AccessProtection	Ma	22, 2019 5:00 AM EDT			
> Acc	ess - Authenticatio	n Tracker - Lookup	Gen		Saved Search		SA-AccessProtection	Ma	21, 2019 7:05 PM EDT			
> Acc	ess - Authenticatio	n Volume Per Day	- Context Gen		Saved Search		SA-AccessProtection	Ma	22, 2019 4:00 AM EDT			
> Acc	ess - Default Acco	unt Usage Over Ti	me		Saved Search		DA-ESS-AccessProtection	on				
) Acc.	oss - Dofault Accou	unt Usage Over Ti	ma Bu Ann		Saved Search		DA-ESS-AccessProtection	00				

- 7. Select Correlation Search.
- 8. Enter information for the correlation search. Refer to the <u>Correlation Search</u> 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:

+ Add New Response Action	
Category All -	Search
Scan Machine for Tenable SC Start a scan for machine on Tenable SC server. Category: Add Active Scan   Task: update   Subj	ject: 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   Subj	iect: endpoint   Vendor: Tenable

n

- 11. Select the appropriate action for your search.
- 12. The field options for the selected option appear:

+ Add New Response Action	n 💌	
✓ ○ Request Scan for	Tenable IO	
Scan Name *		
Scan Name		
		Enter the Scan Name.
Host Name		
		Supports hostname and token both. e.g: 'ipvi
		\$result.dest\$
IP Address		
IF Addless		
		Supports ip and token both. e.g: 'some.example.com'/'21.5.2.1' or \$result.dest_
		\$result.dest\$

-

- 13. Enter the required information in the fields of your added response action.
- 14. Click Save.

A confirmation message appears.

15. Run a search.

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

# **Alert Action Configuration**

## To configure alert actions:

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

#### The **Configuration** page appears:

Configuration         et up your add on         ccount       Logging         Alert Actions Configuration         terms       filter         ccount Name *       Tenable Account Type ÷         dmin       tenable_securitycenter_credentials         dalab       tenable_securitycenter_credentials	plunk> App: Tenable Add-On for Splunk ~		Administrator 🗸 😝 Messages 🗸 Settings 🗸 Activity 🗸 Help 🗸 Find
et up your add on ten gging Alert Actions Configuration tens filter ccount Name • Tenable Account Type \$ Actions ccount Name • Tenable Account Type \$ Actions dmin tenable securitycenter, credentials Action ~ tenable, securitycenter, credentials Action ~	nputs Configuration Search		🔘 tenable
et up your add on ten gging Alert Actions Configuration tens filter ccount Name • Tenable Account Type \$ Actions ccount Name • Tenable Account Type \$ Actions dmin tenable securitycenter, credentials Action ~ tenable, securitycenter, credentials Action ~	Configuration		
Logging     Alert Actions Configuration       Items			
Items     filter     Add       ccount Name •     Tenable Account Type ÷     Accions       dmin     tenable_securitycenter_credentials     Accion >       Id_lab     tenable_securitycenter_credentials     Action >	et up your adu-on		
Action     Tenable Account Type ÷     Actions       dmin     tenable_securitycenter_credentials     Action ~       id_lab     tenable_securitycenter_credentials     Action ~	ccount Logging Alert Actions Configuration		
dmin         tenable_securitycenter_credentials         Action ~           id_lab         tenable_securitycenter_credentials         Action ~	Items	filter	Add
ld_lab tenable_securitycenter_credentials Action >	ccount Name *	Tenable Account Type 💠	Actions
	dmin	tenable_securitycenter_credentials	Action ~
eve_tio tenable_io Action >	ld_lab	tenable_securitycenter_credentials	Action ~
	teve_tio	tenable_io	Action ~
	leve_uo	tenable_lo	Action V

 $\bigcirc$ 

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:

Ø

- <u>Customized Actions</u>
- 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.

Ø

## **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:nnm: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 pidd=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 <u>Tenable Plugin for</u> 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.

odate Account			
Please enter valid Address, SC Acc certificate.	ess key and SC Secret key or configure valid proxy s	settings or verify SSL	
Account Name	scanman		
	Enter a unique name for this account.		
Tenable Account Type	Tenable.sc API Keys	· ×	
	Select the App for Tenable		
Address	sc.integrations.lab		
	Enter the FQDN or IP of your server for this account.		
Verify SSL Certificate	$\checkmark$		
	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.		
Proxy Enable			
	Check to enable the proxy.		

- You need to install the CA for the Splunk integration to trust. For more information, see <u>Configure Tenable Certificates</u>.
- 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.

O

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**

 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.

 $\bigcirc$ 

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

O

#### **Tenable Vulnerability Management**

Source	Sourcetype	Description
tenable_io:// <data input<br="">name&gt;</data>	tenable:io:vuln	This collects all host vulnerability data.
tenable_io:// <data input<br="">name&gt;</data>	tenable:io:assets	This collects all host asset data.
tenable_io:// <data input<br="">name&gt;</data>	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.

O

## To create an input:

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

iputs				🔘 tenable
nage your data inputs				Create New Input 🗸
nputs Services : All 🗸		filter		
Name *	Interval 🗢	Index ¢	Status ¢	Actions
Tenable_io	3600	default	Enabled	Action ~
tenable_70	86400	default	Enabled	Action ~

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

A drop-down box appears:

Create New Input 🗸
Tenable.io
Tenable.sc Vulnerability
Tenable.sc Mobile

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.

O

\_\_\_\_\_

**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 Vul- nerability 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 Vul- nerability	Enable to collect host assets and host vul- nerabilities.	Yes; for at least one data source.

Ø –		
Start Time	The date and time to start collecting host data. If you leave this field blank, the integ- ration collects all his- torical 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 vul- nerabilities 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.	Yes
	<b>Note:</b> 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.	

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 col- lects all historical data.	No
	<b>Note:</b> Uses the YYYY-MM-DD hh:mm:ss format.	
Sync Plugin Details	If selected, the related tags in Tenable assets include plugin details.	Yes
Historical Fixed Vul- nerability	Allows the import of vulnerabilities fixed before the current day.	No
Query Name	A name for Tenable Security Center vul- nerability filter.	No
	<b>Note:</b> The interval must be query type <b>Vul-</b> <b>nerability Detail List</b> .	

- Ø -

\_\_\_\_\_

### **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 vul- nerability filter.	No
	<b>Note:</b> The interval must be query type - <b>Vul-</b> <b>nerability Detail List</b> .	

- 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.
- 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

e Product	Severity Alt X Hills Files				Export			
herabilites Found Today	58	Active Vulnerabilities Pound Today	442	First Vulnesskilless Found Today 1,016				
6,8	867	Active Vulmerabilities	,795	Field Valueshällikee				
na Sanita Yunada a mana ana ing agalana ana Sanita Sana, Janing a amaring agalana na Mari Mari Nasil a mana amaring agalana			2.4 holikoidaa bii 21 a aaang kaon mai Cabb targat tarabi waxoo taron San dado u holikoi San dado u holikoi San dado u holikoi					
with find the source of the second se	80 80 100 120 MO 180 Cavet	160 200 220 340 280 280	avergend20% averge	28 80 78 60 62 60 79 202 20 20 27 20 28 80 27 40 46 46 47 47 with an angle of the state of the	800			
in agus gucha ann ba annsanadhar cha 250. Ann Shanann Shuu, hachig a anns-fig uganta ann gghlad annatu, chig an tha nannais gun		NO 200 220 340 340 240	Top 10 Latest Plugins Publication Date 1 2022-11-13 12:20:30 Eastern	Ceurs				
na program and a constraint of the interaction of t		16 20 22 24 26 26	200 Control Later Plugins Publication Date 2	Puge Name 1				
All the second s	Com		202 Top 10 Later Puper	Image: State in the s				
spectra and an accession in an accession in an accession in an accession in a sector of the sector o			202 To Distance Days of the second se	Puge Name 1       PrestD : Goffee Plags signature byses (estB000-200-11e6-tool-4c1be0172eef)       PrestD : Goffee Data source and plags providents leaking acthentication takens to asse destination plags.       (MSTM14-200-11e6-tool-4c1be0172eef)       PrestD : Goffee Data source and plags providents leaking acthentication takens to asse destination plags.       (MSTM14-200-11e6-tool-4c1be0172eef)				
spectra and an accession in an accession in an accession in an accession in a sector of the sector o	Cover		202 To be determined on the second of the	Pugen Name 1         PrestD 1: Soffen Data zores and allging provy endoloits ledding totalettime interest to some destination plaging.         PrestD 1: Soffen Data zores and allging provy endoloits ledding totalettime interest to some destination plaging.         PrestD 1: Soffen Data zores and allging provy endoloits ledding totalettime interest to some destination plaging.         PrestD 1: Soffen Data zores and allging provy endoloits ledding totalettime interest to some destination plaging.         PrestD 1: Soffen Data zores and allging provy endoloits ledding totalettime interest to some destination plaging.         PrestD 1: Soffen Data zores and allging provy endoloits ledding totalettime interest to some destination plaging.         PrestD 1: Soffen Data zores and allging provy endoloits ledding totalettime interest to some destination plaging.         PrestD 1: Soffen Data zores and allging provy endoloits ledding totalettime interest to some destination plaging.         PrestD 1: Soffen Data zores and allging provy endoloits ledding totalettime interest to some destination plaging.         PrestD 1: Soffen Data zores and allging provy endoloits ledding totalettime interest to some destination plaging.         PrestD 1: Soffen Data zores and allging provy endoloits ledding totalettime interest totalettime.         PrestD 1: Soffen Data zores and allging totalettime.         PrestD 2: Soffen Data zores and allging totalettime.         PrestD 1: Soffen Data zores and allging totalettime.         PrestD 1: Soffen Data zores and allging totalettim				
All the second s	Cover		323         Topological and the second and the se	Image: Name 2         PrestD 1: Soffwa Flagin signature hyses (set8000-220-11e1-toc)-cc1eb1723ec1)         PrestD 2: Soffwa Data source and plagin proxy endpoints leaking anthenionism takes to sum destination plagins (SMI0125-028-11e1-toc)-cc1eb1723ec1)         PrestD 1: Soffwa Data source and plagin proxy endpoints leaking anthenionism takes to sum destination plagins (SMI0125-028-11e1-toc)-cc1eb1723ec1)         PrestD 1: Soffwa Data source and plagin proxy endpoints leaking anthenionism takes to sum destination plagins (SMI0125-028-11e1-toc)-cc1eb1723ec1)         PrestD 1: Soffwa Data source and plagin proxy endpoints leaking anthenionism takes to sum destination plagins (SMI0125-028-11e1-toc)-cc1eb1723ec1)         PrestD 1: Soffwa Data source and plagin proxy endpoints leaking anthenionism takes to sum destination plagins (SMI0125-028-11e1-toc)-toc1eb1723ec1)         PrestD 1: Soffwa Data source and plagin group endpoints leaking anthenionism takes to sum destination plagins (SMI0125-028-11e1-toc)-toc1eb1723ec1)         PrestD 1: Soffwa Data source and plagin group endpoints leaking total-toc)-toc1eb1723ec1)         PrestD 1: Soffwa Data source and plagin group endpoints leaking total-toc)-toc1eb1723ec1)         PrestD 1: Soffwa Data source and plagin group endpoints leaking total-toc)-toc1eb1723ec1)         PrestD 1: Soffwa Data source and plagin group endpoints leaking total-toc)-toc1eb1723ec1)         PrestD 1: Soffwa Data source and plagin group endpoints leaking total-toc)-toc1eb17232ec1)				
All the second s	Cover		323         Topological and the second and the se	Image: Source of the state				
Ange and a man accurate in the second se	Cover		323         Topological States         Topological States <td>Prettio       Configure       Configure</td> <td></td>	Prettio       Configure				
approve the second of the seco	Cover		323         Part Distant Page           744         Part Distant Page           745         Page	Image: Source of the state				

# 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

O

# **Vulnerability Center Dashboard**

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

O

# Drill-down tables

														COL	
ew Searc	h										Save	e As 🔻			Close
signature, o   appendpip "signature" plugin_id a last_found a	ins_name as a e [  inputloo , dns_name as s "Plugin ID" as "Last Foun	sset_name_de kup sc_vuln_ "asset_name , port as Po d", product	etail   tabl data_lookup e_detail"   ort, protoco as Product,	table asse	ND data_source=Host   where lat gin_id, port, protocol, state, e last_found >= "0" AND last_fc plugin_id, port, protocol, stat Protocol, state as State, seven t_name_detail as "Asset Name",	sever: ound < ate, se rity as	ity, signature, solution, asse = "1668418869" AND (severity=" everity, signature, solution, s Severity, signature as Signa	et_na "*") asse	ame_detail, first_foun   eval product="Tenab et_name_detail, first_	nd, last_four ple.sc"   ren found, last	nd, product, dam name synopsis as _found, product und as "First Fo	ta_source s ]   rename pund",		date time	
ents Pattern			Visualizatior		AM) No Event Sampling 🔻						Job 🔻 II	*	0 ¥	Smart	Mode 🔻
) Per Page 🔻	Format	Preview •								< Prev	1 2 3	4 5	6 7	8	Next
ugin /	Protocol ¢	State 🖌	Severity \$	,	Signature 🕈	7	Solution \$	,	Asset Name ¢	/	First 🖌 Found 🗘	Last Found		duct •	Data Source ¢
ID ¢ Port ¢		open	high		The Internet Explorer		Microsoft has released the following security updates t		dc1.dc.demo.io		1635412309	16354123	09 Ten	able.io	Host

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

Tenable Security Center drill-down field	Tenable Secur- ity Center lookup field	Tenable Vulnerability Man- agement-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
-	ір	First Found	first_found
-	last_fixed	-	last_fixed
Last Found	last_found	Last Found	last_found

Ø				
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_pub- lication_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:nnm: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 pidd=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 <u>Tenable Plugin for</u> 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.

odate Account			
Please enter valid Address, SC Acc certificate.	ess key and SC Secret key or configure valid proxy s	settings or verify SSL	
Account Name	scanman		
	Enter a unique name for this account.		
Tenable Account Type	Tenable.sc API Keys	· ×	
	Select the App for Tenable		
Address	sc.integrations.lab		
	Enter the FQDN or IP of your server for this account.		
Verify SSL Certificate	$\checkmark$		
	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.		
Proxy Enable			
	Check to enable the proxy.		

- You need to install the CA for the Splunk integration to trust. For more information, see <u>Configure Tenable Certificates</u>.
- 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.

O

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**

 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.

 $\bigcirc$ 

 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.