

OT Network Security Monitoring Add-on Module for Splunk

Installation/User Guide



Version 1.1 (February 19, 2021)

www.forescout.com

This document provides an overview and installation instructions applicable for version 1.1.0 of the OT Network Security Monitoring Alert Monitoring Add-on Module for Splunk.

Copyright ©2009-2021 Forescout Technologies, Inc. All rights reserved. No portion may be copied without express written consent.

Forescout Technologies B.V., Eindhoven, The Netherlands
Forescout Technologies, Inc., San Jose, CA, United States

Website: <https://www.forescout.com>
Email: ot@forescout.com

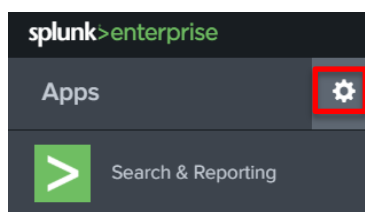
This document is distributed without any warranty.

Table of Contents

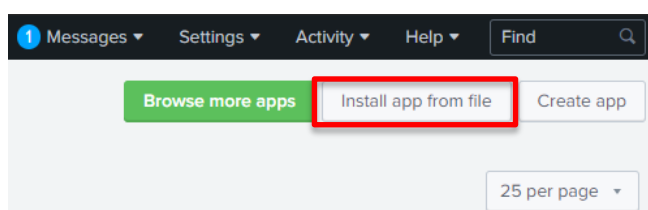
1. Installing OT Network Security Monitoring Add-on Module	4
2. Configuring OT Network Security Monitoring Add-on Module.....	6
3. Configuring OT NSM Command Center Appliance.....	12
3.1. Alert Forwarding	12
3.2. Network Log Forwarding	15
3.3. User Activity Log Forwarding	18
3.4. Health Status Log Forwarding	21
4. OT Network Security Monitoring Add-on Dashboards	24
4.1. Security Dashboard	24
Interval Time Picker	24
Command Center Picker.....	24
Alerts by Sensor Name.....	25
Alerts by L7 Protocol.....	25
ITL Alerts by Category	25
Alerts by Severity	25
Alerts by Event Type	25
Recent OT Network Security Monitoring Alerts.....	25
Alert Types by Source IP	25
Alert Types by IP	25
Alerts by Sensor Name by Protocol	25
ITL Alerts (24h/1h).....	25
DNS Queries – Top 15	25
DNS Queries – Fewest 10.....	25
Resolved DNS Queries – Top 10	25
Resolved DNS Queries – Fewest 10	25
Authentication Success.....	26
Authentication Failures	26
Authentication Details.....	26
SSL Certificates Requested.....	26
File Activity	26
4.2. Asset Inventory Dashboard.....	27
Interval Time Picker	28
Command Center Picker.....	28
Assets – Added to Inventory	28
Assets with Modules – Added to Inventory.....	28
Failed Connections.....	28
TELNET Protocol Used	28
DHCP Protocol Used.....	28
Ghost Nodes.....	28
Links – Last Seen 20.....	28
4.3. Administrative Dashboard	29
Interval Time Picker	29
Command Center Picker.....	29
Failed Logins.....	29
Health Changes.....	29
User Activity	29
Connect/Disconnect Changes	29
5. OT Network Security Monitoring CIM integration	30
6. OT NSM Add-on Compatibility	30
Compatibility with Splunk.....	30
Compatibility with CIM	30
Compatibility with Platforms.....	30

1. Installing OT Network Security Monitoring Add-on Module

From the Splunk web interface homepage menu on the left-hand side, click the cogwheel “Settings” button. You will navigate to a new page with installed Splunk applications and add-ons.

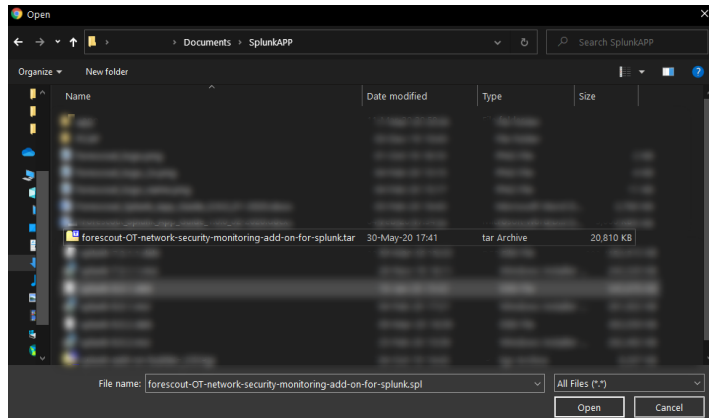


On the right-hand side, click “Install app from a file”.

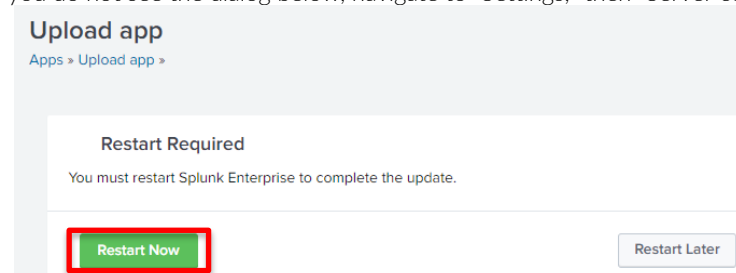


You will be forwarded to the “Upload an app” page. Click “Choose File.”

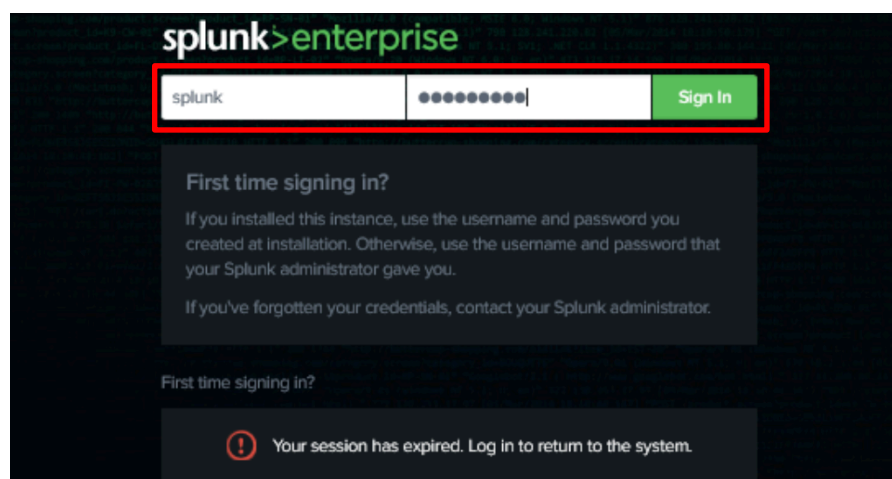
Select **.spl** (or **.tgz**) file that contains the OT Network Security Monitoring solution.



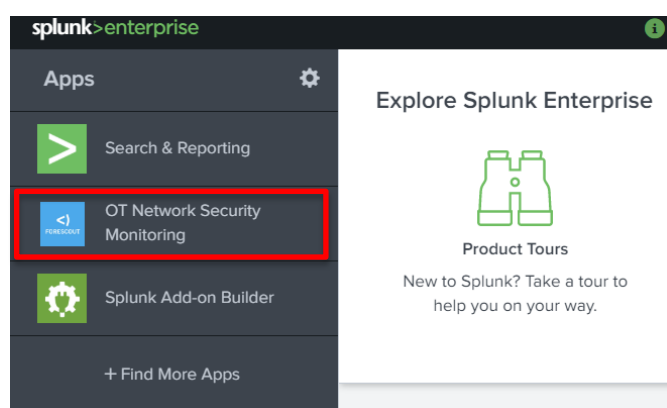
Click “Open,” then “Upload” to complete the installation. After the process completes successfully, restart Splunk. If you do not see the dialog below, navigate to “Settings,” then “Server controls,” then choose “Restart Now.”



Refresh the browser and log in to Splunk.

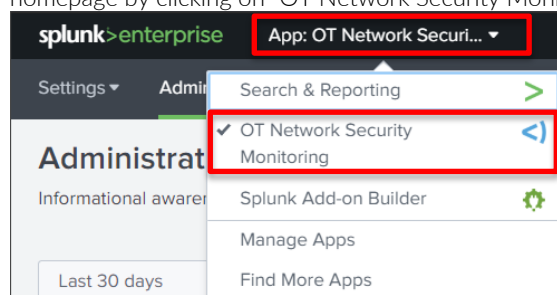


The OT Network Security Monitoring package is now available in the Splunk Apps Menu.

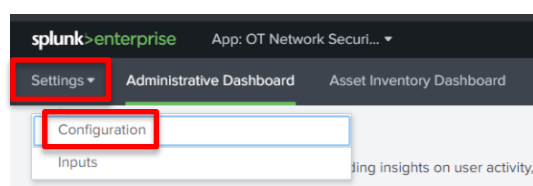


2. Configuring OT Network Security Monitoring Add-on Module

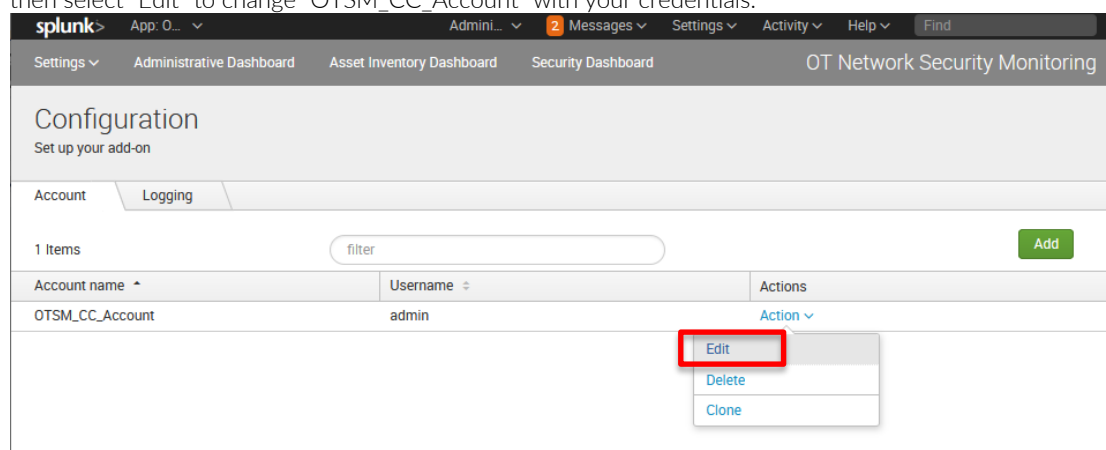
Before using the add-on, it must be configured. Navigate to OT Network Security Monitoring Alert Monitoring homepage by clicking on “OT Network Security Monitoring Alert Monitoring” in the Splunk apps drop-down menu.



In the app homepage, you will see a tab bar menu. Click the “Settings” drop-down and go to “Configuration.”

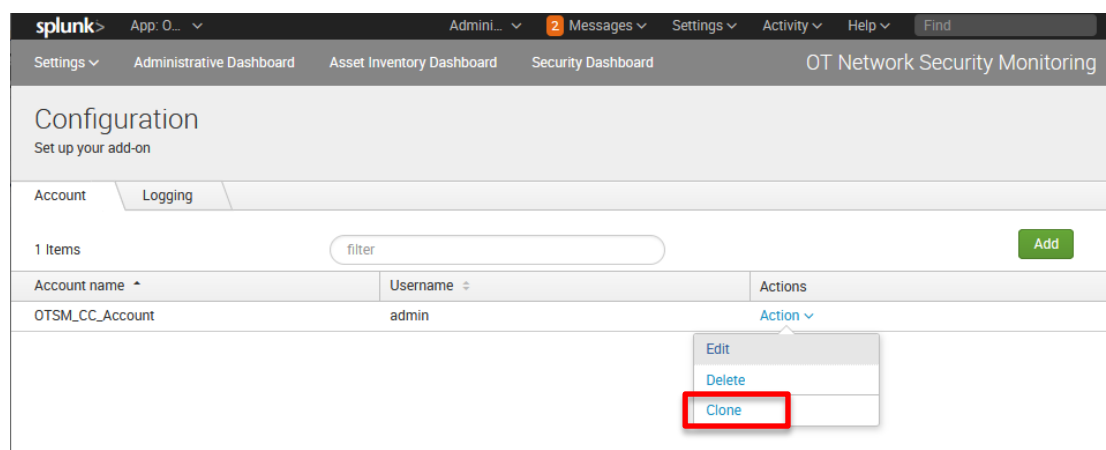


In the “Configuration” page, you will see a tab page control. In the “Account” tab, click on “Action” drop-down menu, then select “Edit” to change “OTSM_CC_Account” with your credentials.



Enter your Command Center server credentials, then click “Update” to save your settings.

To connect to more than one Command Center, you need to add an account for each CC. On the “OTSM_CC_Account” row, click on “Action,” and then click on “Clone”.



Enter an account name, the username and the password. Then, click on “Save”.

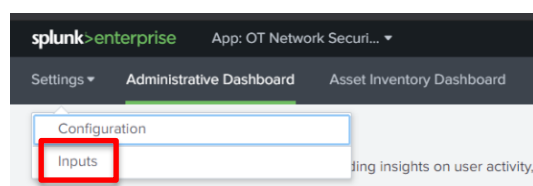
Account name *
Enter a unique name for this account.

Username *
Enter the username for this account.

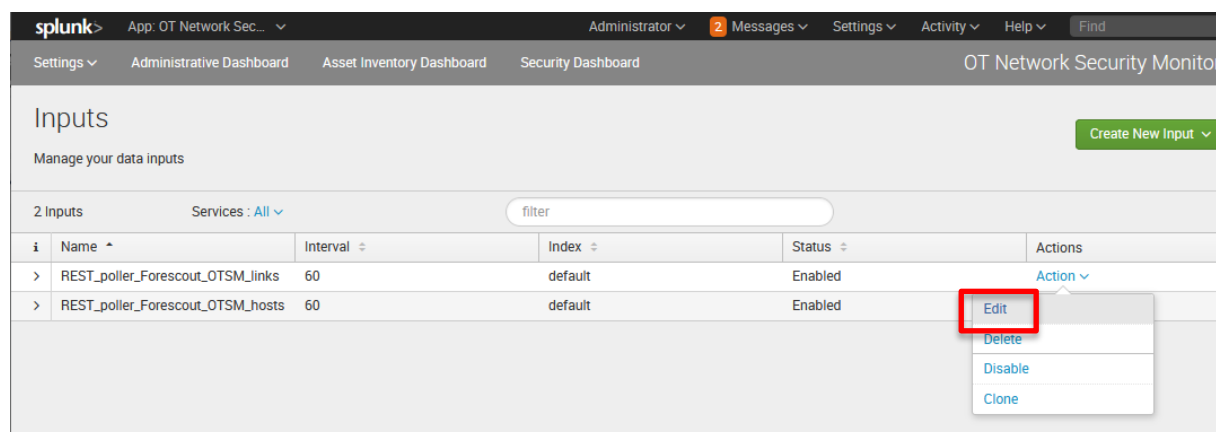
Password *
Enter the password for this account.

Repeat the last two steps for each Command Center installation that you wish to configure.

Next, click the “Settings” drop-down and go to “Inputs.”



On the “Inputs” page, you will see two pre-defined inputs. In the input “REST_poller_Forecout_OTSM_links,” click on the “Action” drop-down menu, then click on “Edit” to specify the Command Center hostname/IP.



Enter the CC Server hostname/IP and click “Save.”

Name *
Enter a unique name for the data input

Interval *
Time interval of input in seconds.

Index *

Global Account *

OTSM CC Server

Repeat the last two steps for the “REST_poller_Forescout_OTSM_hosts” input.

splunk> App: OT Network Sec... Administrator 2 Messages Settings Activity Help Find

Settings Administrative Dashboard Asset Inventory Dashboard Security Dashboard OT Network Security Monitoring

Inputs

Manage your data inputs

2 Inputs Services: All filter

i	Name	Interval	Index	Status	Actions
>	REST_poller_Forescout_OTSM_links	60	default	Enabled	Action
>	REST_poller_Forescout_OTSM_hosts	60	default	Enabled	Action

Edit
Delete
Disable
Clone

To connect to more than one Command Center, you will need to clone both inputs for each CC installation. In the input “REST_poller_Forescout_OTSM_links,” click on the “Action” drop-down menu, then click on “Clone.”

splunk> App: OT Network Sec... Administrator 2 Messages Settings Activity Help Find

Settings Administrative Dashboard Asset Inventory Dashboard Security Dashboard OT Network Security Monitoring

Inputs

Manage your data inputs

2 Inputs Services: All filter

i	Name	Interval	Index	Status	Actions
>	REST_poller_Forescout_OTSM_links	60	default	Enabled	Action
>	REST_poller_Forescout_OTSM_hosts	60	default	Enabled	Action

Edit
Delete
Disable
Clone

Enter a new Name for this input, select the Global account that contains the credentials for this CC and specify the hostname/IP.

Name *

Interval *

Index *

Global Account *

OTSM CC Server

Then, clone the “REST_poller_Forescout_OTSM_hosts” input and repeat the configuration process.

The screenshot shows the Splunk web interface for the 'Inputs' page. The table below represents the data shown in the interface:

i	Name	Interval	Index	Status	Actions
>	REST_poller_Forescout_OTSM_links	60	default	Enabled	Action
>	REST_poller_Forescout_OTSM_links_2	60	default	Enabled	Action
>	REST_poller_Forescout_OTSM_hosts	60	default	Enabled	Action

The 'Clone' button in the Actions column for the third input is highlighted with a red box.

You will need to clone the “Hosts” and “Links” inputs for each Command Center installation.

So far, the Add-on should be able to fetch data via REST calls to the Command Center API. If you have existing data in the CC, you can check if this data is loaded by Splunk via searching for `forescout:OTSM:REST:hosts links` or `sensors` sourcetypes. See `inputs.conf`.

To open a communication with CC to forward its logs, an input port must be setup. OT Network Security Monitoring Alert Monitoring uses an input port to listen for incoming syslog messages and assign the `forescout:OTSM:logs:*event_type*` sourcetype based on transforms defined in `transforms.conf`.

You can setup an input port by performing the following steps. Setup for TCP and UDP input ports is virtually identical on Splunk's side. The only difference is in the Command Center forwarding settings, which are covered in later chapters. For this example, we have used port 5143 via UDP. This port can be any value and must be the same value the CC server uses with its log forwarders to send data. The procedure for setting up log forwarders in CC is defined in the next chapter.

From Splunk's web interface, in the title bar menu, click “Settings” then “Data Inputs” to setup the input listener.

The screenshot shows the Splunk web interface with the 'Settings' menu open. The 'Data inputs' option under the 'DATA' section is highlighted with a red box.

From “UDP” in the “Local inputs” section, click on “Add new” link.

Local inputs
Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to [Forwarding and receiving](#).

Type	Inputs	Actions
Files & directories Index a local file or monitor an entire directory.	6	Add new
HTTP Event Collector Receive data over HTTP or HTTPS.	0	Add new
TCP Listen on a TCP port for incoming data, e.g. syslog.	0	Add new
UDP Listen on a UDP port for incoming data, e.g. syslog.	1	Add new
Scripts Run custom scripts to collect or generate more data.	4	Add new

Enter a new port number in the “Port” textbox, then click “Next” to save your changes.

Add Data Select Source Input Settings Review Done < Back **Next >**

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

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

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

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

Splunk Add-on Builder field extraction modular input
Splunk Add-on Builder field extraction modular input

REST - SilentDefense API - Hosts

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

☐ TCP ☒ UDP

Port ?
Example: 514

Source name override ?
host:port

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

Create the port input using the configuration values below, then click “Review” and verify values.

Add Data Select Source Input Settings Review Done < Back **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.

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](#)

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](#)

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](#)

Review

Input Type TCP Port
Port Number 5143
Source name override N/A
Restrict to Host N/A
Source Type fore scout:OTSM:logs:sink
App Context fore scout-OT-network:security-monitoring-add-on-for-splunk
Host (DNS entry of the remote server)
Index default

Select New

Select Source Type

forescout:
forescout:OTSM:logs:alert
forescout:OTSM:logs:health
forescout:OTSM:logs:network
forescout:OTSM:logs:sink
Global 'sink' object for 'all' output data generated by Forescout's OT Network Security Monitoring solution
forescout:OTSM:logs:useractivity
forescout:OTSM:REST:hosts
forescout:OTSM:REST:links

Index Default Create a new index

You are done configuring the Splunk Add-on! It should now have a working connection with the Command Center to gather host, link and sensor information via REST calls to CC. You can test this by replaying a PCAP on the machine (using tcpdump, not to be confused with PCAP Sensor in CC) where you have a running Sensor instance (and that sensor is associated with a CC) and see some of the information generated in one of the three dashboards from the OT Network Security Monitoring Alert Monitoring add-on or search for the REST source types (i.e. sourcetype="forescout:OTSM:REST:hosts").

To receive full information (alerts, network logs, etc.), CC needs to be setup to send these logs to Splunk, and this is detailed in the next chapter.

Important: The host information may change as eyeInspect analyzes more traffic in the network, thus, the add-on will continuously fetch more host data via the REST API. According to the interval specified in the data input configuration, the add-on fetches 1000 hosts per period. The hosts are fetched sequentially according to their ID number. When the last host is fetched by the add-on, the first 1000 hosts are fetched again in the next period, enabling Splunk to have the most recent host data. The dashboard and add-on queries will always show the recent host data, while the **forescout:OTSM:REST:hosts** source will also contain the old data.

Consider the impact of this continuous information logging on your Splunk instance and plan adequately the polling frequency and Splunk maintenance activities.

3. Configuring OT NSM Command Center Appliance

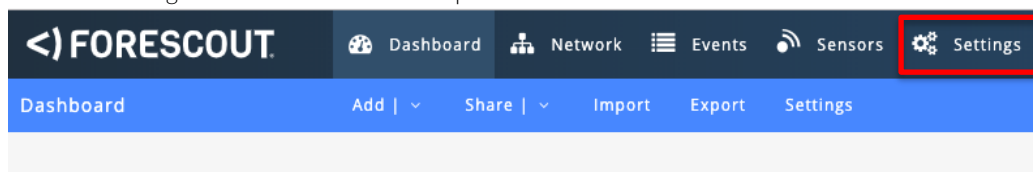
This information covers default log forwarding configuration for Splunk. Please refer to the Operational Guide for instructions on how to configure fields and/or other forwarding options of alerts, host and link information, and/or sensor health information.

To forward the logs from multiple Command Centers, you will need to repeat all the steps from this chapter (Configure Alert, Network Log, User Activity and Health Status Log Forwarding) in each CC installation.

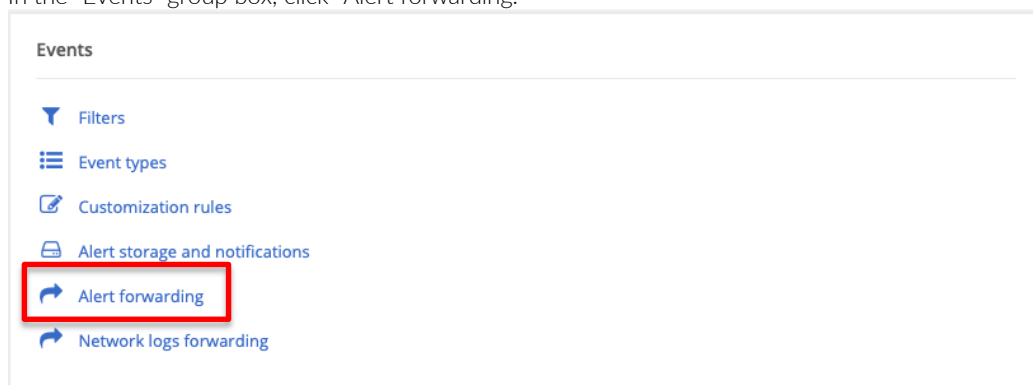
3.1. Alert Forwarding

NOTE: Before proceeding to setup alert forwarding, please ensure that there are *passive* sensors connected to CC. *Active* and *PCAP Replay* sensors **do not** generate these logs.

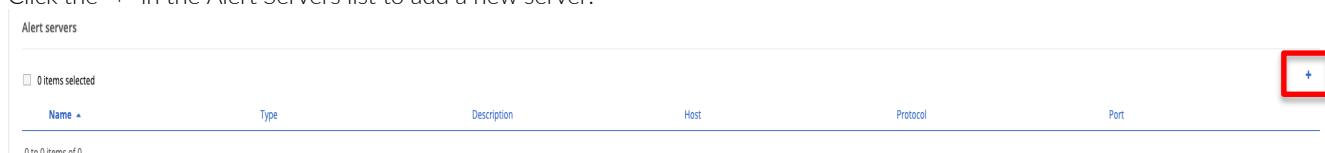
Click on “Settings” in Command Center’s top bar menu.



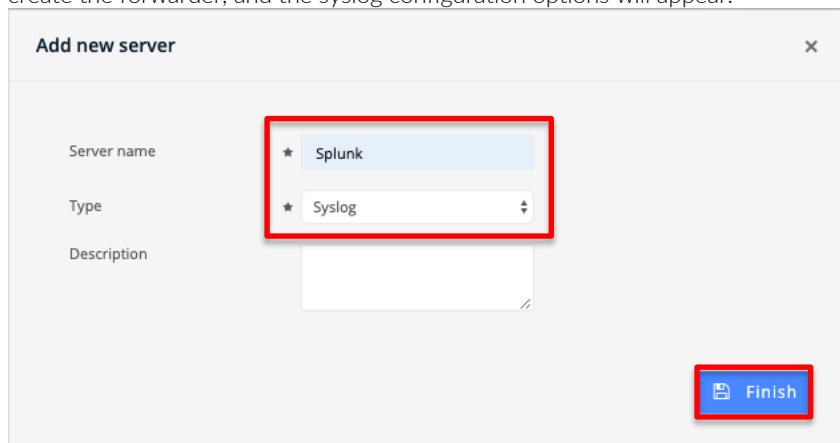
In the “Events” group box, click “Alert forwarding.”



Click the “+” in the Alert Servers list to add a new server.



Enter a name for this forwarder/server, and leave “Syslog” as Type. Enter a description (optional). Click “Finish” to create the forwarder, and the syslog configuration options will appear.



In the left side menu, select “Connectivity,” and the “Connectivity options” group box will appear on the right. Select “UDP” under “Transport protocol,” enter the IP address of your Splunk server and use 5143 for the port.

Forwarding settings

- Basic information
- Connectivity**
- Header
- Message
- Forwarding conditions

Connectivity options

Transport protocol ★ UDP

Remote host ★ 10.11.136.224

Remote port ★ 5143

NOTE: If you are using TCP as the transport protocol, please ensure that “Append line-feed” option is selected from the “Message transfer method” drop-down.

Connectivity options

Transport protocol ★ TCP

Remote host ★ 10.11.136.35

Remote port ★ 5143

Message transfer method ★ **Append line-feed**

Select “Header” from the menu, then verify that “Send message header” box is unchecked.

Syslog forwarder config... Back Finish

Forwarding settings

- Basic information
- Connectivity
- Header**
- Message
- Forwarding conditions

☐ Send message header

Select “Message” from the menu, then click the arrow next to “Use pre-set message” link on the title bar to open the drop-down menu and select “JSON (Splunk).”

Syslog forwarder config... Back Finish **Use pre-set message** ▼

CEF

LEEF

JSON (Splunk)

Forwarding settings

- Basic information
- Connectivity
- Header
- Message**
- Forwarding conditions

A dialog box will appear. Click “Yes” to replace the message.

Request for confirmation

⚠ Are you sure you want to replace the message text?

Yes No

The following content will appear in the Message dialog box.

Message

```
{
  "time": "{tsFormattedRFC5424}",
  "alertid": "{alertid}",
  "caseid": "{caseid}",
  "caseName": "{caseName}",
  "sensorName": "{sensorName}",
  "engineName": "{engineName}",
  "dstNetworkName": "{dstNetworkName}",
  "srcHostName": "{srcHostName}",
  "dstHostName": "{dstHostName}",
  "l2Proto": "{l2Proto}",
  "l3Proto": "{l3Proto}",
  "l4Proto": "{l4Proto}",
  "l7Proto": "{l7Proto}",
  "srcMac": "{srcMac}",
  "srcMacVendor": "{srcMacVendor}",
  "srcIp": "{srcIp}",
  "srcPort": "{srcPort}",
  "dstMac": "{dstMac}",
  "dstMacVendor": "{dstMacVendor}",
  "dstIp": "{dstIp}",
  "vlan": "{vlan}",
  "dstPort": "{dstPort}",
  "severity": "{severity}",
  "status": "{status}",
  "proflid": "{proflid}",
  "profModName": "{profModName}",
  "upDataLength": "{upDataLength}",
  "downDataLength": "{downDataLength}",
  "pcapSha1": "{pcapSha1}",
  "typeId": "{typeId}",
  "name": "{name}",
  "desc": "{desc}",
  "streamDir": "{streamDir}",
  "fieldPath": "{fieldPath}",
  "fieldVal": "{fieldVal}",
  "expFieldVals": "{expFieldVals}",
  "feaState": "{feaState}",
  "feaAlertCount": "{feaAlertCount}",
  "feaAlertDetailCount": "{feaAlertDetailCount}",
  "feaStartMillisec": "{feaStartMillisec}",
  "feaStartFormatted": "{feaStartFormatted}",
  "feaDurationSec": "{feaDurationSec}"
}
```

Leave the Message options with the default settings as shown.

Message options

Truncate large messages ☐

Maximum message size

Replace newlines in rendered tags with

Replace carriage returns in rendered tags with

Replace with

Replace with

Replace with

Select "Forwarding Conditions" from the menu and verify that "Always active" is checked.

Forwarding settings

Basic information

Connectivity

Header

Message

Forwarding conditions

Activation settings

Always active ☒

Click the "Finish" button to save the configuration settings.

Syslog configuration

Back

Finish

Forwarding settings

Basic information

Connectivity

Header

Message

Forwarding conditions

The server will now be listed under Alert Servers.

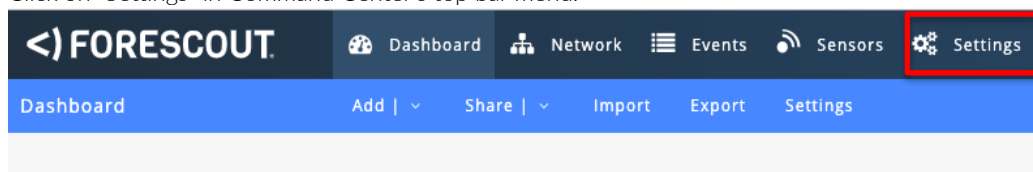
Alert servers					
0 items selected					
Name	Type	Description	Host	Protocol	Port
<input type="checkbox"/> Splunk	Syslog		172.16.30.66	UDP	5143

1 to 1 items of 1

3.2. Network Log Forwarding

NOTE: Before proceeding to setup network log forwarding, please ensure that there are *passive* sensors connected to CC. *Active* and *PCAP Replay* sensors **do not** generate these logs.

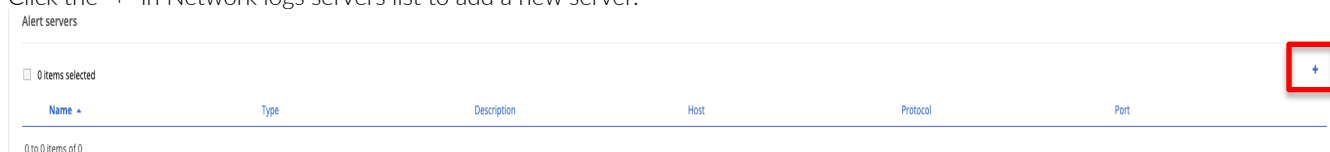
Click on “Settings” in Command Center’s top bar menu.



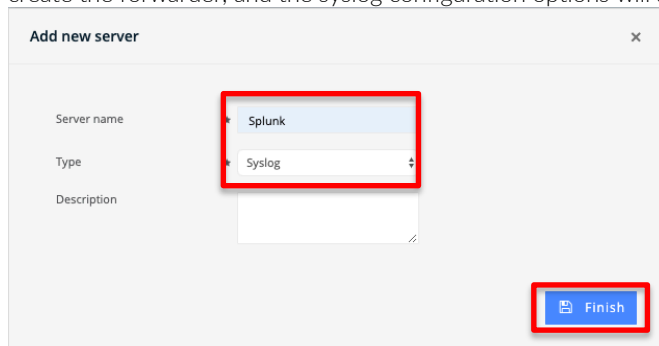
In the “Events” group box, click “Network logs forwarding.”



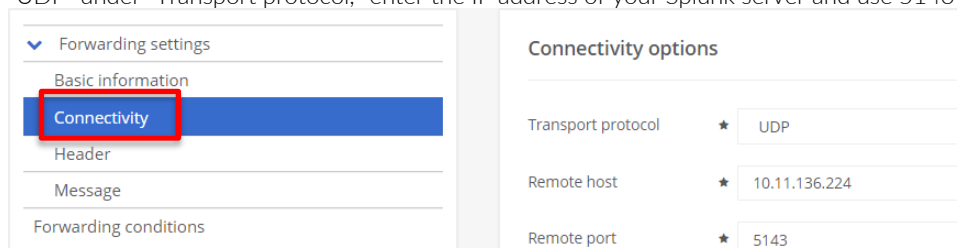
Click the “+” in Network logs servers list to add a new server.



Enter a name for this forwarder/server, and leave “Syslog” as Type. Enter a description (optional). Click “Finish” to create the forwarder, and the syslog configuration options will appear.



In the left side menu, select “Connectivity,” and the “Connectivity options” group box will appear on the right. Select “UDP” under “Transport protocol,” enter the IP address of your Splunk server and use 5143 for the port.



NOTE: If you are using TCP as the transport protocol, please ensure that “Append line-feed” option is selected from the “Message transfer method” drop-down.

Connectivity options

Transport protocol	★	TCP
Remote host	★	10.11.136.35
Remote port	★	5143
Message transfer method	★	Append line-feed

Select "Header" from the menu, then verify that "Send message header" box is unchecked.

Syslog forwarder config... Back Finish

Forwarding settings
Basic information
Connectivity
Header
Message
Forwarding conditions

☐ Send message header

Select "Message" from the menu, then click the arrow next to "User pre-set message" link on the title bar to open the drop-down menu and select "JSON (Splunk)."

Syslog forwarder config... Back Finish Use pre-set message ▾

Forwarding settings
Basic information
Connectivity
Header
Message
Forwarding conditions

CEP
LEEF
JSON (Splunk)

A dialog box will appear. Click "Yes" to replace the message.

Request for confirmation

Are you sure you want to replace the message text?

Yes No

The following content will appear in the Message dialog box.

Message

```
{
  "source_type": "networklog",
  "time": "{tsFormattedRFC5424}",
  "typeId": "{typeId}",
  "name": "{name}",
  "cat": "{cat}",
  "sensorName": "{sensorName}",
  "severity": "{severity}",
  "i2Proto": "{i2Proto}",
  "i3Proto": "{i3Proto}",
  "i4Proto": "{i4Proto}",
  "i7Proto": "{i7Proto}",
  "vlan": "{vlan}",
  "srcMac": "{srcMac}",
  "srcMacVendor": "{srcMacVendor}",
  "srcIp": "{srcIp}",
  "srcHostName": "{srcHostName}",
  "dstMac": "{dstMac}",
  "dstMacVendor": "{dstMacVendor}",
  "dstIp": "{dstIp}",
  "dstHostName": "{dstHostName}",
  "dstPort": "{dstPort}",
  "msgType": "{msgType}",
  "path": "{path}",
  "valStr": "{valStr}",
  "id": "{id}",
  "type": "{type}",
  "user": "{user}",
  "error": "{error}",
  "cust1": "{cust1}",
  "cust2": "{cust2}",
  "cnt": "{cnt}",
  "valNum": "{valNum}",
  "size": "{size}"
}
```

Leave the Message options with the default settings as shown.

Message options

Truncate large messages ☐

Maximum message size

Replace newlines in rendered tags with

Replace carriage returns in rendered tags with

Replace with

Replace with

Replace with

Select "Forwarding conditions" from the menu and verify that "Always active" is checked.

Forwarding settings

Basic information

Connectivity

Header

Message

Forwarding conditions

Activation settings

Always active ☒

Click the "Finish" button to save the configuration settings.

Syslog configuration

Back

Finish

Forwarding settings

Basic information

Connectivity

Header

Message

Forwarding conditions

The server will now be listed under Network log servers.

Alert servers

☐ 0 items selected

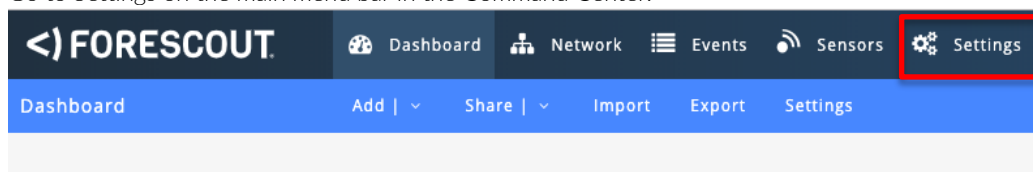
Name	Type	Description	Host	Protocol	Port
<input type="checkbox"/> Splunk	Syslog		172.16.30.66	UDP	5143

1 to 1 items of 1

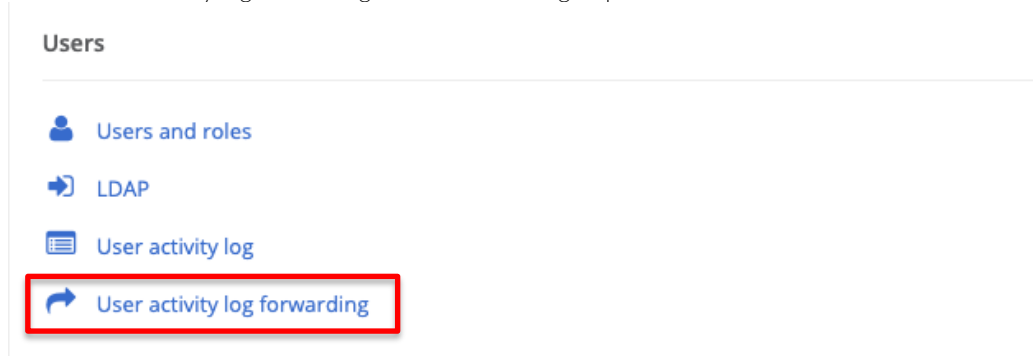
3.3. User Activity Log Forwarding

NOTE: Before proceeding to setup user activity log forwarding, please ensure that there are *passive* sensors connected to CC. *Active* and *PCAP Replay* sensors **do not** generate these logs.

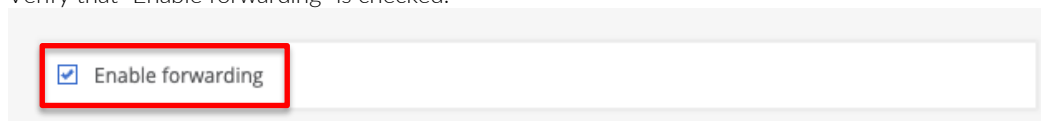
Go to Settings on the main menu bar in the Command Center.



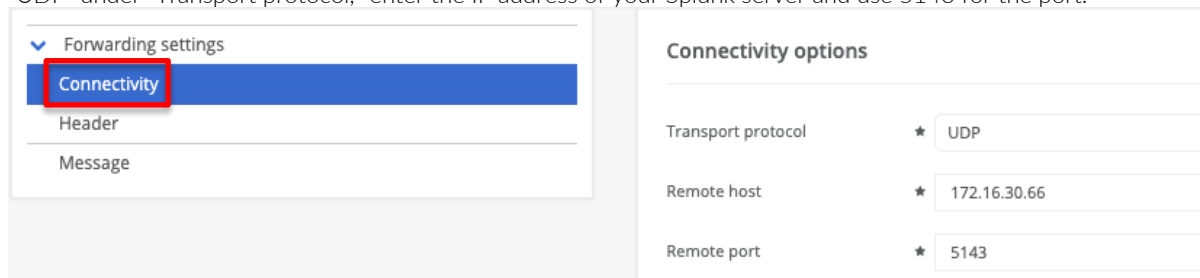
Select "User activity log forwarding" inside the Users group box.



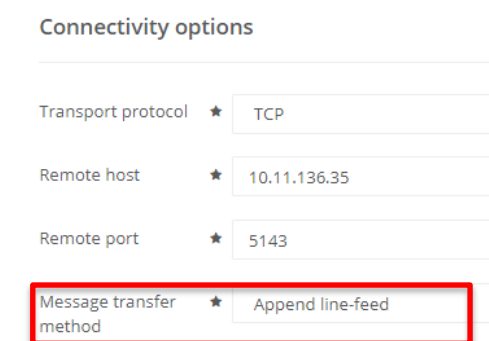
Verify that "Enable forwarding" is checked.



In the left side menu, select "Connectivity," and the "Connectivity options" group box will appear on the right. Select "UDP" under "Transport protocol," enter the IP address of your Splunk server and use 5143 for the port.



NOTE: If you are using TCP as the transport protocol, please ensure that "Append line-feed" option is selected from the "Message transfer method" drop-down.



Select "Header" from the menu, then verify that "Send message header" is unchecked.

User activity forwarding Back Finish

☒ Enable forwarding

▼ Forwarding settings

Connectivity

Header

Message

☐ Send message header

Select "Message" from the menu, then click the arrow next to "User pre-set message" link on the title bar to open the drop-down menu and select "JSON (Splunk)."

User activity forwarding Back Finish Use pre-set message ▼

☒ Enable forwarding

▼ Forwarding settings

Connectivity

Header

Message

CEF

LEEF

JSON (Splunk)

A dialog box will appear. Click "Yes" to replace the message.

Request for confirmation

⚠ Are you sure you want to replace the message text?

Yes No

The following content will appear in the Message dialog box.

Message

```
{ "time": "{timestampFormattedRFC5424}", "sdVersion": "{sdVersion}", "clientIP": "{clientIP}", "user": "{user}", "action": "{action}", "resource": "{resource}", "otherInfo": "{otherInfo}" }
```

Leave the Message options with the default settings as shown:

Message options

Truncate large messages	<input type="checkbox"/>		
Maximum message size	★ 480		
Replace newlines in rendered tags with	<input type="text" value="\n"/>		
Replace carriage returns in rendered tags with	<input type="text" value="\r"/>		
Replace	<input type="text"/>	with	<input type="text"/>
Replace	<input type="text"/>	with	<input type="text"/>
Replace	<input type="text"/>	with	<input type="text"/>

Click "Finish" to save the configuration settings.

User activity forwarding Back **Finish** Use pre-set message | ▾

☒ Enable forwarding

▼ Forwarding settings

Connectivity

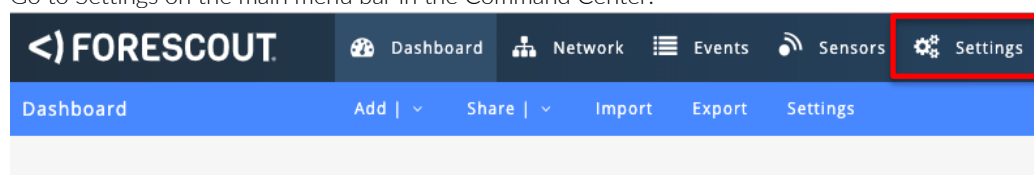
Header

Message

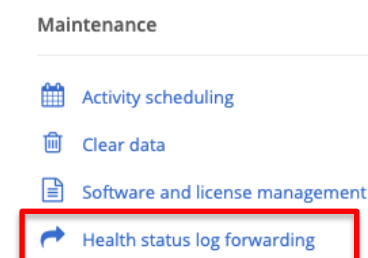
3.4. Health Status Log Forwarding

NOTE: Before proceeding to setup health status log forwarding, please ensure that there are *passive* sensors connected to CC. *Active* and *PCAP Replay* sensors **do not** generate these logs.

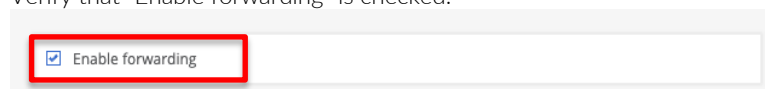
Go to Settings on the main menu bar in the Command Center.



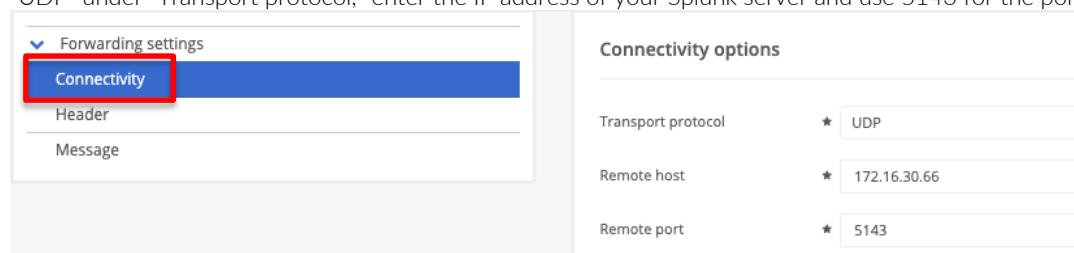
Under the Maintenance box, select “Health status log forwarding.”



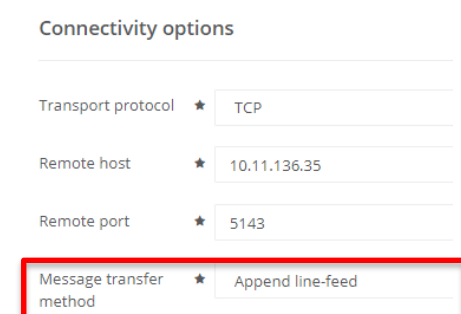
Verify that “Enable forwarding” is checked.



In the left side menu, select “Connectivity,” and the “Connectivity options” group box will appear on the right. Select “UDP” under “Transport protocol,” enter the IP address of your Splunk server and use 5143 for the port.



NOTE: If you are using TCP as the transport protocol, please ensure that the “Append line-feed” option is selected from the “Message transfer method” drop-down.



Select "Header" from the menu, then verify that "Send message header" is unchecked.

Health status forwarding Back Finish

☒ Enable forwarding

Forwarding settings

Connectivity

Header

Message

☐ Send message header

Select "Message" from the menu, then click the arrow next to "Use pre-set message" link on the title bar to open the drop-down menu and select "JSON (Splunk)."

Health status forwarding Back Finish Use pre-set message

☒ Enable forwarding

Forwarding settings

Connectivity

Header

Message

CEP

LEEF

JSON (Splunk)

Message

A dialog box will appear. Click "Yes" to replace the message.

Request for confirmation

⚠ Are you sure you want to replace the message text?

Yes No

The following content will appear in the Message dialog box.

Message

```
{ "time": "{timestampFormattedRFC5424}", "device": "{device}", "sdVersion": "{sdVersion}", "previousHealthStatus": "{previousHealthStatus}", "currentHealthStatus": "{currentHealthStatus}", "monitoredVariable": "{monitoredVariable}", "currentValue": "{currentValue}", "severity": "{currentHealthStatusNum}" }
```

Leave the Message options with the default settings as shown.

Message options

Truncate large messages

☐

Maximum message size

★ 480

Replace newlines in rendered tags with

Replace carriage returns in rendered tags with

Replace

with

Replace

with

Replace

with

Click "Finish button to save the configuration settings:

Health status forwarding

Back

Finish

Use pre-set message | ▾

☒ Enable forwarding

▼ Forwarding settings

Connectivity

Header

Message

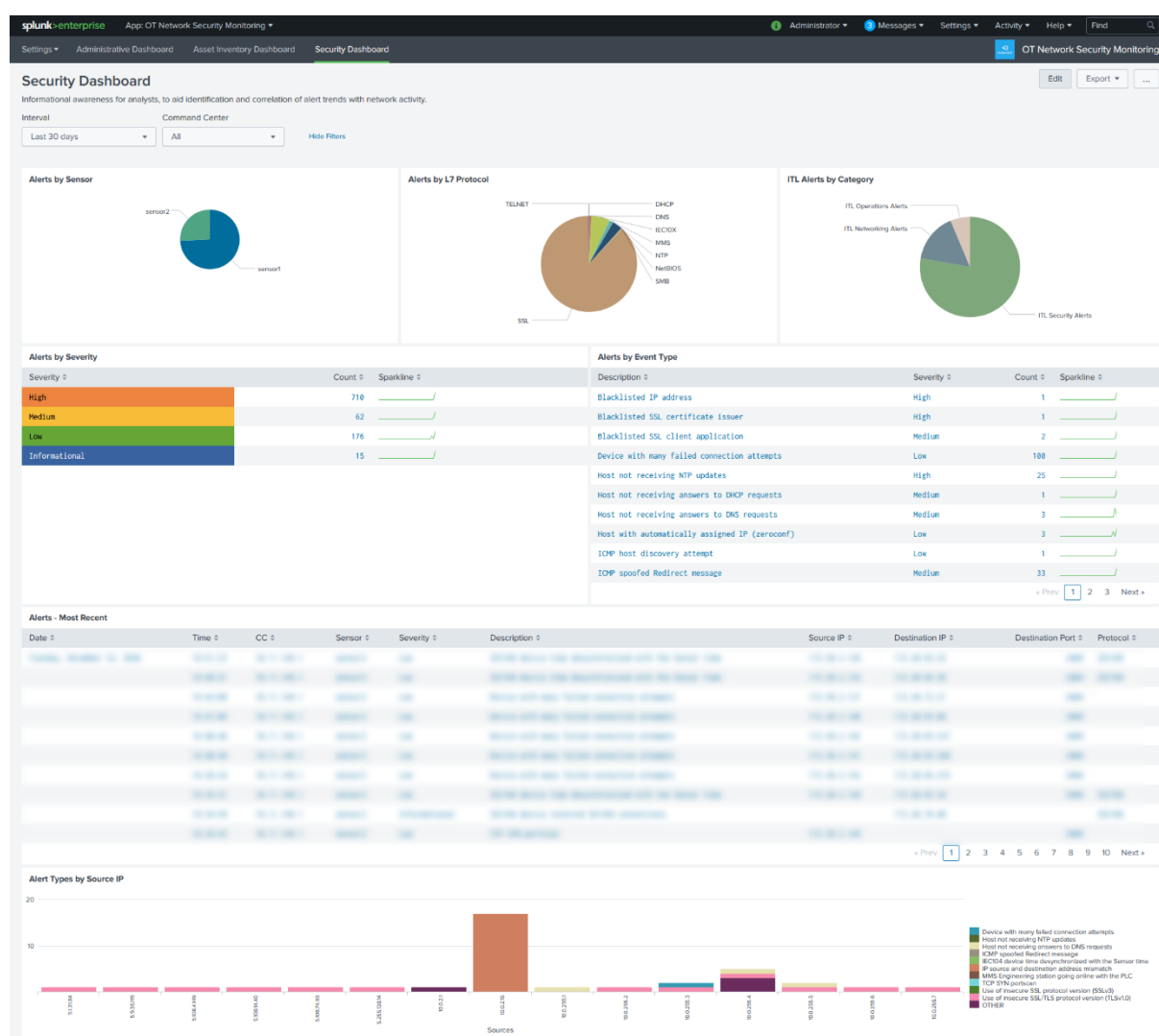
4. OT Network Security Monitoring Add-on Dashboards

The OT Network Security Monitoring dashboard app is a powerful tool that lets you visualize and identify trends within your monitored network. The dashboards allow you to drill down and analyze all the information sent by the OT Network Security Monitoring CC server. Each dashboard includes pre-configured widgets and panels to present information as described in the following pages, plus an interval time picker that can be used to modify the interval of interest on all the widgets, and a Command Center picker that allows you to visualize the information merged from all the CCs or from a single CC.

The App provides the following dashboards:

- [Security Dashboard](#)
- [Asset Inventory Dashboard](#)
- [Administrative Dashboard](#)

4.1. Security Dashboard



The Security Dashboard options and widgets

Interval Time Picker

[Drop-down menu] The shared time picker is used to control the time interval for *all* the widgets on the dashboard.

Command Center Picker

[Drop-down menu] Used to control from which CC the information on *all* dashboard's widgets is shown.

Alerts by Sensor Name

[Pie chart] Displays which sensor[s] have sent alerts. The displayed fields are Sensor Name and Count.

Alerts by L7 Protocol

[Pie chart] Displays which Layer 7 protocols have generated alerts. The displayed fields are Layer 7 Protocol and Count.

ITL Alerts by Category

[Pie chart] Displays the alerts generated by the OT Network Security Monitoring Industrial Threat Library (ITL) module. The ITL is split into three categories: Operations, Security and Networking. The displayed fields are ITL Category and Count.

Alerts by Severity

[Sparkline] Displays the number of alerts of each severity. OT Network Security Monitoring categorizes alerts as Informational, Low, Medium, High and Critical. The displayed fields are Severity, Count and Sparkline.

Alerts by Event Type

[Sparkline] Displays the number of alerts of each event type. The event types are provided by the OT Network Security Monitoring appliance. The displayed fields are Description, Severity, Count and Sparkline.

Recent OT Network Security Monitoring Alerts

[Table] Displays information about the most recent alerts that have been generated by OT Network Security Monitoring. The widget is sorted by time, with the most recent first, by default. The displayed fields are Time, CC, Sensor, Severity, Description, Source IP, Destination IP, Destination Port and Layer 7 Protocol.

Alert Types by Source IP

[Bar Chart] Displays the number of alerts associated with each source IP address. It is a stacked bar chart, and the colors within the bar correspond to the event type of the alerts. By default, only the 15 source IP addresses with the most alerts are included in the widget. The displayed fields are Source IP, Count and Event Type.

Alert Types by IP

[Bar Chart] Displays the number of alerts associated with each IP address (source and/or destination). It is a stacked bar chart, and the colors within the bar correspond to the event type of the alerts. By default, only the 15 IP addresses with the most alerts are included in the widget. The displayed fields are IP Address, Count and Event Type.

Alerts by Sensor Name by Protocol

[Bar Chart] Displays the number of alerts by each sensor. It is a stacked bar chart, and the colors within the bar correspond to the Layer 7 Protocol of the alerts. The displayed fields are Sensor Name, Count and L7 Protocol.

ITL Alerts (24h/1h)

[Count with Trend] Displays the count of ITL alerts by category in the previous 24 hours. It also has a trending arrow that shows whether the count has been increasing, decreasing or the same over the previous one hour. This widget does not use the shared time picker. The displayed fields are ITL Category and Count.

DNS Queries – Top 15

[Bar Chart] Displays the 15 most common DNS hostnames that have been queried. The displayed fields are DNS Query, Source IP, Destination IP and Count.

DNS Queries – Fewest 10

[Table] Displays the 10 least common DNS Queries seen on the network. The displayed fields are DNS Query and Count.

Resolved DNS Queries – Top 10

[Table] Displays the 10 DNS queries that have been resolved the most times. The displayed fields are Query/Response and Count.

Resolved DNS Queries – Fewest 10

[Table] Displays the 10 DNS queries that have been resolved the fewest times. The displayed fields are Query/Response and Count.

Authentication Success

[Bar Chart] Displays successful authentication attempts over cleartext protocols. It shows both the protocol and the username used for the authentication. The displayed fields are Date, Username, L7 Protocol and Count.

Authentication Failures

[Table] Displays authentication failures and the reason for the failure. The displayed fields are Time, Protocol, User, Authentication Error, Source IP and Destination IP.

Authentication Details

[Table] Displays both successful and failed authentication attempts that used cleartext protocols. The displayed fields are Time, CC, Source IP, Destination IP, Username, Protocol and Event (Success or Failure).

SSL Certificates Requested

[Table] Identifies SSL certificates used on the network. The displayed fields are Issuer, Validity, Expiration, Cipher Suite used, Source IP and Destination IP.

File Activity

[Table] Records the file activity happening on the network, such as file reads, writes or deletes. The displayed fields are Time, Source IP, Destination IP, Username, File Activity (delete, create, modify, etc.) and Filename.

4.2. Asset Inventory Dashboard

[illegible]

The Asset Inventory Dashboard options and widgets

Interval Time Picker

[Drop-down menu] The shared time picker is used to control the time interval for the widgets on the dashboard.

Command Center Picker

[Drop-down menu] Used to control from which CC the information on *all* dashboard's widgets is shown.

Assets – Added to Inventory

[Table] Displays assets that have been identified on the network. This widget does not utilize the shared time picker. The displayed fields are Time in Past, CC, IP, Mac Address(es), Vendor/Model, Firmware, Hardware, Serial, Labels, OS Version and First Seen.

Assets with Modules – Added to Inventory

[Table] Displays assets that have been identified on the network that have modules. This widget does not utilize the shared time picker. The displayed fields are Time in Past, CC, IP, MAC Address(es), Vendor/Model, Firmware, Hardware, First Seen and Modules.

Failed Connections

[Table] Displays failed connections seen within the network as reported by OT Network Security Monitoring. The displayed fields are Time, CC, Ports, Sensor, Source IP, Destination IP, Protocol and First Seen.

TELNET Protocol Used

[Table] Displays assets that have used the TELNET protocol. The displayed fields are Time, CC, Sensor, Source IP, Destination IP and First Seen.

DHCP Protocol Used

[Table] Displays assets that have used the DHCP Protocol. The displayed fields are Time, CC, Sensor, Source IP, Destination IP and First Seen.

Ghost Nodes

[Table] Displays ghost nodes (i.e., nodes receiving network packets or requests, but never responding) seen on the network. Ghost nodes are classified by OT Network Security Monitoring. The displayed fields are CC, IP Address, First Seen and Last Seen.

Links – Last Seen 20

[Table] Displays the last 20 communication links seen on the network. The displayed fields are CC, Source IP, Destination IP, Sensor, Protocol and Last Seen.

4.3. Administrative Dashboard

The screenshot displays the Splunk Administrative Dashboard for OT Network Security Monitoring. The dashboard includes a top navigation bar with links to Settings, Administrative Dashboard, Asset Inventory Dashboard, and Security Dashboard. Below the navigation bar, there are filters for Interval (All time) and Command Center (All). The dashboard is divided into four main sections:

- Failed Logins:** A table showing login attempts that failed. Columns include Date, Time, CC, User IP, Username, and Reason. Example data: Tuesday, December 21, 2016, 11:40:55, 19.11.195.26, 19.11.195.26, jrodriga, User account does not exist.
- User Activity:** A table showing user actions. Columns include Date, Time, CC, Client IP, User, Resource, Action, and Details. Example data: Tuesday, December 21, 2016, 11:40:55, 19.11.195.1, 19.11.195.26, jrodriga, System, Failed login, User account does not exist.
- Connect/Disconnect Changes:** A table showing sensor connection status changes. Columns include Date, Time, CC, Sensor, Current Status, Previous Status, and Value. Example data: Monday, December 21, 2016, 11:52:45, 19.11.195.1, sensor2, NORMAL, CRITICAL, connected.
- Health Changes:** A table showing health status changes for sensors. Columns include Date, Time, CC, Sensor, Health Area, Current Status, Previous Status, and Value. Example data: Monday, December 21, 2016, 11:52:45, 19.11.195.1, sensor2, sensor connection, NORMAL, CRITICAL, disconnected.

The Administrative Dashboard options and widgets

Interval Time Picker

[Drop-down menu] The shared time picker is used to control the time interval for *all* the widgets on the dashboard.

Command Center Picker

[Drop-down menu] Used to control from which CC the information on *all* dashboard's widgets is shown.

Failed Logins

[Table] Displays a list of failed OT Network Security Monitoring login attempts and the reason for the failure. The displayed fields are Time, CC, User IP, Username and Reason.

Health Changes

[Table] Displays a list of health changes for Command Center and Sensors. For example, it displays when sensors are at a critical memory usage level and when sensors connect or disconnect with a Command Center. The displayed fields are Time, CC, Sensor, Health Area, Current Status, Previous Status and Current Value.

User Activity

[Table] Shows activity being performed on OT Network Security Monitoring, such as when a user logs in or makes changes to sensor modules or profiles. The displayed fields are Time, CC, Client IP, User, Resource, Action and Details.

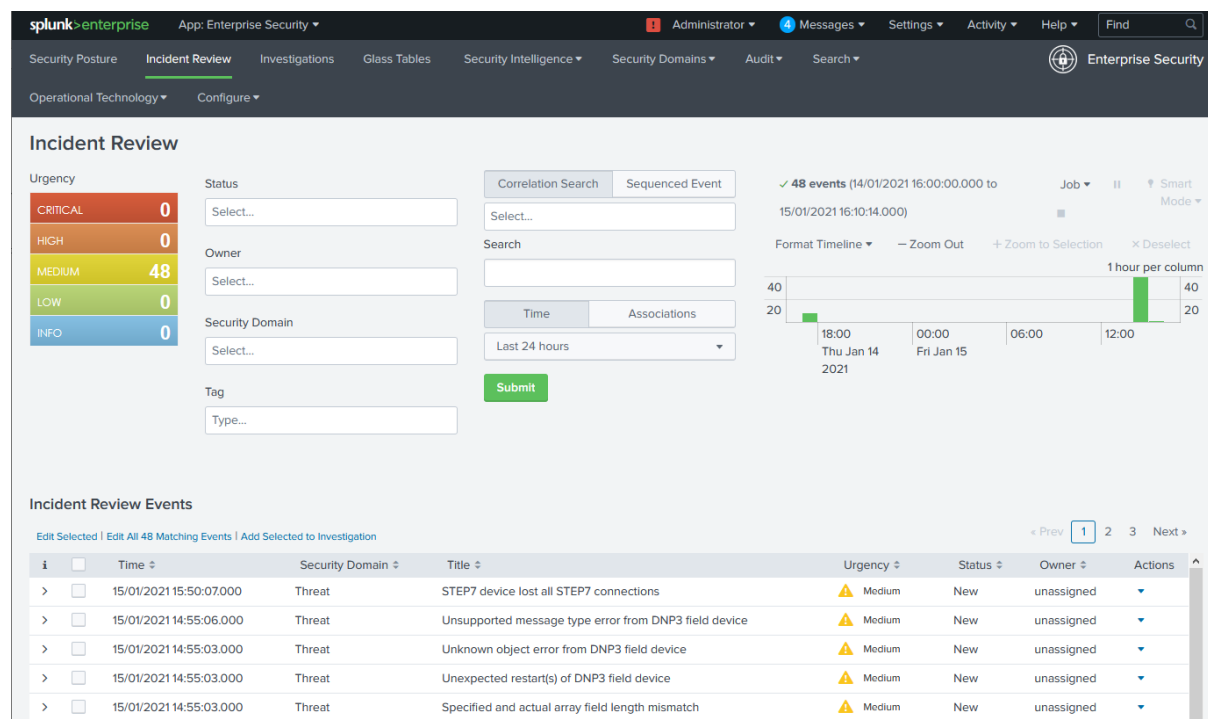
Connect/Disconnect Changes

[Table] Logs when Active Sensors connect or disconnect from a Command Center. The displayed fields are Time, CC, Sensor, Health Area, Current Status, Previous Status and Current Value.

5. OT Network Security Monitoring CIM integration

The Forescout OT Network Security Monitoring Add-on supports integration with the Splunk Common Information Model. The events collected by the OT-NSM Add-on are mapped to the preconfigured data models and can be visualized in compatible add-ons.

The OT Security Add-on for Splunk version 1.0.3 or higher is validated as compatible with the Forescout OT-NSM Add-on. Refer to the OT Security Add-on documentation, available on Splunk Docs for more information on how to configure the add-on and the integration.



The OT Security Add-on for Splunk - Incidents Review Dashboard

6. OT NSM Add-on Compatibility

Compatibility with Splunk

The OT NSM Add-on is compatible with the following Splunk versions: 8.0

Compatibility with CIM

The OT NSM Add-on is compatible with the following Splunk Common Information Model versions: 4.x

Compatibility with Platforms

The OT NSM Add-on is compatible with the following platforms: Windows, Linux.