



Tenable and Splunk Integration

August 17, 2016

(Revision 1)

Table of Contents

Introduction	3
Recommended Configurations	3
SecurityCenter + Splunk.....	3
SecurityCenter Continuous View™ + Splunk (SecurityCenter + LCE + PVS + Splunk).....	3
Optional Configuration.....	4
Passive Vulnerability Scanner Only (Standalone) + Splunk	4
SecurityCenter	4
Integration Requirements.....	4
Integration Configuration	5
Splunk Add-on for Tenable Configuration.....	5
Nessus	9
Integration Requirements.....	10
Integration Configuration	10
Splunk Add-on for Tenable Configuration.....	10
Passive Vulnerability Scanner	15
Integration Requirements.....	15
Integration Configuration	15
Tenable PVS Configuration.....	15
Splunk Configuration.....	17
Log Correlation Engine	21
Integration Requirements.....	21
Integration Configuration	21
Tenable LCE Splunk Client Configuration	21
Splunk Configuration.....	23
Tenable LCE Syslog Forwarding.....	26
About Tenable Network Security	28

Introduction

Tenable™ and Splunk have a history of collaboration and interaction between our enterprise security solutions. Many customers want Tenable vulnerability and continuous monitoring data shared with their Splunk environment.

This document describes how to deploy integrations between Tenable Nessus®, SecurityCenter™, Passive Vulnerability Scanner™ (PVS™), and Log Correlation Engine™ (LCE®) and Splunk solutions, specifically Splunk Enterprise, and covers multiple methods of integration; we have worked to provide flexibility to support many different configurations. Please email any comments and suggestions about this document or its instructions to support@tenable.com.

Tenable Solution	Integration Type	Owner	Description
SecurityCenter	Vulnerability Metrics	Splunk	Splunk receives vulnerability data collected by SecurityCenter
Nessus	Nessus Host Scans, Nessus Plugins	Splunk	Splunk receives vulnerability data collected by Nessus, Splunk collects Nessus plugin information from the Tenable Knowledgebase
PVS	Passive Syslog Collection	Tenable	Real-time vulnerability and event data is sent from PVS to Splunk via syslog
LCE	Syslog Forwarding (bi-directional)	Tenable	LCE server collects data from Splunk, or log and event data collected by a LCE Client is sent to Splunk

Recommended Configurations

SecurityCenter + Splunk

SecurityCenter API → Splunk Connector → Splunk DB

How it works: SecurityCenter collects vulnerability data. The Splunk connector then connects to the SecurityCenter API to extract the vulnerability data and insert it into the Splunk DB.

Why: Fast and easy export of your Tenable vulnerability data to Splunk allows your correlation of vulnerabilities with the events in the Splunk console.

SecurityCenter Continuous View™ + Splunk (SecurityCenter + LCE + PVS + Splunk)

SecurityCenter API → Splunk Connector → Splunk DB

Event Traffic (syslog) → LCE (forward) → Splunk DB (syslog)

How it works: SecurityCenter collects vulnerability data. The Splunk connector connects to the SecurityCenter API to extract vulnerability data and insert the data into the Splunk DB. By forwarding event traffic to LCE first, rich vulnerability and threat data can be correlated with all the SecurityCenter vulnerability sensor data.

Why: Fast and easy export of your Tenable vulnerability data to Splunk allows your correlation of vulnerabilities with the events in the Splunk console. Using LCE's Syslog Forwarding and Event Rules features, it can send all, or selected, logs to Splunk Enterprise for storage. This can result in a significant reduction in the cost of Splunk storage costs.

Optional Configuration

SecurityCenter API → Splunk Connector → Splunk DB

Event Traffic (syslog) → Splunk DB (forward) → LCE

How it works: SecurityCenter collects vulnerability data. The Splunk connector connects to the SecurityCenter API to extract the vulnerability data and insert it into the Splunk DB. The Tenable LCE Splunk Client forwards data that Splunk collects to the LCE server. Once the data reaches the LCE server, the data is reviewed and normalized so it can be queried in SecurityCenter.

Why: In addition to having Splunk collect events, the LCE Client for Splunk (available on the [Tenable Support Portal](#)) allows you to extract event data for correlation with all SecurityCenter vulnerability sensor data, allowing a better view of vulnerabilities and their impact from the SecurityCenter console. Check out the many SecurityCenter dashboards for some ideas of the pre-built event data that can be reported: <https://www.tenable.com/sc-dashboards>.

Passive Vulnerability Scanner Only (Standalone) + Splunk

PVS (syslog) → Splunk PVS Connector → Splunk DB

How it works: PVS collects vulnerability data. The Splunk PVS connector connects to PVS to extract the vulnerability data and insert it into the Splunk DB.

Why: PVS performs the completely passive collection of vulnerability data (via TAP/Mirror/SPAN). This data and device discovery provides tremendous insight into the applications and systems on your network, which is extremely important to incident response teams as deep knowledge about unmanaged systems are automatically imported to Splunk.

SecurityCenter

SecurityCenter consolidates and evaluates vulnerability data across an organization, prioritizing security risks and providing a clear view of the organization's security posture. With SecurityCenter's pre-built, highly customizable dashboards and reports, and the industry's only Assurance Report Cards (ARCs), users can visualize, measure, and analyze the effectiveness of their security program. The Splunk Add-on for Tenable allows Splunk users to collect SecurityCenter data, which is then indexed for further analysis.

This section assumes that the user has working knowledge of SecurityCenter and Splunk.

Integration Requirements

The following are required in order to integrate SecurityCenter with Splunk:

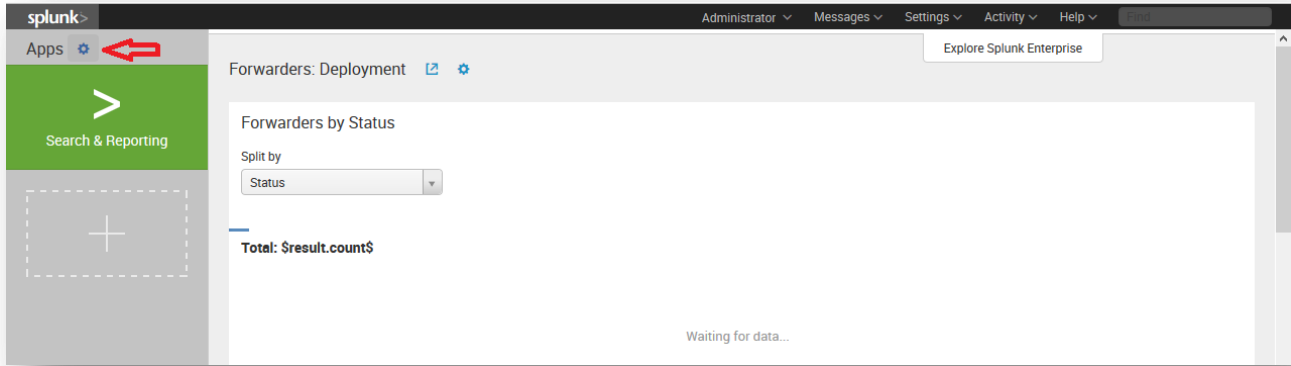
- SecurityCenter 5.3.1 or 5.3.2
- Splunk 6.x or higher

Integration Configuration

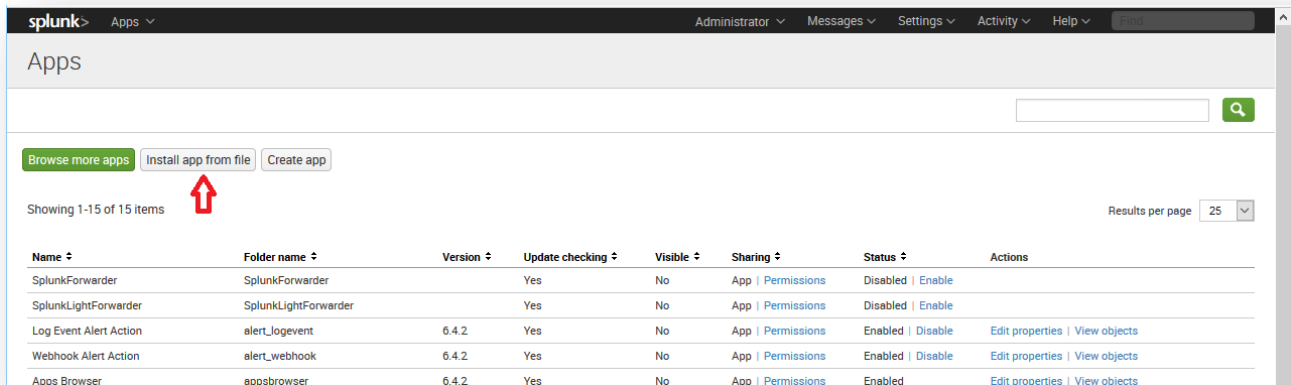
Splunk Add-on for Tenable Configuration

The Splunk Add-on for Tenable is available for download at <https://splunkbase.splunk.com/app/1710/> (login required).

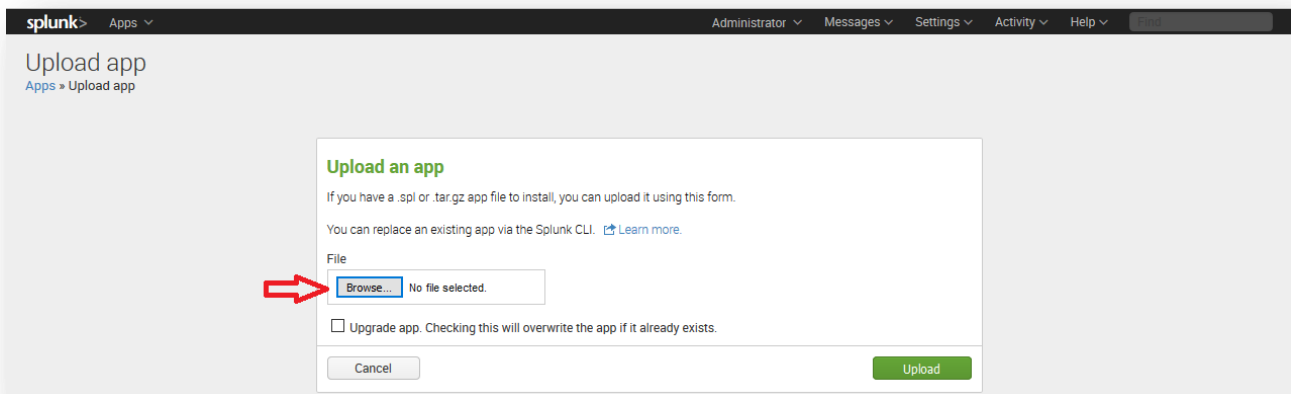
From Splunk, click the Manage Apps “gear” icon, located in the upper-left side of the screen.



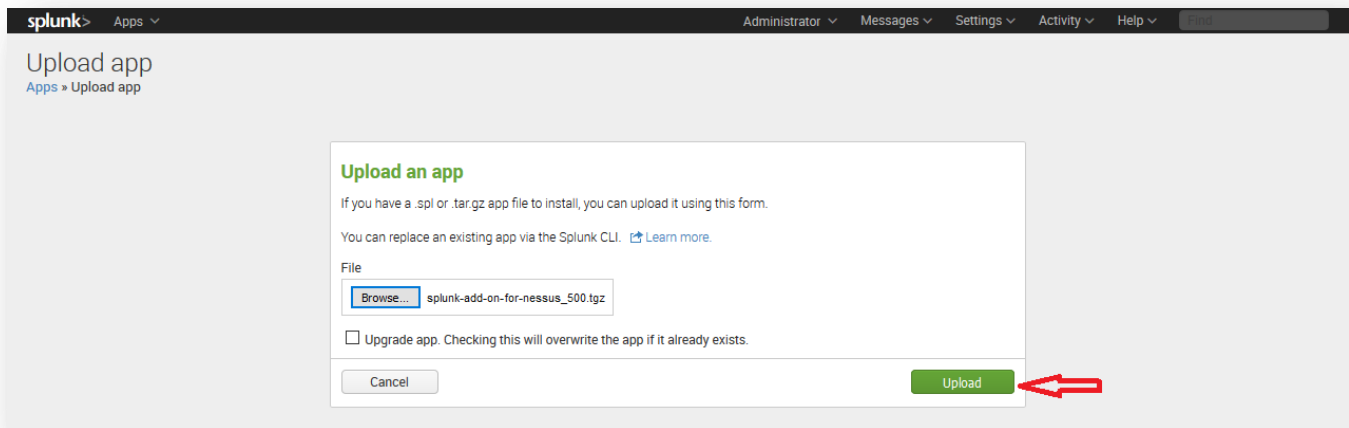
Select “Install app from file”.



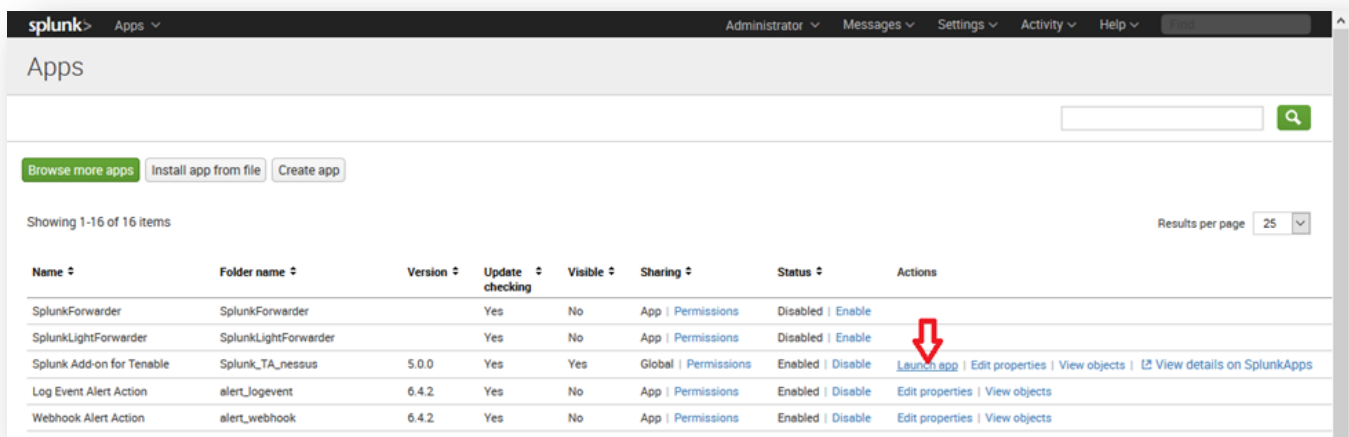
Click “Browse”.



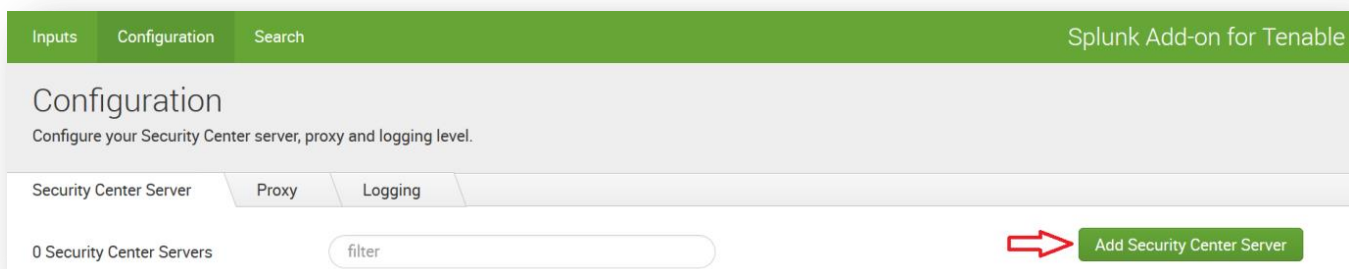
Select the downloaded Splunk Add-on for Tenable file, and click **“Upload”**.



When Splunk has completed processing, it will require a restart. After restarting and logging back into Splunk, navigate back to **“Managing Apps”**, as described in the first step. You will now see a **“Splunk Add-on for Tenable”** listed under **“Apps”**. Click the **“Launch app”** link under **“Actions”** to the right of the app name.



Click the **“Configuration”** tab at the top of the screen then the **“Add SecurityCenter Server”** button to the right of the screen.



A window is displayed where users can uniquely name the SecurityCenter server, as well as input the URL and login credentials for SecurityCenter. Complete the fields and click **“Add”**.

Add Security Center Server

Name* Remote SecurityCenter Server
Enter a unique name for each security center server.

URL* http://172.16.1.118
For example, https://10.10.10.10:443

Username* technanalyst

Password*

Cancel Add

From the **“Inputs”** screen, select **“Create New Input”** and click **“SecurityCenter”**.

splunk> App: Splunk Add-on for Tenable Administrator Messages Settings Activity Help Find

Inputs Configuration Search Splunk Add-on for Tenable

Inputs

Create data inputs to collect data from Tenable.

0 Inputs Service: All filter

Create New Input

Security Center

Nessus

i	Name	Service	Interval	Index	Status	Actions
0 Inputs						

A window is displayed where users can name the SecurityCenter input, and utilize the **“Server”** parameter to select the SecurityCenter server that was previously set up in the Configurations tab.

Add Security Center Input

Name* Perimeter SecurityCenter
Enter a unique name for each security center input.

Server* SC5.3.2

Metrics* Vulnerability

Start Time 2016-08-01T09:00:00+0800
The add-on starts collecting data with a date later than this UTC time. The default time is 30 days ago.

Interval* 60
Time interval of input in seconds.

Index* default

Cancel Add

Enter or select values for the remaining parameters (from the Splunk [documentation](#)):

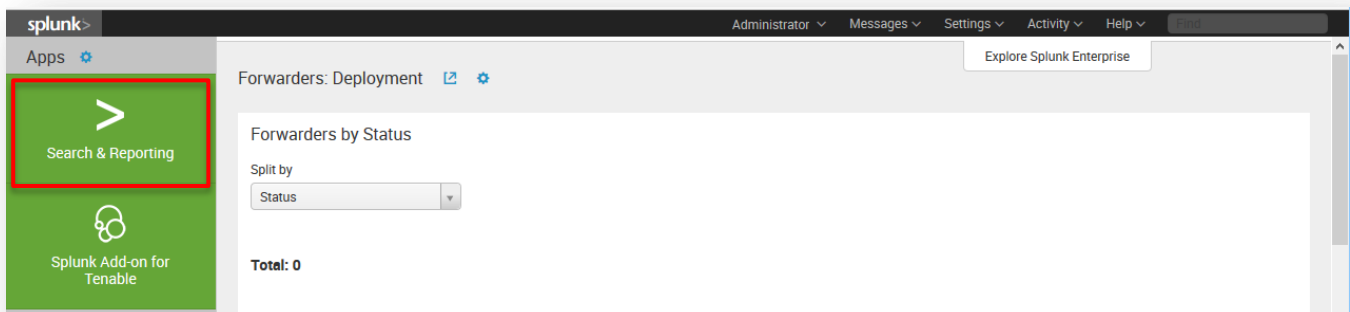
- **Metrics:** Select Vulnerabilities to collect vulnerability data discovered on SecurityCenter. The source type for this data is automatically set to `tenable:sc:vuln`
- **Start Time:** The add-on starts collecting data with a date later than this time. The default is 30 days before the configuration. The format is “YYYY-DD-MMThh:mm:ssTZD”, e.g., 2016-08-01T09:00:00+0800 stands for fetching data from 2016-08-01 09:00:00 in UTC+8 time zone.
- **Interval:** The number of seconds to wait before the Splunk platform runs the command again. The default is 60.
- **Index:** The index in which to store SecurityCenter data.

Click “**Add**” to finalize the “Inputs” configuration.

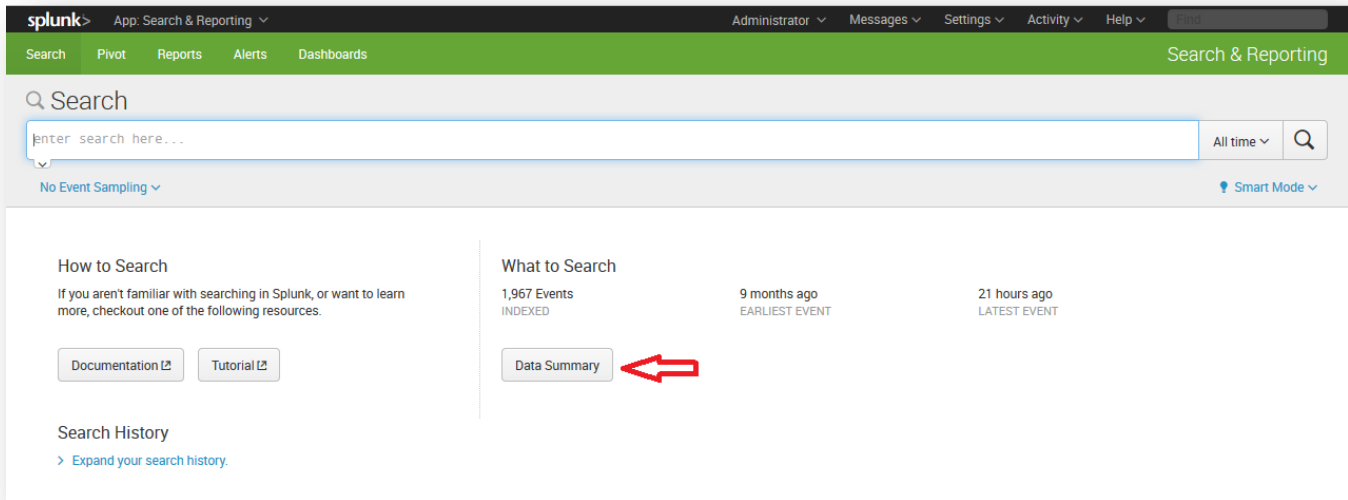
The SSL certificate from the SecurityCenter server must be copied to the Splunk server for full communication to occur between SecurityCenter and Splunk. Refer to Splunk’s documentation under “Check the warning messages of Tenable SecurityCenter” at:

<http://docs.splunk.com/Documentation/AddOns/released/Nessus/ConfigureModularInput2>

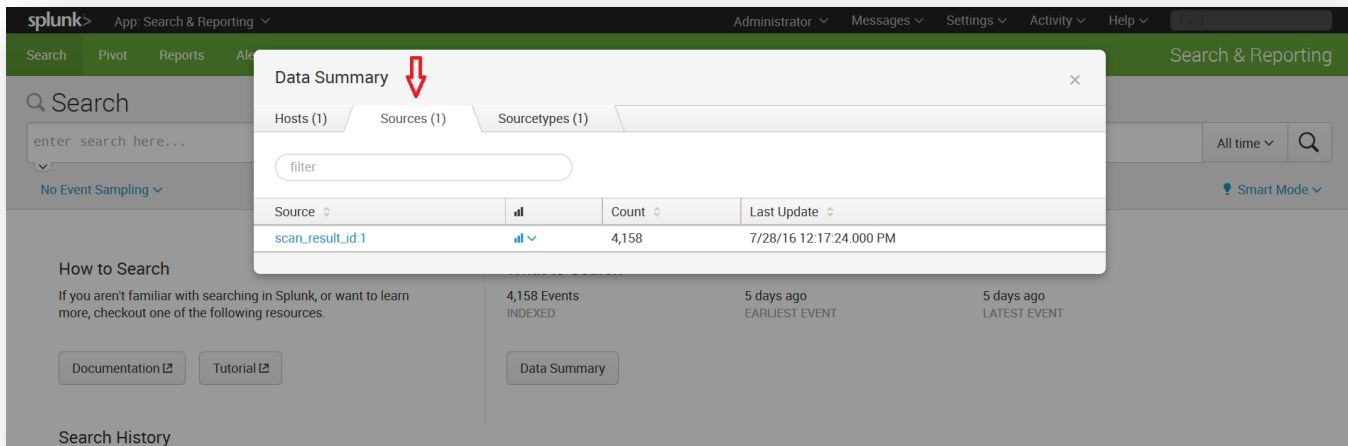
From the main Splunk screen, click “**Search & Reporting**” (or “**Search**” from the Splunk Add-on for Tenable screen).



If configured correctly, the “What to Search” portion of the screen has populated with your SecurityCenter data. You can then click “Data Summary” for detailed information.



Click the “Sources” tab for access to the SecurityCenter scan data.



If you encounter any issues with Splunk installation or configuration, or have any feature requests for this integration, contact Splunk Support.

Nessus

Tenable Nessus prevents network attacks by identifying the vulnerabilities and configuration issues that hackers use to penetrate your network. The Splunk Add-on for Tenable allows a Splunk software administrator to collect Tenable vulnerability scan data from Nessus and SecurityCenter via the REST API. The add-on supports Nessus 6.x, as well as 5.x for backwards compatibility.

This section assumes that the user has working knowledge of Nessus and Splunk, and a working instance of Splunk Enterprise. For information on obtaining and installing Splunk Enterprise, please refer to the [Splunk Enterprise Installation Manual](#).

Integration Requirements

The following are required in order to integrate Tenable Nessus with Splunk:

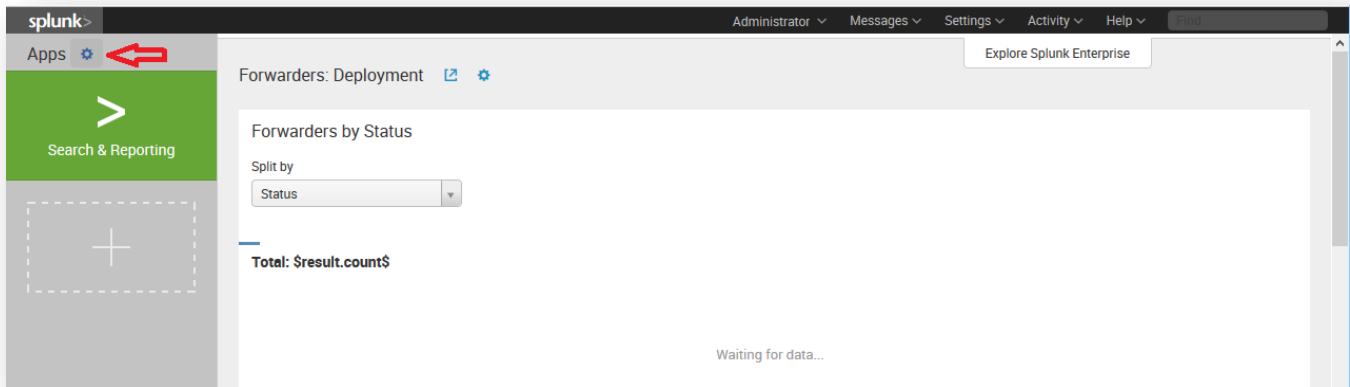
- Nessus 6.x or 5.x
- Splunk Add-on for Tenable
- Splunk 6.x or higher

Integration Configuration

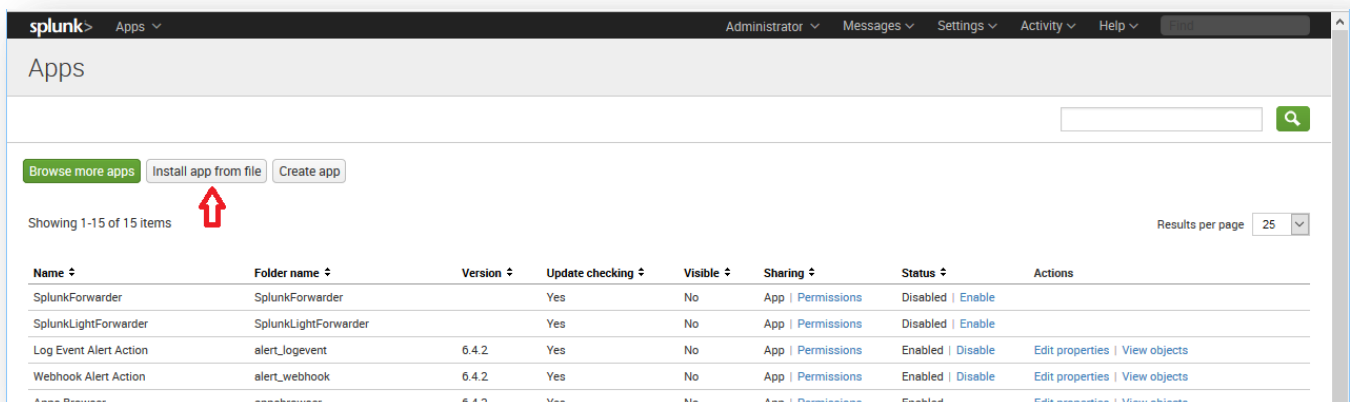
Splunk Add-on for Tenable Configuration

The Splunk Add-on for Tenable is available for download at <http://splunkbase.splunk.com/app/1710> (login required).

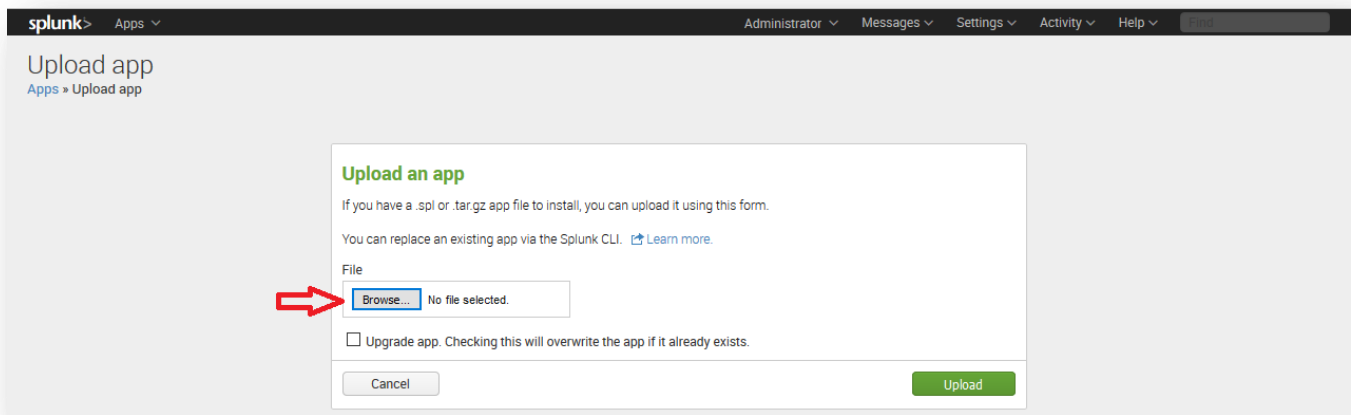
From Splunk, click on the Manage Apps “gear” icon, located in the upper-left side of the screen.



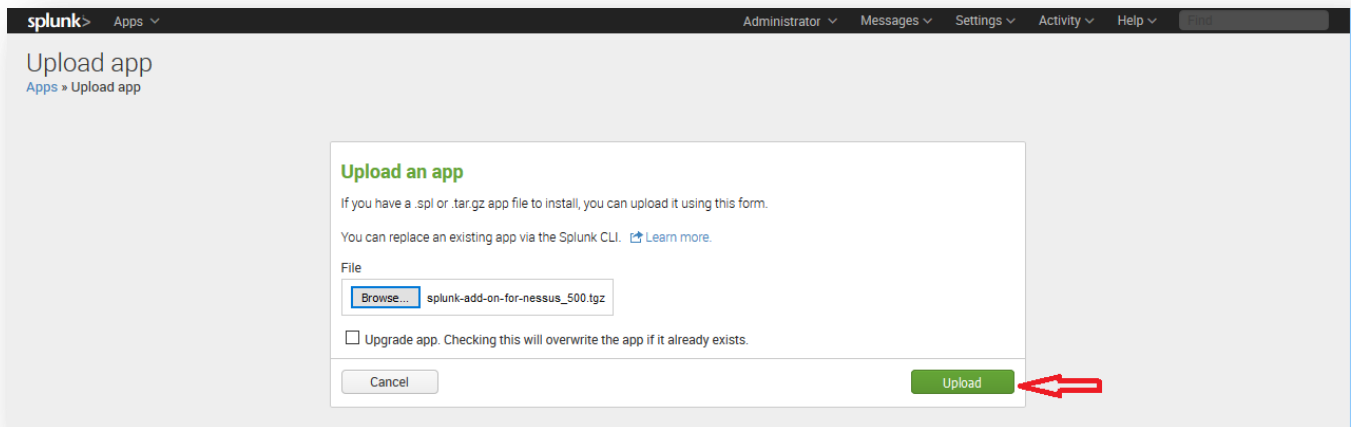
Select “Install app from file”.



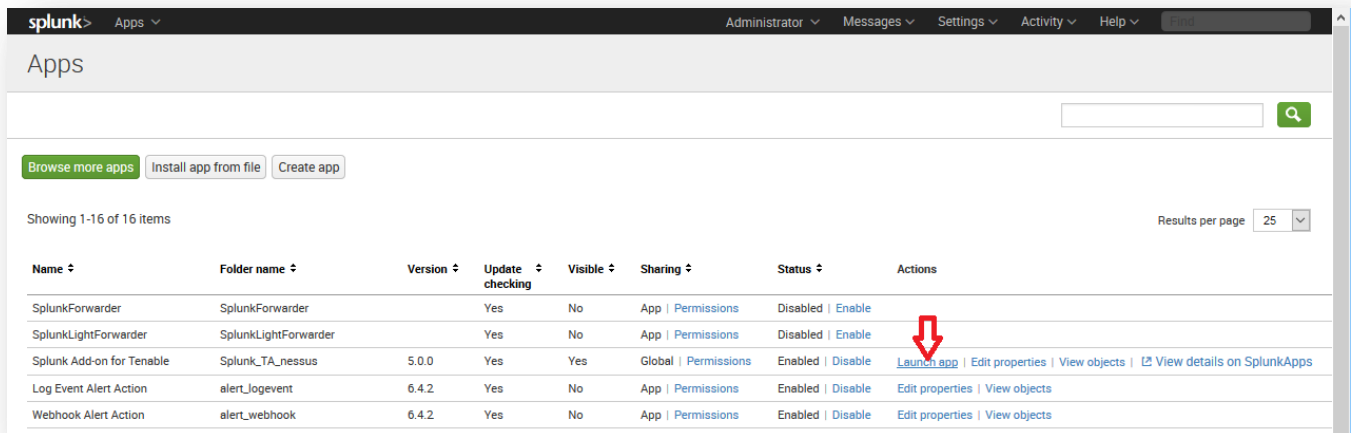
Click “Browse”.



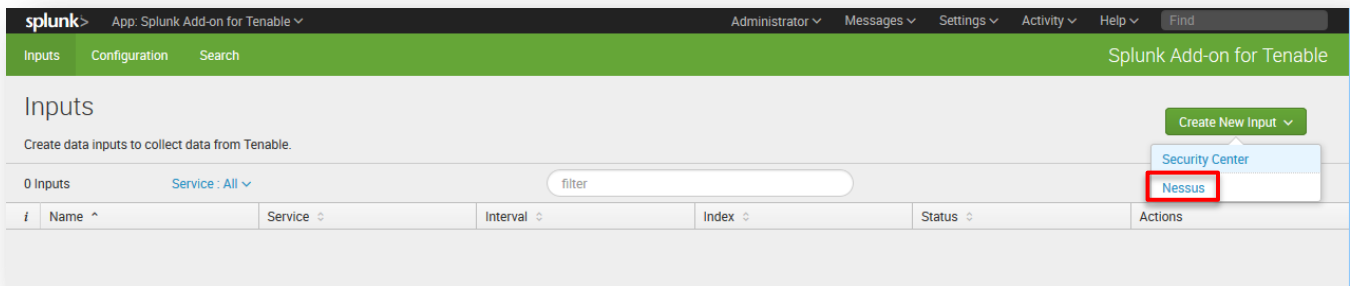
Select the downloaded Splunk Add-on for Tenable file, and click “Upload”.



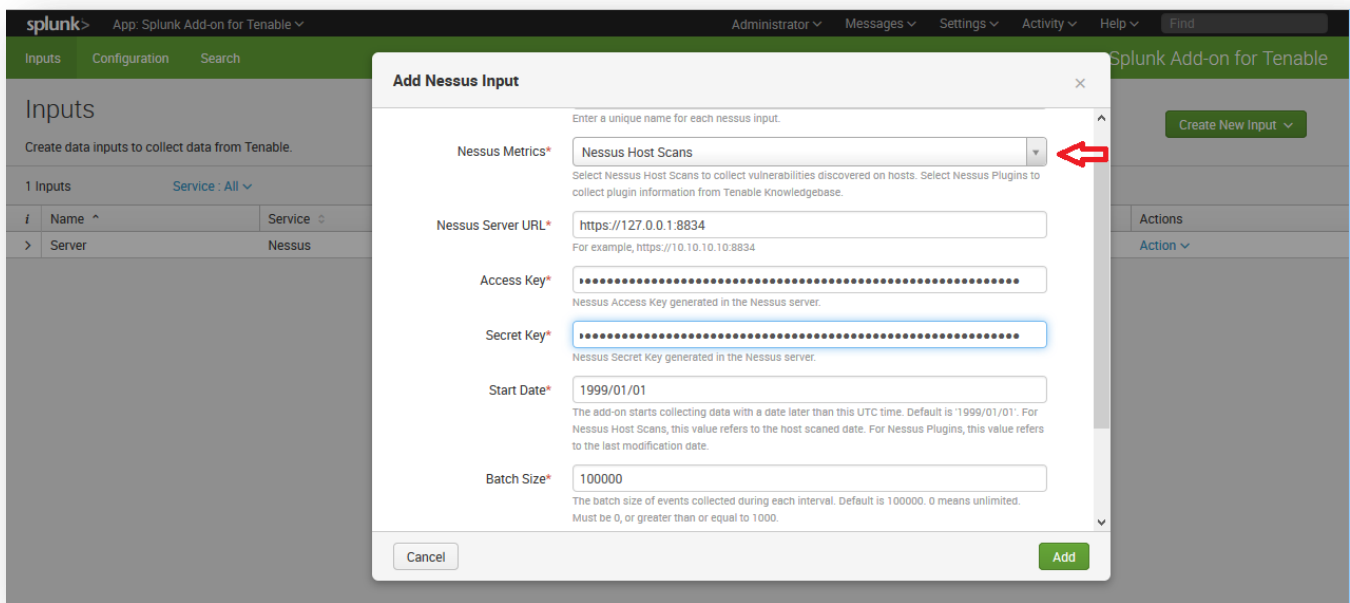
When Splunk has completed processing, it will require a restart. After restarting and logging back into Splunk, navigate back to “Managing Apps”, as described in the first step. You will now see a “Splunk Add-on for Tenable” listed under “Apps”. Click the “Launch app” link under “Actions” to the right of the app name.



From the “Inputs” screen, select “Create New Input” and click “Nessus”.

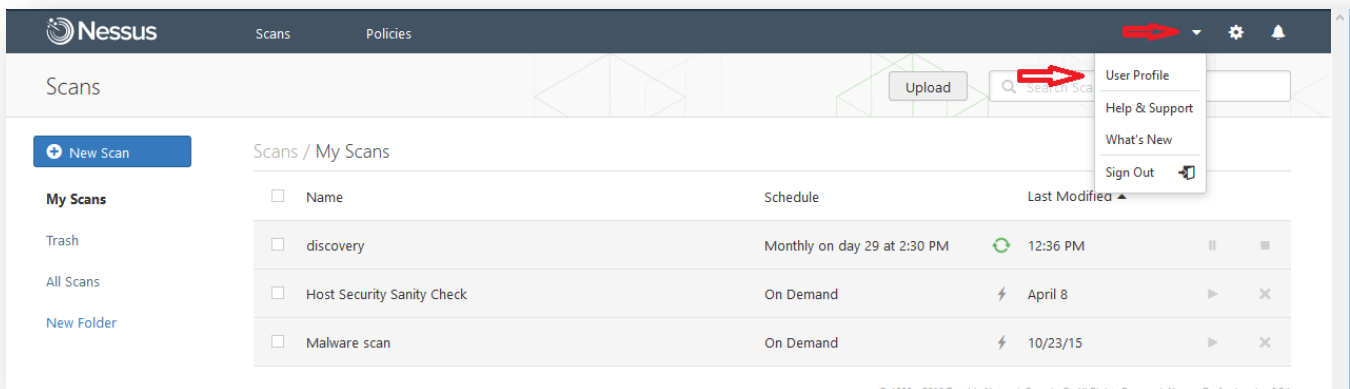


Fill in the required information and change the Nessus Metrics drop-down to “Nessus Host Scans”.

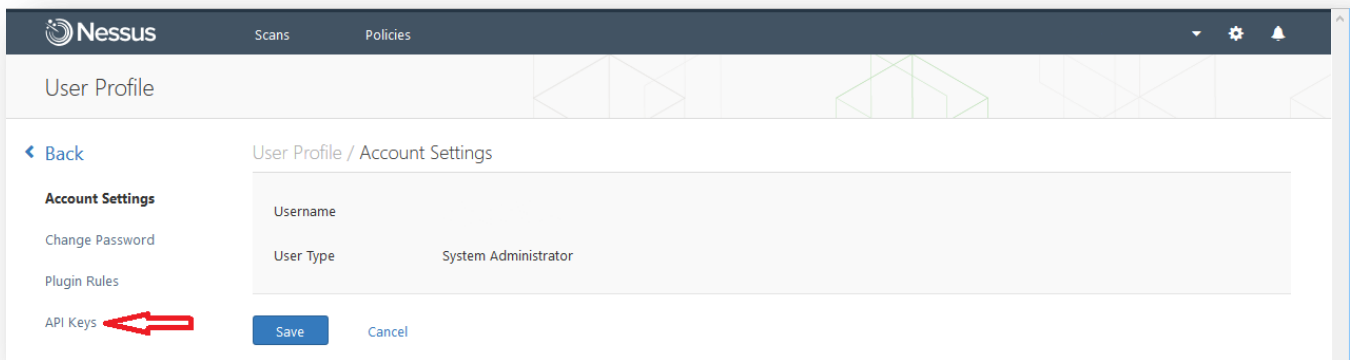


The Access Key and Secret Key required from Nessus are located in Nessus under “User Profile” > “API Keys”.

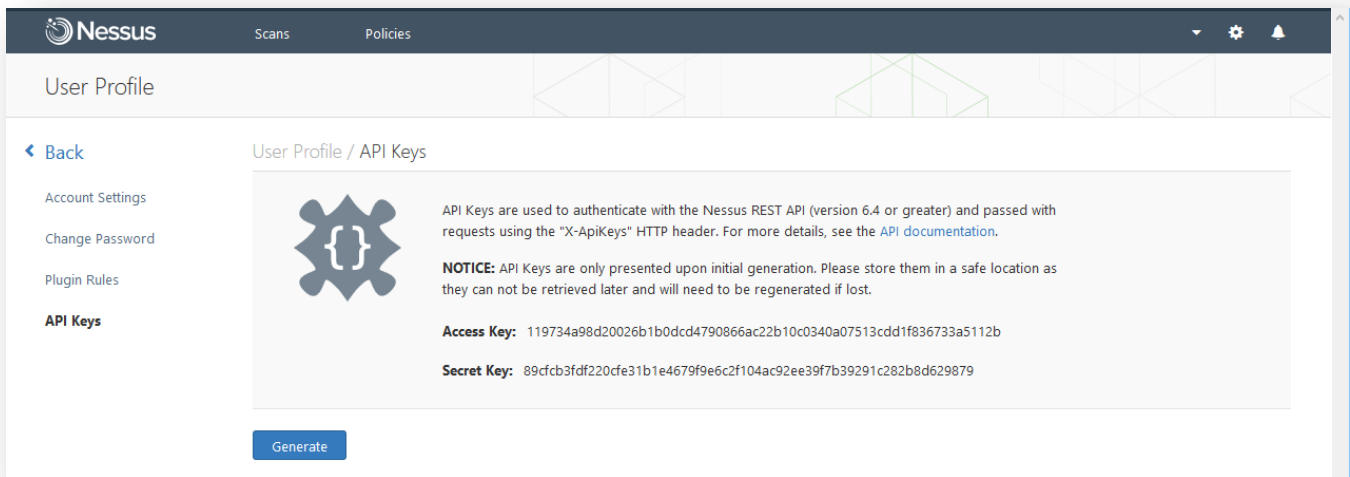
Log in to Nessus, and click the down arrow on the right side of the menu bar beside the user name. Next, select “User Profile”.



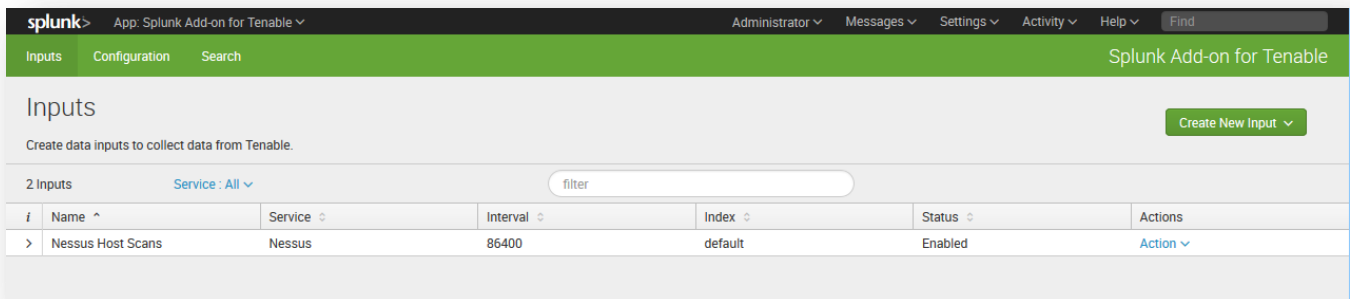
Click "API Keys".



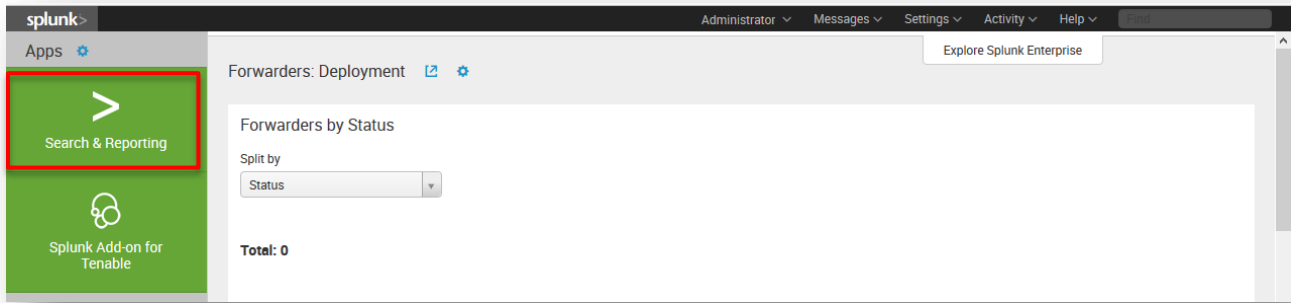
Generate the API keys, and then copy and paste the Access Key and Secret Key from the screen to the Access Key and Secret Key fields of the "Add Nessus Input" screen in Splunk.



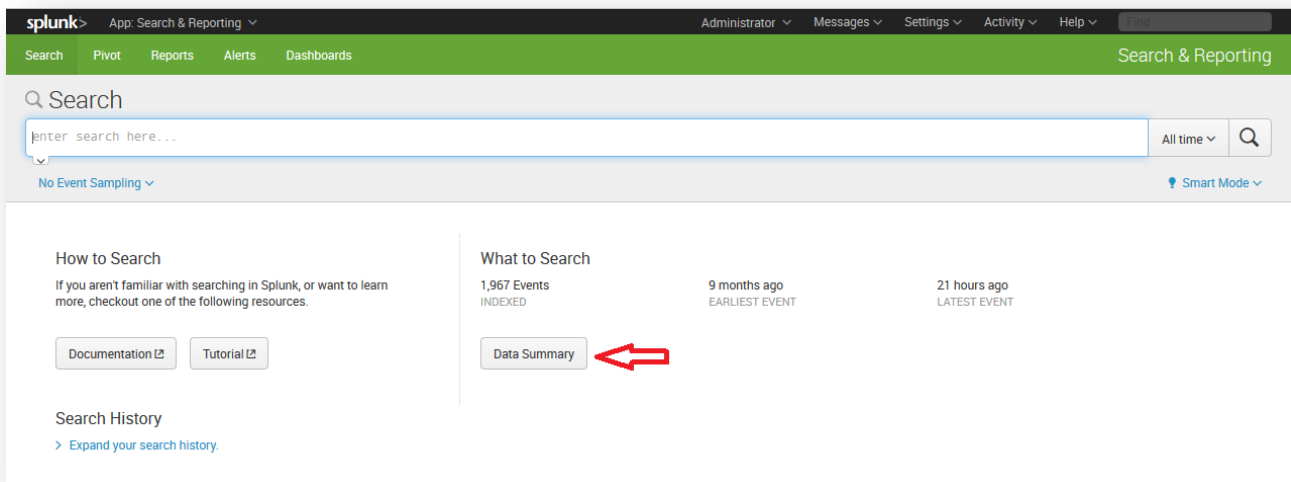
In Splunk, click "Add" to complete the action.



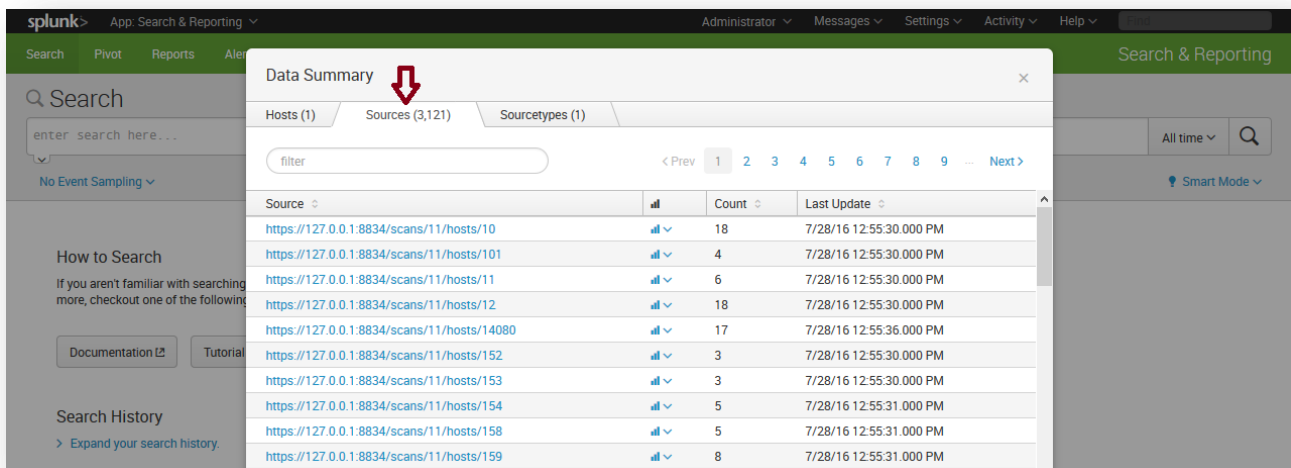
From the main Splunk screen, click “Search & Reporting” (or “Search” from the Splunk Add-on for Tenable screen).



If configured correctly, the “What to Search” portion of the screen has populated with your Nessus data. You can then click “Data Summary” for detailed information.



Click the “Sources” tab for access to the Nessus scan data.



If you encounter any issues with Splunk installation or configuration, or have any feature requests for this integration, contact Splunk Support.

Passive Vulnerability Scanner

Tenable PVS eliminates network blind spots by continuously monitoring network traffic in real time to discover active assets, identify cloud applications, and detect anomalous activity. The PVS app for Splunk is able to process tens of terabytes of data per day and find security-relevant information through comprehensive analysis. In order to uncover threats carried on mobile, virtual, and cloud devices, Splunk requires reliable data to analyze. The vulnerability and device discovery power of PVS used with the comprehensive analysis of Splunk provides network and security information for effective threat intelligence.

This section assumes that the user has working knowledge of Tenable PVS and Splunk. To download the Tenable Network Security PVS App for Splunk, see: <https://splunkbase.splunk.com/app/1844/>.

Integration Requirements

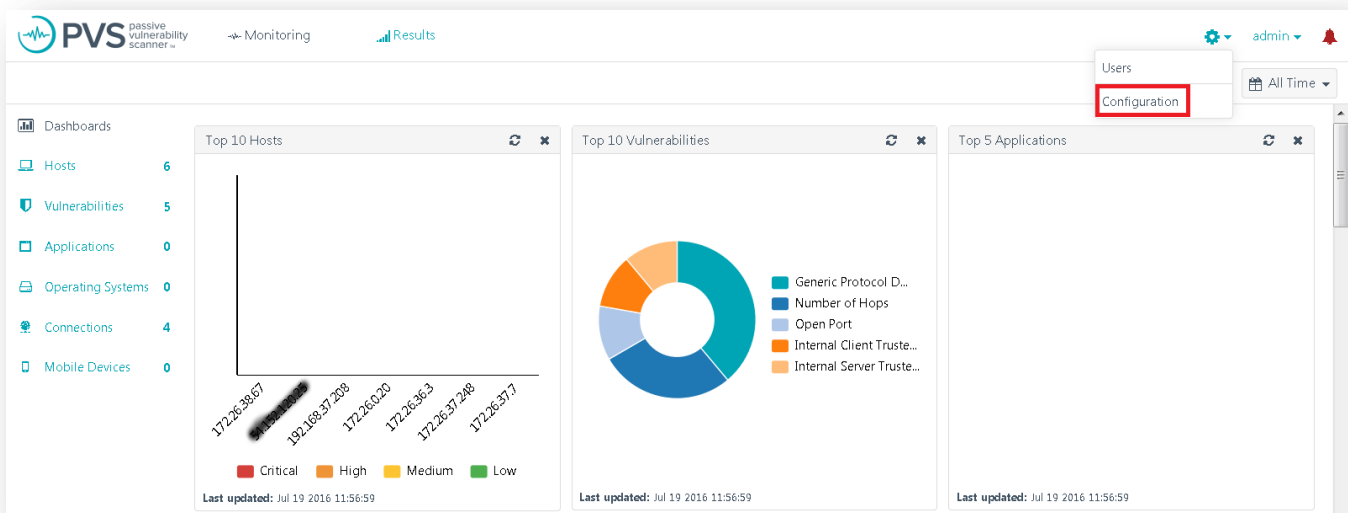
The following are required in order to integrate Tenable PVS with Splunk:

- Tenable Passive Vulnerability Scanner, Version 4.x or higher (including 5.x). To obtain a PVS evaluation, see: <http://www.tenable.com/products/passive-vulnerability-scanner/evaluate>.
- Splunk 6.x and higher.

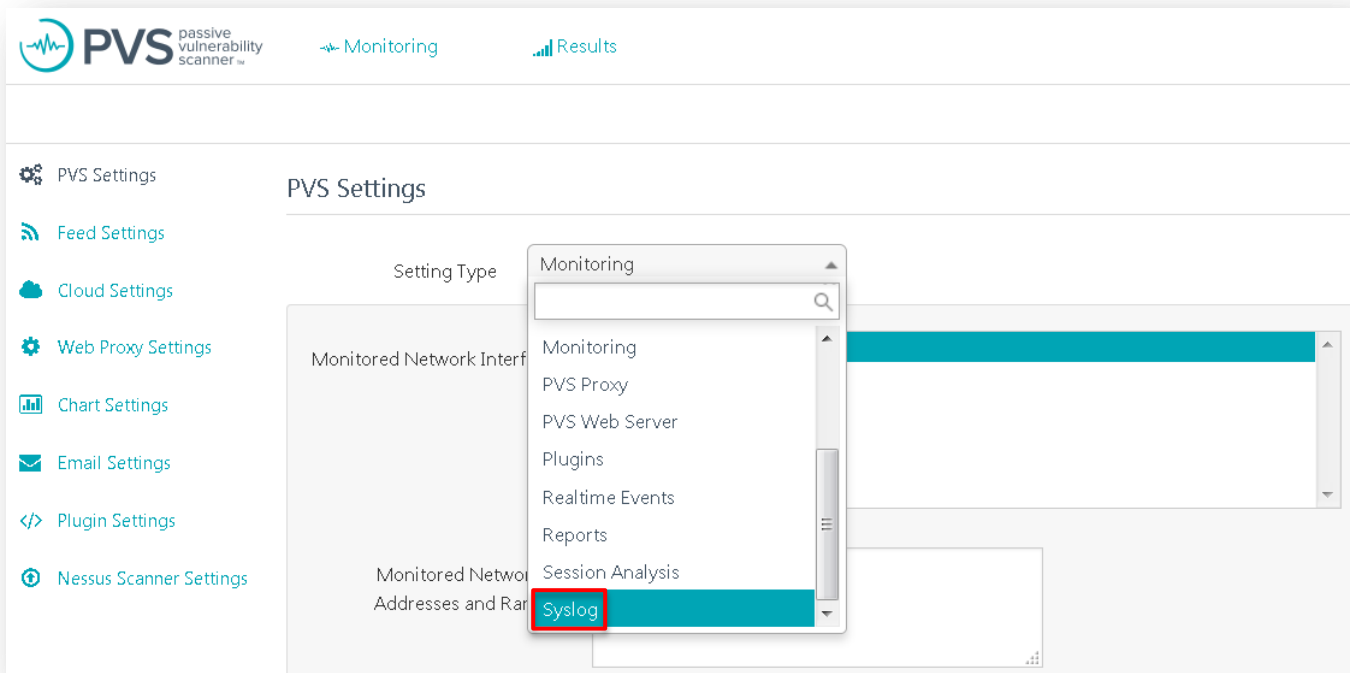
Integration Configuration

Tenable PVS Configuration

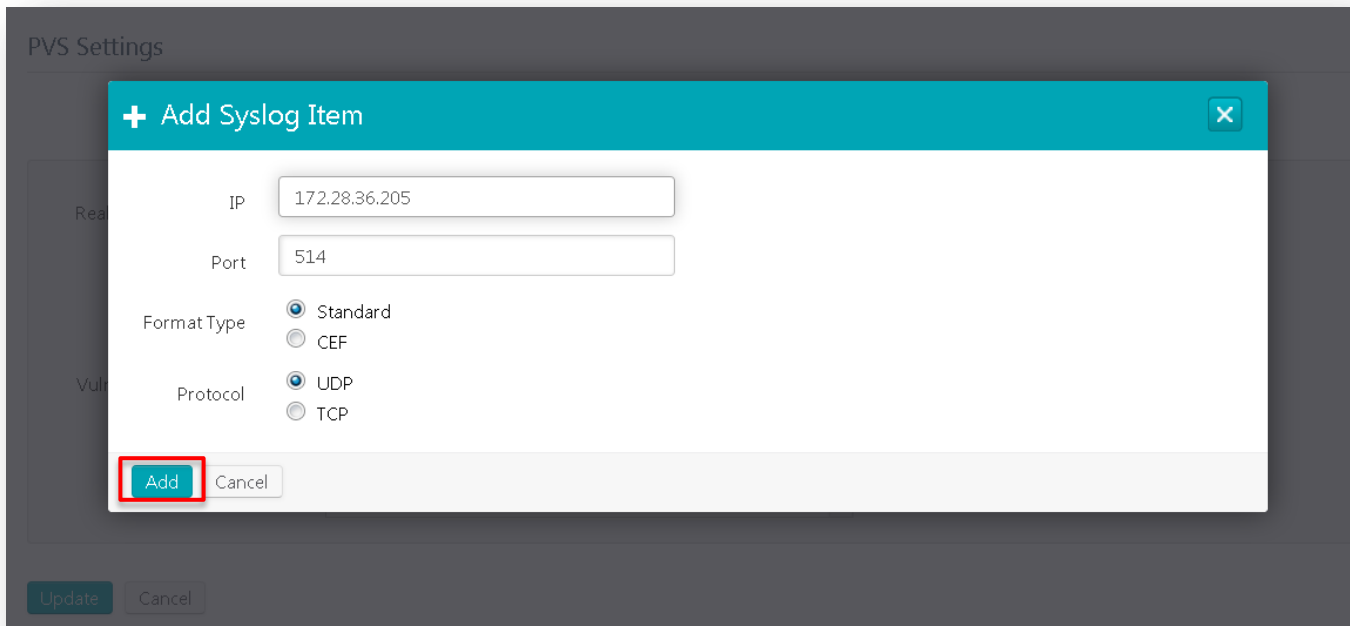
From the PVS UI, navigate to “**Configuration**”.



Select “Syslog” in the “Setting Type” drop-down menu.



In the “Realtime Syslog Server List”, click “Add” to enter the IP address and UDP port of the Splunk server and then click “Add” to finalize the addition.



Click “Update” to complete the process.

The screenshot shows the PVS Settings page. On the left is a navigation menu with options: PVS Settings, Feed Settings, Cloud Settings, Web Proxy Settings, Chart Settings, Email Settings, Plugin Settings, and Nessus Scanner Settings. The main content area is titled 'PVS Settings' and features a 'Setting Type' dropdown menu set to 'Syslog'. Below this are two lists: 'Realtime Syslog Server List' and 'Vulnerability Syslog Server List'. The first list contains the IP address '172.28.36.205:514'. To the right of each list are 'Add', 'Edit', and 'Remove' buttons. At the bottom of the settings area, the 'Update' button is highlighted with a red rectangular box, and a 'Cancel' button is also visible.



The IP address and UDP port must be entered in the format of “IP:PORT” (e.g., 10.1.1.10:514).

Splunk Configuration

Download the Tenable Network Security PVS App for Splunk from <https://splunkbase.splunk.com/app/1844/>. Log in to Splunk and click the gear icon next to “Apps”.

The screenshot shows the Splunk web interface. The top navigation bar includes 'splunk >', 'Administrator', 'Messages', 'Settings', 'Activity', and 'Help'. On the left sidebar, the 'Apps' menu item is highlighted with a red box and has a gear icon next to it. Below 'Apps' are 'Search & Reporting' and a plus sign icon. The main content area is titled 'Explore Splunk Enterprise' and contains four cards: 'Product Tours', 'Add Data', 'Explore Data', and 'Splunk Apps'. The 'Splunk Apps' card includes a link to the app page. A 'Close' button is located at the bottom right of the main content area.

On the “Apps” screen, click “Install app from file”, browse to the Tenable Network Security PVS App for Splunk .tgz file, and click “Upload”.

Upload an app

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

You can replace an existing app via the Splunk CLI. [Learn more.](#)

File

tenable-network-security-pvs-app-for-splunk_102.tgz

Upgrade app. Checking this will overwrite the app if it already exists.

The app is now listed and enabled.

[Browse more apps](#) [Install app from file](#) [Create app](#)

Showing 1-17 of 17 items Results per page 25

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
SplunkForwarder	SplunkForwarder		Yes	No	App Permissions	Disabled Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App Permissions	Disabled Enable	
Log Event Alert Action	alert_logevent	6.4.2	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Webhook Alert Action	alert_webhook	6.4.2	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Apps Browser	appsbrowser	6.4.2	Yes	No	App Permissions	Enabled	Edit properties View objects
framework	framework		Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Getting started	gettingstarted	1.0	Yes	Yes	App Permissions	Disabled Enable	
Introspection_generator_addon	Introspection_generator_addon	6.4.2	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Home	launcher		Yes	Yes	App Permissions	Enabled	Launch app Edit properties View objects
learned	learned		Yes	No	App Permissions	Enabled Disable	Edit properties View objects
legacy	legacy		Yes	No	App Permissions	Disabled Enable	
TenableNetwork Security PVS	pvs	1.0.2	Yes	Yes	App Permissions	Enabled Disable	Launch app Edit properties View objects View details on SplunkApps
sample data	sample_app		Yes	No	App Permissions	Disabled Enable	
Search & Reporting	search	6.4.2	Yes	Yes	App Permissions	Enabled	Launch app Edit properties View objects
Splunk Archiver App	splunk_archiver	1.0	Yes	No	App Permissions	Enabled Disable	Edit properties View objects View details on SplunkApps

In the Splunk UI, navigate to “Settings” > “Data” > “Data Inputs”. To the right of “UDP”, click “Add new”.

The screenshot shows the Splunk Data Inputs page. The navigation bar at the top includes 'splunk > Apps', 'Administrator', 'Messages', 'Settings', 'Activity', and 'Help'. The main heading is 'Data inputs'. Below it, there is a section for 'Local inputs' with a description: '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](#).' A table lists various input types:

Type	Inputs	Actions
Files & directories Index a local file or monitor an entire directory.	5	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.	2	Add new

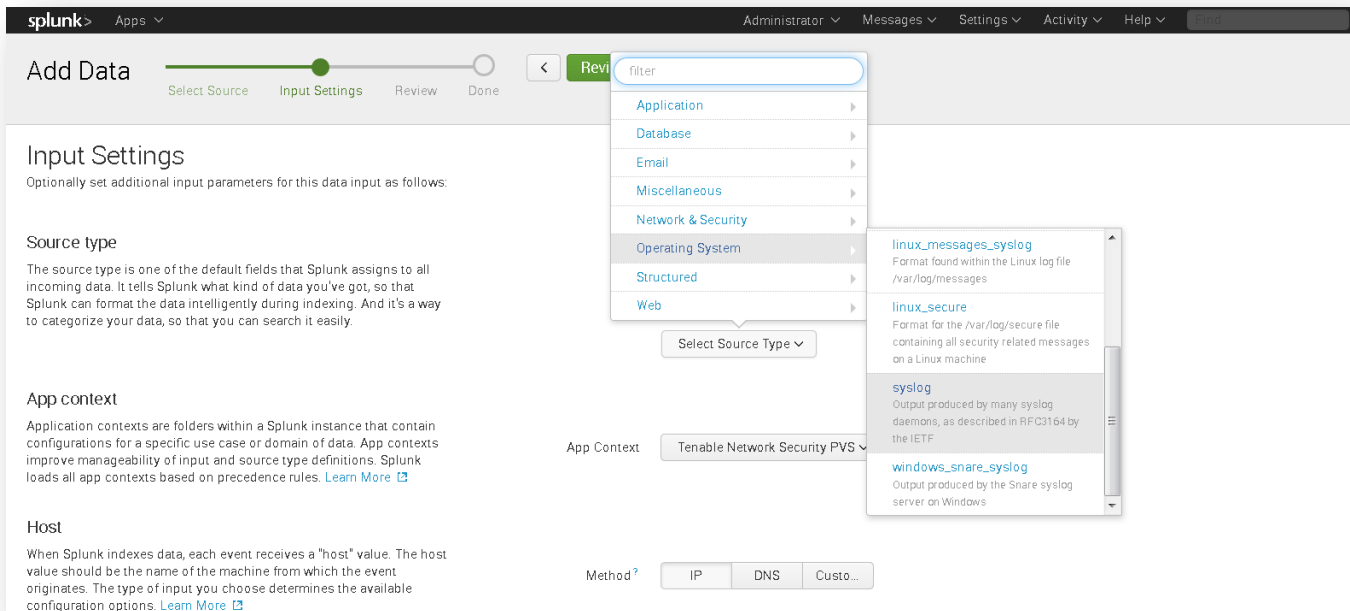
Under “Select Source”, select “UDP” and enter “514” for the port. Click “Next”.

The screenshot shows the 'Add Data' configuration page in Splunk. The navigation bar at the top includes 'splunk > Apps', 'Administrator', 'Messages', 'Settings', and 'Activity'. The main heading is 'Add Data'. Below it, there is a progress bar with four steps: 'Select Source', 'Input Settings', 'Review', and 'Done'. The 'Next >' button is highlighted with a red box. The left sidebar shows the following options:

- 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 Splunk to listen on a network port. (Selected)
- Scripts**: Get data from from any API, service, or database with a script.

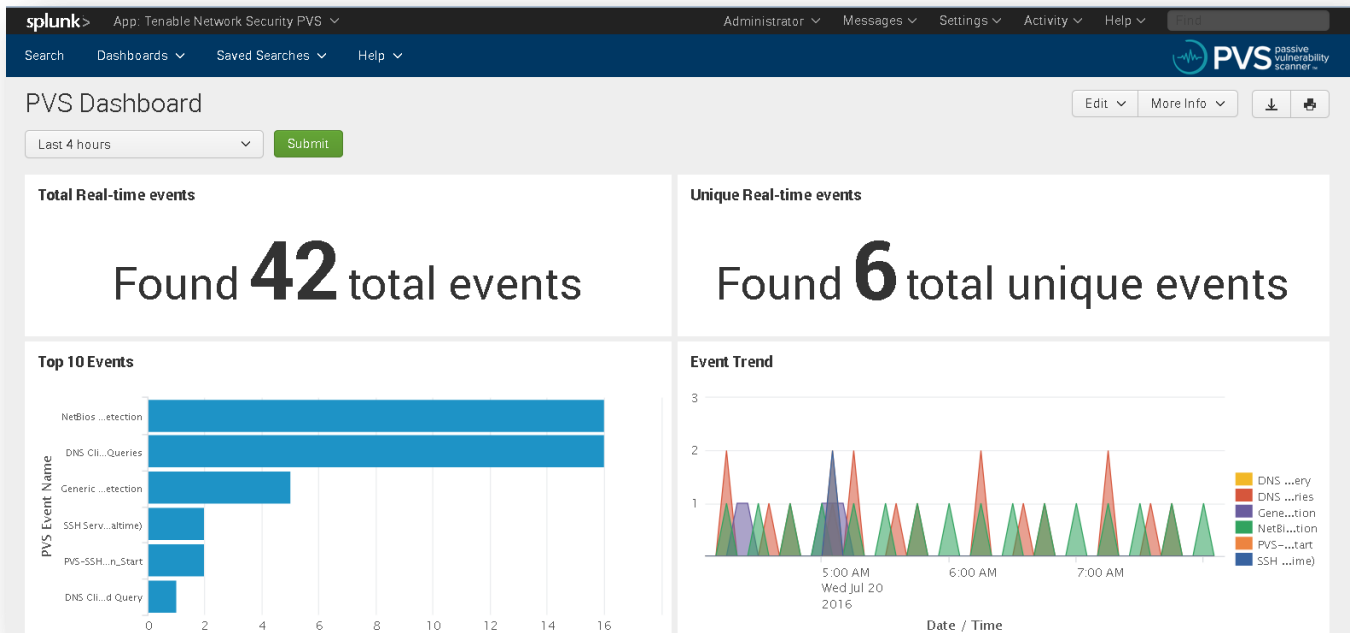
The main content area shows the configuration for the selected source. It includes a radio button for 'TCP' and 'UDP', with 'UDP' selected. The 'Port?' field is set to '514' with an example of '514'. The 'Source name override?' field is set to 'optional' with a sub-label 'host.port'. The 'Only accept connection from?' field is set to 'optional' with an example of '10.1.2.3, !badhost.splunk.com, *.splunk.com'.

In the “Input Settings” screen, click the drop-down for “Select Source Type”. Under “Operating System”, select “syslog”. If not already selected, choose “Tenable Network Security PVS” next to “App Context”, and select “IP” next to “Method”.



Click “Review” to review all changes, and then “Submit” to finalize the configuration.

Select “Apps” and “Tenable Network Security PVS” in the upper-left corner of the screen to display your initial PVS Dashboard.



If you encounter any issues with Splunk installation or configuration, or have any feature requests for this integration, contact Splunk Support.

Log Correlation Engine

Tenable LCE unifies vulnerability collection and event analysis data through Tenable SecurityCenter, which provides easy-to-use dashboards to display multiple data points in a centralized view. Organizations that choose to send Splunk logs to the LCE have a unique advantage in that Splunk data is normalized by LCE and can be included for automatic anomaly detection, asset discovery, and additional vulnerability information, including botnet and malware detection.

The Tenable LCE Splunk Client forwards data that Splunk collects to the LCE server. Once the data reaches the LCE server, the data is reviewed and normalized so it can be queried in SecurityCenter.

Tenable LCE also has the ability to forward any log it receives to one or more syslog servers, including Splunk. Using LCE's Syslog Forwarding and Event Rules features, it can send all, or selected, logs to Splunk Enterprise. Once the logs are received in Splunk, the data can be filtered and queried to produce meaningful dashboards and reports for a more complete view of the enterprise.

This section assumes that the user has working knowledge of Tenable LCE and Splunk, and a working instance of Splunk Enterprise. For information on obtaining and installing Splunk Enterprise, please refer to the [Splunk Enterprise Installation Manual](#).

Integration Requirements

The following are required in order to integrate Tenable LCE with Splunk:

- Log Correlation Engine version 4.8 and higher
- Log Correlation Engine Splunk Client version 4.6 and higher
- Splunk 6.x and higher

Integration Configuration

To configure Splunk Enterprise to forward logs to Tenable LCE, follow the steps in the “[Tenable LCE Splunk Client Configuration](#)” and “[Splunk Configuration](#)” sections.

For detailed steps on configuring syslog forwarding from Tenable LCE to Splunk Enterprise, see the “[Tenable LCE Syslog Forwarding](#)” section.

Tenable LCE Splunk Client Configuration

The LCE Splunk Client is available for download from the Tenable Support Portal at <https://support.tenable.com> (login required). Log in and navigate to the “Downloads > Log Correlation Engine” section and download the “Log Correlation Engine Splunk Client”.

Once downloaded, copy the LCE Splunk Client to the host it will be installed on. The LCE Client can be installed directly onto a Splunk server. For LCE Splunk Client installation tips, refer to the [LCE 4.8 User Guide](#).

After the LCE Splunk Client is installed, log in to the system it is installed on to begin the configuration.



All shell commands need to be executed by a user with root privileges.

To configure the LCE Splunk client, execute the “**set-server-ip.sh**” script (as shown below). Once prompted, enter the LCE server IP address or hostname and LCE server port (default is 31300). Once the information is updated, the LCE Splunk Client daemon is restarted.

```
# /opt/lce_splunk/set-server-ip.sh

Enter the new desired LCE server IP or host name.
>>
192.168.22.11

Enter the new desired LCE server port [31300].
>>
31300
Updating LCE Server IP from 203.0.113.1 to 192.168.22.11...
Updating LCE Server Port from 31300 to 31300...
Done
Stopping LCE Splunk Client daemon [
OK ]
Starting LCE Splunk Client daemon [
OK ]
```

Optionally, you can execute the “**set-server-ip.sh**” script (as shown below) with the LCE server IP address or hostname and LCE server port as arguments. Once the information is updated, the LCE Splunk Client daemon is restarted.

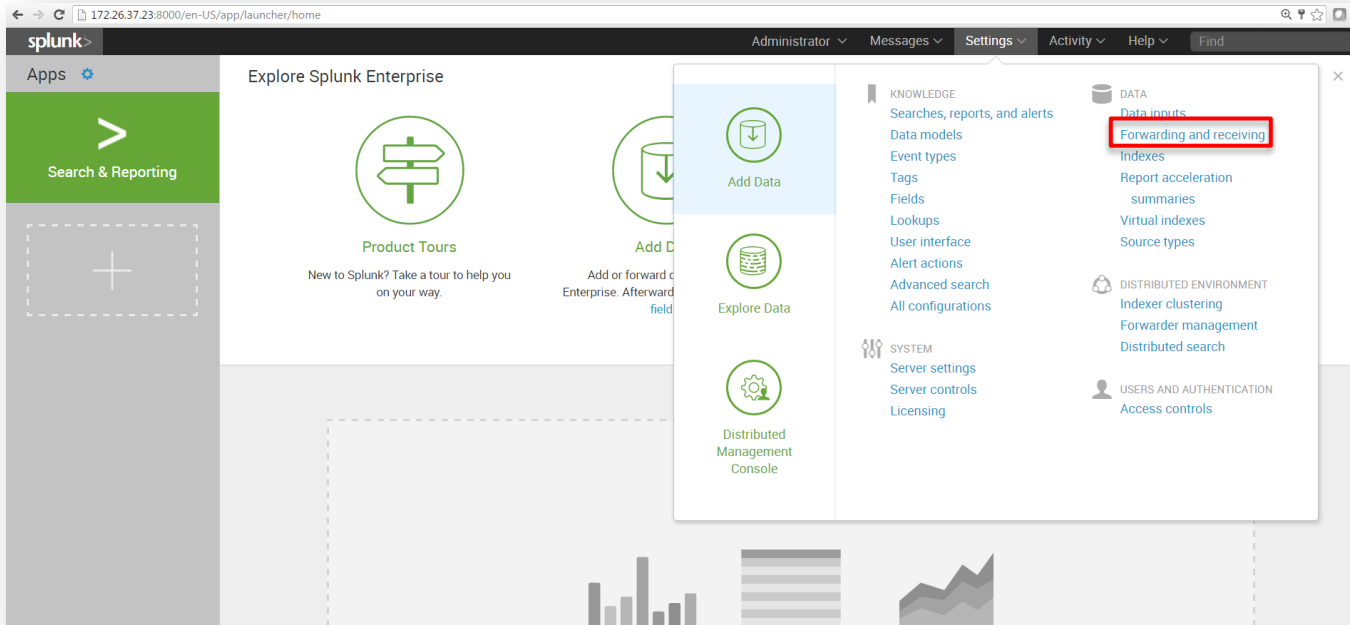
```
# /opt/lce_splunk/set-server-ip.sh 192.168.22.11 31300
Updating LCE Server IP from 172.26.20.66 to 192.168.11...
Updating LCE Server Port from 31300 to 31300...
Done
Stopping LCE Splunk Client daemon [
OK ]
Starting LCE Splunk Client daemon [
OK ]
```

If you encounter any issues with LCE Client installation or configuration, or have any feature requests for this integration, contact [Tenable Support](#).

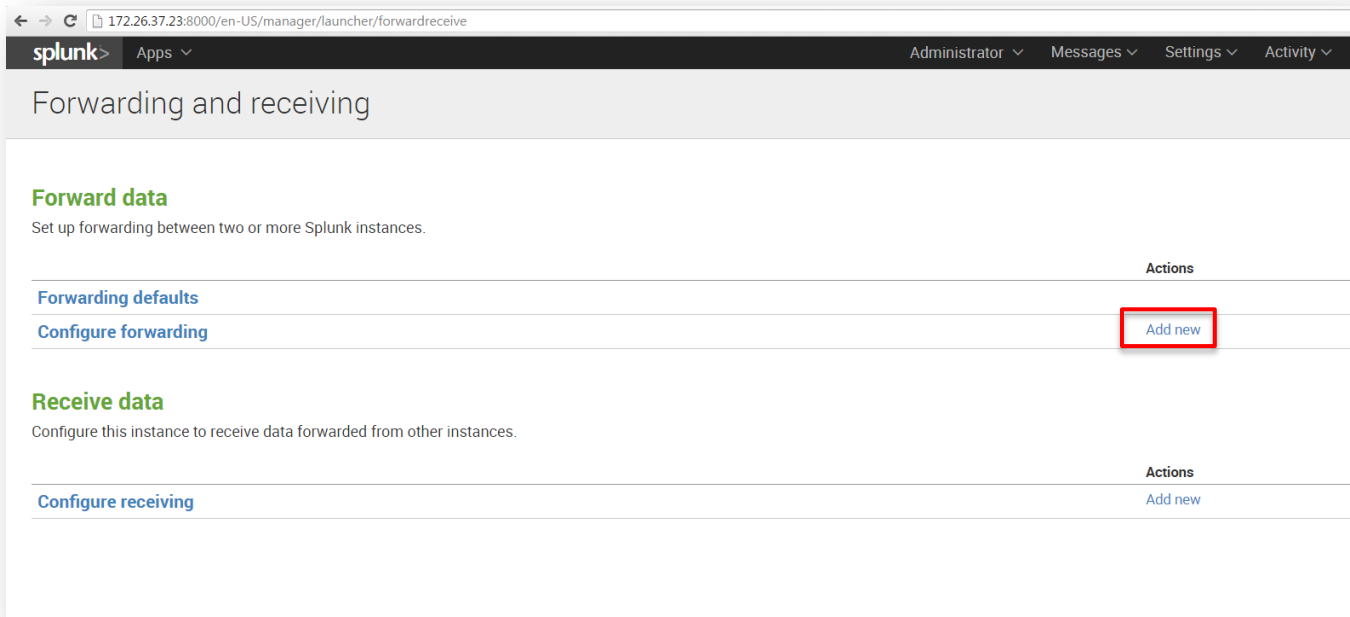
Splunk Configuration

After the LCE Splunk Client is installed and configured, the Splunk Indexer has to be configured in order to send data from Splunk to the LCE Splunk Client. That data is then sent from the LCE Splunk Client to the LCE server, where it is normalized before being forwarded on to SecurityCenter.

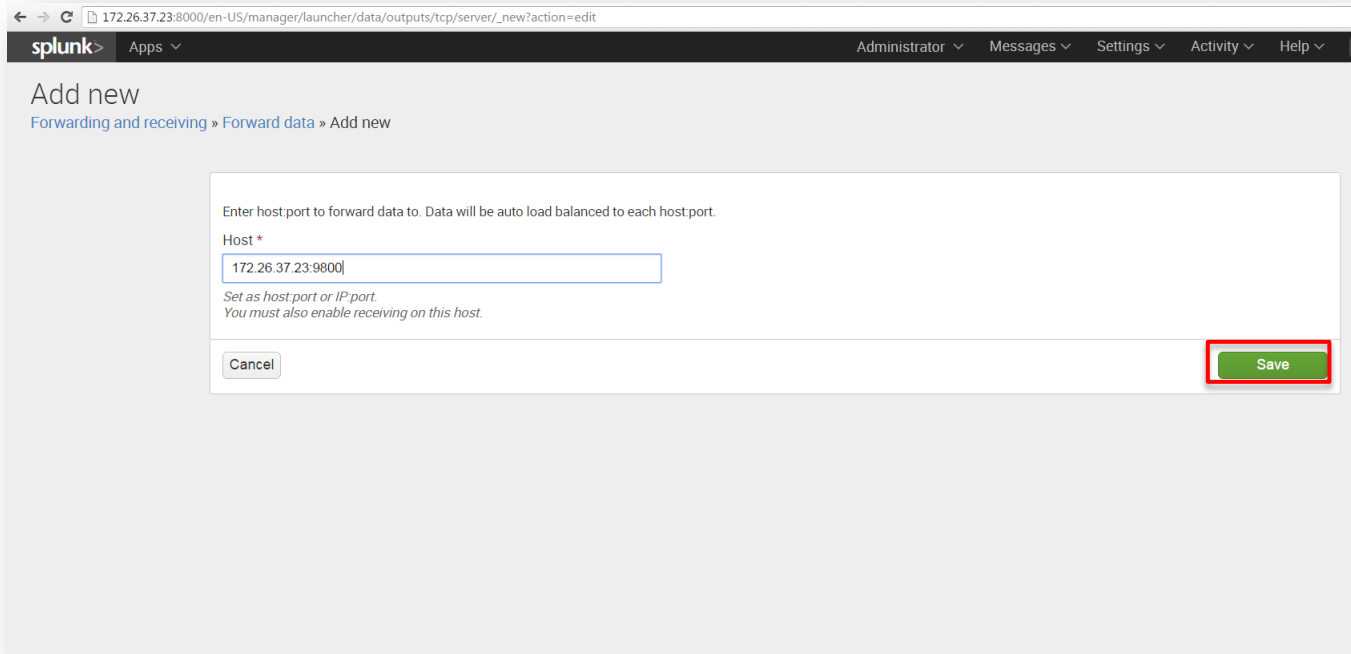
To begin the Splunk configuration, log in to Splunk Web (<http://<IP address or hostname>:8000>) as a user with administrator privileges. Once logged in, click **“Settings”** in the top menu bar and select **“Forwarding and receiving”**.



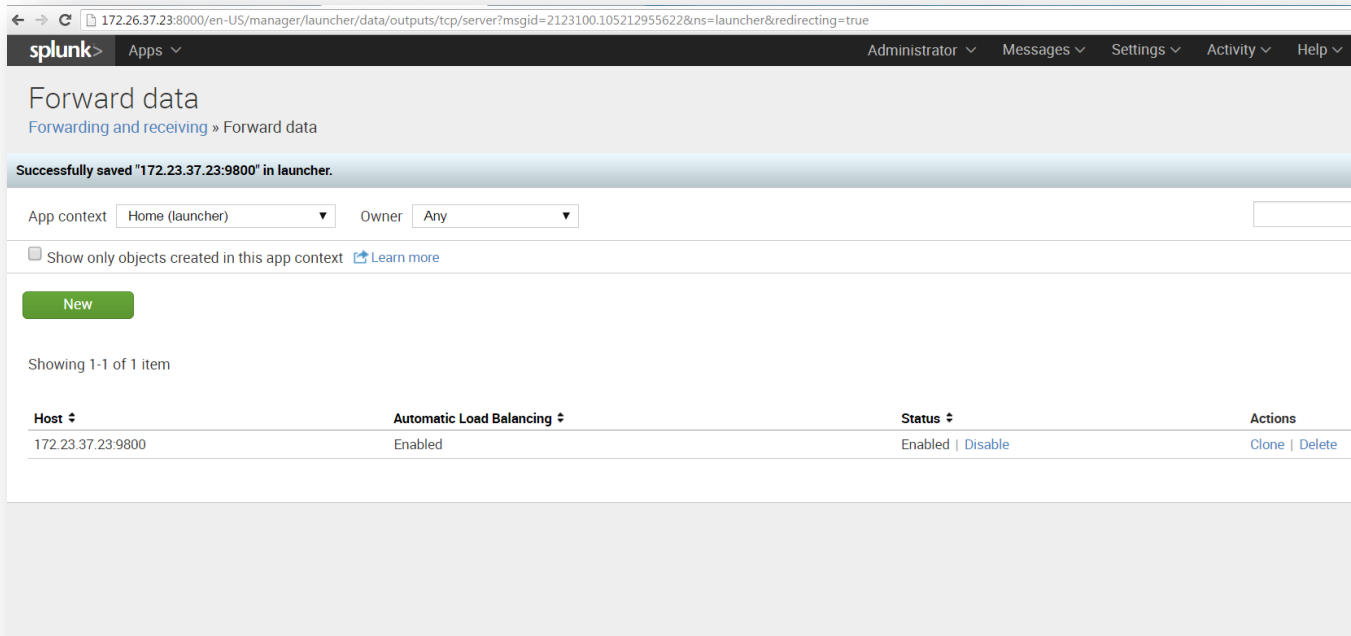
Click **“Add new”** under the **“Configure forwarding”** action.



In the “Host” box, enter the IP address or hostname and port (default 9800) of the LCE Splunk Client host. Click “Save” to finalize the settings.



Once saved, the LCE Splunk Client will be listed in the “Host” list. Verify that the “Status” is set to “Enabled”.



To finalize the Splunk configuration, log in to the Splunk Indexer as a root user. Once logged in, edit the “`outputs.conf`” file and add the lines below in bold.



The default location of the `outputs.conf` file is `/opt/splunk/etc/system/local/outputs.conf`.

```
[tcpout]
defaultGroup = default
disabled = 0
indexAndForward = 1
[tcpout-server://LCE_IP_OR_Hostname:9800]
[tcpout:default]
disabled = 0
server = LCE_IP_OR_Hostname:9800
sendCookedData = false
```

Save the file, and then restart the Splunk services. Once the services restart, Splunk data is now able to be forwarded to the LCE Splunk Client.

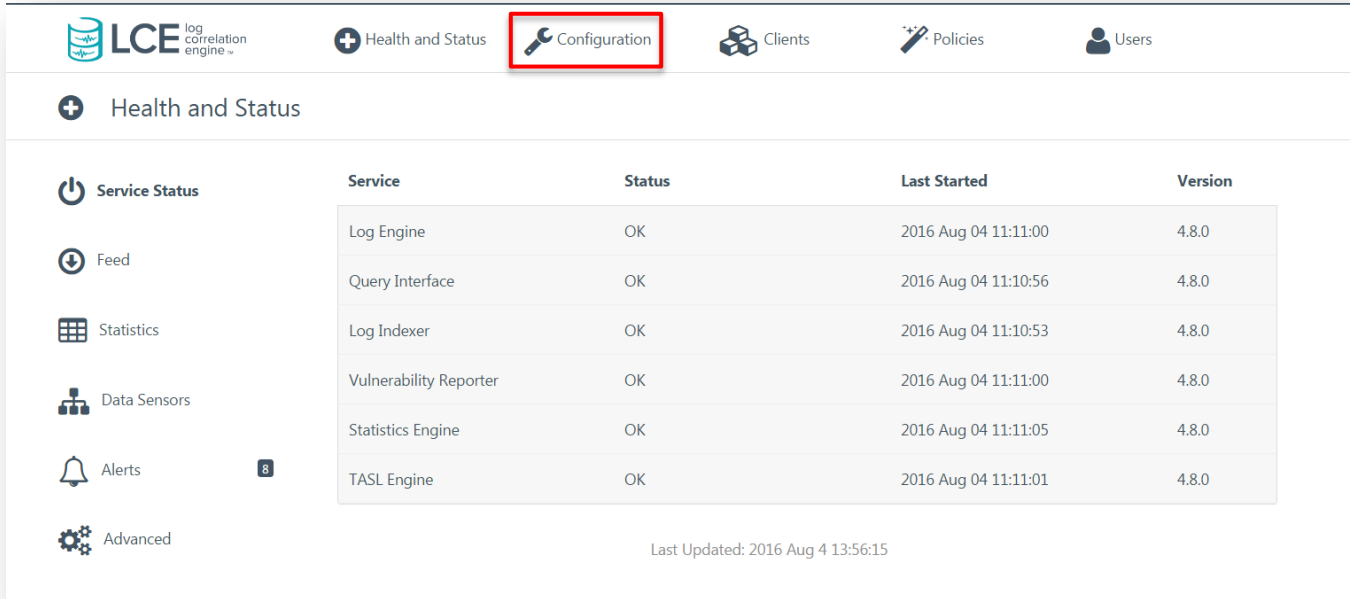
To complete the setup, log in to the web interface of the LCE server previously configured to communicate with the LCE Splunk Client. Once logged in to the LCE server, the following steps will need to be performed:

- Authorize the LCE Splunk Client
- Configure the LCE Splunk Client Policy
- Assign the Policy to the LCE Splunk Client

For detailed instruction on how to perform these steps and finalize the configuration, please refer to the [LCE 4.8 User Guide](#).

Tenable LCE Syslog Forwarding

To configure syslog forwarding from LCE to Splunk, log in to LCE's web interface and navigate to "Configuration".

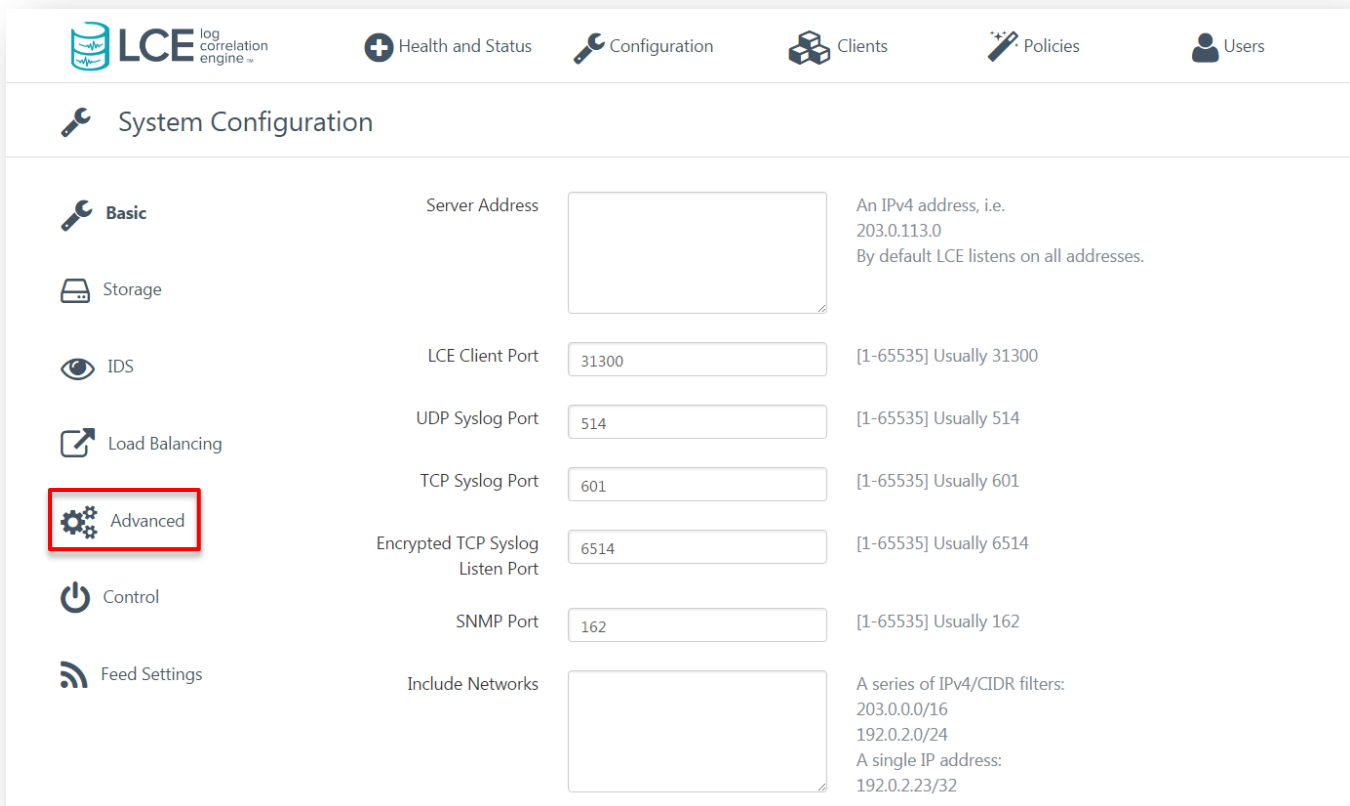


The screenshot shows the LCE web interface. The top navigation bar includes the LCE logo, a "Health and Status" button, a "Configuration" button (highlighted with a red box), a "Clients" button, a "Policies" button, and a "Users" button. Below the navigation bar, the "Health and Status" section is active, displaying a table of service status.

Service	Status	Last Started	Version
Log Engine	OK	2016 Aug 04 11:11:00	4.8.0
Query Interface	OK	2016 Aug 04 11:10:56	4.8.0
Log Indexer	OK	2016 Aug 04 11:10:53	4.8.0
Vulnerability Reporter	OK	2016 Aug 04 11:11:00	4.8.0
Statistics Engine	OK	2016 Aug 04 11:11:05	4.8.0
TASL Engine	OK	2016 Aug 04 11:11:01	4.8.0

Left-hand menu items: Service Status, Feed, Statistics, Data Sensors, Alerts (8), Advanced. Last Updated: 2016 Aug 4 13:56:15

Click "Advanced" in the left-hand menu.

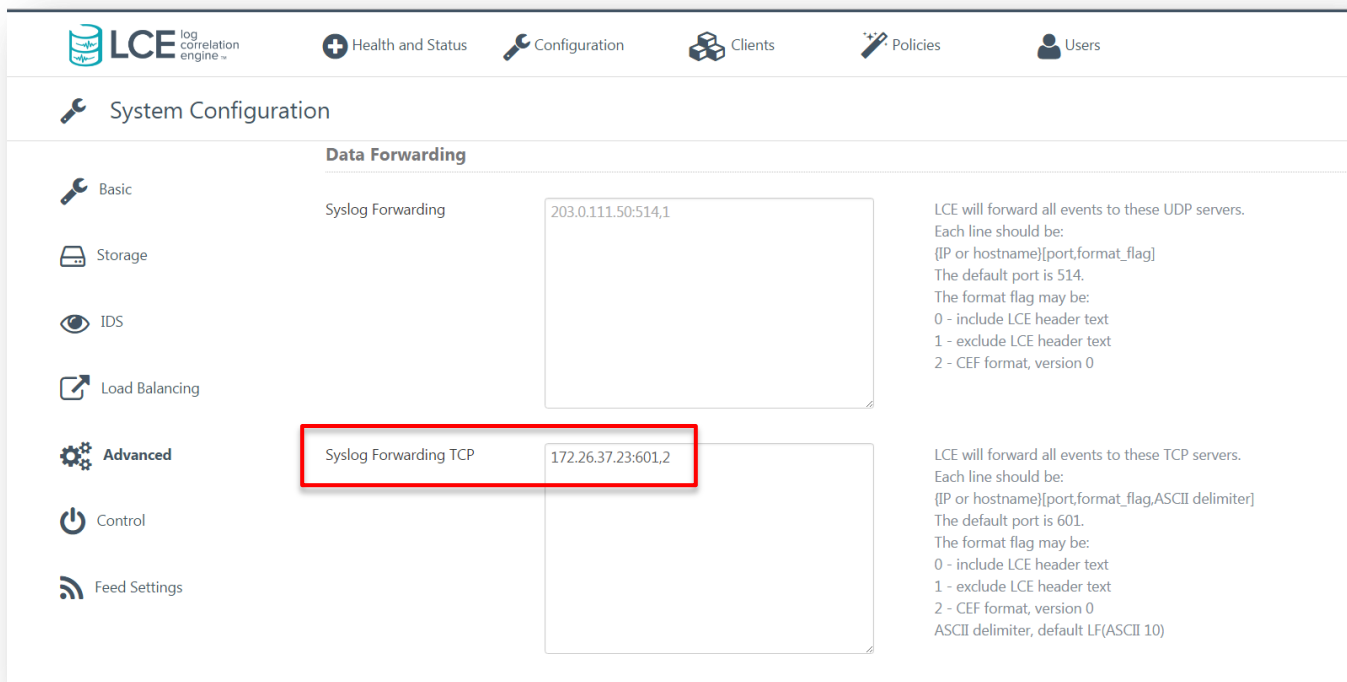


The screenshot shows the LCE web interface with the "System Configuration" page. The top navigation bar is the same as in the previous screenshot. The left-hand menu includes "Basic", "Storage", "IDS", "Load Balancing", "Advanced" (highlighted with a red box), "Control", and "Feed Settings". The main content area displays configuration fields for various services.

Category	Field Name	Value	Description
Basic	Server Address	<input type="text"/>	An IPv4 address, i.e. 203.0.113.0 By default LCE listens on all addresses.
IDS	LCE Client Port	31300	[1-65535] Usually 31300
Load Balancing	UDP Syslog Port	514	[1-65535] Usually 514
	TCP Syslog Port	601	[1-65535] Usually 601
	Encrypted TCP Syslog Listen Port	6514	[1-65535] Usually 6514
Control	SNMP Port	162	[1-65535] Usually 162
Feed Settings	Include Networks	<input type="text"/>	A series of IPv4/CIDR filters: 203.0.0/16 192.0.2.0/24 A single IP address: 192.0.2.23/32

Scroll down until you reach the “Data Forwarding” section and enter the IP address or hostname of the Splunk server, the port number, and the format flag (e.g., 172.26.37.23:601,2 as shown in the screenshot below) in the “Syslog Forwarding TCP” section. The format flag can be set as 0 (include LCE header text), 1 (exclude LCE header text), or 2 (CEF format).

Tenable recommends using format flag “2”, which sends the logs to Splunk in the Common Event Format (CEF), and prevents having to create new parsing rules. To use this format, download the “[Splunk CEFUtils Add-on](#)” from SplunkBase (login required) and install it on your Splunk Enterprise instance. Installation and configuration instructions are included on the download page.



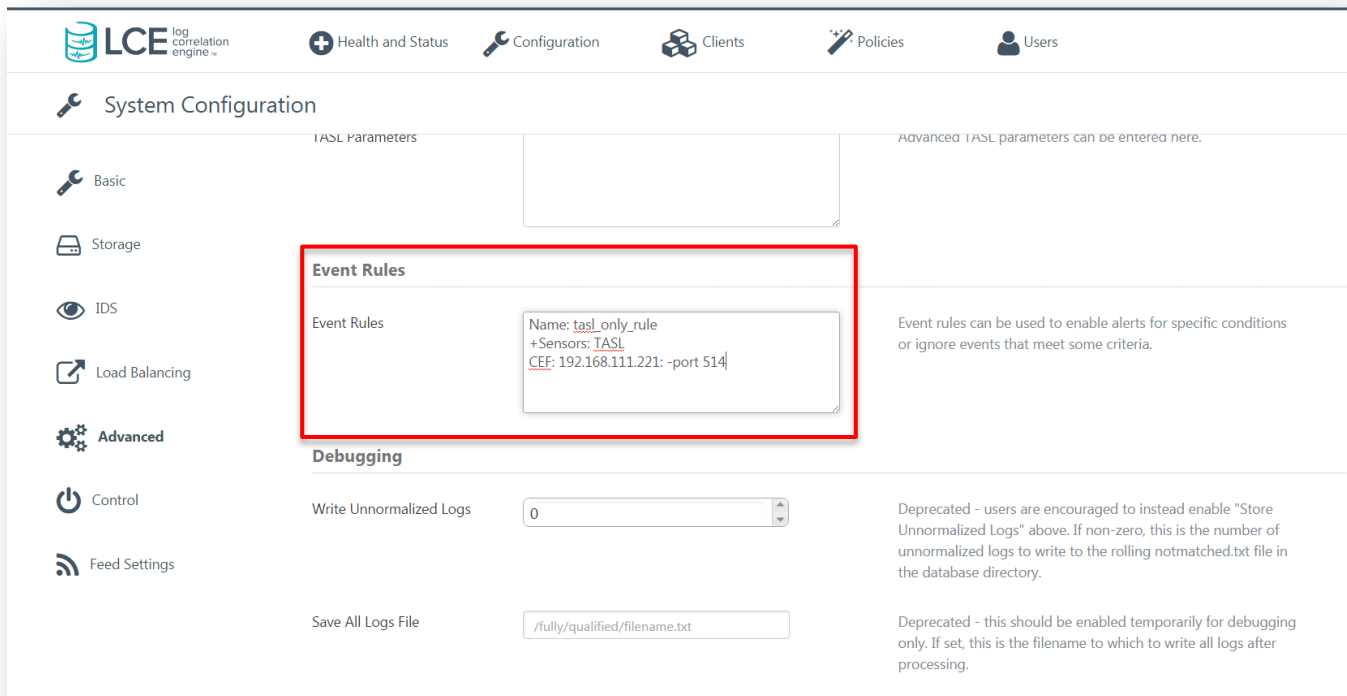
After entering the Splunk server information, scroll to the bottom of the window and click “**Update**” to save changes.



Note: While Splunk Enterprise can be configured to accept syslog data on any TCP or UDP port, Splunk recommends using TCP. The default TCP port is 610, but can be changed to a different port that suits your environment. Please refer to the “[Getting Data In](#)” document by Splunk for more details.

LCE can also be configured to send only selected events to Splunk through the use of “Event Rules”. “Event Rules” are located in the “Advanced” section of the “Configuration” menu.

In the example below, the “Event Rule” is set to filter on the sensor name “TASL”. Once the rule is applied, LCE will only send those related events to Splunk.



For more detailed instructions on creating “Event Rules”, refer to the [LCE 4.8 User Guide](#).

If you encounter any issues with Splunk installation or configuration, or have any feature requests for this integration, contact Splunk Support.

About Tenable Network Security

Tenable Network Security transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the U.S. Department of Defense, to mid-sized and small businesses in all sectors, including finance, government, healthcare, higher education, retail, and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring, by visiting tenable.com.