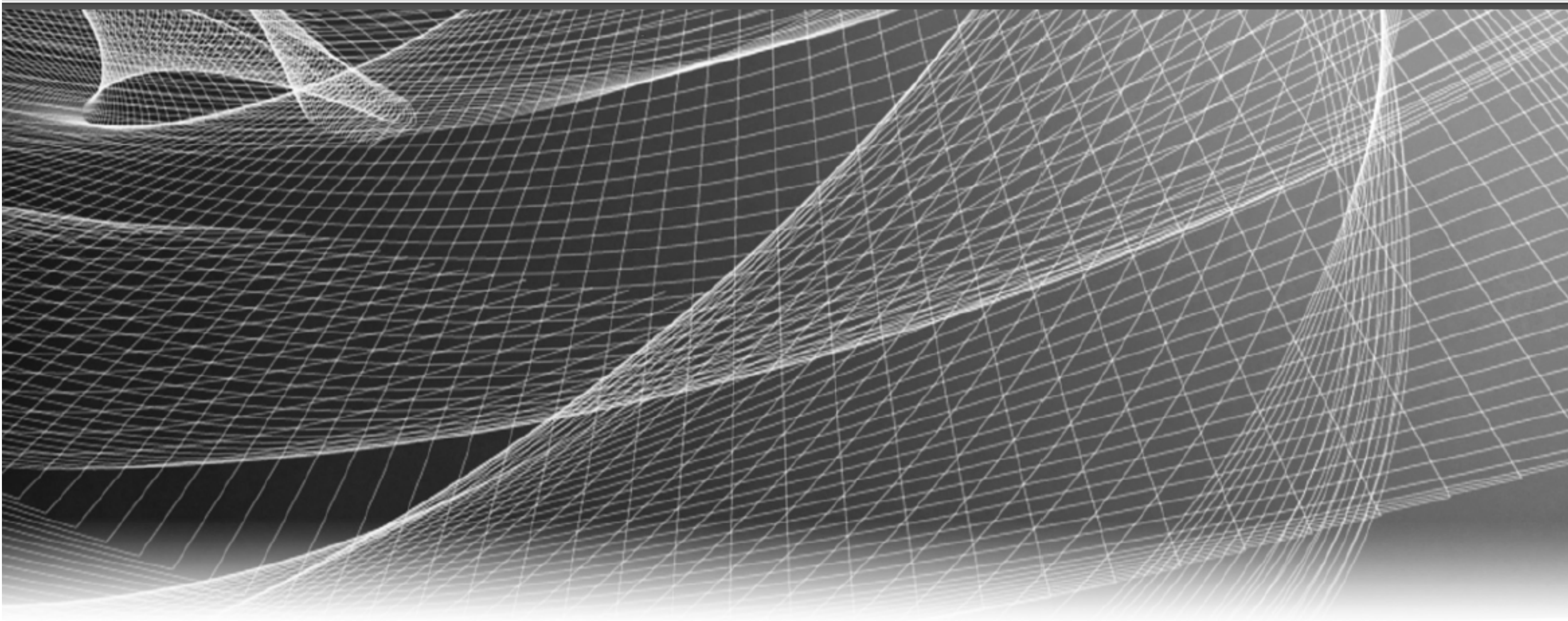


RSA Security Analytics

Splunk Integration

Copyright © 2017 EMC Corporation. All Rights Reserved.

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of EMC trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm.

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by EMC.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed in the thirdpartylicenses.pdf file.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license. EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Contents

RSA Security Analytics Integration with Splunk

Splunk captures, indexes and correlates real-time data in a searchable repository from which it can generate graphs, reports, alerts, dashboards and visualizations.

These integrations allow customers with Security Analytics and Splunk the ability to forward relevant data between the systems as well as pivot from one to the other in order to improve an investigation’s workflow.

The Splunk package is delivered as a ZIP archive that contains the components for the different integration points. You download the file from RSA Link. You can find the package on the RSA Link Downloads space here.

Additionally, the source is supplied in this document, in the Appendix: Source Code section.

Currently, the following integration points are supported on Security Analytics 10.6:

- RSA Security Analytics Context Actions Integration
- Forward Security/Audit Logs to Splunk
- Splunk to RSA Security Analytics Integration
- Forward ESA Alert Syslog Notifications to Splunk
- Forward Security/RE Logs to Splunk

RSA Security Analytics Context Actions Integration

The Security Analytics/Splunk integration enables analysts to pivot from meta information in Security Analytics to the Splunk search screen with source IP and/or destination IP data from a Security Analytics Investigation screen used as the starting drill-point into the Splunk dataset. This enables focused, time-based searches of the Splunk dataset instead of broad IP-only searches.

We use the context actions integration to configure RSA Security Analytics-to-Splunk integration. Each of the integrations provide a different field or result in Splunk. The general context action allows searching for the meta key value from Security Analytics in any message in Splunk (no field context). The rest are specific for the meta key from Security Analytics. For example, using the **Search Splunk - Source IP** action looks up the `SRC` key in Splunk.

Complete Integration Procedure

The overview of the entire process is:

I. Add a Context Menu Action in Security Analytics.

II. Using the Integration from the Security Analytics Investigation screen to:

- Select a meta value that is part of the integration (source IP, destination IP, or hostname),
- Use the context sensitive menu (right-click) to open a Splunk browser window. This window opens to the Splunk search screen, already searching for the meta key value that you selected in Security Analytics.

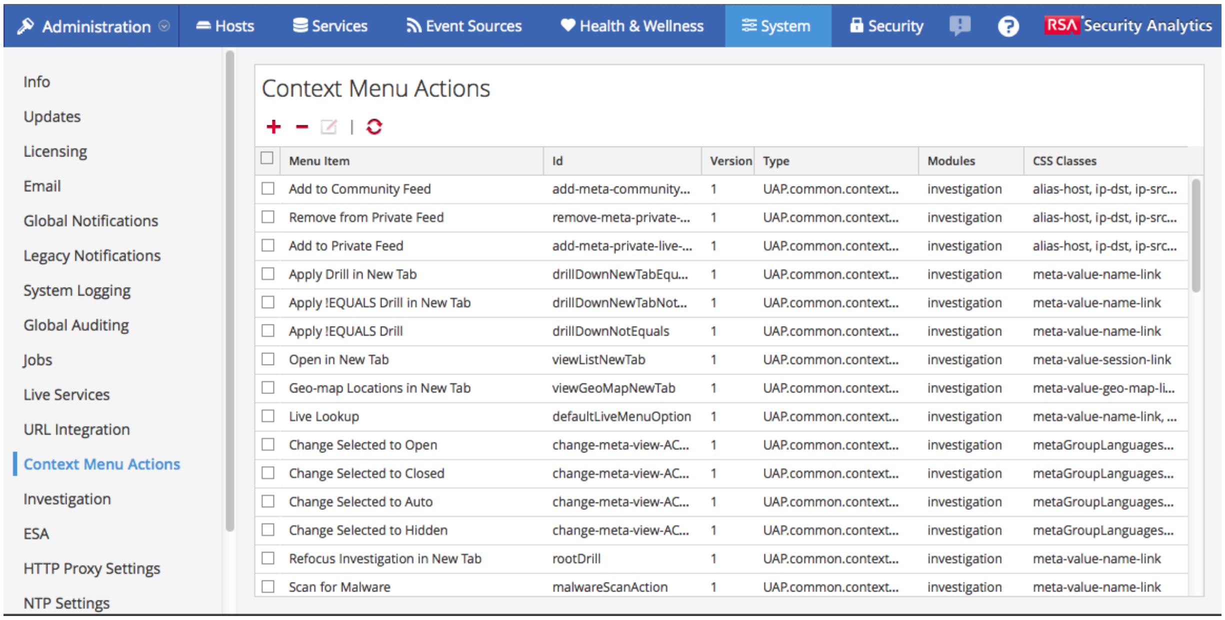
The following section walks through an example using the Source IP integration.

Note: You will need to repeat the procedure for the other available context menu actions (destination IP, hostname, and general).

Add a Context Menu Action

This procedure walks through adding the Search Splunk - Source IP context menu action in Security Analytics.

1. Log into Security Analytics.
2. Navigate to the **Context Menu Actions**.
   a. In the Security Analytics menu, select **Administration** > **System**.
   b. In the options panel, select **Context Menu Actions**.



Context Menu Actions

□	Menu Item	Id	Version	Type	Modules	CSS Classes
□	Add to Community Feed	add-meta-community...	1	UAP.common.context...	investigation	alias-host, ip-dst, ip-src...
□	Remove from Private Feed	remove-meta-private-...	1	UAP.common.context...	investigation	alias-host, ip-dst, ip-src...
□	Add to Private Feed	add-meta-private-live-...	1	UAP.common.context...	investigation	alias-host, ip-dst, ip-src...
□	Apply Drill in New Tab	drillDownNewTabEqu...	1	UAP.common.context...	investigation	meta-value-name-link
□	Apply !EQUALS Drill in New Tab	drillDownNewTabNot...	1	UAP.common.context...	investigation	meta-value-name-link
□	Apply !EQUALS Drill	drillDownNotEquals	1	UAP.common.context...	investigation	meta-value-name-link
□	Open in New Tab	viewListNewTab	1	UAP.common.context...	investigation	meta-value-session-link
□	Geo-map Locations in New Tab	viewGeoMapNewTab	1	UAP.common.context...	investigation	meta-value-geo-map-li...
□	Live Lookup	defaultLiveMenuOption	1	UAP.common.context...	investigation	meta-value-name-link, ...
□	Change Selected to Open	change-meta-view-AC...	1	UAP.common.context...	investigation	metaGroupLanguages...
□	Change Selected to Closed	change-meta-view-AC...	1	UAP.common.context...	investigation	metaGroupLanguages...
□	Change Selected to Auto	change-meta-view-AC...	1	UAP.common.context...	investigation	metaGroupLanguages...
□	Change Selected to Hidden	change-meta-view-AC...	1	UAP.common.context...	investigation	metaGroupLanguages...
□	Refocus Investigation in New Tab	rootDrill	1	UAP.common.context...	investigation	meta-value-name-link
□	Scan for Malware	malwareScanAction	1	UAP.common.context...	investigation	meta-value-name-link

3. Add the Splunk Context Menu Action.

   a. In the toolbar, click +.

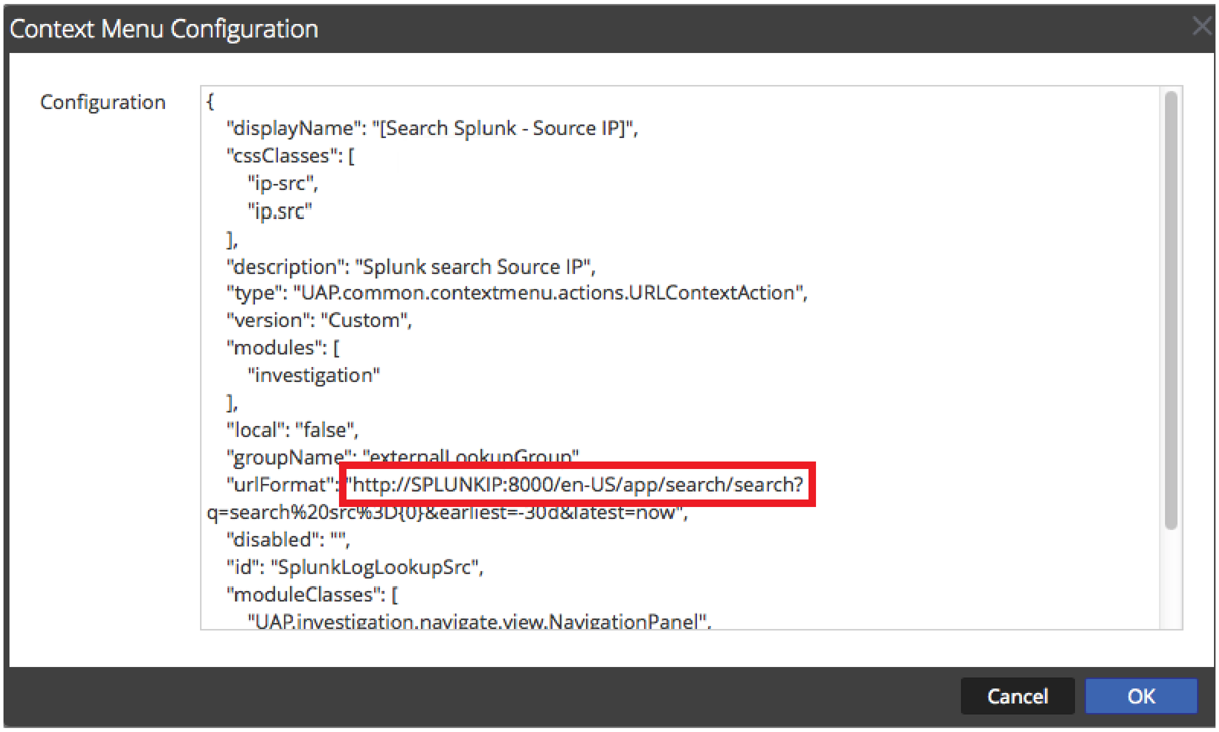
   b. The following text represents the code for the Source IP context action.

   > **Note:** To copy the source into Security Analytics, use the code listing in the Appendix: Source Code section.

```
{
      "displayName": "[Search Splunk - Source IP]",
      "cssClasses": [
         "ip-src",
         "ip.src"
      ],

      "description": "Splunk search Source IP",
      "type": "UAP.common.contextmenu.actions.URLContextAction",
      "version": "Custom",
      "modules": [
         "investigation"
      ],

      "local": "false",
      "groupName": "externalLookupGroup",
      "urlFormat": "http://SPLUNKIP:8000/en-
      US/app/search/search?q=search%20src%3D{0}&earliest=-30d&latest=now",
      "disabled": "",
      "id": "SplunkLogLookupSrc",
      "moduleClasses": [
         "UAP.investigation.navigate.view.NavigationPanel",
         "UAP.investigation.events.view.EventGrid"
```

```
        ],
        "openInNewTab": "true"

  }
```

The screen should look similar to this (without the red box):



```
{
   "displayName": "[Search Splunk - Source IP]",
   "cssClasses": [
      "ip-src",
      "ip.src"
   ],
   "description": "Splunk search Source IP",
   "type": "UAP.common.contextmenu.actions.URLContextAction",
   "version": "Custom",
   "modules": [
      "investigation"
   ],
   "local": "false",
   "groupName": "externalLookupGroup",
   "urlFormat": "http://SPLUNKIP:8000/en-US/app/search/search?
q=search%20src%3D{0}&earliest=-30d&latest=now",
   "disabled": "",
   "id": "SplunkLogLookupSrc",
   "moduleClasses": [
      "UAP.investigation.navigate.view.NavigationPanel",
```

c. Edit the following line (shown outlined in red in the image above), replacing **SPLUNKIP** with the IP address of your Splunk server:

```
"urlFormat": "http://SPLUNKIP:8000/en-US/app/search/search?
```

For example:

```
"urlFormat": "http://10.100.32.8:8000/en-US/app/search/search?
```

Note: If you are using SSL, change **http** to **https**.

d. **Optional**. If your source, destination, and hostname meta keys in Splunk are not named **src**, **dest**, and **hostname** respectively, then you need to update the context actions language to match your meta keys.

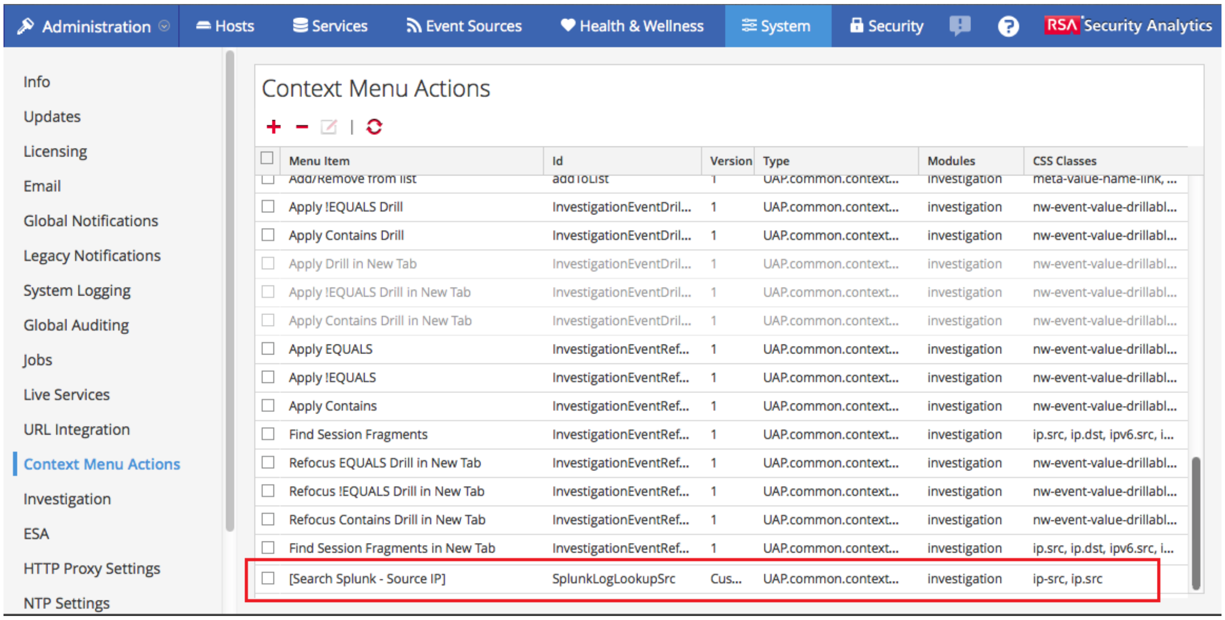
For example, in the above code, note the following line:

```
"urlFormat": "http://SPLUNKIP:8000/en-US/app/search/search?q=search%20src%3D
```

If your source IP meta key in Splunk is not named **src**, replace **src** in the line above with the actual name of your meta key.

e. Click OK.

The context menu action is added to the end of the list, as shown below (outlined in red):



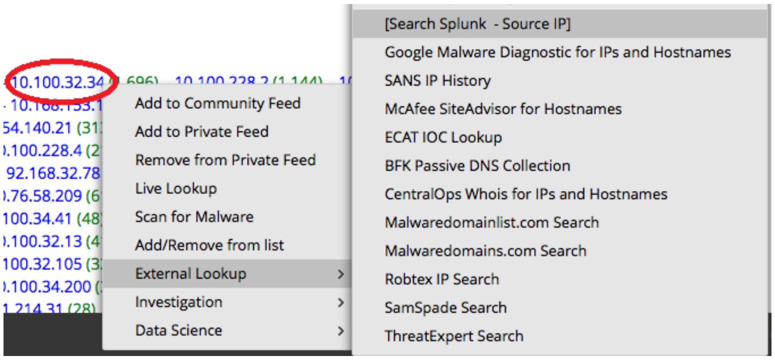
Context Menu Actions

□	Menu Item	Id	Version	Type	Modules	CSS Classes
□	Add/Remove from list	addToList	1	UAP.common.context...	investigation	meta-value-name-link, ...
□	Apply !EQUALS Drill	InvestigationEventDril...	1	UAP.common.context...	investigation	nw-event-value-drillabl...
□	Apply Contains Drill	InvestigationEventDril...	1	UAP.common.context...	investigation	nw-event-value-drillabl...
□	Apply Drill in New Tab	InvestigationEventDril...	1	UAP.common.context...	investigation	nw-event-value-drillabl...
□	Apply !EQUALS Drill in New Tab	InvestigationEventDril...	1	UAP.common.context...	investigation	nw-event-value-drillabl...
□	Apply Contains Drill in New Tab	InvestigationEventDril...	1	UAP.common.context...	investigation	nw-event-value-drillabl...
□	Apply EQUALS	InvestigationEventRef...	1	UAP.common.context...	investigation	nw-event-value-drillabl...
□	Apply !EQUALS	InvestigationEventRef...	1	UAP.common.context...	investigation	nw-event-value-drillabl...
□	Apply Contains	InvestigationEventRef...	1	UAP.common.context...	investigation	nw-event-value-drillabl...
□	Find Session Fragments	InvestigationEventRef...	1	UAP.common.context...	investigation	ip.src, ip.dst, ipv6.src, i...
□	Refocus EQUALS Drill in New Tab	InvestigationEventRef...	1	UAP.common.context...	investigation	nw-event-value-drillabl...
□	Refocus !EQUALS Drill in New Tab	InvestigationEventRef...	1	UAP.common.context...	investigation	nw-event-value-drillabl...
□	Refocus Contains Drill in New Tab	InvestigationEventRef...	1	UAP.common.context...	investigation	nw-event-value-drillabl...
□	Find Session Fragments in New Tab	InvestigationEventRef...	1	UAP.common.context...	investigation	ip.src, ip.dst, ipv6.src, i...
□	[Search Splunk - Source IP]	SplunkLogLookupSrc	Cus...	UAP.common.context...	investigation	ip-src, ip.src

Using the Integration

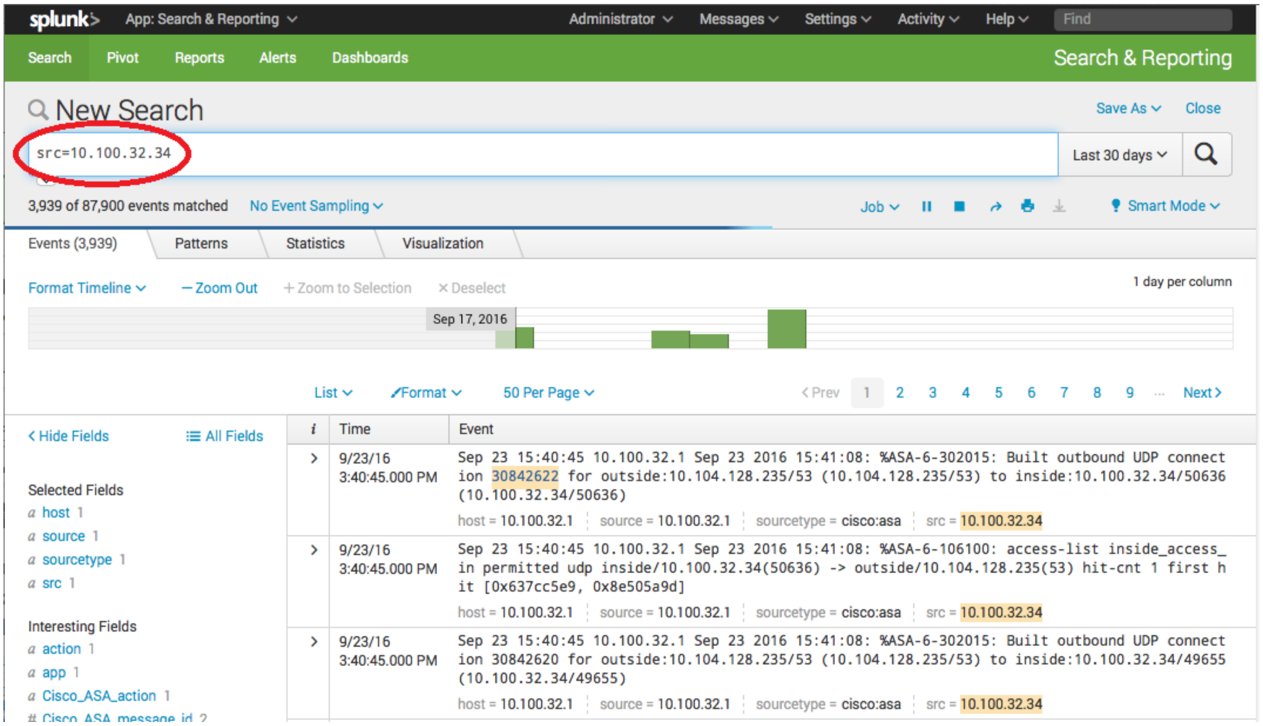
This section walks through how to view the meta in the Splunk interface.

1. Log into Security Analytics.
2. In the Security Analytics menu, select **Investigation** > **Navigate**.
3. Select an event that has values for the source IP (**ip.src**) meta key.
4. Right click on a meta key value (these are in blue text, with the selected address circled in red) in the Source IP Address key, and select **External Lookup** > **Search Splunk - Source IP** from the menu:



5. The Splunk application launches and executes a search against the IP address you selected. Note that the IP address in the Splunk search field matches the meta key value in the Security Analytics Investigation

view that you selected.



```
src=10.100.32.34
```

3,939 of 87,900 events matched

i	Time	Event
>	9/23/16 3:40:45.000 PM	Sep 23 15:40:45 10.100.32.1 Sep 23 2016 15:41:08: %ASA-6-302015: Built outbound UDP connection 30842622 for outside:10.104.128.235/53 (10.104.128.235/53) to inside:10.100.32.34/50636 (10.100.32.34/50636) host = 10.100.32.1 source = 10.100.32.1 sourcetype = cisco:asa src = 10.100.32.34
>	9/23/16 3:40:45.000 PM	Sep 23 15:40:45 10.100.32.1 Sep 23 2016 15:41:08: %ASA-6-106100: access-list inside_access_in permitted udp inside/10.100.32.34(50636) -> outside/10.104.128.235(53) hit-cnt 1 first hit [0x637cc5e9, 0x8e505a9d] host = 10.100.32.1 source = 10.100.32.1 sourcetype = cisco:asa src = 10.100.32.34
>	9/23/16 3:40:45.000 PM	Sep 23 15:40:45 10.100.32.1 Sep 23 2016 15:41:08: %ASA-6-302015: Built outbound UDP connection 30842620 for outside:10.104.128.235/53 (10.104.128.235/53) to inside:10.100.32.34/49655 (10.100.32.34/49655) host = 10.100.32.1 source = 10.100.32.1 sourcetype = cisco:asa src = 10.100.32.34

Forward Security/Audit Logs to Splunk

You can forward the RSA Security Analytics security (audit) logs to Splunk.

How it Works

RSA uses Global Audit Logging feature to send the security logs to the Splunk Syslog server that you specify from the Global Audit Logging screen in Security Analytics.

These are the steps required to send Security Analytics audit logs to Splunk:

I. Set Splunk as a Syslog Notification Server

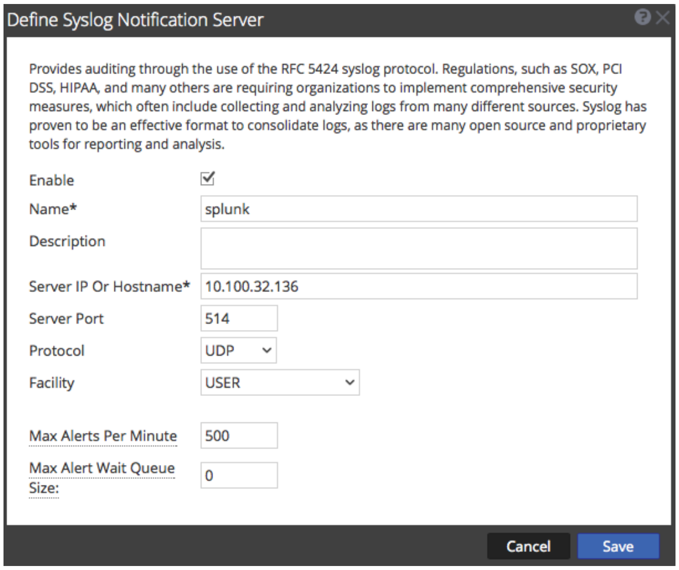
II. Add a New Configuration to Global Audit Logging

Set Splunk as a Syslog Notification Server

Set Splunk as a Global Notification Server

1. In the **Security Analytics** menu, select **Administration > System**.
2. In the options panel, select **Global Notifications**.
3. Click the **Servers** tab.
4. From the + ⌄ drop-down menu, select **Syslog**.

   The **Define Syslog Notification Server** dialog is displayed.



Define Syslog Notification Server

Provides auditing through the use of the RFC 5424 syslog protocol. Regulations, such as SOX, PCI DSS, HIPAA, and many others are requiring organizations to implement comprehensive security measures, which often include collecting and analyzing logs from many different sources. Syslog has proven to be an effective format to consolidate logs, as there are many open source and proprietary tools for reporting and analysis.

Enable	☑
Name*	splunk
Description	
Server IP Or Hostname*	10.100.32.136
Server Port	514
Protocol	UDP
Facility	USER
Max Alerts Per Minute	500
Max Alert Wait Queue Size:	0

5. Configure the Syslog notification server as described in the following table.

Field	Description
Enable	Select to enable the notification server.
Name	A name to identify or label the Splunk syslog server.
Description	(Optional) A brief description of the notification server.
Server IP or Hostname	The Splunk server hostname or IP address.
Server Port	For the port, use the value that you configured Splunk to listen on for Syslog.
Protocol	Select UDP.
Facility	Select USER for the syslog facility.

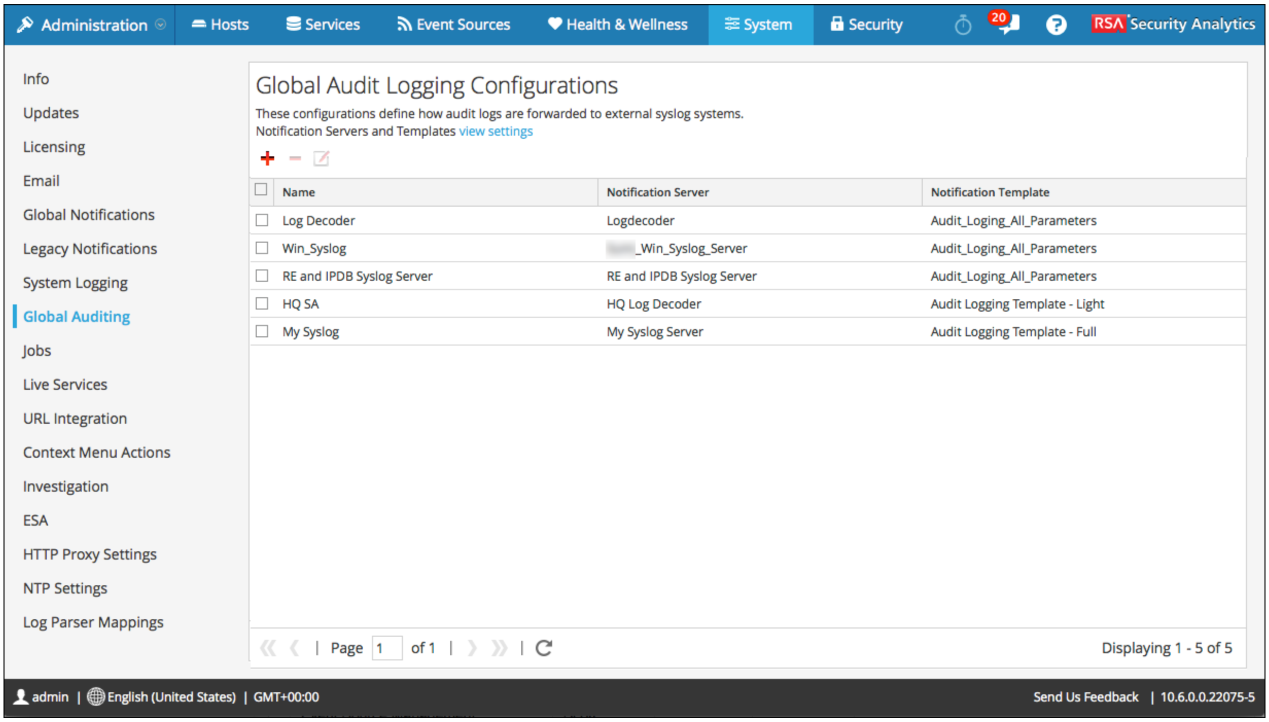
Note: The **Max Alerts Per Minute** and **Max Alert Wait Queue Size** fields are not used for Global Audit Logging.

6. Click **Save**.

Add a New Configuration to Global Audit Logging

1. In the **Security Analytics** menu, select **Administration > System**.
2. In the options panel, select **Global Auditing**.

   The **Global Audit Logging Configurations** panel is displayed.



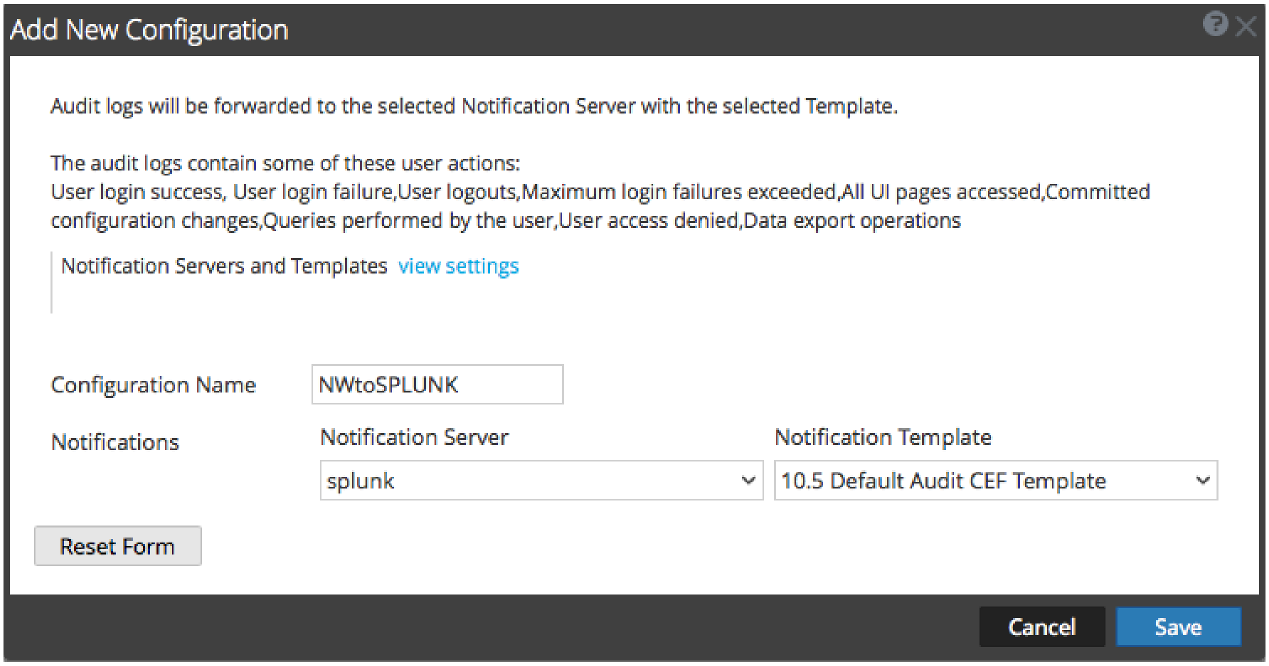
Global Audit Logging Configurations

These configurations define how audit logs are forwarded to external syslog systems.
Notification Servers and Templates view settings

☐	Name	Notification Server	Notification Template
☐	Log Decoder	Logdecoder	Audit_Loging_All_Parameters
☐	Win_Syslog	[redacted]_Win_Syslog_Server	Audit_Loging_All_Parameters
☐	RE and IPDB Syslog Server	RE and IPDB Syslog Server	Audit_Loging_All_Parameters
☐	HQ SA	HQ Log Decoder	Audit Logging Template - Light
☐	My Syslog	My Syslog Server	Audit Logging Template - Full

3. Click ✚ to add a global audit logging configuration.

   The **Add New Configuration** dialog is displayed.



Add New Configuration

Audit logs will be forwarded to the selected Notification Server with the selected Template.

The audit logs contain some of these user actions:
User login success, User login failure,User logouts,Maximum login failures exceeded,All UI pages accessed,Committed configuration changes,Queries performed by the user,User access denied,Data export operations

Notification Servers and Templates view settings

Configuration Name: NWtoSPLUNK

Notifications
Notification Server: splunk
Notification Template: 10.5 Default Audit CEF Template

4. In the **Configuration Name** field, type a unique name for the global audit logging configuration.

5. In the **Notifications** section, select the syslog **Notification Server** to use for this configuration. Use the global notification server that you created when you Set Splunk as a Syslog Notification Server.
6. For the **Notification Template**, select the **10.5 Default Audit CEF Template**.
7. Click **Save**.

Splunk to RSA Security Analytics Integration

The Splunk/Security Analytics integration enables analysts to pivot from meta information in Splunk to the Security Analytics Investigation screen. The source IP and/or destination IP data from the Splunk dataset is used as starting drill-point into Security Analytics.

RSA uses the Splunk built in functions for Workflow actions to enable right click ability to pivot into Security Analytics, with parameters injected to search for the equivalent data in Security Analytics.

Limitations

When pivoting from Splunk to Security Analytics, note that the most recent, one year's worth of data is queried against. Depending on how much data you have in Security Analytics, this query can take a while to run.

This limitation is due to the way that Splunk stores the Month value; Splunk represents the Month value as text, while Security Analytics requires a digit. As a result, retrieving data for a shorter duration cannot be accomplished at this time.

Complete Integration Procedure

The overview of the entire process is:

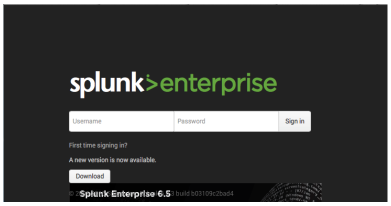
I. Install the App in Splunk

II. Configure Splunk to Point to Security Analytics

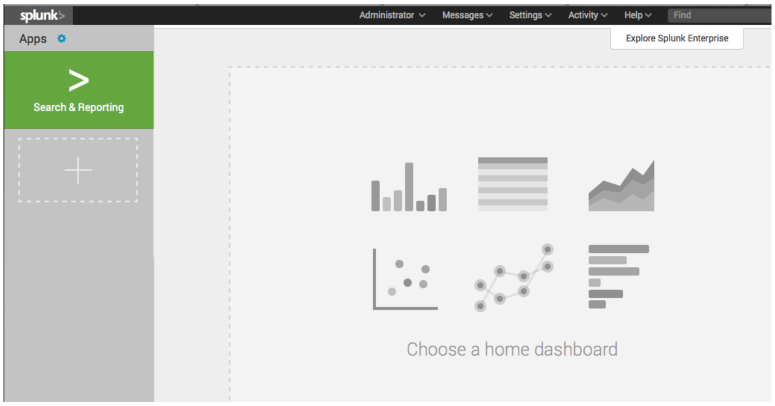
III. Use the Integration

Install the App in Splunk

1. Download the RSA Security Analytics Splunk app to a location that is accessible to the Splunk web interface. RSA distributes this file as a compressed TAR file, **Splunk_RSA_SecurityAnalytics.tar.gz** in the RSA Link Downloads space.
2. Log into Splunk.

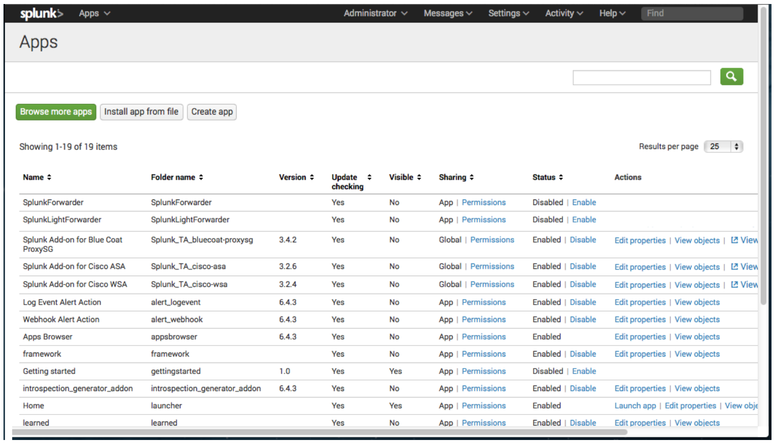


You will see the main Splunk screen:



3. Select **Apps** > ⚙ (Manage Apps).

The following screen is displayed:

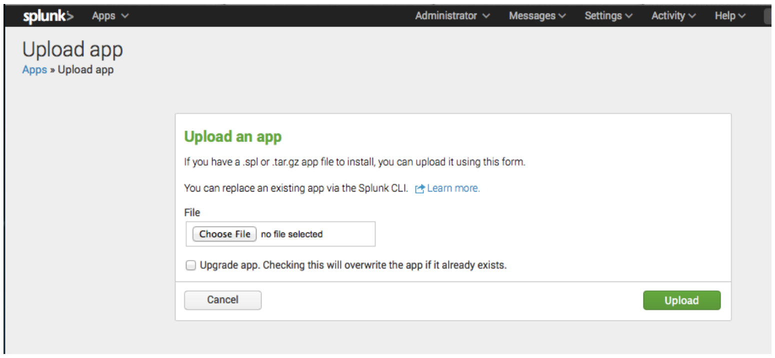


Apps

Showing 1-19 of 19 items

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	
Splunk Add-on for Blue Coat ProxySG	Splunk_TA_bluecoat-proxysg	3.4.2	Yes	No	Global | Permissions	Enabled | Disable	Edit properties | View objects | View
Splunk Add-on for Cisco ASA	Splunk_TA_cisco-asa	3.2.6	Yes	No	Global | Permissions	Enabled | Disable	Edit properties | View objects | View
Splunk Add-on for Cisco WSA	Splunk_TA_cisco-wsa	3.2.4	Yes	No	Global | Permissions	Enabled | Disable	Edit properties | View objects | View
Log Event Alert Action	alert_logevent	6.4.3	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
Webhook Alert Action	alert_webhook	6.4.3	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
Apps Browser	appsbrowser	6.4.3	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	6.4.3	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
Home	launcher		Yes	Yes	App | Permissions	Enabled	Launch app | Edit properties | View obje
learned	learned		Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects

4. Select **Install app from file**.



Upload app

Apps » Upload app

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

Choose File no file selected

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

5. Browse to the RSA Security Analytics Splunk App file (**Splunk_RSA_SecurityAnalytics.tar.gz**).

6. Click **Upload**.

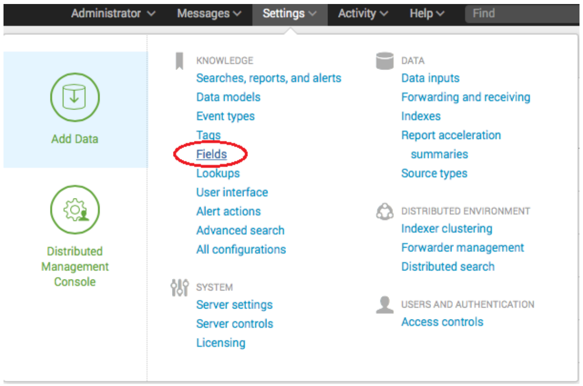
The Apps page will show all of Splunk’s installed applications.

Once installation has been completed, the user will be brought back to the Apps page where they will see that RSA Security Analytics Analytics App is now listed as an installed App.

Configure Splunk to Point to Security Analytics

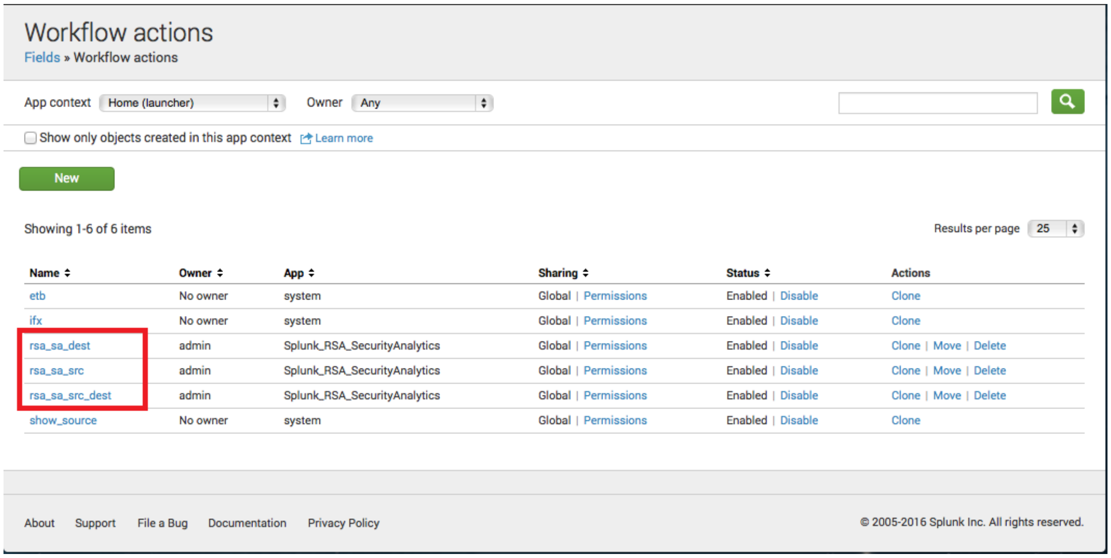
You must update settings in Splunk to point to your Security Analytics server.

1. From the Splunk top navigation menu, select **Settings** > **Fields**.



2. Select **Workflow actions**.

   Your screen should look similar to the following:


Workflow actions
Fields » Workflow actions
App context Home (launcher)
Owner Any
□ Show only objects created in this app context
Learn more
New
Results per page 25
About
Support
File a Bug
Documentation
Privacy Policy
© 2005-2016 Splunk Inc. All rights reserved.

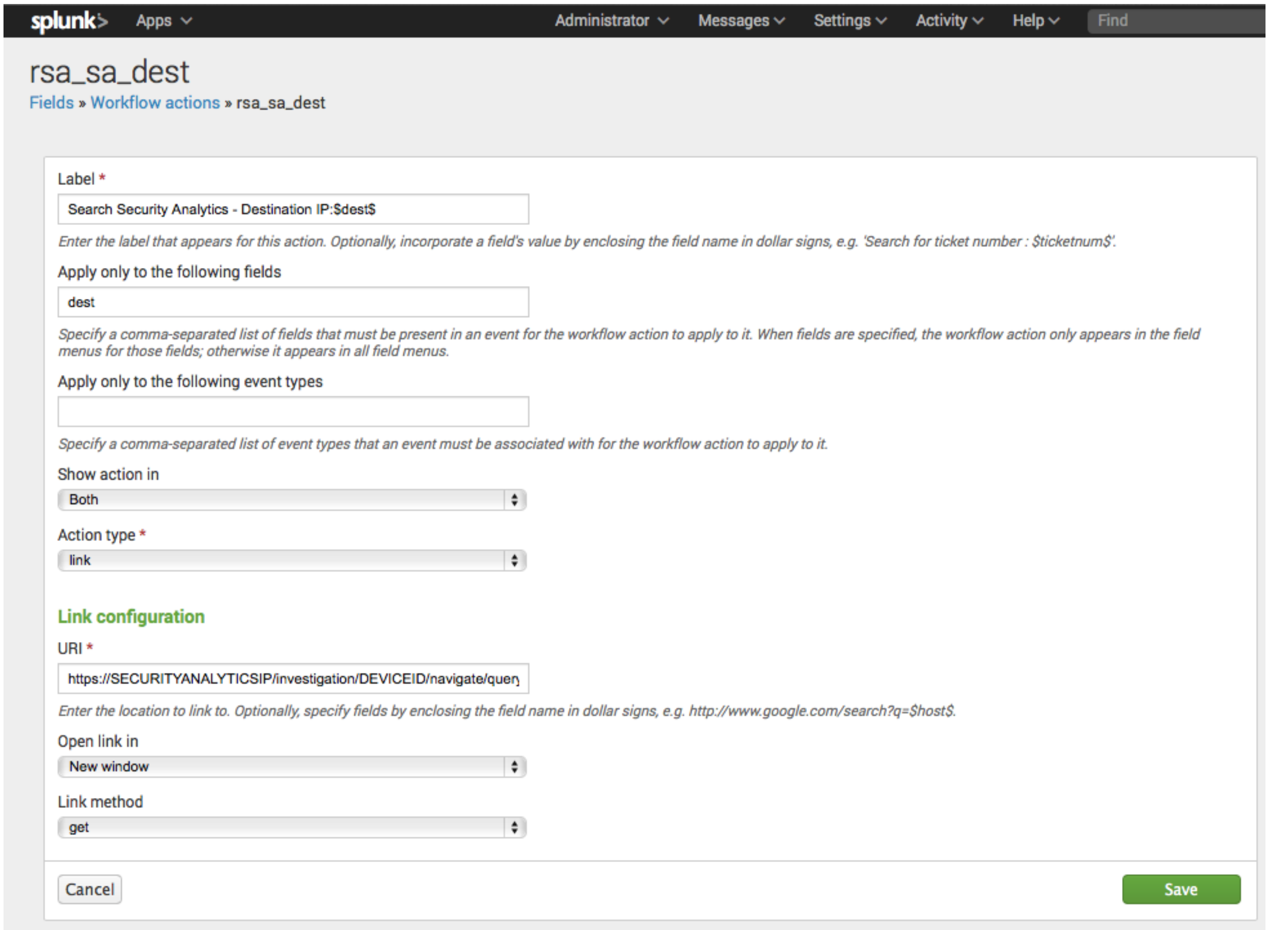
Showing 1-6 of 6 items

Name	Owner	App	Sharing	Status	Actions
etb	No owner	system	Global | Permissions	Enabled | Disable	Clone
ifx	No owner	system	Global | Permissions	Enabled | Disable	Clone
rsa_sa_dest	admin	Splunk_RSA_SecurityAnalytics	Global | Permissions	Enabled | Disable	Clone | Move | Delete
rsa_sa_src	admin	Splunk_RSA_SecurityAnalytics	Global | Permissions	Enabled | Disable	Clone | Move | Delete
rsa_sa_src_dest	admin	Splunk_RSA_SecurityAnalytics	Global | Permissions	Enabled | Disable	Clone | Move | Delete
show_source	No owner	system	Global | Permissions	Enabled | Disable	Clone

You need to edit all three of the workflow actions that begin with **rsa**:

- rsa_sa_dest
- rsa_sa_src
- rsa_sa_src_dest

3. Select one of the rsa actions to open the Workflow Actions properties screen. The following image shows the screen for **rsa_sa_dest**:



rsa_sa_dest

Fields » Workflow actions » rsa_sa_dest

Label *

Search Security Analytics - Destination IP:$dest$

Enter the label that appears for this action. Optionally, incorporate a field's value by enclosing the field name in dollar signs, e.g. 'Search for ticket number : $ticketnum$'.

Apply only to the following fields

dest

Specify a comma-separated list of fields that must be present in an event for the workflow action to apply to it. When fields are specified, the workflow action only appears in the field menus for those fields; otherwise it appears in all field menus.

Apply only to the following event types

Specify a comma-separated list of event types that an event must be associated with for the workflow action to apply to it.

Show action in

Both

Action type *

link

Link configuration

URI *

https://SECURITYANALYTICSIP/investigation/DEVICEID/navigate/quer

Enter the location to link to. Optionally, specify fields by enclosing the field name in dollar signs, e.g. http://www.google.com/search?q=$host$.

Open link in

New window

Link method

get

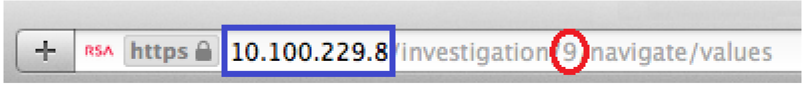
4. Make sure the field name in the **Apply only to the following fields** is set to the field that is in your event (**dest** for this example).

5. In the URI field, update two strings:

   - Replace **SECURITYANALYTICSIP** with the IP address or hostname of your Security Analytics server.

   - Replace **DEVICEID** with your Security Analytics device ID. To find your device ID, log into Security Analytics and select Investigation from the Security Analytics menu.

   The following screen shows both the IP (surrounded by a blue rectangle) and the device ID surrounded by a red circle):

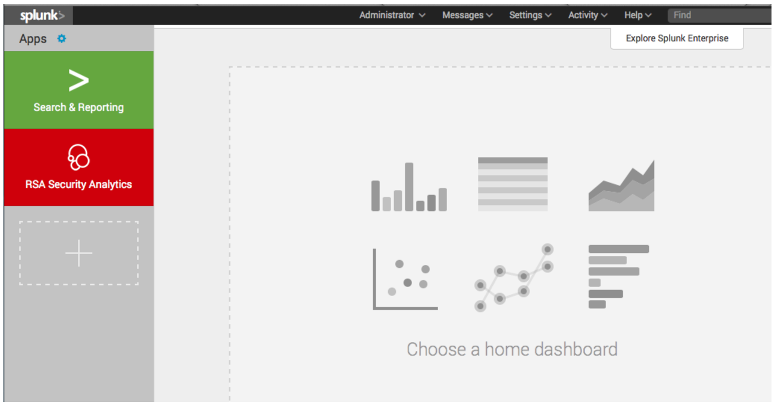


https 10.100.229.8/investigation/9/navigate/values

6. Repeat the process for the other workflow actions, **rsa_sa_src** and **rsa_sa_src_dest**.

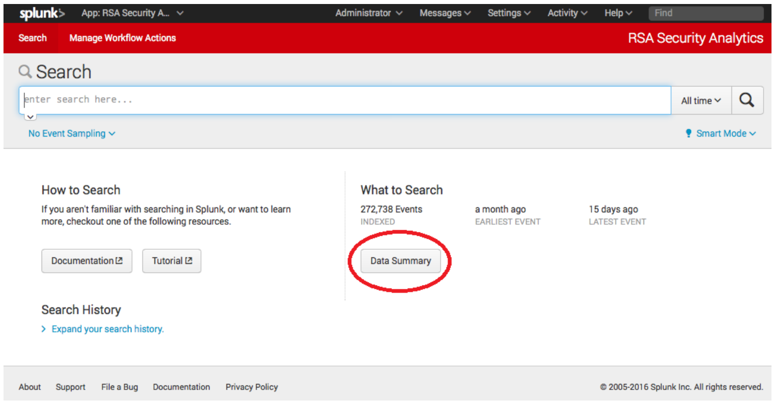
Use the Integration

1. Log into Splunk, or just return to the main screen:



Note the new menu item for RSA Security Analytics.

2. Select RSA Security Analytics.
3. Click **Data Summary**.



How to Search

If you aren't familiar with searching in Splunk, or want to learn more, checkout one of the following resources.

What to Search

272,738 Events INDEXED

a month ago EARLIEST EVENT

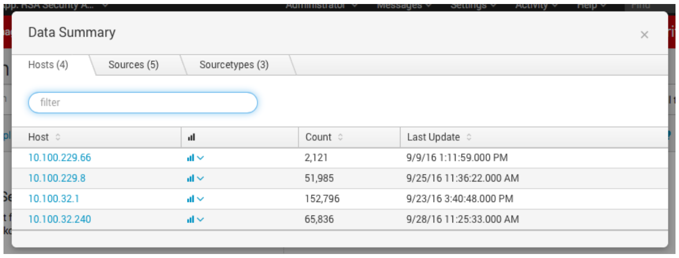
15 days ago LATEST EVENT

Search History

Expand your search history.

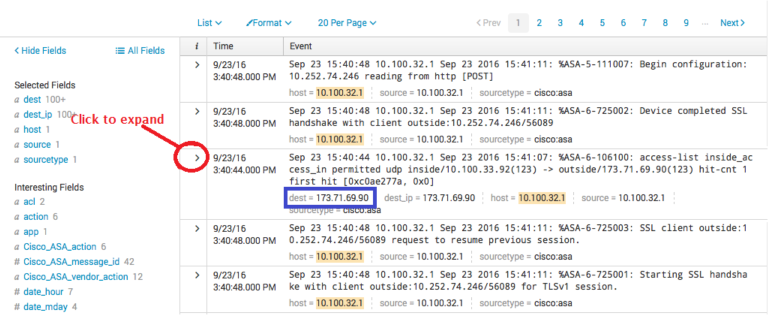
© 2005-2016 Splunk Inc. All rights reserved.

4. Select one of the values in the **Host** column.



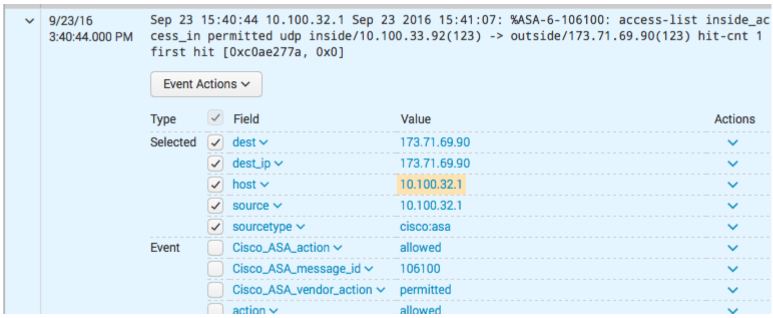
Host		Count	Last Update
10.100.229.66		2,121	9/9/16 1:11:59.000 PM
10.100.229.8		51,985	9/25/16 11:36:22.000 AM
10.100.32.1		152,796	9/23/16 3:40:48.000 PM
10.100.32.240		65,836	9/28/16 11:25:33.000 AM

5. All the fields for that entry are displayed:



i	Time	Event
>	9/23/16 3:40:48.000 PM	Sep 23 15:40:48 10.100.32.1 Sep 23 2016 15:41:11: %ASA-5-111007: Begin configuration: 10.252.74.246 reading from http [POST] host = 10.100.32.1 source = 10.100.32.1 sourcetype = cisco:asa
>	9/23/16 3:40:48.000 PM	Sep 23 15:40:48 10.100.32.1 Sep 23 2016 15:41:11: %ASA-6-725002: Device completed SSL handshake with client outside:10.252.74.246/56089 host = 10.100.32.1 source = 10.100.32.1 sourcetype = cisco:asa
>	9/23/16 3:40:44.000 PM	Sep 23 15:40:44 10.100.32.1 Sep 23 2016 15:41:07: %ASA-6-106100: access-list inside_access_in permitted udp inside/10.100.33.92(123) -> outside/173.71.69.90(123) hit-cnt 1 first hit [0xc0ae277a, 0x0] dest = 173.71.69.90 dest_ip = 173.71.69.90 host = 10.100.32.1 source = 10.100.32.1 sourcetype = cisco:asa
>	9/23/16 3:40:48.000 PM	Sep 23 15:40:48 10.100.32.1 Sep 23 2016 15:41:11: %ASA-6-725003: SSL client outside:10.252.74.246/56089 request to resume previous session. host = 10.100.32.1 source = 10.100.32.1 sourcetype = cisco:asa
>	9/23/16 3:40:48.000 PM	Sep 23 15:40:48 10.100.32.1 Sep 23 2016 15:41:11: %ASA-6-725001: Starting SSL handshake with client outside:10.252.74.246/56089 for TLSv1 session. host = 10.100.32.1 source = 10.100.32.1 sourcetype = cisco:asa

6. Choose an event that has a value for source, destination, or hostname, and click the > to expand the details.

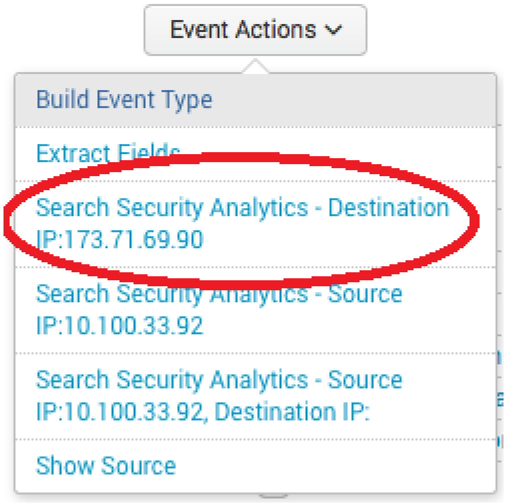


9/23/16
3:40:44.000 PM

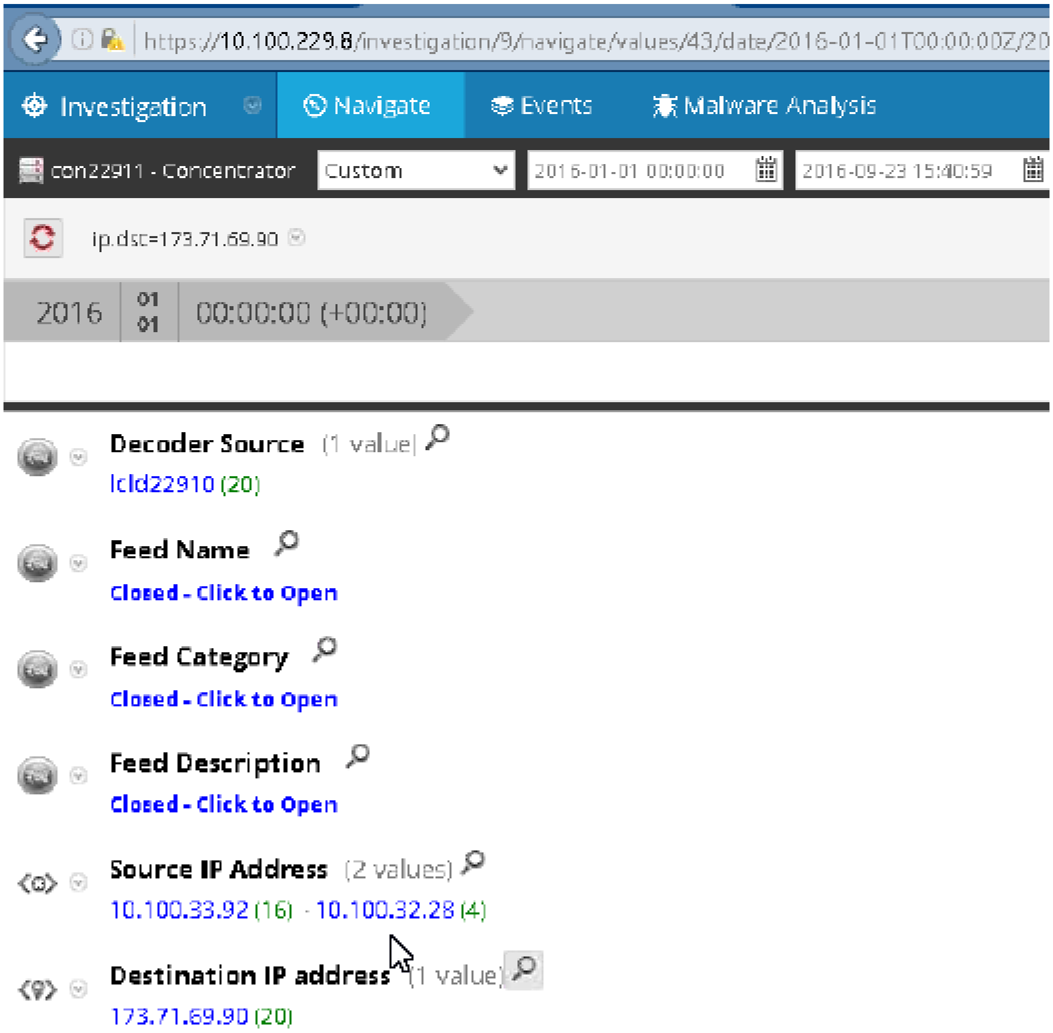
```
Sep 23 15:40:44 10.100.32.1 Sep 23 2016 15:41:07: %ASA-6-106100: access-list inside_ac
cess_in permitted udp inside/10.100.33.92(123) -> outside/173.71.69.90(123) hit-cnt 1
first hit [0xc0ae277a, 0x0]
```

Type	☑	Field	Value	Actions
Selected	☑	dest	173.71.69.90	⌄
	☑	dest_ip	173.71.69.90	⌄
	☑	host	10.100.32.1	⌄
	☑	source	10.100.32.1	⌄
	☑	sourcetype	cisco:asa	⌄
Event	□	Cisco_ASA_action	allowed	⌄
	□	Cisco_ASA_message_id	106100	⌄
	□	Cisco_ASA_vendor_action	permitted	⌄
	□	action	allowed	⌄

7. Click Event Actions, then choose one of the Security Analytics actions. In this example, we are choosing **Search Security Analytics - Destination**:


Event Actions
Build Event Type
Extract Fields
Search Security Analytics - Destination IP:173.71.69.90
Search Security Analytics - Source IP:10.100.33.92
Search Security Analytics - Source IP:10.100.33.92, Destination IP:
Show Source

The Investigation screen opens in Security Analytics.



https://10.100.229.8/investigation/9/navigate/values/43/date/2016-01-01T00:00:00Z/20
Investigation
Navigate
Events
Malware Analysis

con22911 - Concentrator | Custom | 2016-01-01 00:00:00 | 2016-09-23 15:40:59

ip.dst=173.71.69.90

2016 01 01 00:00:00 (+00:00)

Decoder Source (1 value)
lcld22910 (20)

Feed Name
Closed - Click to Open

Feed Category
Closed - Click to Open

Feed Description
Closed - Click to Open

Source IP Address (2 values)
10.100.33.92 (16) - 10.100.32.28 (4)

Destination IP address (1 value)
173.71.69.90 (20)

Note that the Destination IP address that we selected in Splunk is entered into the Security Analytics Drill field.

Forward ESA Alert Syslog Notifications to Splunk

You can configure RSA Security Analytics to send ESA alert notifications via Syslog to Splunk.

How it Works

In Splunk, you configure a data input to receive Syslog. In Security Analytics, you configure a Syslog notification, server, and template, then configure your ESA alerts to use that notification.

These are the steps required to send ESA alert notifications via Syslog to Splunk.

I. Configure a Splunk Data Input

II. Add Global Notification Items

   a. Define a Syslog Notification for Splunk

   b. Define a Syslog Notification Server for Splunk

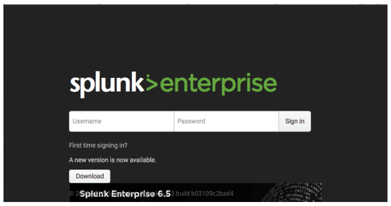
   c. Define a Syslog Template for Splunk

III. Configure Alerts to Send Logs to Splunk

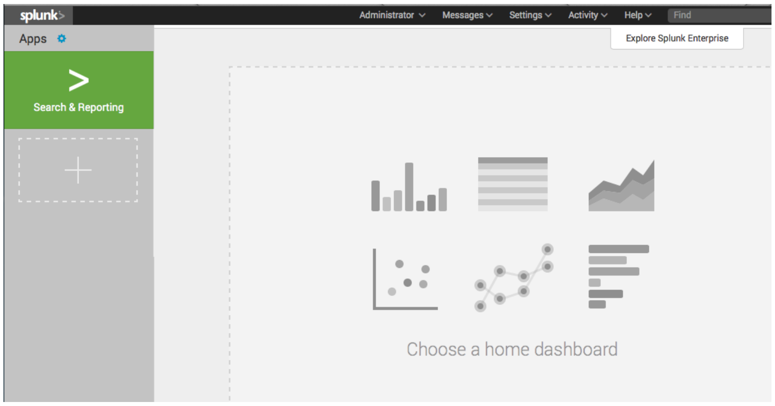
Configure a Splunk Data Input

You need to configure a Splunk data input to receive logs from RSA Security Analytics.

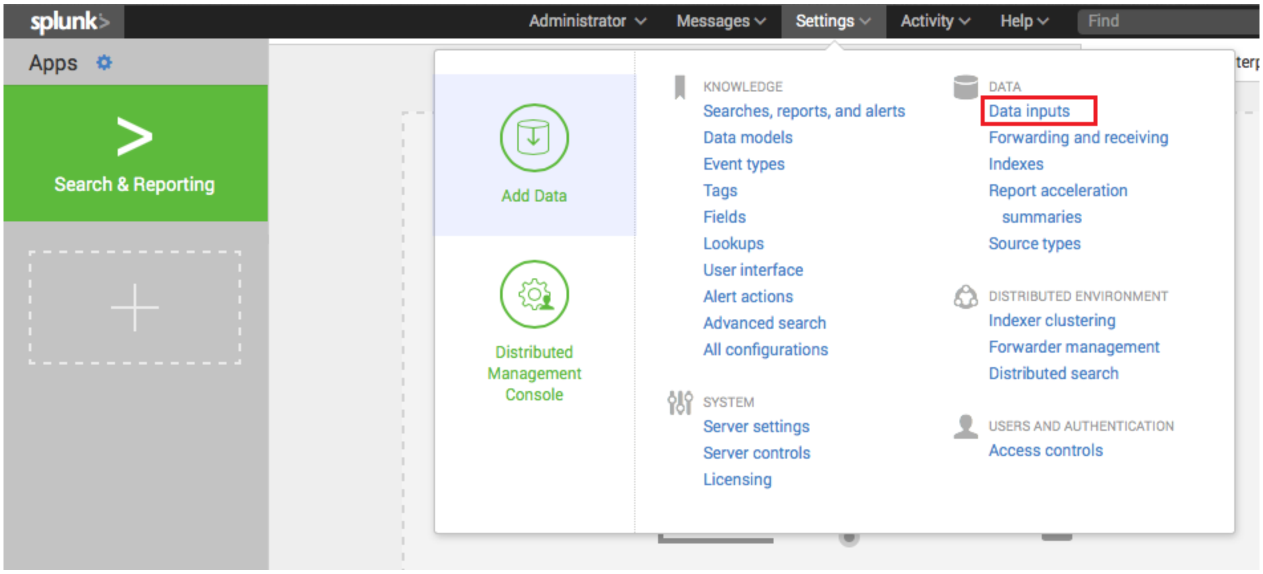
1. Log into Splunk.



   You will see the main Splunk screen:

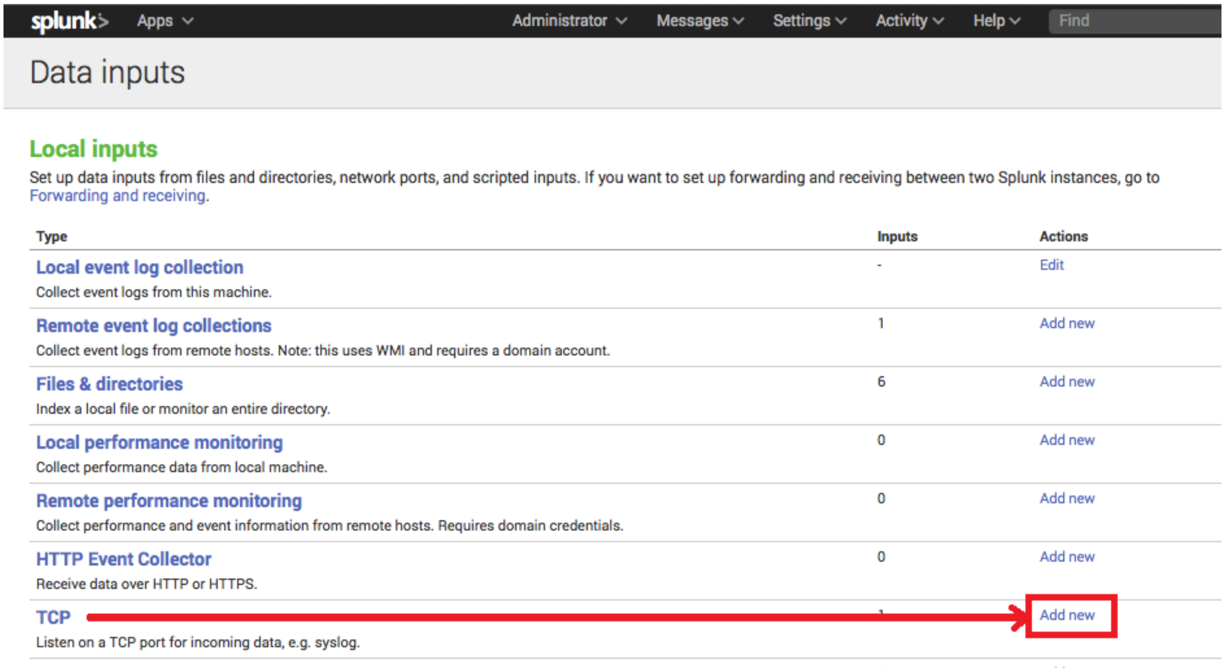


2. Select **Settings > Data Inputs**.



3. Set up a collector. In this example, we are setting up a TCP collector.

   a. Select Add new for the TCP input type.



Data inputs

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.

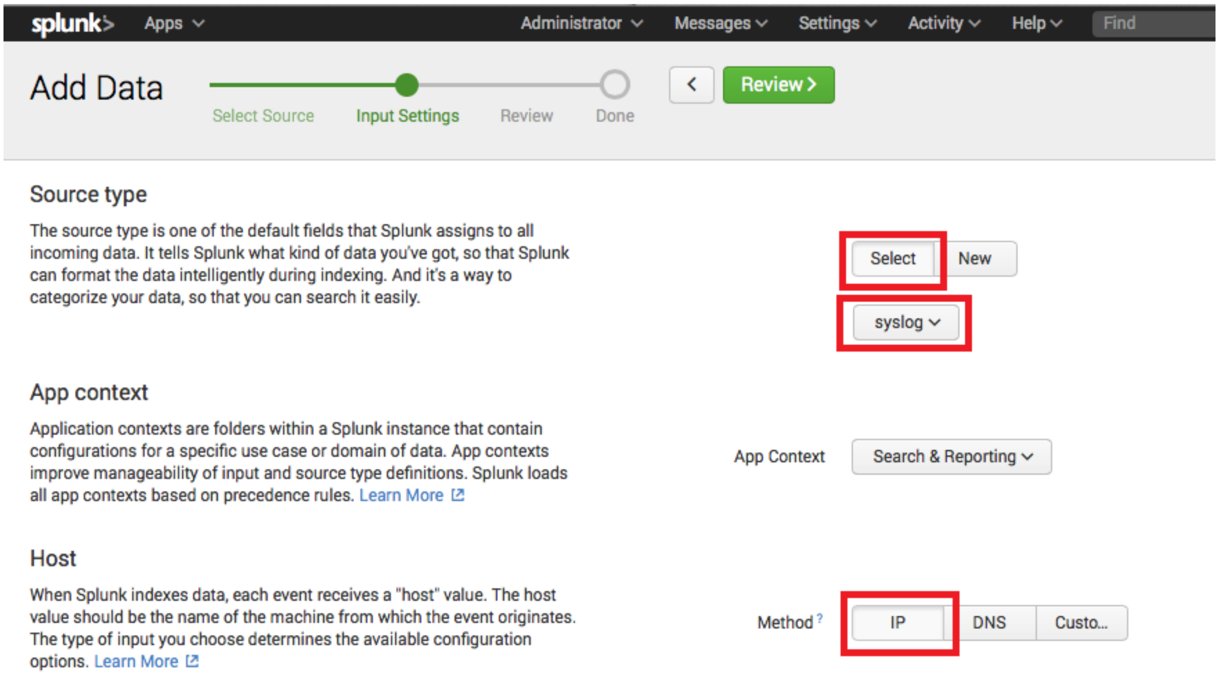
Type	Inputs	Actions
Local event log collection Collect event logs from this machine.	-	Edit
Remote event log collections Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.	1	Add new
Files & directories Index a local file or monitor an entire directory.	6	Add new
Local performance monitoring Collect performance data from local machine.	0	Add new
Remote performance monitoring Collect performance and event information from remote hosts. Requires domain credentials.	0	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.	1	Add new

   b. In the Add Source screen enter:

   - the TCP port to listen on (standard Syslog port is 514).
   - a value for **Source name override**, if desired.

   c. Click **Next**, and set the following:

   - For the **Source type**, select **syslog** from the drop-down menu.
   - For the **Host Method**, select **IP**.



Source type

The source type is one of the default fields that Splunk assigns to all incoming data. It tells Splunk what kind of data you've got, so that Splunk 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 instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. Splunk loads all app contexts based on precedence rules. Learn More

App Context: Search & Reporting

Host

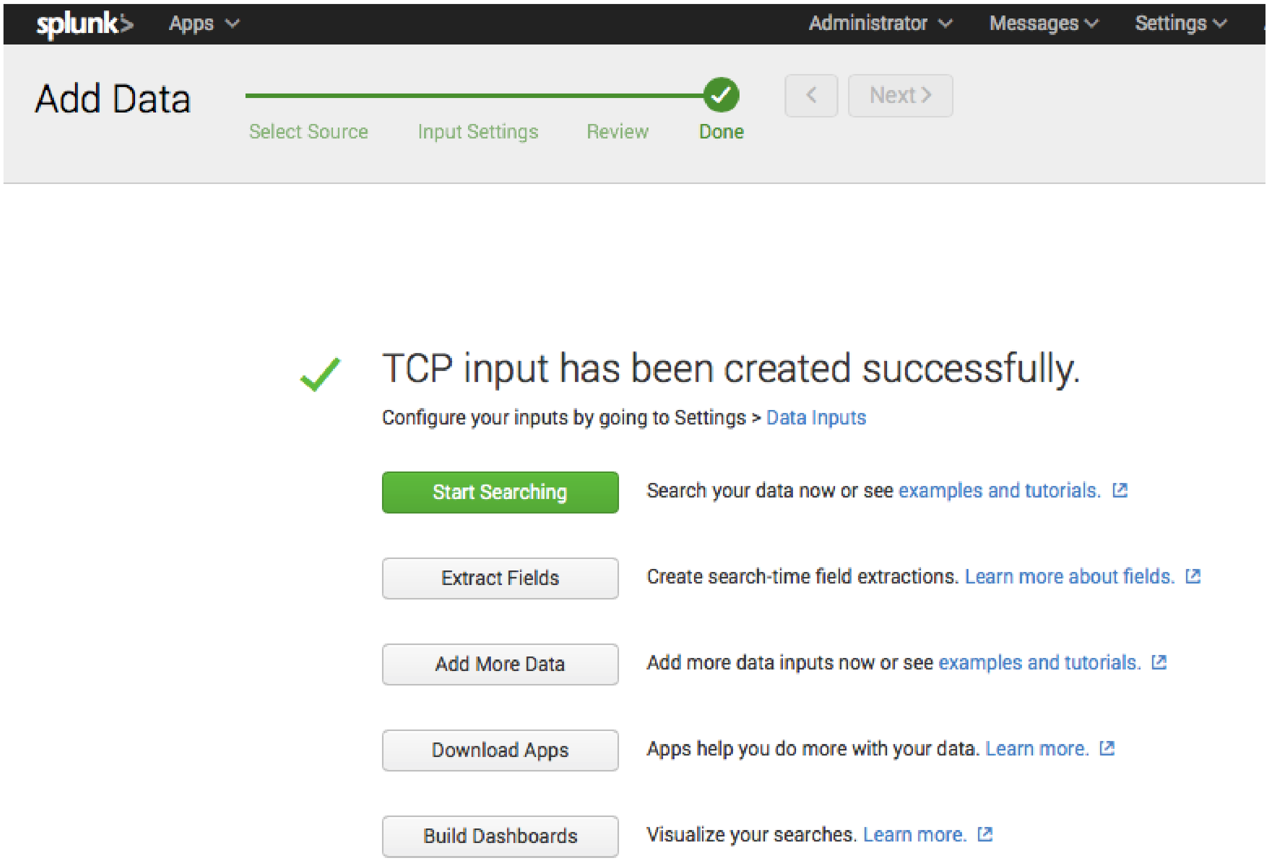
When Splunk indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More

Method: IP

d. Click **Review**.

e. Click **Submit** to create the data input. If you need to change any of your settings, click the back button (<), make your changes, and return here to submit when you are ready.

You receive confirmation that your data input was created successfully:



TCP input has been created successfully.

Configure your inputs by going to Settings > Data Inputs

Search your data now or see examples and tutorials.

Create search-time field extractions. Learn more about fields.

Add more data inputs now or see examples and tutorials.

Apps help you do more with your data. Learn more.

Visualize your searches. Learn more.

Define a Syslog Notification for Splunk

In Global Notifications, define a Syslog Notification for Splunk.

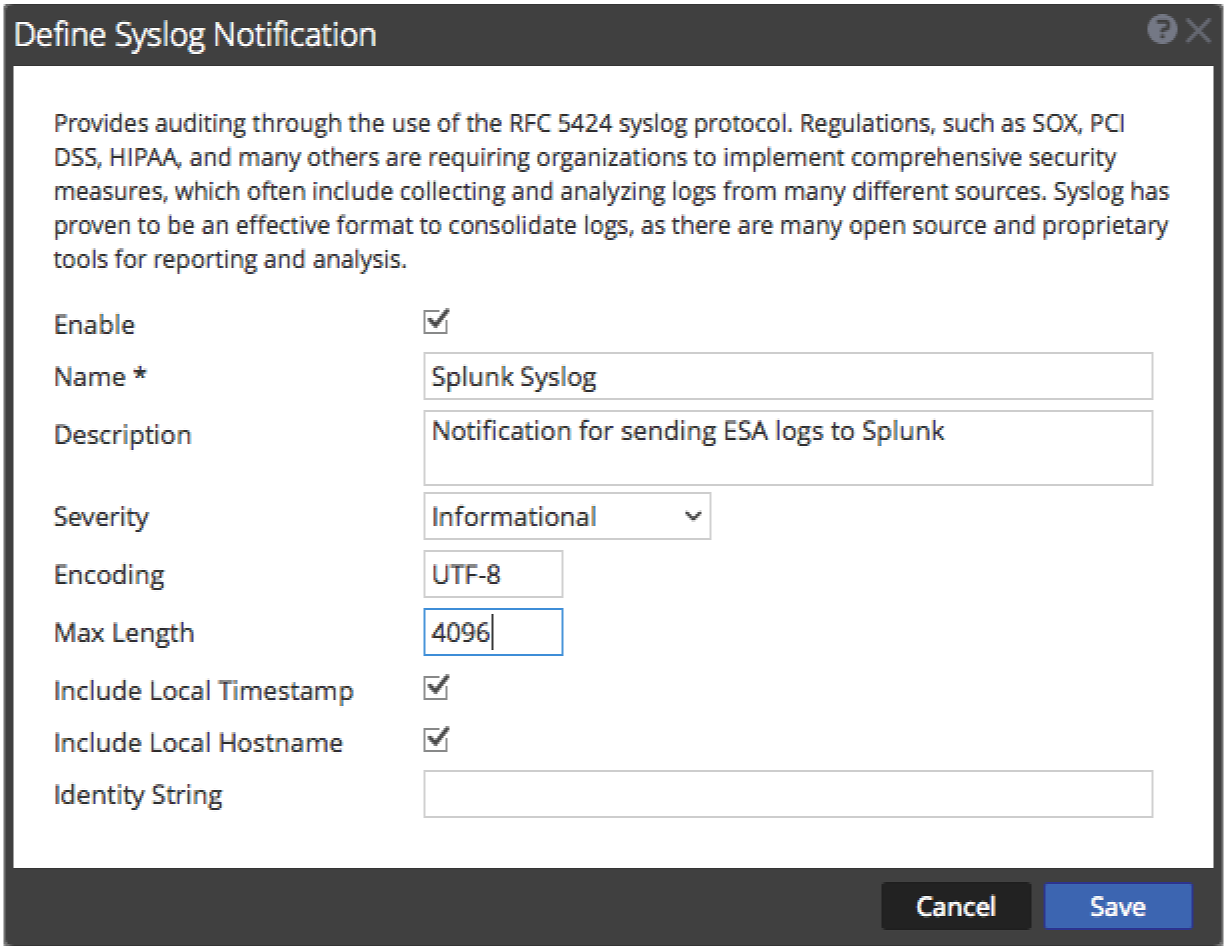
1. In the **Security Analytics** menu, select **Administration** > **System**.
2. In the options panel, select **Global Notifications**.
3. Click the **Output** tab.
4. From the + ⌄ drop-down menu, select **Syslog**.

   The **Define Syslog Notification** dialog is displayed.
5. Configure the Syslog notification server as described in the following table.

Field	Description
Enable	Select to enable the notification server.
Name	Enter a name to identify or label the Splunk notification.

Field	Description
Description	(Optional) A brief description of the Syslog notification.
Severity	Choose a severity level, based on your organization.
Encoding	Enter **UTF-8**
Max Length	RSA recommends you set this to **4096**.
Include Local Timestamp	Select to include the timestamp when sending syslog to Splunk.
Include Local Hostname	Select to include the hostname when sending syslog to Splunk.
Identity String	Leave blank.

Here is an example of this screen with data filled in:



Define Syslog Notification

Provides auditing through the use of the RFC 5424 syslog protocol. Regulations, such as SOX, PCI DSS, HIPAA, and many others are requiring organizations to implement comprehensive security measures, which often include collecting and analyzing logs from many different sources. Syslog has proven to be an effective format to consolidate logs, as there are many open source and proprietary tools for reporting and analysis.

Enable	☑
Name *	Splunk Syslog
Description	Notification for sending ESA logs to Splunk
Severity	Informational
Encoding	UTF-8
Max Length	4096
Include Local Timestamp	☑
Include Local Hostname	☑
Identity String	

6. Click **Save**.

Define a Syslog Notification Server for Splunk

In Global Notifications, define a Syslog Notification Server for Splunk.

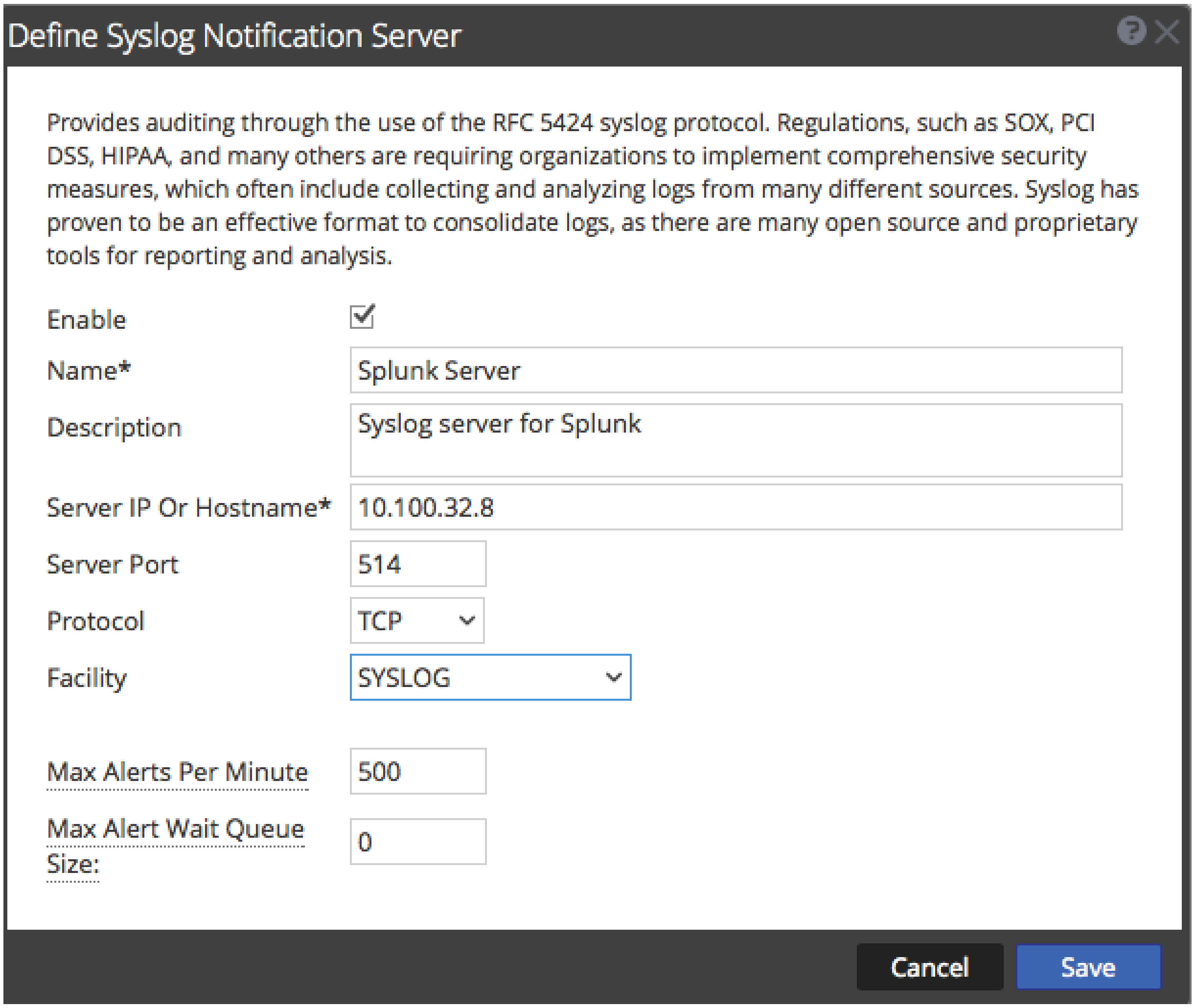
1. In the **Security Analytics** menu, select **Administration** > **System**.
2. In the options panel, select **Global Notifications**.
3. Click the **Servers** tab.
4. From the + ⌄ drop-down menu, select **Syslog**.

   The **Define Syslog Notification Server** dialog is displayed.
5. Configure the Syslog notification server as described in the following table.

Field	Description
Enable	Select to enable the notification server.
Name	A name to identify or label the Splunk syslog server.
Description	(Optional) A brief description of the notification server.
Server IP or Hostname	The Splunk server hostname or IP address.
Server Port	For the port, use the value that you configured Splunk to listen on for Syslog.
Protocol	Select TCP.
Facility	Select SYSLOG for the syslog facility.

Note: The **Max Alerts Per Minute** and **Max Alert Wait Queue Size** fields are not used for Global Audit Logging.

Here is an example of this screen with data filled in:



Define Syslog Notification Server

Provides auditing through the use of the RFC 5424 syslog protocol. Regulations, such as SOX, PCI DSS, HIPAA, and many others are requiring organizations to implement comprehensive security measures, which often include collecting and analyzing logs from many different sources. Syslog has proven to be an effective format to consolidate logs, as there are many open source and proprietary tools for reporting and analysis.

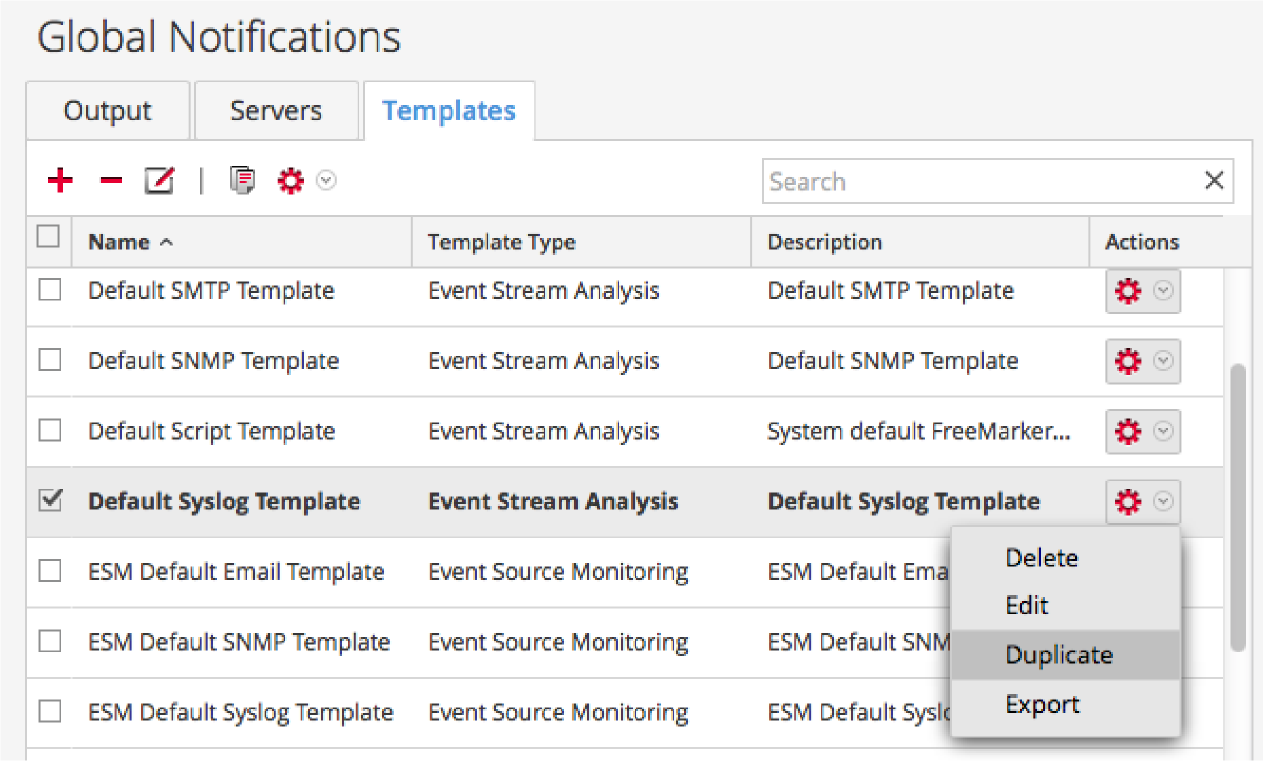
Enable	☑
Name*	Splunk Server
Description	Syslog server for Splunk
Server IP Or Hostname*	10.100.32.8
Server Port	514
Protocol	TCP
Facility	SYSLOG
Max Alerts Per Minute	500
Max Alert Wait Queue Size:	0

6. Click **Save**.

Define a Syslog Template for Splunk

In Global Notifications, define a template for Splunk.

1. In the **Security Analytics** menu, select **Administration** > **System**.
2. In the options panel, select **Global Notifications**.
3. Click the **Templates** tab.
4. From the action menu for the default Syslog template, choose **Duplicate**:



□	Name ^	Template Type	Description	Actions
□	Default SMTP Template	Event Stream Analysis	Default SMTP Template	
□	Default SNMP Template	Event Stream Analysis	Default SNMP Template	
□	Default Script Template	Event Stream Analysis	System default FreeMarker...	
☑	**Default Syslog Template**	**Event Stream Analysis**	**Default Syslog Template**	
□	ESM Default Email Template	Event Source Monitoring	ESM Default Ema	
□	ESM Default SNMP Template	Event Source Monitoring	ESM Default SNM	
□	ESM Default Syslog Template	Event Source Monitoring	ESM Default Syslo	

5. In the Duplicate Alert Template Name field, enter a name for the template, then click OK.

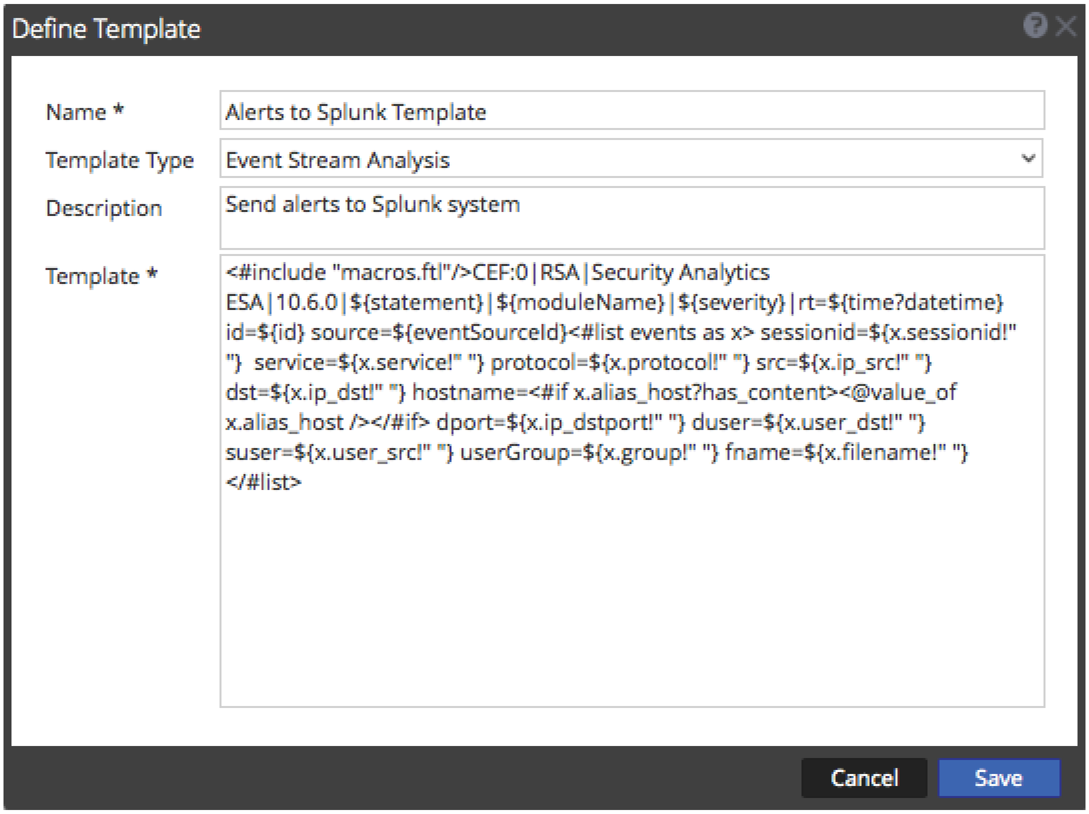
   The new template is added to the list of templates.

6. Add a Description, and then paste in the text listed below (or copy it from the file that you downloaded from RSA Link).

```
<#include "macros.ftl"/>CEF:0|RSA|Security Analytics
ESA|10.6.0|${statement}|${moduleName}|${severity}|rt=${time?datetime} id=${id}
source=${eventSourceId}<#list events as x> sessionid=${x.sessionid!" "}
service=${x.service!" "} protocol=${x.protocol!" "} src=${x.ip_src!" "} dst=${x.ip_dst!"
"} hostname=<#if x.alias_host?has_content><@value_of x.alias_host /></#if> dport=${x.ip_
dstport!" "} duser=${x.user_dst!" "}  suser=${x.user_src!" "} userGroup=${x.group!" "}
fname=${x.filename!" "} </#list>
```

Note: If pasting the above text into an editor, combine the text into a single line by replacing all new lines with spaces. The text is also available in the Code for ESA Alerts Notification Template section of the Appendix.

Here is the template that we have defined:



Name * Alerts to Splunk Template

Template Type Event Stream Analysis

Description Send alerts to Splunk system

Template *

```
<#include "macros.ftl"/>CEF:0|RSA|Security Analytics
ESA|10.6.0|${statement}|${moduleName}|${severity}|rt=${time?datetime}
id=${id} source=${eventSourceId}<#list events as x> sessionid=${x.sessionid!"
"}  service=${x.service!" "} protocol=${x.protocol!" "} src=${x.ip_src!" "}
dst=${x.ip_dst!" "} hostname=<#if x.alias_host?has_content><@value_of
x.alias_host /></#if> dport=${x.ip_dstport!" "} duser=${x.user_dst!" "}
suser=${x.user_src!" "} userGroup=${x.group!" "} fname=${x.filename!" "}
</#list>
```

7. **Optional**. Depending on the alerts in your system, you can add or remove fields to the template text listed above.

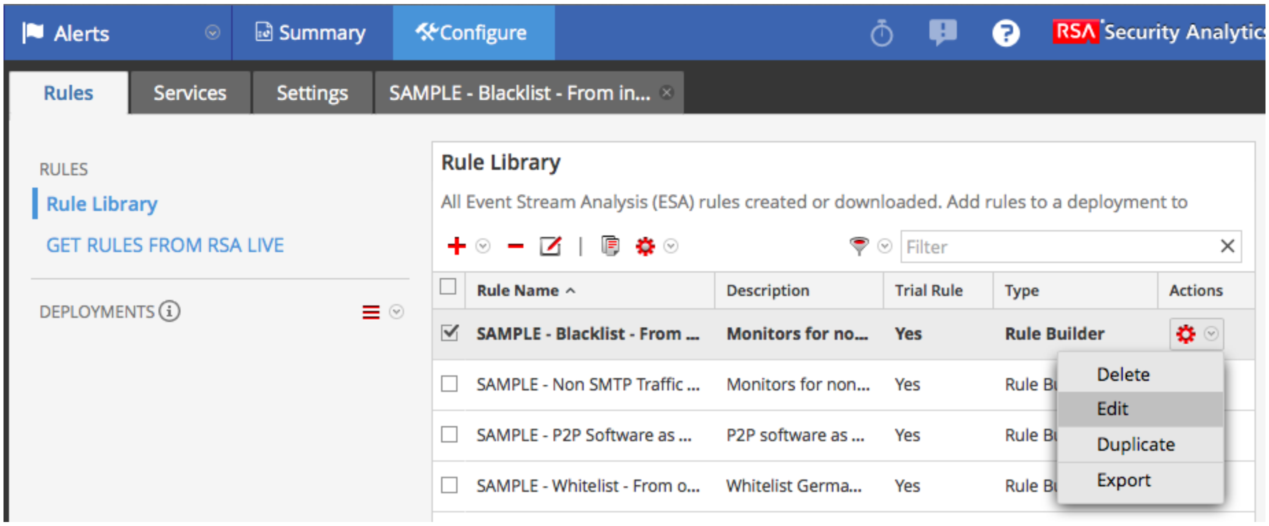
8. Click **Save**.

Configure Alerts to Send Logs to Splunk

After you have configured the notification items, you need to configure your ESA alerts to use these items.

1. In the **Security Analytics** menu, select **Administration > Alerts > Configure**.

2. From the Rule Library, select a rule and choose **Edit** from the Actions menu.



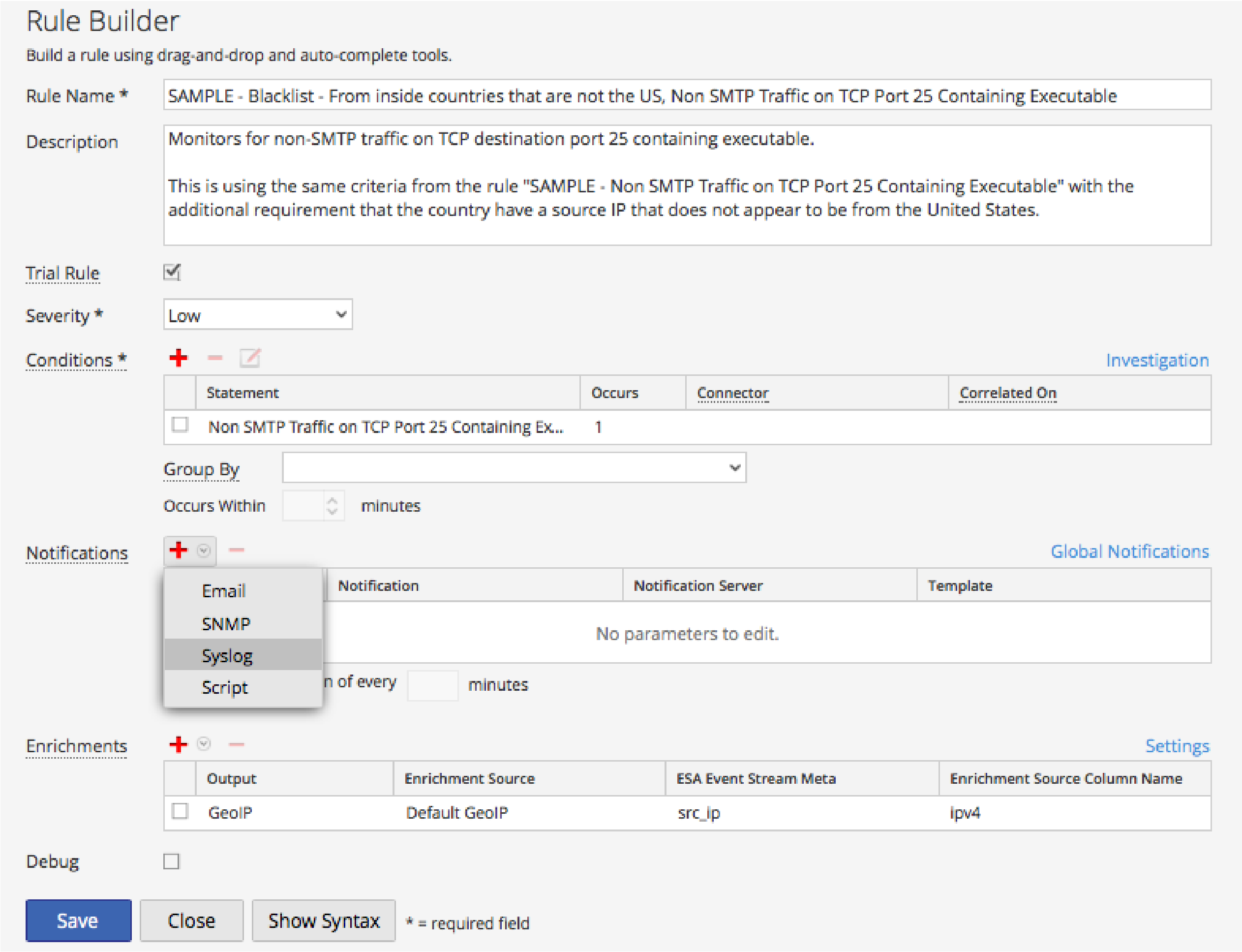
Rule Library

All Event Stream Analysis (ESA) rules created or downloaded. Add rules to a deployment to

	Rule Name	Description	Trial Rule	Type	Actions
☑	SAMPLE - Blacklist - From ...	Monitors for no...	Yes	Rule Builder	
□	SAMPLE - Non SMTP Traffic ...	Monitors for non...	Yes	Rule Bu	
□	SAMPLE - P2P Software as ...	P2P software as ...	Yes	Rule Bu	
□	SAMPLE - Whitelist - From o...	Whitelist Germa...	Yes	Rule Bu	

The Rule Builder screen appears.

3. In the Notifications section, click + ⌄ > **Syslog** to configure Syslog notifications for the rule.



Rule Builder

Build a rule using drag-and-drop and auto-complete tools.

Rule Name * SAMPLE - Blacklist - From inside countries that are not the US, Non SMTP Traffic on TCP Port 25 Containing Executable

Description Monitors for non-SMTP traffic on TCP destination port 25 containing executable.

This is using the same criteria from the rule "SAMPLE - Non SMTP Traffic on TCP Port 25 Containing Executable" with the additional requirement that the country have a source IP that does not appear to be from the United States.

Trial Rule ☑

Severity * Low

Conditions *

	Statement	Occurs	Connector	Correlated On
□	Non SMTP Traffic on TCP Port 25 Containing Ex...	1		

Group By

Occurs Within minutes

Notifications

Notification	Notification Server	Template
	No parameters to edit.	

n of every minutes

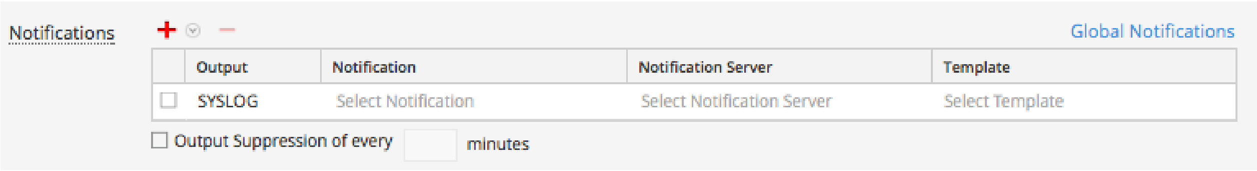
Enrichments

	Output	Enrichment Source	ESA Event Stream Meta	Enrichment Source Column Name
□	GeoIP	Default GeoIP	src_ip	ipv4

Debug □

* = required field

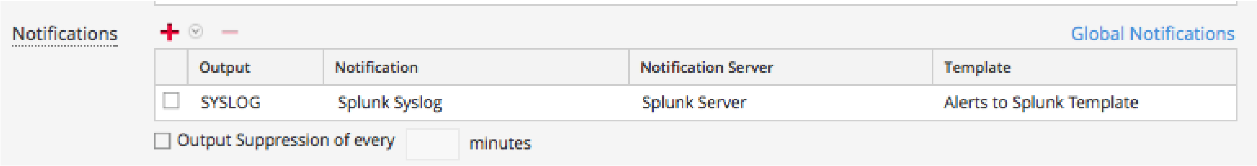
A notification row is added to the Notifications section.



	Output	Notification	Notification Server	Template
☐	SYSLOG	Select Notification	Select Notification Server	Select Template

☐ Output Suppression of every minutes

4. Select the notification, notification server, and template that you created earlier.



	Output	Notification	Notification Server	Template
☐	SYSLOG	Splunk Syslog	Splunk Server	Alerts to Splunk Template

☐ Output Suppression of every minutes

5. Click **Save** to save your changes and close the Rule Builder screen.

Repeat these steps for any other rules that you want to send information to Splunk.

Conclusion

This chapter described how to configure your notifications and rules, and have a data input in Splunk to listen on. Once this is done, when alerts are triggered, the information that you configured in your Notification template is sent to Splunk. You can then use Splunk to search for and view the Security (ESA) logs that are sent from RSA Security Analytics.

Forward Security/RE Logs to Splunk

You can forward the RSA Security Analytics security (Reporting Engine) logs to Splunk.

How it Works

RSA uses Reporting Alerts feature to send the security logs to the Splunk Syslog server that you specify from the Reporting Engine Output Actions screen in Security Analytics.

These are the steps required to send Security Analytics ESA logs to Splunk:

I. Configure a Splunk Data Input

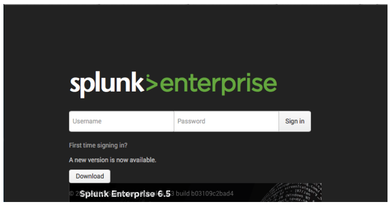
II. Add a Reporting Engine Output Action

III. Configure a Rule to Send Logs to Splunk

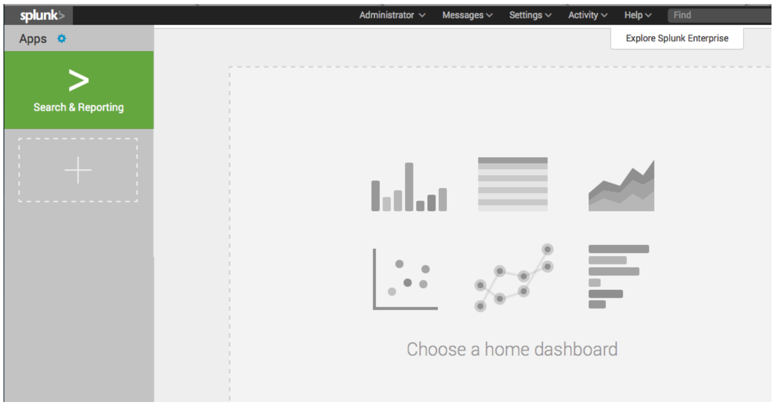
Configure a Splunk Data Input

You need to configure a Splunk data input to receive logs from RSA Security Analytics.

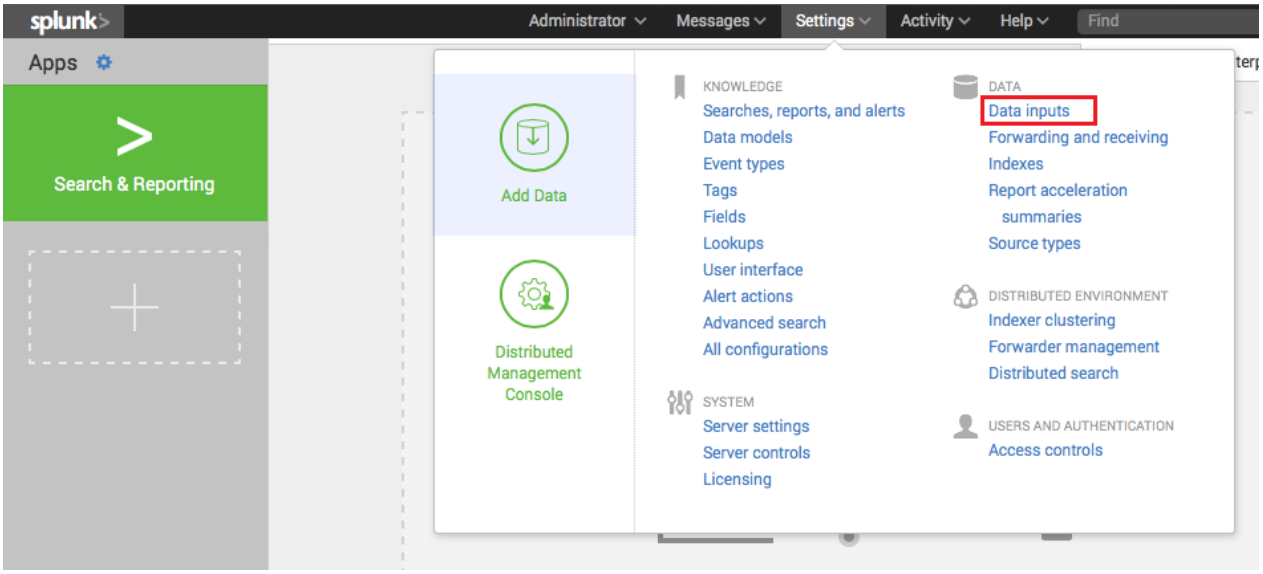
1. Log into Splunk.



You will see the main Splunk screen:

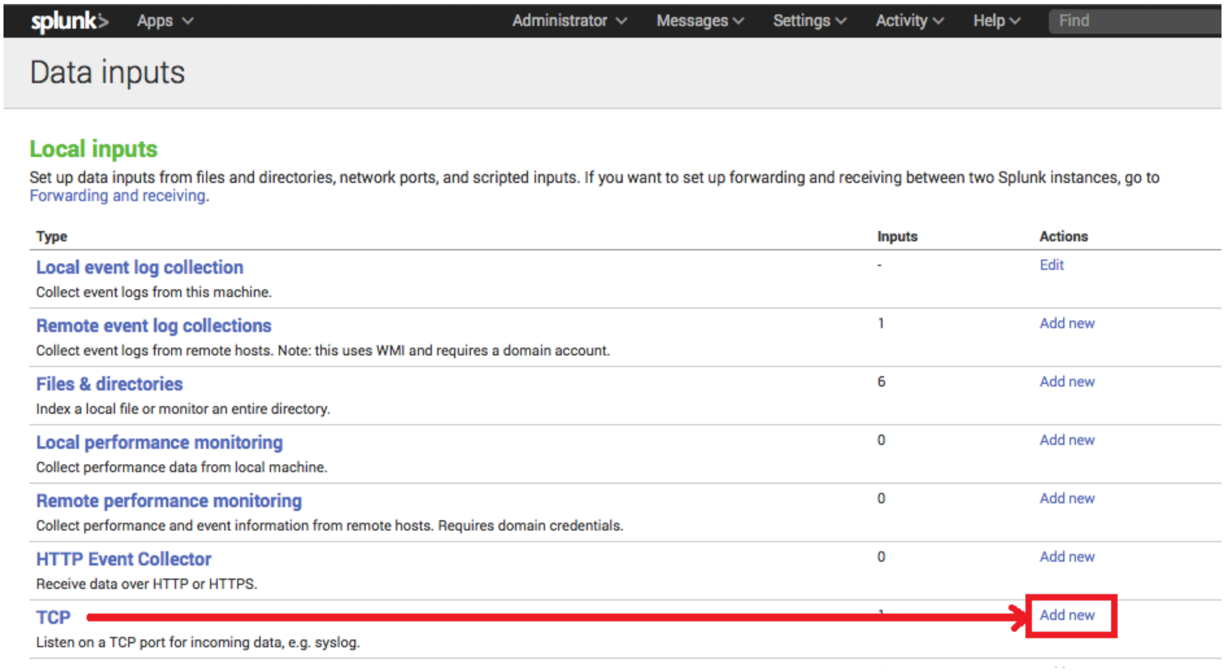


2. Select **Settings > Data Inputs**.



3. Set up a collector. In this example, we are setting up a TCP collector.

    a. Select Add new for the TCP input type.



Data inputs

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.

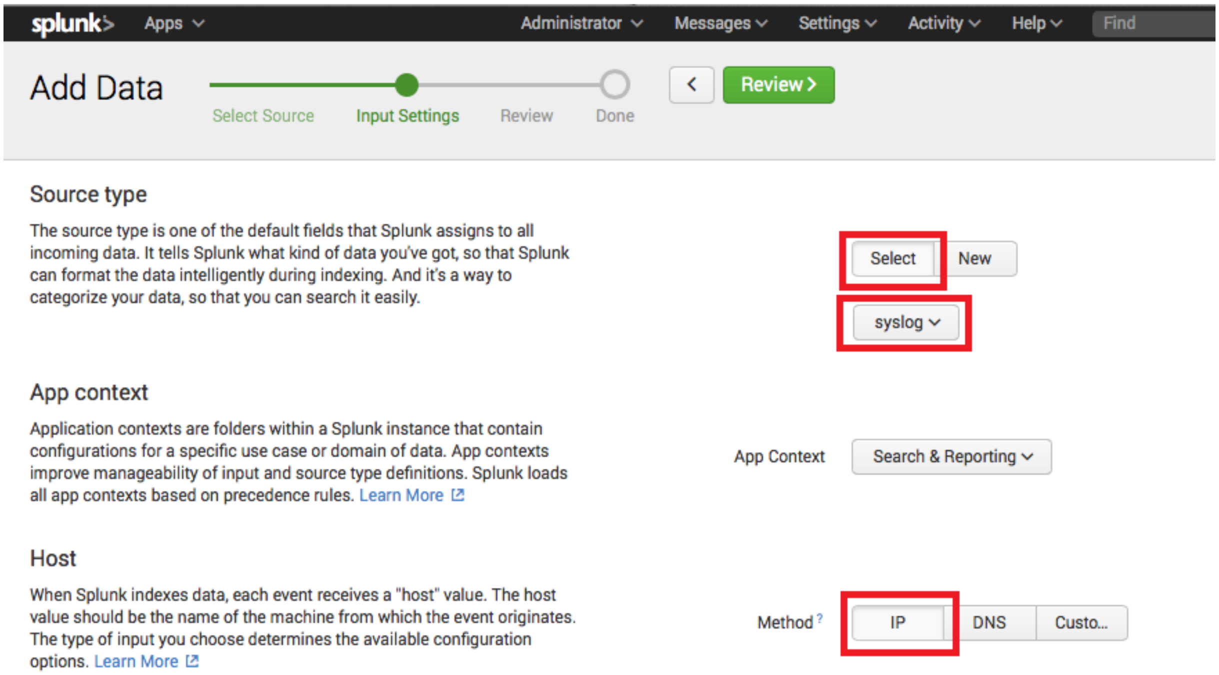
Type	Inputs	Actions
Local event log collection Collect event logs from this machine.	-	Edit
Remote event log collections Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.	1	Add new
Files & directories Index a local file or monitor an entire directory.	6	Add new
Local performance monitoring Collect performance data from local machine.	0	Add new
Remote performance monitoring Collect performance and event information from remote hosts. Requires domain credentials.	0	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.	1	Add new

    b. In the Add Source screen enter:

    - the TCP port to listen on (standard Syslog port is 514).
    - a value for **Source name override**, if desired.

    c. Click **Next**, and set the following:

    - For the **Source type**, select **syslog** from the drop-down menu.
    - For the **Host Method**, select **IP**.



Source type

The source type is one of the default fields that Splunk assigns to all incoming data. It tells Splunk what kind of data you've got, so that Splunk 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 instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. Splunk loads all app contexts based on precedence rules. Learn More

App Context: Search & Reporting

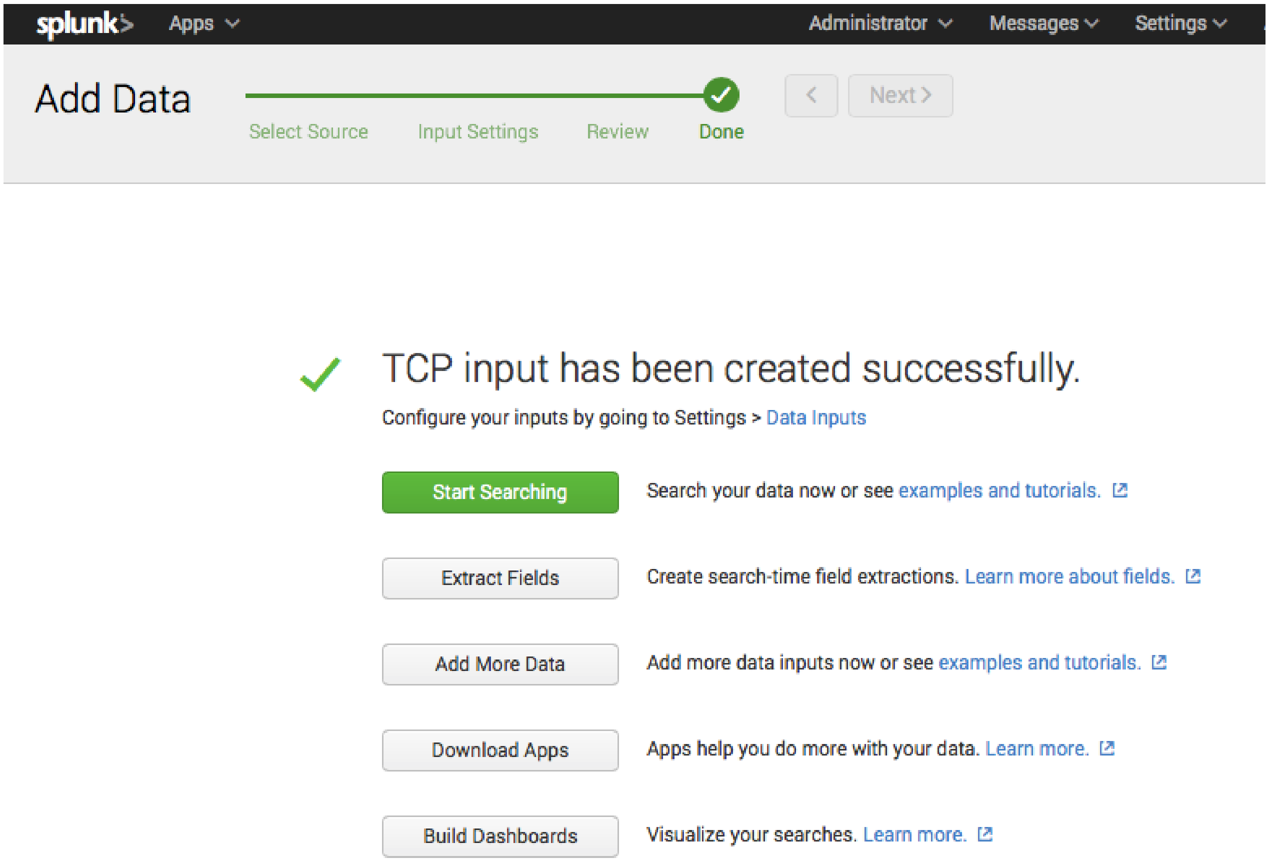
Host

When Splunk 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

d. Click **Review**.

e. Click **Submit** to create the data input. If you need to change any of your settings, click the back button (<), make your changes, and return here to submit when you are ready.

You receive confirmation that your data input was created successfully:



TCP input has been created successfully.

Configure your inputs by going to Settings > Data Inputs

Start Searching — Search your data now or see examples and tutorials.

Extract Fields — Create search-time field extractions. Learn more about fields.

Add More Data — Add more data inputs now or see examples and tutorials.

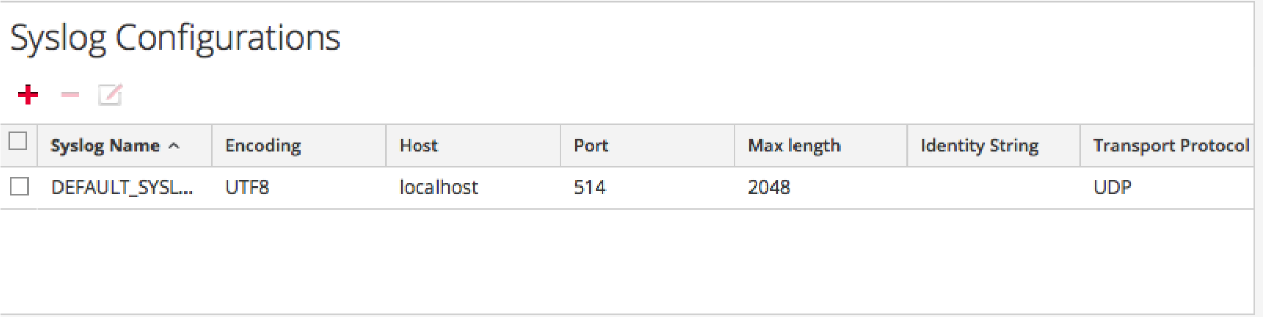
Download Apps — Apps help you do more with your data. Learn more.

Build Dashboards — Visualize your searches. Learn more.

Add a Reporting Engine Output Action

In the Reports view, define an Output Action.

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the Services Grid, select a **Reporting Engine** service.
3. Click ⚙ > **View** > **Config**.
4. Select the **Output Actions** tab, and navigate down to the **Syslog Configurations** section.



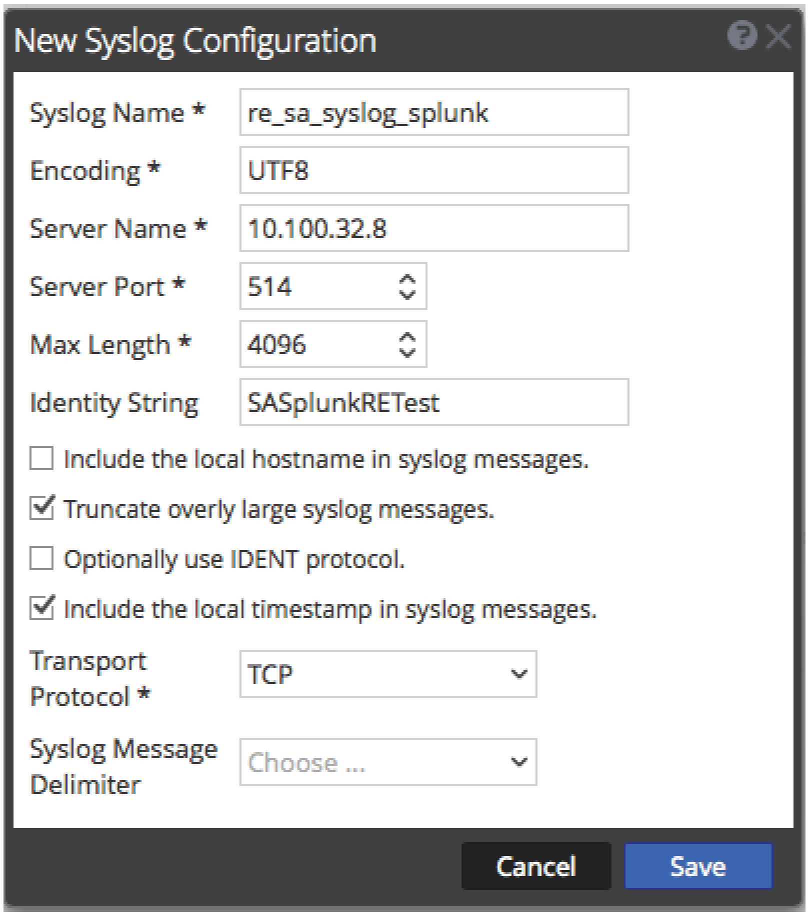
Syslog Configurations

□	Syslog Name ^	Encoding	Host	Port	Max length	Identity String	Transport Protocol
□	DEFAULT_SYSL...	UTF8	localhost	514	2048		UDP

5. Click + to add a Syslog configuration. Fill in the following information:

   - In the **Server Name** field, enter the IP address or hostname of the Splunk server.
   - In the **Transport Protocol** field, select TCP from the drop-down menu.

   For the other fields, select values based on your needs. For details on these parameters, see Reporting Engine Output Actions Parameters. Below is an example configuration screen.



Syslog Name * re_sa_syslog_splunk

Encoding * UTF8

Server Name * 10.100.32.8

Server Port * 514

Max Length * 4096

Identity String SASplunkRETest

☐ Include the local hostname in syslog messages.

☑ Truncate overly large syslog messages.

☐ Optionally use IDENT protocol.

☑ Include the local timestamp in syslog messages.

Transport Protocol * TCP

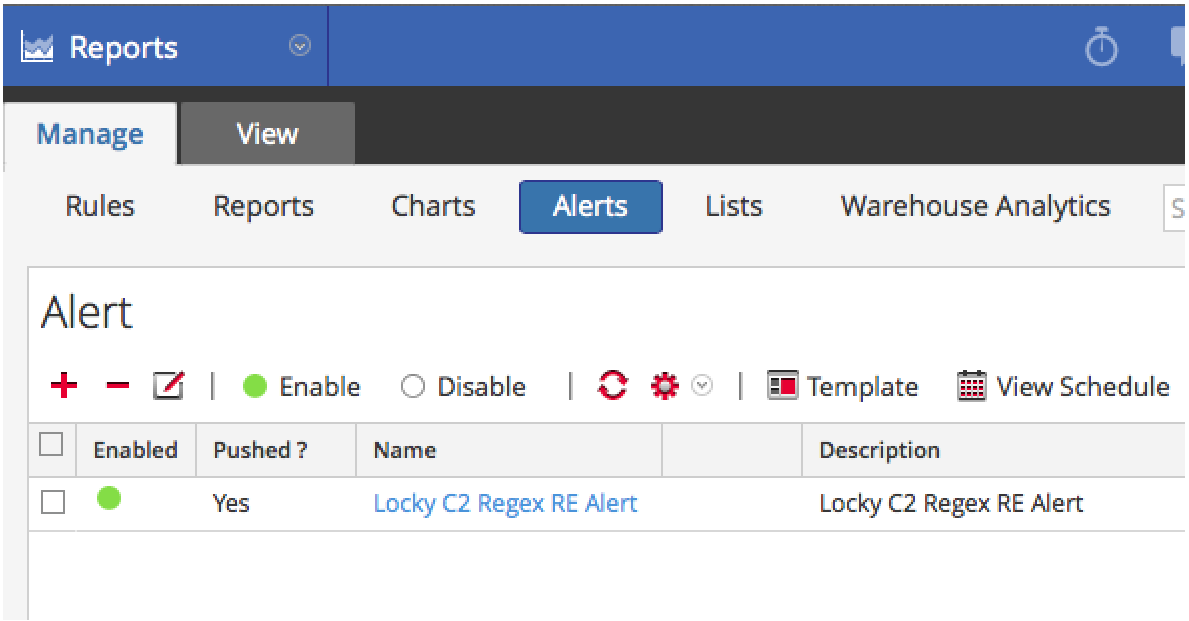
Syslog Message Delimiter Choose ...

6. Click **Save**.

Configure a Rule to Send Logs to Splunk

In the Reports view, add an alert that, when triggered, will send log information to Splunk.

1. In the **Security Analytics** menu, select **Reports**.
2. From the **Manage** tab, select **Alerts** from the navigation bar.



□	Enabled	Pushed ?	Name		Description
□	●	Yes	Locky C2 Regex RE Alert		Locky C2 Regex RE Alert

3. In the Alerts section, select Template.

4. Create a new template.

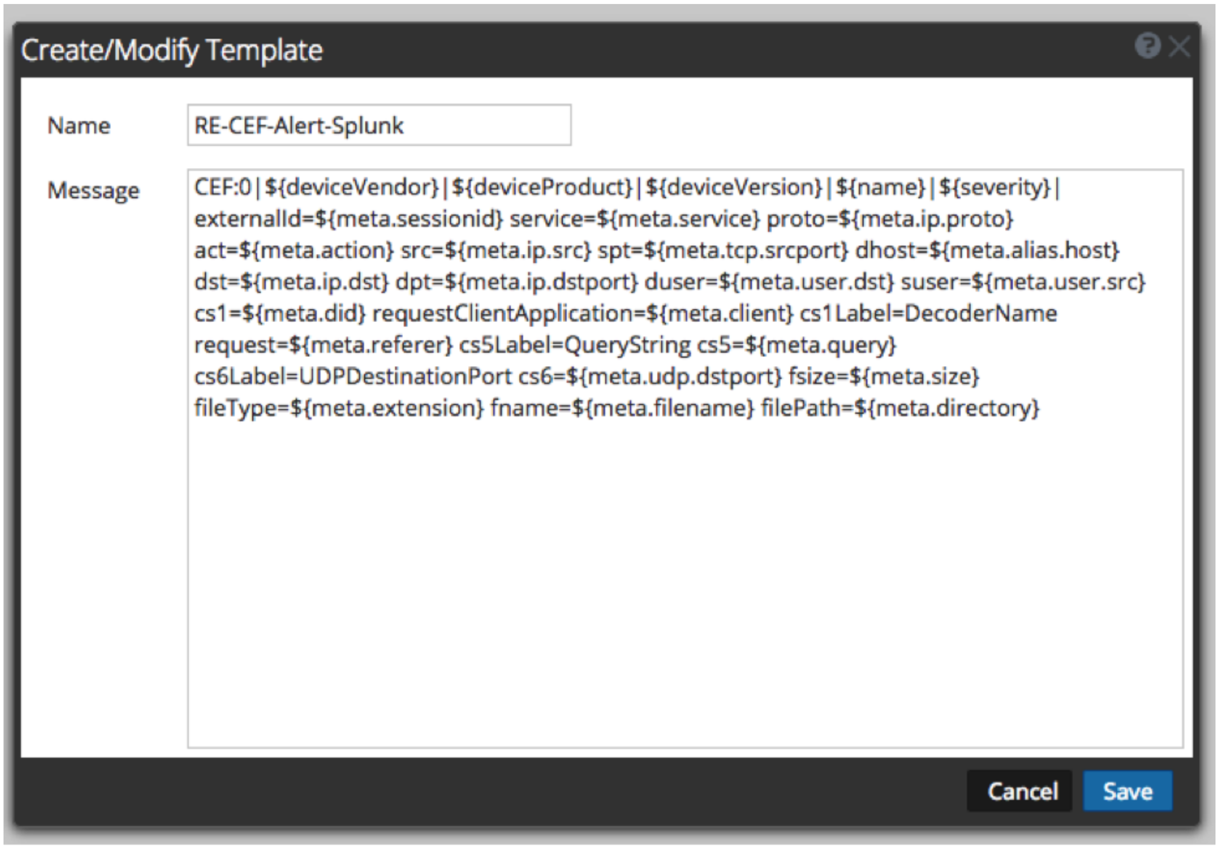
   a. For **Name**, enter a descriptive name.

   b. In the Message field, enter the following text:

```
CEF:0|${deviceVendor}|${deviceProduct}|${deviceVersion}|${name}|${severity}|
externalId=${meta.sessionid} service=${meta.service} proto=${meta.ip.proto}
act=${meta.action} src=${meta.ip.src} spt=${meta.tcp.srcport} dhost=${meta.alias.host}
dst=${meta.ip.dst} dpt=${meta.ip.dstport} duser=${meta.user.dst} suser=${meta.user.src}
cs1=${meta.did} requestClientApplication=${meta.client} cs1Label=DecoderName
request=${meta.referer} cs5Label=QueryString cs5=${meta.query}
cs6Label=UDPDestinationPort cs6=${meta.udp.dstport} fsize=${meta.size}
fileType=${meta.extension} fname=${meta.filename} filePath=${meta.directory}
```

Note: If pasting the above text into an editor, combine the text into a single line by replacing all new lines with spaces. The text is also available in the Code for RE Alerts Notification Template section of the Appendix.

This show as example of the dialog box:



Name: RE-CEF-Alert-Splunk

Message:

```
CEF:0|${deviceVendor}|${deviceProduct}|${deviceVersion}|${name}|${severity}|
externalId=${meta.sessionid} service=${meta.service} proto=${meta.ip.proto}
act=${meta.action} src=${meta.ip.src} spt=${meta.tcp.srcport} dhost=${meta.alias.host}
dst=${meta.ip.dst} dpt=${meta.ip.dstport} duser=${meta.user.dst} suser=${meta.user.src}
cs1=${meta.did} requestClientApplication=${meta.client} cs1Label=DecoderName
request=${meta.referer} cs5Label=QueryString cs5=${meta.query}
cs6Label=UDPDestinationPort cs6=${meta.udp.dstport} fsize=${meta.size}
fileType=${meta.extension} fname=${meta.filename} filePath=${meta.directory}
```

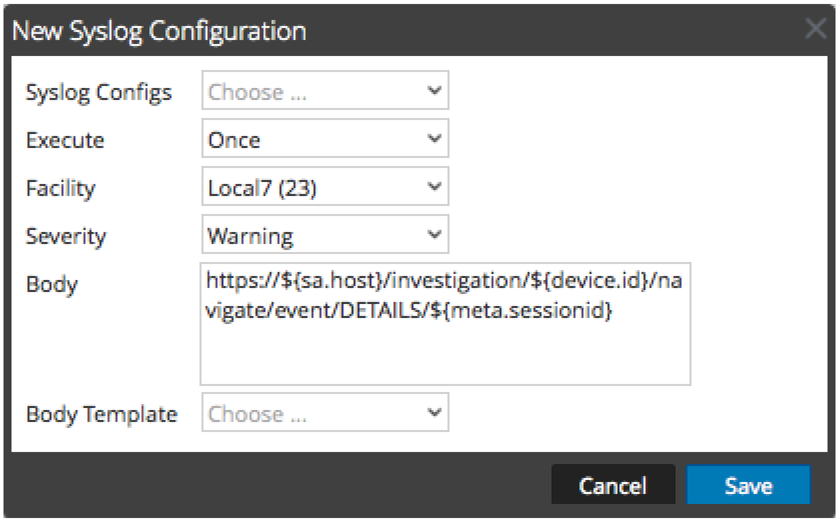
c. Click **Save**.

5. Select an Alert, and click the ✎ (Edit) icon to modify the alert.

   The Create/Modify Alert screen is displayed.

6. In the Notification section, select the **Syslog** tab, and click ✚.

   The New Syslog Configuration dialog box is displayed.



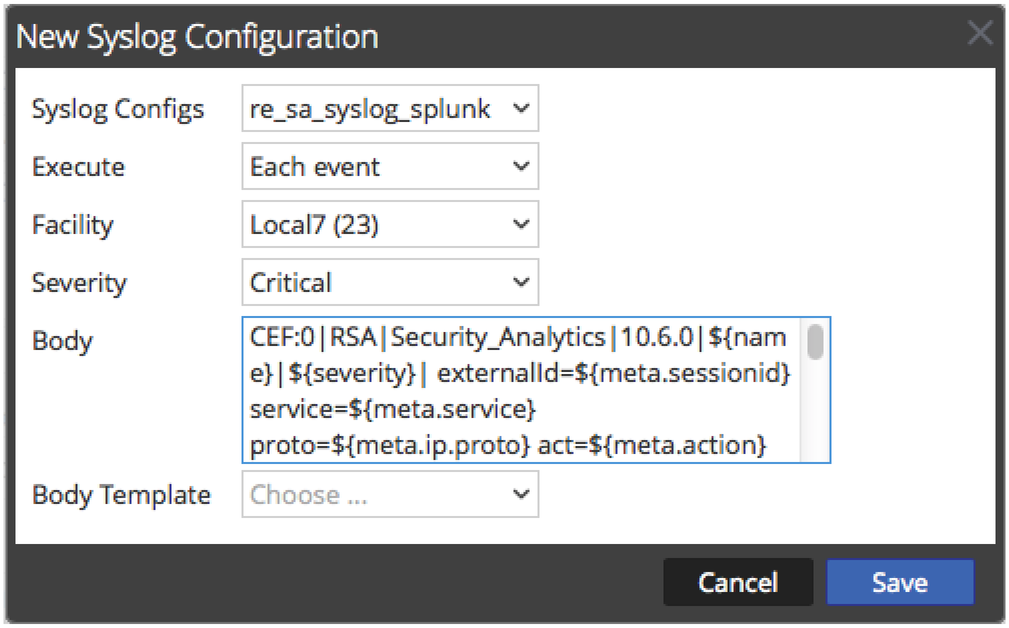
New Syslog Configuration

Syslog Configs	Choose ...
Execute	Once
Facility	Local7 (23)
Severity	Warning
Body	https://${sa.host}/investigation/${device.id}/navigate/event/DETAILS/${meta.sessionid}
Body Template	Choose ...

7. Fill in the parameters as follows.

   - In the **Syslog Configs** field, select the Syslog Configuration that you created in Add a Reporting Engine Output Action.
   - In the **Execute** field, select **Each event**.
   - Select a **Facility** and **Severity** based on the needs of your organization.
   - In the **Body Template** field, select the template that you just created in step 4.

   Here is an example of the dialog box with the fields filled in:



New Syslog Configuration

Syslog Configs	re_sa_syslog_splunk
Execute	Each event
Facility	Local7 (23)
Severity	Critical
Body	CEF:0|RSA|Security_Analytics|10.6.0|${name}\|${severity}| externalId=${meta.sessionid} service=${meta.service} proto=${meta.ip.proto} act=${meta.action}
Body Template	Choose ...

Note: If you make any changes to the template, you need to edit the Syslog Configuration again, and re-select the Body Template.

8. Click **Save**.

Conclusion

This chapter described how to configure output actions and rules, and have a data input in Splunk to listen on. Once this is done, when alerts are triggered, the information that you configured in your Reports Alerts view is sent to Splunk. You can then use Splunk to search for and view the Security (RE) logs that are sent from RSA Security Analytics.

Appendix: Source Code

The Splunk package is delivered as a ZIP archive that contains the components for the different integration points. You download the file from RSA Link. You can find the package on the RSA Link Downloads space here.

Note: You can cut and paste the code below. Use an editor that can save it as text. You can then use this if you cannot download the posted ZIP archive.

Search Source IP

The following code contains the necessary source for implementing the **Search Splunk - Source IP** context menu action.

```
{

      "displayName": "[Search Splunk - Source IP]",
      "cssClasses": [
         "ip-src",
         "ip.src"
      ],

      "description": "Splunk search Source IP",
      "type": "UAP.common.contextmenu.actions.URLContextAction",
      "version": "Custom",
      "modules": [
         "investigation"
      ],

      "local": "false",
      "groupName": "externalLookupGroup",
      "urlFormat": "http://SPLUNKIP:8000/en-US/app/search/search?q=search%20src%3D{0}&earliest=-30d&latest=now",
      "disabled": "",
      "id": "SplunkLogLookupSrc",
      "moduleClasses": [
         "UAP.investigation.navigate.view.NavigationPanel",
         "UAP.investigation.events.view.EventGrid"
      ],
      "openInNewTab": "true"

}
```

Search Destination IP

The following code contains the necessary source for implementing the **Search Splunk - Destination IP** context menu action.

```
{

      "displayName": "[Search Splunk - Destination IP]",
      "cssClasses": [
         "ip-dst",
         "ip.dst"
      ],

      "description": "Splunk search Destination IP",
      "type": "UAP.common.contextmenu.actions.URLContextAction",
      "version": "Custom",
      "modules": [
         "investigation"
      ],

      "local": "false",
      "groupName": "externalLookupGroup",
      "urlFormat": "http://SPLUNKIP:8000/en-US/app/search/search?q=search%20dest%3D{0}&earliest=-30d&latest=now",
      "disabled": "",
      "id": "SplunkLogLookupDest",
      "moduleClasses": [
         "UAP.investigation.navigate.view.NavigationPanel",
         "UAP.investigation.events.view.EventGrid"
      ],
      "openInNewTab": "true"

}
```

Search Hostname

The following code contains the necessary source for implementing the **Search Splunk - Hostname** context menu action.

```
{

      "displayName": "[Search Splunk - Hostname]",
      "cssClasses": [
         "alias-host",
         "alias.host"
      ],

      "description": "Splunk search Hostname",
      "type": "UAP.common.contextmenu.actions.URLContextAction",
      "version": "Custom",
      "modules": [
         "investigation"
      ],

      "local": "false",
      "groupName": "externalLookupGroup",
      "urlFormat": "http://SPLUNKIP:8000/en-US/app/search/search?q=search%20hostname%3D{0}&earliest=-30d&latest=now",
      "disabled": "",
      "id": "SplunkLogLookupHostname",
      "moduleClasses": [
         "UAP.investigation.navigate.view.NavigationPanel",
         "UAP.investigation.events.view.EventGrid"
      ],
      "openInNewTab": "true"

}
```

General Search

The General search can be used for events that do not have values for any of the meta keys used in the other context actions—source IP, destination IP or hostname. The **Search Splunk - General** menu item performs a generic search on any IP address or host name. RSA Security Analytics passes the value that you select and enters it to Splunk, into the search field. The following code contains the necessary source for implementing the **Search Splunk - General** context menu action.

```
{

      "displayName": "[Search Splunk - General (IP and hostname)]",
         "cssClasses": [
         "ip-src",
         "ip-dst",
         "alias-host",
         "ip.src",
         "ip.dst",
         "alias.host"
      ],

      "description": "Splunk search Generic",
      "type": "UAP.common.contextmenu.actions.URLContextAction",
      "version": "Custom",
      "modules": [
         "investigation"
      ],

      "local": "false",
      "groupName": "externalLookupGroup",
      "urlFormat": "http://SPLUNKIP:8000/en-US/app/search/search?q=search%20{0}&earliest=-30d&latest=now",
      "disabled": "",
      "id": "SplunkLogLookupGeneral",
      "moduleClasses": [
         "UAP.investigation.navigate.view.NavigationPanel",
         "UAP.investigation.events.view.EventGrid"
      ],
      "openInNewTab": "true"

}
```

Code for ESA Alerts Notification Template

The following code is entered into the Global Notifications template that you add in the Define a Syslog Template for Splunk section.

```
<#include "macros.ftl"/>CEF:0|RSA|Security Analytics ESA|10.6.0|${statement}|${moduleName}|${severity}|rt=${time?datetime}
id=${id} source=${eventSourceId}<#list events as x> sessionid=${x.sessionid!" "}  service=${x.service!" "}
protocol=${x.protocol!" "} src=${x.ip_src!" "} dst=${x.ip_dst!" "} hostname=<#if x.alias_host?has_content><@value_of x.alias_
host /></#if> dport=${x.ip_dstport!" "} duser=${x.user_dst!" "}  suser=${x.user_src!" "} userGroup=${x.group!" "}
fname=${x.filename!" "} </#list>
```

Code for RE Alerts Notification Template

The following code is entered into the Syslog Configuration dialog box for any Reporting rules whose logs you want to send to Splunk. The procedure is describe in Configure a Rule to Send Logs to Splunk.

```
CEF:0|${deviceVendor}|${deviceProduct}|${deviceVersion}|${name}|${severity}| externalId=${meta.sessionid}
service=${meta.service} proto=${meta.ip.proto} act=${meta.action} src=${meta.ip.src} spt=${meta.tcp.srcport}
dhost=${meta.alias.host} dst=${meta.ip.dst} dpt=${meta.ip.dstport} duser=${meta.user.dst} suser=${meta.user.src}
cs1=${meta.did} requestClientApplication=${meta.client} cs1Label=DecoderName request=${meta.referer} cs5Label=QueryString
cs5=${meta.query} cs6Label=UDPDestinationPort cs6=${meta.udp.dstport} fsize=${meta.size} fileType=${meta.extension}
fname=${meta.filename} filePath=${meta.directory}
```