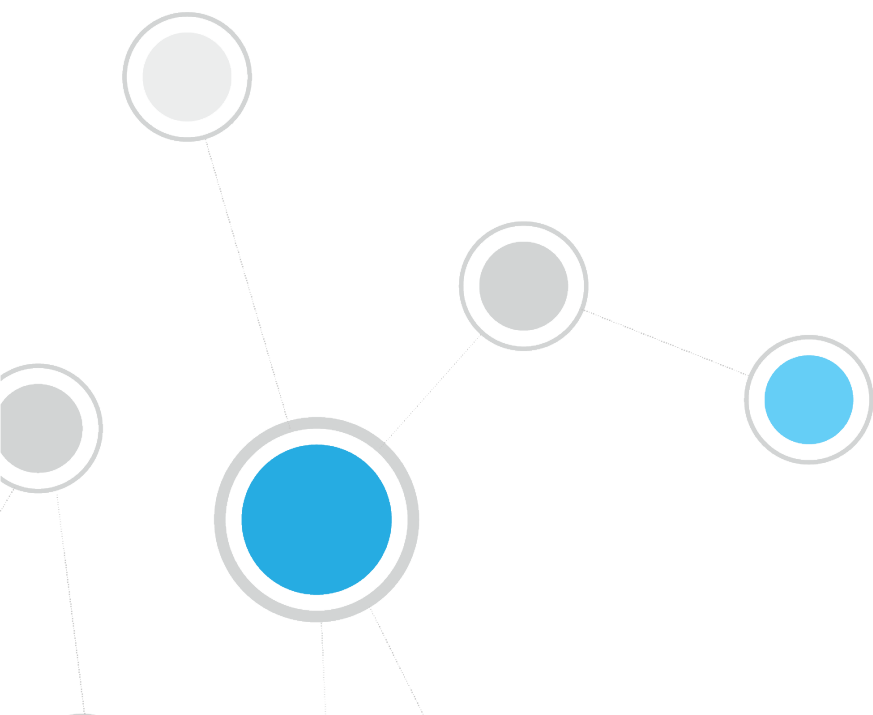




# ForeScout App & Add-ons for Splunk®

## How-to Guide

**Version 2.7**



## Table of Contents

<b>About Splunk Integration</b>	<b>4</b>
Support for Splunk Adaptive Response	5
What's New	5
Support for Batch Messaging	5
Support for Customized Indexes	7
Use Cases	7
Data Mining and Trend Analysis of CounterACT Data	7
Continuous Posture Tracking Based on a Broad Range of CounterACT Data	7
Adaptive Response Actions Triggered by Splunk Data Correlation	7
Additional Splunk Documentation	8
<b>About ForeScout App and Add-ons for Splunk</b>	<b>8</b>
ForeScout App for Splunk	8
ForeScout Technology Add-on for Splunk	9
ForeScout Adaptive Response Add-on for Splunk	9
<b>About the ForeScout Extended Module for Splunk</b>	<b>9</b>
<b>Requirements</b>	<b>10</b>
External Systems Connections	10
Install CounterACT	10
Install ForeScout Extended Module for Splunk	10
Splunk Requirements	11
ForeScout App for Splunk Enterprise (on-premise) Communication Requirements	11
About Certificates for Secured Messaging	12
Secured Messaging from ForeScout Adaptive Response Add-On to CounterACT Splunk Module	12
<b>Installation and Configuration</b>	<b>14</b>
Create a Data Index for CounterACT	14
Define a new Event Collector	14
Install the ForeScout Apps for Splunk	18
Upgrading	18
Rollback Support	19
Install the ForeScout Apps for Splunk	20
Configure the ForeScout Technology Add-on for Splunk	21
Splunk Roles for CounterACT	23
<b>CounterACT Workflow for Adaptive Response</b>	<b>23</b>
Correlation Searches and Saved Searches	25
Alerts	27
Configuring your Alerts	28

How to create an Alert with Trigger Actions .....	29
Customizing your own Alerts.....	32
CounterACT Response to Alert Messages .....	33
Targeting Devices in Alerts Sent to CounterACT .....	36
Best Practices for Scheduling Saved Searches .....	36
<b>Working with Dashboards .....</b>	<b>37</b>
Summary Dashboard .....	38
CounterACT Policy Dashboard .....	39
Network Insight and Discovery Dashboard.....	40
Response Dashboard .....	41
System Overview Dashboard .....	42
Host Detail View Dashboard.....	43
<b>Appendix A: Distributed Deployment.....</b>	<b>44</b>
Forwarding Event Data from CounterACT to Splunk .....	44
Possible Communication Channels .....	44
Forward Event Data to On-premise Distributed Splunk Deployments .....	45
Forward Event Data to Splunk Cloud Deployments .....	45
<b>Appendix B: Upgrade to Splunk Module version 2.8 and ForeScout Apps for Splunk 2.7 .....</b>	<b>46</b>
<b>Appendix C: Working with CounterACT Data in Splunk.....</b>	<b>48</b>
About CounterACT Data Events .....	48
Considerations When Working with CounterACT Events in Splunk.....	49
Mapping CounterACT Data to the CIM Model.....	50
Certificates .....	50
Compute_Inventory: CPU .....	51
Compute_Inventory: Network.....	51
Compute_Inventory: Memory .....	51
Compute_Inventory: Storage.....	51
Blocked_Malware .....	52
Subset of Core Properties .....	52
<b>Appendix D: System Certificate for Web Portal .....</b>	<b>53</b>
<b>Appendix E: Tuning Data Traffic .....</b>	<b>55</b>
<b>Appendix F - Compatibility with CIM Data Models .....</b>	<b>57</b>
CIM Model: Certificates .....	57
CIM Model: Compute_Inventory: CPU .....	57
CIM Model: Compute_Inventory: Network .....	58
CIM Model: Compute_Inventory: Memory .....	58
CIM Model: Compute_Inventory: Storage.....	59
CIM Model: Blocked_Malware.....	59

## About Splunk Integration

Splunk® Enterprise data analytics help organizations:

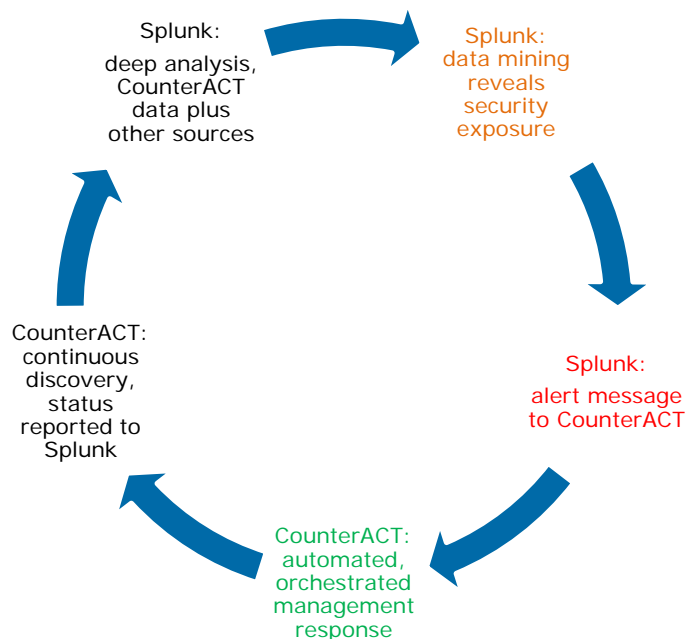
- Leverage the data that their infrastructure and security tools provide
- Understand their security posture
- Pinpoint and investigate anomalies
- Create alerts and reports

However, IT staff must then respond to any identified threats, violations and attacks. Any delay in response can result in significant security risks.

By combining ForeScout CounterACT® dynamic device visibility, access and security capabilities with Splunk Enterprise's data mining capabilities, security managers can:

- Achieve a broader understanding of their security posture
- Visualize key control metrics
- Respond more quickly to mitigate a range of security incidents.

Integration is fully bi-directional – CounterACT sends property, policy, and event information to Splunk, Splunk sends alerts and action requests to CounterACT, CounterACT responds to action requests through policy and sends action status to Splunk



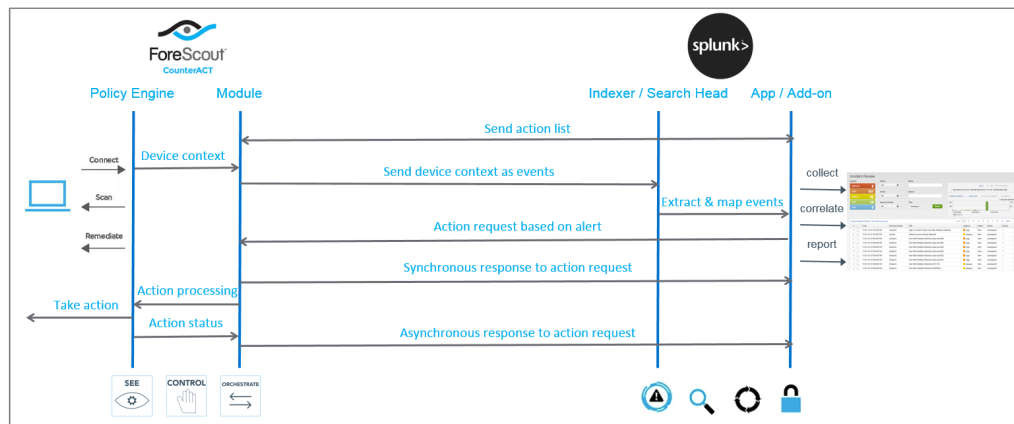
The result is enhanced threat insight, automated control, and greater operational efficiency.

## Support for Splunk Adaptive Response

Splunk's Adaptive Response Framework containing pre-populated search queries triggers alerts and action requests to CounterACT. Based on alert data received from Splunk, the CounterACT policy engine initiates remediation actions to identified endpoints. Examples of actions are: isolating breached systems or initiating less-intrusive actions such as security scans. The statuses of the actions are reported back to Splunk where it may be visualized on a dashboard.

This integration utilizes the ForeScout Adaptive Response Add-on for Splunk which supports the Splunk Adaptive Response framework as follows:

- The ForeScout Adaptive Response Add-on for Splunk maintains a list of available actions from CounterACT. Splunk can instruct CounterACT to respond to potential threats by applying any of these actions to endpoints that match search/trend criteria.
- To complete the action flow, CounterACT reports the status of actions applied to endpoints.



## What's New

### Support for Batch Messaging

Batched Messages were added as part of the ForeScout Extended Module for Splunk (Splunk Module) release. The saved searches and dashboard aspect in the ForeScout App for Splunk was enhanced.

The screenshot shows the Splunk search interface. At the top, the search bar contains 'index=fsctcenter'. Below the search bar, there are tabs for 'Events (24,174)', 'Patterns', 'Statistics', and 'Visualization'. The 'Events' tab is selected. The search results are displayed in a table format with columns for 'Time' and 'Event'. The event data is shown in a JSON format, including fields like 'ctupdate', 'host\_properties', 'auth\_login', and 'tenant\_id'. The interface also includes a sidebar with 'Selected Fields' and 'Interesting Fields'.

After configuring the Splunk target and the *Send Endpoint and Policy Details to Splunk* policy in the Splunk Module, batched messages are automatically sent to the Splunk Enterprise server. In order to work with these batched messages, all the underlying queries have been updated accordingly. You can view these underlying queries in the ForeScout App for Splunk Alerts page.

For the relevant search, select Open in Search link. In this example, the trigger\_ioc\_scanner\_notification search was selected. The relevant page opens.

The screenshot shows the ForeScout App for Splunk Alerts page. The search query is displayed in a text area, and the results are shown in a table format. The search query is as follows:

```

'get_index' 'get_sourcetypes' 'ct_hostinfo' atc_detected_ioc
| rename host_properties.atc_detected_ioc{}.value as atc_detected_ioc
| mvexpand atc_detected_ioc
| rex field=atc_detected_ioc "IOC Type:\s*(?<IOCType>[^\s]*).*Raw IOC Data:\s*(?<RawIOCData>[^\s]*).*"
| search IOCType="DNS Query" OR IOCType="CnC Address"
| where isNotNull(RawIOCData)
| dedup ip RawIOCData
| eventstats count as eventcount by ip RawIOCData
| where eventcount>5 AND eventcount<=10

```

The information that comprises the search query displays.

For configuring these batched messages, see the *ForeScout Extended Module for Splunk Configuration Guide*.

## Support for Customized Indexes

In version 2.5, *fsctcenter* is the default index and the only index used for the Forescout Extended Module for Splunk and the Forescout Apps for Splunk. In this version, Forescout Extended Module for Splunk is capable of forwarding messages to the Forescout Apps for Splunk with customized indexes in addition to the default *fsctcenter*.

For more information, see [Index](#).

## Use Cases

This section describes important use cases supported by the ForeScout Splunk App. To understand how this App helps you achieve these goals, see [About ForeScout App and Add-ons for Splunk](#).

- [Data Mining and Trend Analysis of CounterACT Data](#)
- [Continuous Posture Tracking Based on a Broad Range of CounterACT Data](#)
- [Adaptive Response Actions Triggered by Splunk Data Correlation](#)

### Data Mining and Trend Analysis of CounterACT Data

Splunk's strength is storing and indexing data over long periods of time. To complement CounterACT's real-time monitoring and management tools, Splunk provides long term data storage and in-depth history and trend analysis tools as standard options.

### Continuous Posture Tracking Based on a Broad Range of CounterACT Data

Integration with Splunk includes a dedicated Splunk app with custom dashboards that let security managers quickly monitor the current operational/security posture. CounterACT reports a wider range of data to Splunk, and the dashboards display real-time metrics derived from this information, such as:

- Endpoint compliance status summaries
- Trends in CounterACT policy matches
- Changes in endpoint processes and applications

Experienced Splunk users can customize the searches and dashboards provided with the ForeScout App, or combine CounterACT information with other data sources in the Splunk environment.

### Adaptive Response Actions Triggered by Splunk Data Correlation

Splunk's Adaptive Response Framework containing pre-populated search queries triggers alerts and action requests to CounterACT. Based on alert data received from Splunk, the CounterACT policy engine initiates remediation actions to identified endpoints. Examples of actions are: isolating breached systems or initiating less-

intrusive actions such as security scans. The statuses of the actions are reported back to Splunk where it may be visualized on a dashboard.

## Additional Splunk Documentation

Refer to online documentation for more information about the Splunk solution:

<http://docs.splunk.com/Documentation/Splunk>


## About ForeScout App and Add-ons for Splunk

Paired with CounterACT, the ForeScout Extended Module for Splunk (Splunk Module) along with the ForeScout App for Splunk and the ForeScout Technology Add-ons for Splunk allow bi-directional communication with Splunk Enterprise and Splunk Enterprise Security. This gives you visibility into devices on the network, including corporate owned, BYOD, guest and IoT devices. Now, you can get visibility into MAC-addressed devices. You can also leverage device context from CounterACT to improve correlation and prioritize incidents within Splunk solutions, and take precise, automated response actions based on correlated security data.

The ForeScout has published three Apps:

- [ForeScout App for Splunk](#)
- [ForeScout Technology Add-on for Splunk](#)
- [ForeScout Adaptive Response Add-on for Splunk](#)

You can choose to install and use the two Add-ons with or without the ForeScout App for Splunk, however, the benefits increase with the utilization of all Add-ons. See [Installation and Configuration](#).

 *The ForeScout Extended Module for Splunk needs to be deployed on the ForeScout CounterACT appliance. You also need to read the ForeScout Extended Module for Splunk Configuration Guide.*

To use the ForeScout App and Add-ons for Splunk, you should have a solid understanding of Splunk concepts, functionality and terminology, and a basic understanding of how CounterACT policies work.

## ForeScout App for Splunk

The ForeScout App for Splunk allows you to view CounterACT data in a dedicated, customizable Splunk dashboard. This bidirectional interaction with Splunk allows security managers to quickly monitor the current operational/security posture.

Splunk can instruct CounterACT to respond to potential threats by applying any of these actions to endpoints that match search/trend criteria. To complete the action flow, CounterACT reports the status of actions applied to endpoints.



## ForeScout Technology Add-on for Splunk

The ForeScout Technology Add-on for Splunk (TA-forescout) consists of:

- **Configurations** - The TA-forescout add-on presents a setup page to the user to allow storing information such as CounterACT credentials needed to send alerts to the Splunk Module on CounterACT. It also displays the index name that the Splunk Module is sending its update messages to.
- **Authentication** - TA-forescout add-on stores credentials entered by the user on the setup page. These credentials are used for authentication when communicating with CounterACT.
- **Field Extraction** - TA-forescout defines any field extraction rules needed to extract events from properties received from CounterACT.

## ForeScout Adaptive Response Add-on for Splunk

Forescout Adaptive Response Add-on for Splunk (TA-forescout\_response) consists of:

- **Adaptive Response** - TA-forescout\_response implements the Adaptive Response framework for ForeScout-Splunk integration.
- **Actions Mapping** - TA-forescout\_response stores the CounterACT actions information which are available as *Trigger Actions* in alerts.
- **Sync Response** - This is the synchronous response sent by the Splunk Module on CounterACT, once it receives an alert sent by the ForeScout App for Splunk. It contains information indicating if the alert was correctly received and applied to the endpoint included in the alert.
- **Async Response** - This is the asynchronous response sent by the Splunk Module on CounterACT containing the outcome of the action that was executed on an endpoint because of an alert sent by the ForeScout App for Splunk.

## About the ForeScout Extended Module for Splunk

The ForeScout Extended Module for Splunk and the ForeScout Apps work together to support communications between CounterACT and Splunk.

- Use Splunk search queries to search and filter information in Splunk. See [Correlation Searches and Saved Searches](#).
- Configure to have alerts processed and have request for action messages sent from Splunk Enterprise server to the Splunk Module.
- See [Alerts](#).

In CounterACT, you can define policies that respond to alerts sent by Splunk. Refer to the *ForeScout Extended Module for Splunk Configuration Guide*.


- View data from CounterACT in a dedicated, customizable Splunk dashboard. See [Working with Dashboards](#).

You must install and configure both components to work with the features described in this document. For example, CounterACT policies and actions provided by the Splunk Module are used to populate Splunk with CounterACT data. Read this document together with the *ForeScout Extended Module for Splunk Configuration Guide*.

## Requirements

This section describes system requirements, including:

- [External Systems Connections](#)
- [Splunk Requirements](#)
- [ForeScout App for Splunk Enterprise \(on-premise\) Communication Requirements](#)

 *Splunk Enterprise Security works best using Google Chrome. Microsoft no longer supports Internet Explorer 9 and 10. Because of this, Splunk has ended its support for Splunk Web. When you upgrade, be sure to use Internet Explorer 11 or later. An alternative is to use another browser that Splunk supports.*

## External Systems Connections

This section covers the CounterACT-related installation and configuration.

### Install CounterACT

ForeScout CounterACT is required to be installed and configured in order to get data into Splunk. Contact your ForeScout team for more details or reach out to [support@forescout.com](mailto:support@forescout.com).

### Install ForeScout Extended Module for Splunk

The ForeScout Extended Module for Splunk is required to be installed and configured in order to get data into Splunk. Contact your ForeScout team for more details or reach out to [support@forescout.com](mailto:support@forescout.com).

After installing ForeScout Extended Module for Splunk, you will need to do the following:

- **Establish Connection to Splunk**- this establishes a connection between your CounterACT Appliance and a Splunk instance.
- **Test your Configuration** - test your connection between your CounterACT Appliance and a Splunk instance.

For more information on how to use the ForeScout Extended Module for Splunk, refer to the *ForeScout Extended Module for Splunk Configuration Guide*.

## Splunk Requirements


To integrate CounterACT with a Splunk environment, the following needs to be installed:

- Create an account on Splunkbase.
- Splunk Enterprise version 6.4, 6.5, or 6.6.
- Splunk Enterprise Security version 4.5 or 4.7.
- Splunk Processing Capacity - See [Splunk Enterprise Capacity Planning Manual](#) version 6.6.
- Splunk System Configuration - See [Splunk Enterprise Distributed Deployment Manual](#), version 6.6.
- Splunk User Permissions - See [About Users and User Roles](#) version 6.6.

To integrate CounterACT with a Splunk environment that **does not** run Splunk Enterprise Security (for more information, refer to the Splunk deployment guides at <https://docs.splunk.com/Documentation/Splunk/6.6.3/Installation/SystemRequirements>

## ForeScout App for Splunk Enterprise (on-premise) Communication Requirements

The CounterACT-Splunk integration is based on the following data sharing/messaging interactions.

 Before installing, be sure the recommended ports are allowed by the firewall.

Communication	Recommended	Alternative
Retrieve Action Info The ForeScout App for Splunk polls CounterACT's action_info API to retrieve a list of available actions.	REST API Default port: 443	REST API on HTTP
Ongoing Data Reporting CounterACT sends endpoint data to Splunk. This is the protocol used by the Splunk Module in CounterACT to implement the <b>Splunk: Send Update from CounterACT</b> action.	Event Collector Default port: 8088	Syslog (port 515/TCP/UDP) RESTful API HTTPS (8089)
Splunk Action Request <ul style="list-style-type: none"> <li>▪ Splunk sends alerts to CounterACT's alert API.</li> <li>▪ The alert API confirms receipt of alert message (Synchronous response - see <a href="#">CounterACT Response to Alert Messages</a>).</li> </ul>	REST API Default port: 443	REST API on HTTP

Splunk Action Final Status CounterACT reports the status of actions requested by Splunk (Asynchronous response - see <a href="#">CounterACT Response to Alert Messages</a> ).	Event Collector Default port: 8088	Syslog (port 515/TCP/UDP) RESTful API HTTPS (8089)
--	---------------------------------------	---

After installing, ensure that HTTP Listener is enabled (disabled by default.)

## About Certificates for Secured Messaging

Some of the communications that supports integration must use the secured hypertext (HTTPS) protocol.

- EventCollector and REST API messaging from CounterACT to Splunk do not require HTTPS, but can support it.
- Splunk alert messages sent to CounterACT's alert API do not require HTTPS, but can support it.

## Secured Messaging from ForeScout Adaptive Response Add-On to CounterACT Splunk Module

The alerts forwarded by the ForeScout Adaptive Response Add-On to CounterACT Splunk Module are sent over via HTTPS.

### To enable HTTPS communication using Splunk Module version 2.7:

1. In CounterACT, operators must not use the default self-signed web-portal certificate; instead, they need to procure their own certificate. Use 'fstool cert' utility to create a Certificate Signing Request (CSR) using the following steps:
  - a. Use 'fstool cert gen' to generate the certificate request.
  - b. Answer the questions required for certificate generating. Below is an example:

```

[root@ML ~]# fstool cert gen
-----
Generating new Certificate request:
-----
DNS name of this Enterprise Manager : test.forescout.com
Organization name : forescout
Organizational unit name :
City or Locality name : san jose
State or Province : ca
Two-letter country code for this unit : US
Add Email address to the certificate request? (yes/no) : yes
Email address : test@forescout.com
Number of months this certificate is valid for [120] :
RSA key size [2048] :
Signature digest algorithm (one of: SHA1, SHA256, SHA384, SHA512) [SHA256] :

A random seed must be generated that will be used in the
creation of your key. One of the easiest ways to create a
random seed is to use the timing of keystrokes on a keyboard.

To begin, type keys on the keyboard until this progress meter
is full. DO NOT USE THE AUTOREPEAT FUNCTION ON YOUR KEYBOARD!

Continue typing until the progress meter is full:

|*****|

Finished. Press enter to continue:

Generating key. This may take a few moments...

-----
Certificate request stored at /tmp/ca_request.csr
-----

The following steps should be taken in order to complete the
web server certification:

- sign the certificate request (/tmp/ca_request.csr) by your organizational
  Certificate Authority
- Copy the signed certificate to this machine (e.g. to /tmp/signed-certificates)
- Run the command: fstool cert import /tmp/signed-certificates

[root@ ~]#
[root@ ~]# ll /tmp/ca_request.csr
-rw----- 1 root root 1303 Mar 1 16:59 /tmp/ca_request.csr
[root@ ~]#

```

c. A file containing the request is created in '/tmp/ca\_request.csr'.

2. Get the CSR signed by a trusted Certificate Authority (for example, VeriSign) or by your own Certificate Authority.
3. If using a self-signed certificate: Once the certificates are installed on the CounterACT appliance using **fstool cert import** CLI and confirmed by **fstool cert test** CLI, the CounterACT Public Key Certificate must be appended to the cacert.pem file at the following location:

**\$SPLUNK\_HOME/lib/python2.7/site-packages/requests/cacert.pem**

Please refer to the *ForeScout Extended Module for Splunk Configuration Guide* for instructions on secured messaging from the Splunk Module to ForeScout Adaptive Response Add-On for Splunk.

### To enable HTTPS communication using Splunk Module version 2.8:

1. In CounterACT, operators must not use the default self-signed web-portal certificate; instead, they need to procure their own certificate. See [Appendix D: System Certificate for Web Portal](#).

2. If using a self-signed certificate: Once the certificates are installed on the CounterACT appliance using the CounterACT Public Key Certificate must be appended to the cacert.pem file at the following location:

`$SPLUNK_HOME/lib/python2.7/site-packages/requests/cacert.pem`

Please refer to the *ForeScout Extended Module for Splunk Configuration Guide* for instructions on secured messaging from the Splunk Module to ForeScout Adaptive Response Add-On for Splunk.

## Installation and Configuration

This section describes installation scenarios and procedures for the ForeScout App and Add-ons. For installation of ForeScout Splunk App and Add-ons in a distributed Splunk environment, see [Appendix A: Distributed Deployment](#).

Perform the following steps to work with the dashboard. For steps performed in the CounterACT Console, refer to the *ForeScout Extended Module for Splunk Configuration Guide*.

1. Review the *ForeScout Extended Module for Splunk Configuration Guide* and this *How-to Guide*.
2. Verify that [Requirements](#) are met.
3. Create an account on Splunkbase.
4. [Create a Data Index for CounterACT](#).
5. [Define a new Event Collector](#).
6. [Install the ForeScout Apps for Splunk](#).
7. [Configure the ForeScout Technology Add-on for Splunk](#).
8. [Splunk Roles for CounterACT](#).
9. (Optional) Test and tune the frequency of data reporting based on your network conditions and the volume of data you want to work with in Splunk.

## Create a Data Index for CounterACT

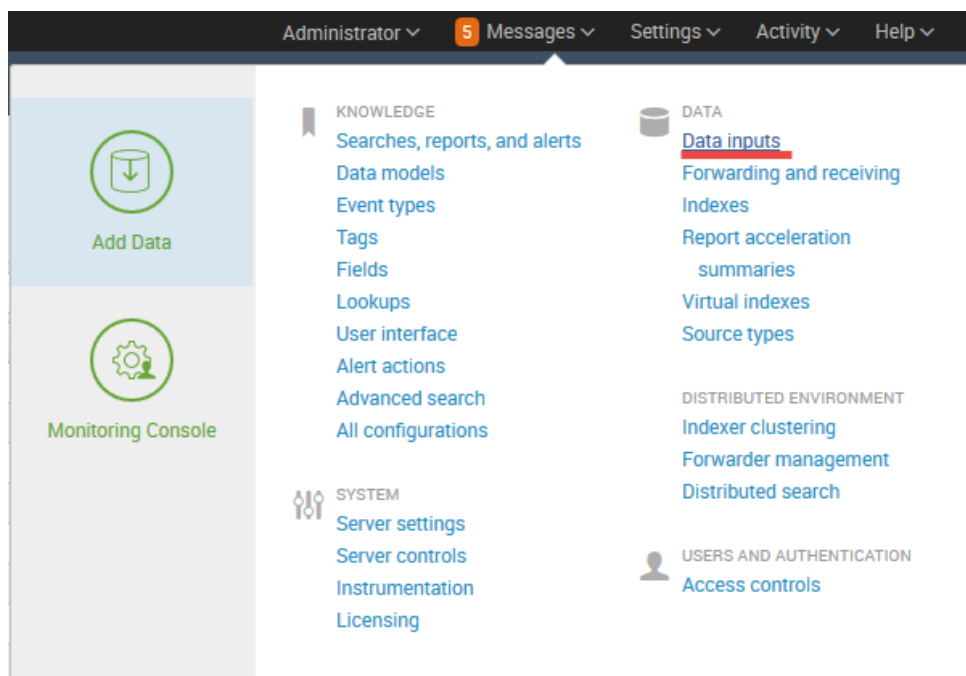
Follow the procedure described in the Splunk knowledge base to create an index that identifies information sent to Splunk by CounterACT.

<http://docs.splunk.com/Documentation/Splunk/6.6.3/Indexer/Setupmultipleindexes>

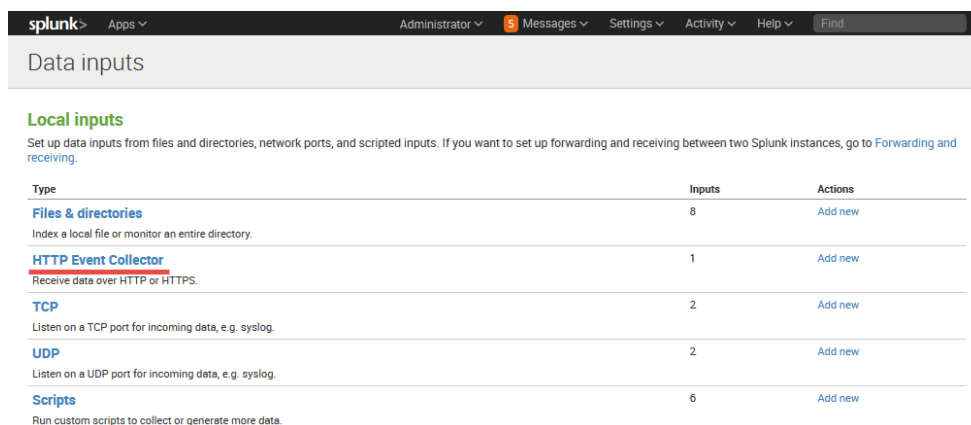
## Define a new Event Collector

You will need to get a token value (key) from the ForeScout App for Splunk so that event collectors can be created.

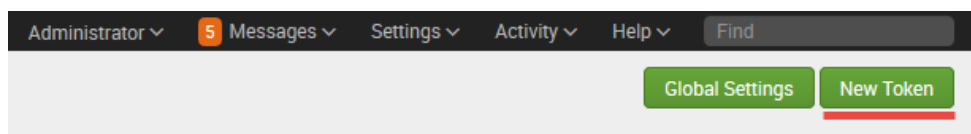
1. In the ForeScout App for Splunk, select **Messages** and then select **Data inputs**.



2. The Data Inputs page displays. Select **HTTP Event Collector**.



3. Select **New Token**.



4. The Add Data page opens to the Select Source pane.

**Add Data** | Select Source | Input Settings | Review | Done

**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.

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

Configure a new token for receiving data over HTTP. [Learn More](#)

Name:

Source name override?:

Description?:

Output Group (optional):

Enable indexer acknowledgement: ☐

5. Enter the Name of the Event Collector and then select **Next**. The Input Settings pane displays.

**Add Data** | Select Source | Input Settings | Review | Done

**Input Settings**

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

**Source type**

The source type is one of the default fields that 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.

Automatic | **Select** | New

**Index**

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

Select Allowed Indexes: Available item(s) [add all](#) | Selected item(s) [remove all](#)

fsctcenter  
history  
main  
summary

Select indexes that clients will be able to select from.

Default Index:  [Create a new index](#)

6. In the Source type section, select **Select**. The Select Source Type displays.
7. Select **Select Source Type** and enter *fsctcenter* into the search field. From the drop-down, select **fsctcenter\_json**.



Automatic Select New

Select Source Type ▾

fscntcenter

fscntcenter\_avp  
Syslog sent by CounterACT

**fscntcenter\_json**  
JSON sent by CounterACT

8. In the Index section, select one or more allowed indexes.

Automatic Select New

fscntcenter\_json ▾

Select Allowed Indexes

Available item(s) [add all »](#)

fscntcenter  
history  
main  
summary

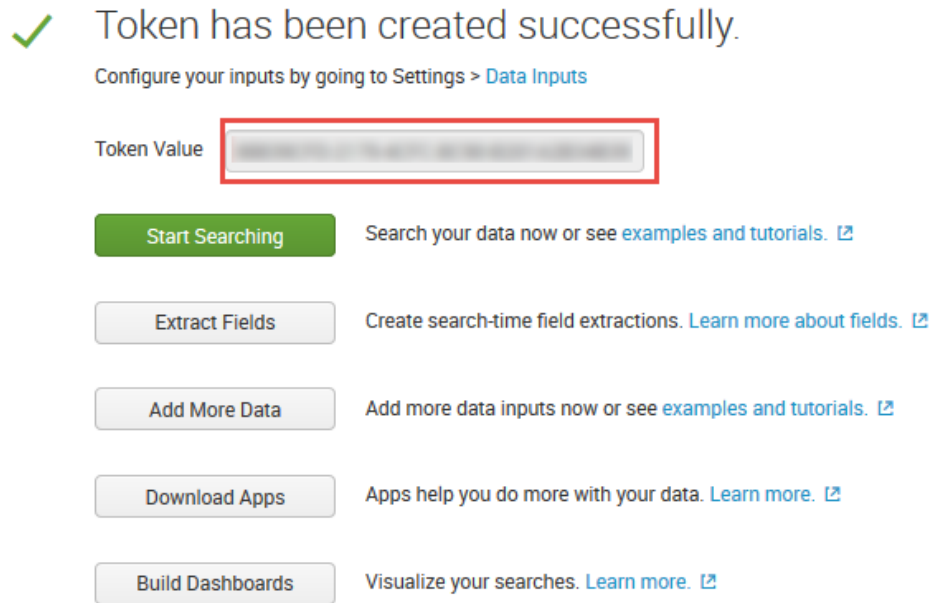
Selected item(s) « [remove all](#)

fscntcenter  
main

Select indexes that clients will be able to select from.

Default Index fscntcenter ▾ [Create a new index](#)

9. Select **Review**. Check your settings.
10. Select **Submit**. The new token value is created.



11. Copy this token value and paste it into a Notepad document. **Save** this Token.
12. The Token Value will be used when you add a Splunk HTTP target. Refer to the *ForeScout Extended Module for Splunk Configuration Guide*.

## Install the ForeScout Apps for Splunk

Before proceeding, please consult the latest Release Notes for upgrade and rollback instructions. It is best practice to install directly from Splunkbase.

## Upgrading

This section covers upgrading:

- [Upgrade to Splunk Module version 2.7 and ForeScout Apps for Splunk 2.7](#)
- [Upgrade to Splunk Module version 2.8 and ForeScout Apps for Splunk 2.7](#)

## Upgrade to Splunk Module version 2.7 and ForeScout Apps for Splunk 2.7

This section covers upgrading from Splunk Module 2.5 and ForeScout Apps for Splunk version 2.5 or 2.6. This release introduces significant functional and structural changes in both the Splunk Module and ForeScout Apps for Splunk.

**It is recommended to upgrade Forescout Splunk Apps and then upgrade the Forescout Extended Module for Splunk in the following sequence:**

1. On the Splunk Enterprise server, back up the following three ForeScout Splunk App and Add-ons to a secure location:
  - a. ForeScout Technology Add-on for Splunk

- b. ForeScout App for Splunk
  - c. ForeScout Adaptive Response Add-on for Splunk
2. On Splunkbase, use **Browse More Apps** to find all three ForeScout Splunk Apps v2.7.
3. Select **Load an App** with the **Upgrade App** feature to upgrade them in any order.
4. After all the App and Add-ons are upgraded and configured, restart Splunk by selecting **Settings/SYSTEM > Server Controls > Restart**.
5. On the CounterACT Console, upgrade the ForeScout Extended Module for Splunk to version 2.7.
6. In the left pane, Select **Options** and then select **Splunk**. The Splunk configuration pane displays the Splunk Syslog Targets tab.
7. Select each of the channels and then select **Test**.
8. Select the **Splunk HTTPS Targets** tab.
9. Select each of the channels and then select **Test**.
10. Upgrade is now complete.

### Upgrade to Splunk Module version 2.8 and ForeScout Apps for Splunk 2.7

Please see Appendix B: Upgrade to Splunk Module version 2.8 and ForeScout Apps for Splunk 2.7.

## Rollback Support

Under certain circumstances you may want to roll back the module to a previously installed version. This may happen, for example, if your system does not operate as expected after the module upgrade.

- If you are using ForeScout App for Splunk version 2.8, then rollback is not supported.
- If you are using the ForeScout App for Splunk version 2.7, then rollback is supported.


Modules on Appliances connected to the Enterprise Manager are rolled back to the selected version. Modules on Appliances that are not connected to the Enterprise Manager during the rollback are rolled back when the Enterprise Manager next reconnects to the Appliances.

### Rollback for Splunk Module version 2.7 and ForeScout Apps for Splunk 2.7

**The rollback of the ForeScout Extended Module for Splunk version 2.7 and rollback of the ForeScout App & Add-ons for Splunk version 2.7 should be performed in the following sequence:**

1. On the CounterACT Console, select the **Rollback** feature to roll the ForeScout Extended Module for Splunk back to the previous version.
2. On the Splunk Enterprise server, browse to the \$Splunk\_HOME/etc/apps folder and **delete/remove the three ForeScout Splunk Apps**:

- a. ForeScout Technology Add-on for Splunk
  - b. ForeScout App for Splunk
  - c. ForeScout Adaptive Response Add-on for Splunk
3. Without shutdown of the Splunk Enterprise server, copy or move the three previously-backed up ForeScout Splunk Apps from the secure location and paste them into the **\$Splunk\_HOME/etc/apps** folder.
  4. Restart Splunk by selecting **Settings/SYSTEM > Server Controls > Restart**.


 Due to data formatting changes on ForeScout Extended Module for Splunk version 2.7, some dashboards on the ForeScout Splunk App may not reflect data generated by a different Splunk module version.

### Rollback for Splunk Module version 2.8 and ForeScout Apps for Splunk 2.7

Rollback for Splunk Module version 2.8 is not supported.

## Install the ForeScout Apps for Splunk

The ForeScout App for Splunk consists of the following components.

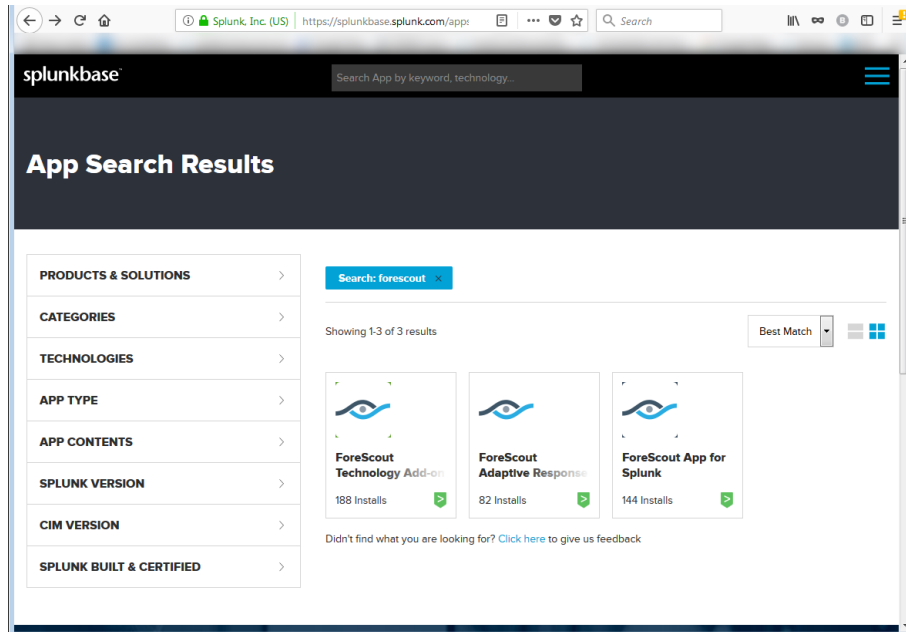
 You must restart Splunk service after all the intended components are installed and again after configuration.

Install Order	Component	Description	File
1.	<b>ForeScout App for Splunk (forescout_app)</b> See <a href="#">About ForeScout App and Add-ons for Splunk</a>	A visualization App containing dashboards to monitor endpoints using data provided by CounterACT.	<b>forescout_app.tar.gz</b>
2.	<b>Forescout Adaptive Response Add-on for Splunk (TA-forescout_response)</b> See <a href="#">ForeScout Adaptive Response Add-on for Splunk</a>	Supports Adaptive Response action calls to CounterACT.	<b>TA-forescout_response.tar.gz</b>
3.	<b>Forescout Technology Add-on for Splunk (TA-forescout)</b> See <a href="#">ForeScout Technology Add-on for Splunk</a>	Handles data collection from CounterACT.	<b>TA-forescout.tar.gz</b>
4.	<b>Restart</b>	Restart the Splunk service.	N/A

You will need to install these components on your Splunk Enterprise server. Download these components to a location that can be accessed for installation.

**To install and configure each App:**

1. **Login** into Splunkbase.
2. Search for the App by entering **ForeScout** into the search field.
3. In the App Search Results page, download all three Apps:
  - ForeScout Technology Add-on for Splunk
  - ForeScout Adaptive Response Add-on for Splunk
  - ForeScout App for Splunk



4. **Login** to the Splunk Enterprise server.
5. Go to the Splunk/Apps page and select the **Install app from file** button.
6. **Upload** each of the above apps.
7. You are now ready to [Configure the ForeScout Technology Add-on for Splunk](#).

The Apps display in your Splunk Console homepage view, and is listed under the Apps menu.

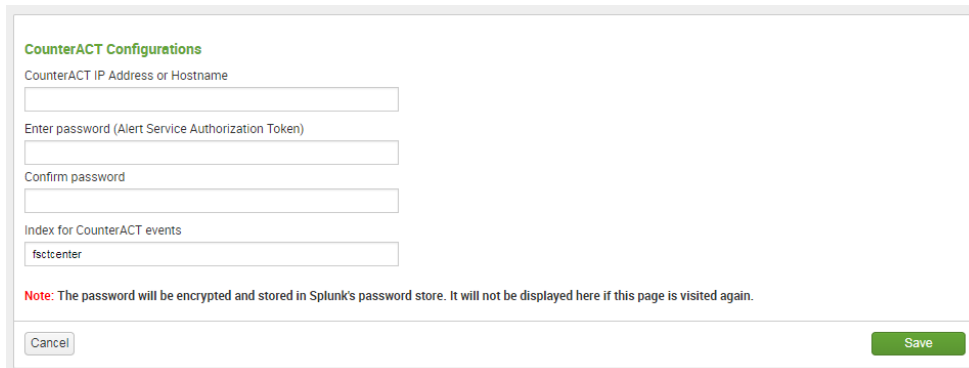
## Configure the ForeScout Technology Add-on for Splunk

The ForeScout Technology Add-on for Splunk supports data communication between CounterACT and the ForeScout App for Splunk. It is best practice to install from Splunkbase.

**To configure the Technology Add-on for Splunk:**

1. **Login** to the Splunk Enterprise server.

- Go to the Splunk/Apps page and within the ForeScout Technology Add-on for Splunk row, select **Set up**. The configuration page for the app displays.



**CounterACT Configurations**

CounterACT IP Address or Hostname

Enter password (Alert Service Authorization Token)

Confirm password

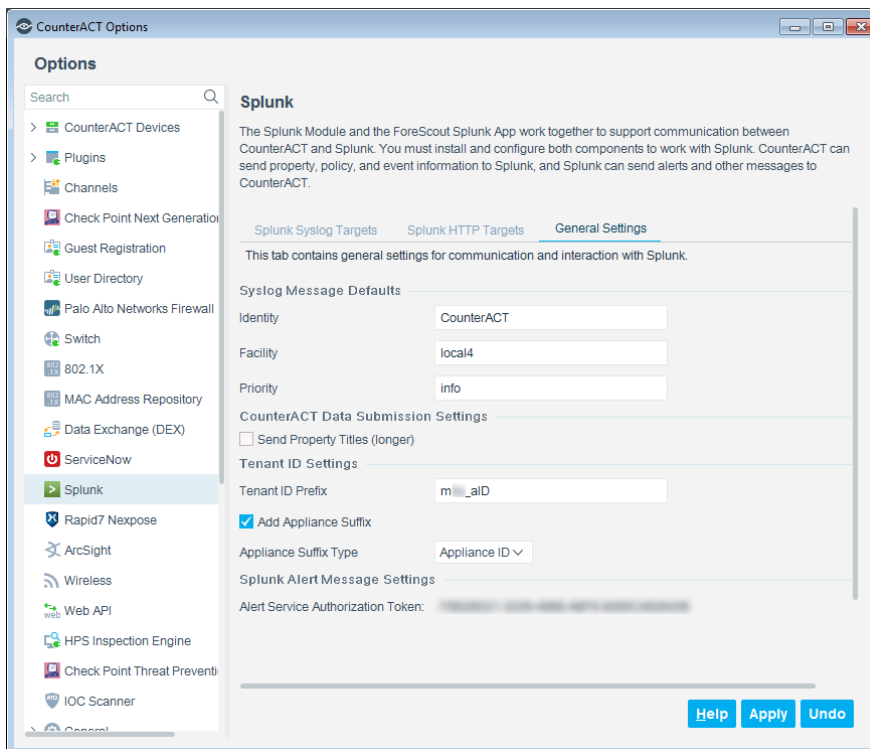
Index for CounterACT events

**Note:** The password will be encrypted and stored in Splunk's password store. It will not be displayed here if this page is visited again.

- In the CounterACT IP Address or Hostname field, enter the **IP address** of the Enterprise Manager or standalone CounterACT Appliance in your environment.

*If you are configuring ForeScout Technology Add-on for Splunk with CounterACT's Fully Qualified Domain Name (FQDN), then it must be specified in all lower case characters.*

- In the Enter password field, enter the **Alert Service Authorization Token**. You can get this token from the General Settings pane of the Splunk Module configuration. Refer to the *ForeScout Extended Module for Splunk Configuration Guide* for details.



**CounterACT Options**

**Options**

Search

- CounterACT Devices
- Plugins
- Channels
- Check Point Next Generation
- Guest Registration
- User Directory
- Palo Alto Networks Firewall
- Switch
- 802.1X
- MAC Address Repository
- Data Exchange (DEX)
- ServiceNow
- Splunk**
- Rapid7 Nexpose
- ArcSight
- Wireless
- Web API
- HPS Inspection Engine
- Check Point Threat Prevention
- IOC Scanner

**Splunk**

The Splunk Module and the ForeScout Splunk App work together to support communication between CounterACT and Splunk. You must install and configure both components to work with Splunk. CounterACT can send property, policy, and event information to Splunk, and Splunk can send alerts and other messages to CounterACT.

**Splunk Syslog Targets** **Splunk HTTP Targets** **General Settings**

This tab contains general settings for communication and interaction with Splunk.

**Syslog Message Defaults**

Identity:

Facility:

Priority:

**CounterACT Data Submission Settings**

☐ Send Property Titles (longer)

**Tenant ID Settings**

Tenant ID Prefix:

☒ Add Appliance Suffix

Appliance Suffix Type:

**Splunk Alert Message Settings**

Alert Service Authorization Token:

- Select **Save**.

6. **Restart** the Splunk Enterprise server.

## Splunk Roles for CounterACT

The following new Splunk roles are created when the ForeScout App for Splunk is installed. You can assign these roles when you create new users.

It is recommended to assign these roles to users who will work with the dashboards of the ForeScout App for Splunk.

### **counteract\_admin**

Users with this role can:

- Create alerts
- Create saved searches
- Create dashboards
- View Dashboards
- Create indices
- Search on all indices
- Enable/disable saved searches

### **counteract\_user**

Users with this role can:

- Create Dashboard
- View Dashboards
- Search on all indexes

User with this role cannot:

- Create alerts
- Create saved searches
- Enable/disable saved searches

## CounterACT Workflow for Adaptive Response

The ForeScout App for Splunk provides elements that support Splunk's Adaptive Response initiative in the following ways:

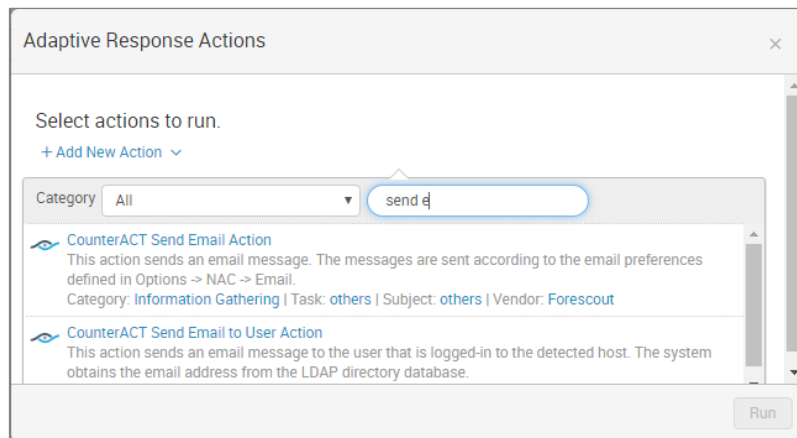
- **CounterACT alert action list:** the CounterACT Adaptive Response add-on initializes and maintains a list of actions by polling CounterACT's action\_info API. The frequency of update polling can be configured. This list represents the actions that CounterACT can apply to an endpoint based on Splunk alerts.
- **CounterACT events:** the rich stream of endpoint information that Splunk receives from CounterACT can be combined with information from other sources in searches that identify suspect endpoints or network events of concern.

- **CounterACT alerts (saved search):** The add-on provides predefined searches that mine standard endpoint properties reported by CounterACT to Splunk.
- **CounterACT Alert API:** Splunk sends action requests to CounterACT through a REST API interface.
- **CounterACT action response:** When it applies the requested actions to endpoints, CounterACT initiates the following messages:
  - *Synchronous response* - CounterACT acknowledges the action request, and initiates policy-based implementation of the action.
  - *Asynchronous response* - CounterACT reports the status of the requested action 4 hours after the request is received (configurable).
 See [CounterACT Response to Alert Messages](#).

In addition, the ForeScout App provides a dashboard that tracks actions requested by Splunk. See [Response Dashboard](#).

### With Splunk Enterprise Security

When Splunk Enterprise Security is deployed in the Splunk environment, the SOC team can use correlation searches provided with the ForeScout Add-on. When a correlation search generates a notable event, the SOC team can manually apply Adaptive Response Actions that invoke CounterACT actions on matching endpoints.



### In Splunk Enterprise Environments without Enterprise Security

Saved searches provided by the ForeScout Add-on for Splunk identify devices that match certain criteria based on various data feeds including CounterACT device data. The search results are associated with Alerts that invoke CounterACT actions. The result is scheduled searches that trigger action requests to CounterACT, which through policy decision act on devices identified by the periodic search queries.



## Correlation Searches and Saved Searches

The ForeScout App for Splunk installs the following predefined searches that mine standard device properties reported by CounterACT to Splunk.

Title	Actions	Owner	App	Sharing	Status
es_trigger_appt_cp_antivirus_ioc_notification	Open in Search	ForeScout	TA-forescout_response	Global	Enabled
es_trigger_appt_cp_threatemulation_ioc_notification	Open in Search	ForeScout	TA-forescout_response	Global	Enabled
es_trigger_bad_dns_notification	Open in Search	ForeScout	TA-forescout_response	Global	Enabled
es_trigger_bad_dns_send_email	Open in Search	ForeScout	TA-forescout_response	Global	Enabled
es_trigger_bad_dns_switch_block	Open in Search	ForeScout	TA-forescout_response	Global	Enabled
es_trigger_dot1x_action_failure_email	Open in Search	ForeScout	TA-forescout_response	Global	Enabled
es_trigger_dot1x_action_failure_notification	Open in Search	ForeScout	TA-forescout_response	Global	Enabled
es_trigger_ioc_scanner_notification	Open in Search	ForeScout	TA-forescout_response	Global	Enabled
es_trigger_ioc_scanner_send_email	Open in Search	ForeScout	TA-forescout_response	Global	Enabled
es_trigger_ioc_scanner_switch_block	Open in Search	ForeScout	TA-forescout_response	Global	Enabled
trigger_appt_cp_antivirus_ioc_notification	Open in Search	ForeScout	TA-forescout_response	Global	Enabled
trigger_appt_cp_threatemulation_ioc_notification	Open in Search	ForeScout	TA-forescout_response	Global	Enabled
trigger_bad_dns_notification	Open in Search	ForeScout	TA-forescout_response	Global	Enabled
trigger_bad_dns_send_email	Open in Search	ForeScout	TA-forescout_response	Global	Enabled
trigger_bad_dns_switch_block	Open in Search	ForeScout	TA-forescout_response	Global	Enabled
trigger_dot1x_action_failure_email	Open in Search	ForeScout	TA-forescout_response	Global	Enabled
trigger_dot1x_action_failure_notification	Open in Search	ForeScout	TA-forescout_response	Global	Enabled
trigger_ioc_scanner_notification	Open in Search	ForeScout	TA-forescout_response	Global	Enabled
trigger_ioc_scanner_send_email	Open in Search	ForeScout	TA-forescout_response	Global	Enabled
trigger_ioc_scanner_switch_block	Open in Search	ForeScout	TA-forescout_response	Global	Enabled
trigger_test_alerts_to_counteract	Open in Search	ForeScout	TA-forescout_response	Global	Enabled

The default saved searches are defined below:

Saved Search	Purpose
es_trigger_appt_cp_antivirus_ioc_notification	Enterprise Security Correlation Search based on CounterACT Malicious File Download that applies the CounterACT <i>Send Message to Syslog</i> action.
es_trigger_appt_cp_threatmulation_ioc_notification	Enterprise Security Correlation Search based on CounterACT Malware Activity that applies the CounterACT <i>HTTP Notification</i> action.
es_trigger_bad_dns_notification	Enterprise Security Correlation Search based on CounterACT Bad DNS Activity and applies the CounterACT <i>HTTP Notification</i> action.
es_trigger_bad_dns_send_email	Enterprise Security Correlation Search based on CounterACT Bad DNS Activity that applies the CounterACT <i>Send Email</i> action.
es_trigger_bad_dns_switch_block	Enterprise Security Correlation Search based on CounterACT Bad DNS Activity that applies the CounterACT <i>Switch Block</i> .
es_trigger_dot1x_action_failure_email	Enterprise Security Correlation Search based on CounterACT Authentication Failures that applies the CounterACT <i>Send Email</i> action.
es_trigger_dot1x_action_failure_notification	Enterprise Security Correlation Search based on CounterACT Authentication Failure Exceeding Threshold that applies the CounterACT <i>HTTP Notification</i> action.
es_trigger_ioc_scanner_notification	Enterprise Security Correlation Search

Saved Search	Purpose
	based on CounterACT IOC Scanner Activity that applies the CounterACT <i>HTTP Notification</i> action.
es_trigger_ioc_scanner_send_email	Enterprise Security Correlation Search based on CounterACT IOC Scanner Activity that applies the CounterACT <i>Send Email</i> action.
es_trigger_ioc_scanner_switch_block	Enterprise Security Correlation Search based on CounterACT IOC Scanner Activity that applies the CounterACT <i>Switch Block</i> .
trigger_appt_cp_antivirus_ioc_notification	Saved Search based on CounterACT Malicious File Download that applies the CounterACT <i>Send Message to Syslog</i> action.
trigger_appt_cp_threatemulation_ioc_notification	Saved Search based on CounterACT Malware Activity that applies the CounterACT <i>HTTP Notification</i> action.
trigger_bad_dns_notification	Saved Search based on CounterACT Bad DNS Activity and that applies the CounterACT <i>HTTP Notification</i> action.
trigger_bad_dns_send_email	Saved Search based on CounterACT Bad DNS Activity that applies the CounterACT <i>Send Email</i> action.
trigger_bad_dns_switch_block	Saved Search based on CounterACT Bad DNS Activity that applies the CounterACT <i>Switch Block</i> .
trigger_dot1x_action_failure_email	Saved Search based on CounterACT Authentication Failures that applies the <i>Send Email</i> action.
trigger_dot1x_action_failure_notification	Saved Search based on CounterACT Authentication Failures that applies the CounterACT <i>HTTP Notification</i> action.
trigger_ioc_scanner_notification	Saved Search based on CounterACT IOC Scanner Activity and that applies the CounterACT <i>HTTP Notification</i> action.
trigger_ioc_scanner_send_email	Saved Search based on CounterACT IOC Scanner Activity that applies the CounterACT <i>Send Email</i> action.
trigger_ioc_scanner_switch_block	Saved Search based on CounterACT IOC Scanner Activity that applies the CounterACT <i>Switch Block</i> .
trigger_test_alerts_to_counteract	Searches for test events from CounterACT and replies with a test alert message. See <a href="#">Alerts</a> for more information.

## Alerts

The ForeScout App for Splunk installs a set of Alerts that instruct CounterACT to apply actions to matching endpoints in real time.

### To view an alert:

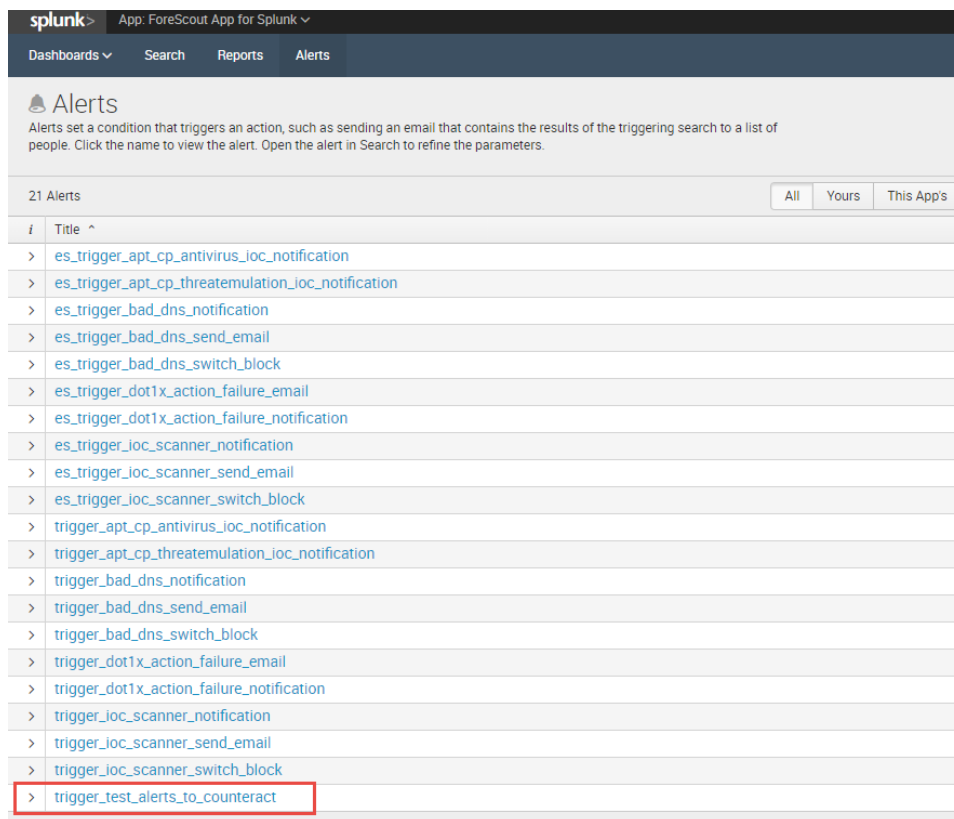
1. In the left corner, select **App Search and Reporting**. The Alerts page displays the default Saved Searches.

One default search that is especially helpful is the Trigger Test Alerts to CounterACT. This searches for test events from CounterACT and replies with a test alert message. The purpose is to mimic an actual alert message and verify that it got delivered to CounterACT.

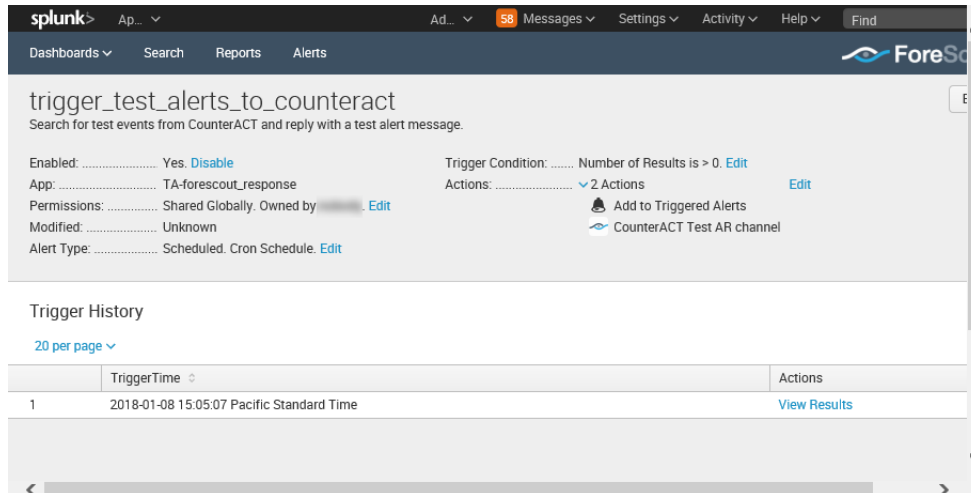
### To view the contents of an alert / saved search:

You can optionally view the details of a saved search and see what it contains. We will use the *trigger\_test\_alerts\_to\_counteract* alert as an example.

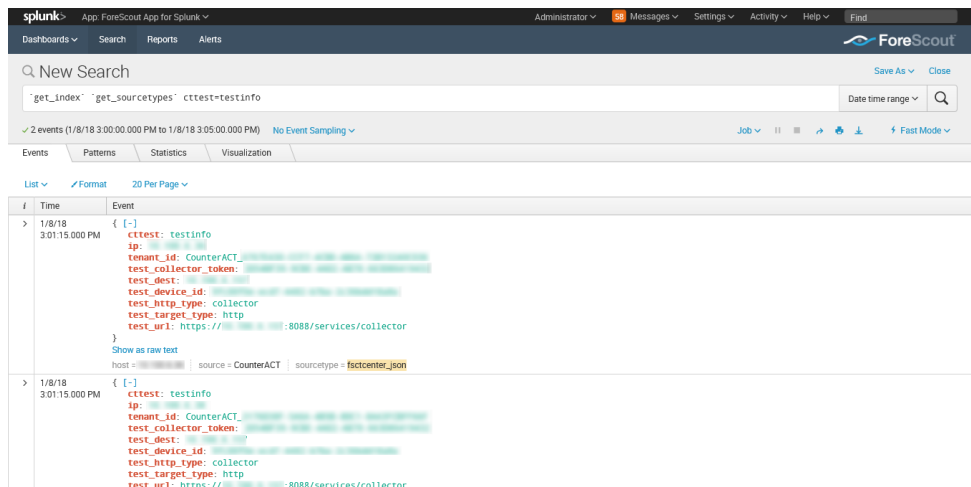
1. In the Alerts page, select **trigger\_test\_alerts\_to\_counteract**.



2. The *trigger\_test\_alerts\_to\_counteract* page displays. Select the **View Results** link.



### 3. The event details of the search results displays.



### 4. You can view information like IP address, target device details, etc. These are configured in the Splunk Module. Refer to the *ForeScout Extended Module for Splunk Configuration Guide* for more information.

## Configuring your Alerts

This section provides an example of the default alert. Please note that with Splunk Module version 2.7, the structure of the query has changed. When you are creating your alert, you will need to fill in the Search Description, Search Name, Search Query, Action Name, API call to CounterACT, and Sample log/event fields.

#### To create an alert:

1. Select **New**.
2. Enter information into the Search Name and Search fields. All other fields are optional.
3. Select **Save**.

Sample Alert configurations are shown below.

### **Search Description:**

Search for CounterACT Bad DNS Activity

### **Search Name:**

trigger\_bad\_dns\_notification

### **Search Query:**

```
`get_index` `get_sourcetypes` `ct_hostinfo` dnsniff_event
| rename host_properties.dnsniff_event{}.value as dnsniff_event
| mvexpand dnsniff_event
| rex field=dnsniff_event "DNS Query
Type:\s*(?<DNSQueryType>[^\s]*);DNS Query/Response: Query;DNS Zone:
;DNS Addresses.*"
| search DNSQueryType="A"
| eventstats count as eventcount by ip
| dedup ip
| where eventcount>5 AND eventcount<=10
```

### **Action Name:**

CounterACT HTTP Notification Action

### **API call to counterACT:**

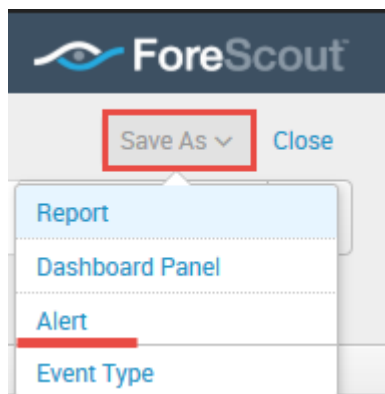
[http://em\\_ip/splunk/alerts?disposition=3&action\\_group=notify&auth=CounterACT%20token](http://em_ip/splunk/alerts?disposition=3&action_group=notify&auth=CounterACT%20token)

### **Sample log/event:**

```
> 1/24/18 12:38:53.000 AM { [-]
  ctupdate: hostinfo
  dntdomain: calab.forescout.com
  host_properties: { [-]
    dnsniff_event: { [-]
      { [-]
        since: 1516747030
        value: DNS Name: 10.10.10.1 In-addr.arpa;DNS Query Type: PTR;DNS Query/Response: Query;DNS Zone: ;DNS Addresses: ;DNS Server Address: ;DNS Monitoring Tag: policy
      }
      { [-]
        since: 1516747030
        value: DNS Name: 10.10.10.1 In-addr.arpa;DNS Query Type: PTR;DNS Query/Response: Response;DNS Zone: 10.10.10.1 IN SOA f60.forescout.com. hostmaster.forescout.com. ;DNS
        Addresses: ;DNS Server Address: ;DNS Monitoring Tag: policy
      }
      { [-]
        since: 1516747119
        value: DNS Name: 10.10.10.1 In-addr.arpa;DNS Query Type: PTR;DNS Query/Response: Query;DNS Zone: ;DNS Addresses: ;DNS Server Address: ;DNS Monitoring Tag: policy
      }
      { [-]
        since: 1516747119
        value: DNS Name: 10.10.10.1 In-addr.arpa;DNS Query Type: PTR;DNS Query/Response: Response;DNS Zone: 10.10.10.1 IN SOA f60.forescout.com. hostmaster.forescout.com. ;DNS
        Addresses: ;DNS Server Address: ;DNS Monitoring Tag: policy
      }
      { [-]
        since: 1516747129
        value: DNS Name: 10.10.10.1 In-addr.arpa;DNS Query Type: PTR;DNS Query/Response: Query;DNS Zone: ;DNS Addresses: ;DNS Server Address: ;DNS Monitoring Tag: policy
      }
      { [-]
        since: 1516747129
        value: DNS Name: 10.10.10.1 In-addr.arpa;DNS Query Type: PTR;DNS Query/Response: Response;DNS Zone: 10.10.10.1 IN SOA f60.forescout.com. hostmaster.forescout.com. ;DNS
        Addresses: ;DNS Server Address: ;DNS Monitoring Tag: policy
      }
      { [-]
        since: 1516747059
        value: DNS Name: 10.10.10.1 In-addr.arpa;DNS Query Type: PTR;DNS Query/Response: Query;DNS Zone: ;DNS Addresses: ;DNS Server Address: ;DNS Monitoring Tag: policy
      }
      { [-]
        since: 1516747059
        value: DNS Name: 10.10.10.1 In-addr.arpa;DNS Query Type: PTR;DNS Query/Response: Response;DNS Zone: 10.10.10.1 IN SOA f60.forescout.com. hostmaster.forescout.com. ;DNS
        Addresses: ;DNS Server Address: ;DNS Monitoring Tag: policy
      }
      { [-]
        since: 1516747052
        value: DNS Name: 10.10.10.1 In-addr.arpa;DNS Query Type: PTR;DNS Query/Response: Query;DNS Zone: ;DNS Addresses: ;DNS Server Address: ;DNS Monitoring Tag: policy
      }
    }
  }
}
```

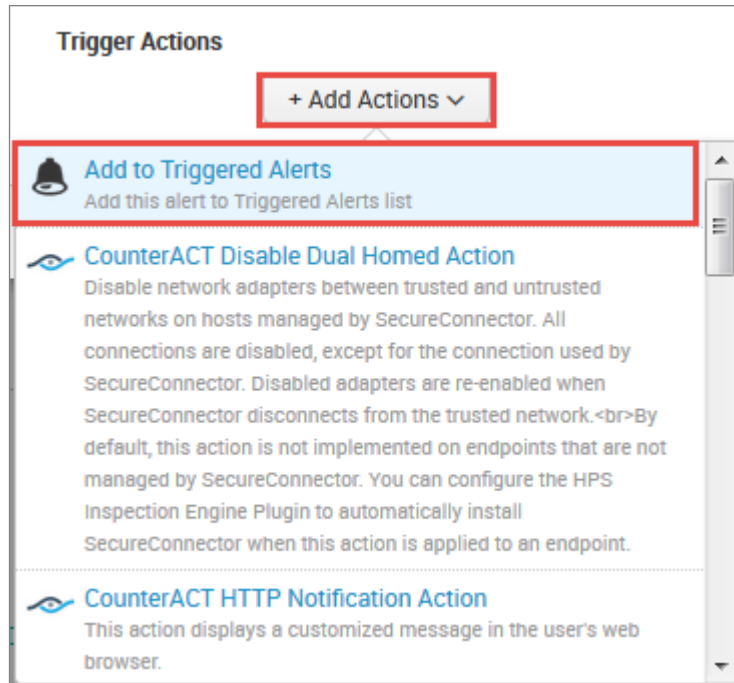
## How to create an Alert with Trigger Actions

1. In the ForeScout App for Splunk, run a search.
2. Under the ForeScout logo, select **Save As** and then select **Alert**.

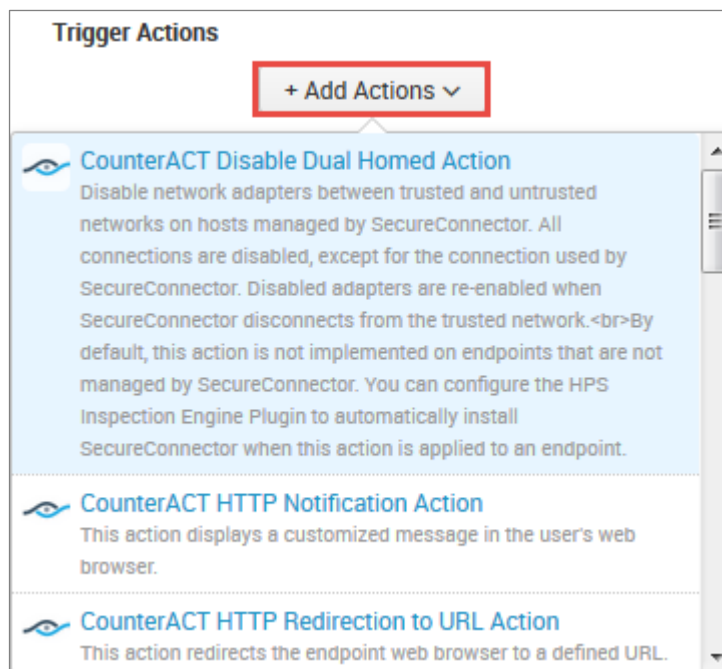


3. The Save As Alert dialog box opens.

4. Define the schedule and trigger conditions.
5. In the Trigger Actions section, select **Add Actions** and then select **Add to Triggered Alerts**. This step is always required when you want to save a new Alert.



6. In the Trigger Actions section, select **Add Actions** again and then **select a ForeScout action** item from the list.



7. The bottom of the Saved As Alert dialog box displays the triggered alert setting.

When triggered	<div>  CounterACT HTTP Redirection to URL </div> <div>Remove</div>
Action	
>	<div>  Add to Triggered Alerts </div> <div>Remove</div>

8. Select **Save**; your new saved search displays in the Alert page. When the saved search runs, the alert message tells CounterACT to apply the action to endpoints that match the search.

For more information on configuring alert trigger conditions, refer to the [Splunk Alerting Manual](#).

## Customizing your own Alerts

The Index, Source, and Sourcetype, fields must be addressed in the Search Query for the customized alert.

### Index

In Splunk, any application event data is stored in indexes. It is good practice to create indexes at the time of installation of the apps before any app configuration is done. For ForeScout Apps, different indexes are used for different purposes as described below:

Index Name	Created in App/Manual	Purpose/Type of event data
fsctcenter (or name of your choice)	Should be created Manually	<p>All the event data forwarded from CounterACT to Splunk using any of the Channels viz. Syslog/UDP, REST API or HEC Collector is stored in this index.</p> <p>It also stores all Modular Alert Action execution logs, events that triggered this actions and the response events of the Action API calls are stored in this index</p>
_internal	Available as part of Splunk framework.	All the Saved Search and their execution time related information are stored in this index.
_introspection	Available as part of Splunk framework.	All the Splunk Performance related metrics are logged here

Above indexes are used in various dashboards of “ForeScout CounterACT App for Splunk” and “Enterprise Security”. It should be noted that these indexes should not be cleaned otherwise the information on Modular Alert Action executions will be lost.



## Source and Sourcetype

Source and Sourcetype are default Splunk fields to categorize and parse indexed data in a proper way. Below is the table which shows how the CounterACT related event data is distributed in these fields.

Please read more about the default fields at:

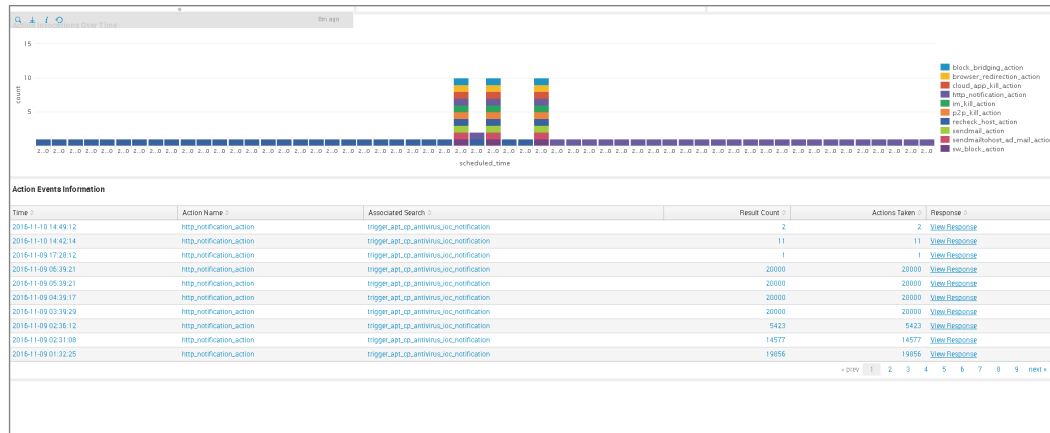
<http://docs.splunk.com/Documentation/Splunk/6.4.3/Data/Aboutdefaultfields>

Index Name	Source	Sourcetype	Purpose/Type of event data
fsctcenter (or name of your choice)	CounterACT	fsctcenter_avp	This contains all the event data sent from CounterACT to Splunk using Syslog UDP/TCP ports
fsctcenter (or name of your choice)	CounterACT	fsctcenter_json	This contains all the event data sent from CounterACT to Splunk using either REST API or HEC Collector
fsctcenter (or name of your choice)	modactions	counteract_alerts	All the Adaptive Response Framework Alert Action related logs are written in this category. This will also have the Alert Action API call responses.
fsctcenter (or name of your choice)	modactions	counteract_orig_event	The original events from index=fsctcenter which triggered any Modular Alert Action are stored here with their corresponding Splunk search_id and row_id of the event results.
_internal	/opt/splunk/var/log/splunk/scheduler.log	scheduler	All the Saved Search and their execution time related information are stored here.

## CounterACT Response to Alert Messages

When CounterACT receives a Splunk alert message:

- It sends a confirmation message to Splunk indicating that the alert has been received. This is called the *synchronous response* to the alert message.
- It parses alert fields to update the Splunk Alerts and Splunk Last Alert host properties for devices listed in the alert message.
- It initiates CounterACT policies that evaluate Splunk alert host properties, and apply the requested action to these devices.
- The synchronous response to Splunk Alert messages can be seen on the Response dashboard. The Action Events Information table displays each alert message together with the synchronous response received for each from CounterACT.



The Splunk Module tracks the progress of actions requested by Splunk alerts, and reports the final status of the action. This is called the *asynchronous response* to the alert message. By default this report is generated 4 hours after the alert message is received. The report interval is configurable. Refer to the *ForeScout Extended Module for Splunk Configuration Guide* for details. If an alert requested several actions, a report is generated for each action, identifying its alert message.


To yield significant action status values:

- Endpoints must exist in CounterACT when the report is generated.
- There should be an active CounterACT policy that detects the Splunk Alert property that is updated by the alert message, and apply the action requested by the alert.

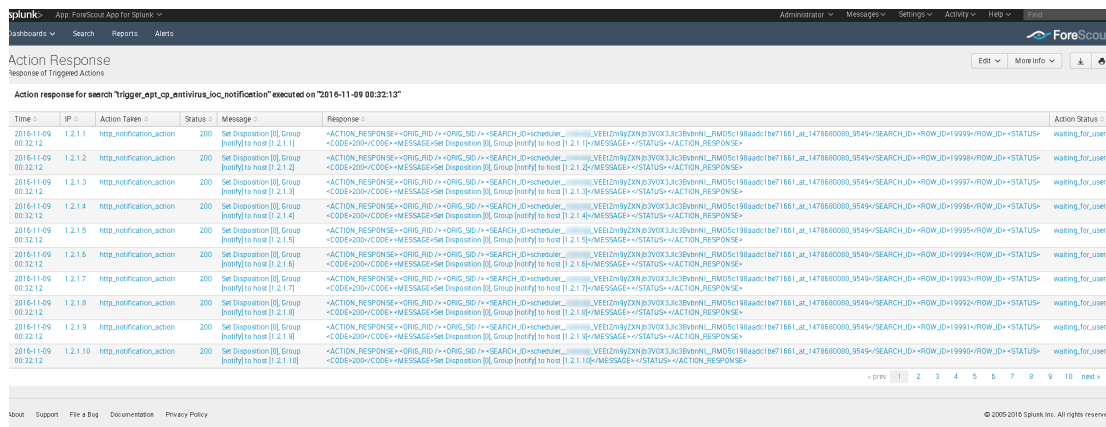
In other situations, error status values are returned.

The following action status values are reported by CounterACT.

Value	Description
<b>Success</b>	The action completed without failure.
<b>Failure</b>	The action completed with a failure, or timed out.
<b>Pending</b>	At the time the report is generated, the action is not yet complete. For example, HTTP redirection actions may be waiting for user interaction to complete.
<b>Init</b>	The action is in Initializing state, and not yet complete.

Value	Description
<b>No Status</b>	<p>No status can be reported for one of the following reasons:</p> <ul style="list-style-type: none"> <li>No active policy detects the relevant Splunk Last Alert property, or applies the requested action.</li> <li>The endpoint has been deleted from CounterACT.</li> <li>Even though the IP address of the endpoint is within CounterACT's network scope, the endpoint has not been detected by CounterACT.</li> <li>Scheduled CounterACT data purges clear action data before reports are generated.</li> </ul> 
<b>Invalid</b>	<ul style="list-style-type: none"> <li>The endpoint IP is outside the network scope defined in CounterACT.</li> <li>An unspecified internal error occurred.</li> </ul>

The Response dashboard can also map the synchronous and asynchronous responses to alert messages. In the Action Events Information table, select the **View Response** hyperlink. The Action Response page displays.



The screenshot shows the 'Action Response' dashboard in Splunk. The title is 'Response of Triggered Actions'. Below the title, it says 'Action response for search "trigger\_apt\_op\_mitigates\_loc\_notification" executed on "2016-11-09 00:32:13"'. The table has columns: Time, IP, Action Taken, Status, Message, Response, and Action Status. The table contains 10 rows of data, all with a status of 200. The 'Action Status' column shows 'waiting\_for\_user' for all entries.

The screenshot above shows the alert details given from Splunk to the CounterACT Module. For example, some fields listed are the endpoint's IP address that the event was triggered by, the action triggered by the saved search, and synchronous and asynchronous response for the same.

Note that:

- For HTTP Redirection actions, the module can only report either *Pending* or *No Status*. The module cannot report *Success* for these actions.
- If CounterACT users or other CounterACT policies apply the same action to an endpoint that was requested by a Splunk alert, CounterACT will report the result of the most recent application of the action. The report cannot distinguish between the triggers that applied the action to an endpoint.

## Targeting Devices in Alerts Sent to CounterACT

A list of actions provided by CounterACT are specified in the Splunk search or manually added by the Splunk user and triggered. The alert messages sent to CounterACT must reference a specified device. Typically CounterACT acts in response to the Splunk alert message by applying the requested action on the endpoint. IP address is used to identify an device. This leads to the following considerations:

## Best Practices for Scheduling Saved Searches

Follow these suggested guidelines to distribute launch of saved searches, preventing resource peaks and bottlenecks.

- Configure offsets in the Cron Schedule parameter.  
  
All Cron expressions are evaluated based on an internal clock maintained by the Splunk framework. When searches are configured with a simple time period expression in the Cron interval, all searches with the same interval tend to be launched nearly simultaneously based on the internal clock.
- It is recommended to configure Cron expressions that offset the start of search launch in relation to the internal clock. For example, the following expression configures the search to repeat every 5 minutes, but delays search launch by 3 minutes relative to the internal clock.  
  
`3-59/5 * * * *`
- The repeat interval should exceed evaluation time. For example, if the action script attached to a search times out after 10 minutes, the search should repeat at a greater interval than 10 minutes.

If the operator decides to write custom saved searches and associated correlation searches, it is very important to stagger the searches so that they run at different times. If this is not done, the searches will all start at the same time and compete with each other for resources. Below are some guidelines for configuring scheduling time intervals so that all searches will be evenly distributed on the Splunk server.

- a. The Cron Schedule parameter should be properly configured in order to spread the execution time of saved searches. Referring to the screen shot below, `*/5 * * * *` means that this saved search will run every 5 minutes according to an internal clock which is managed by Splunk framework. For example, the operator created a search and saved it at 5:15pm. If Splunk's 5-minute period is ending at 5:18pm, the saved search will start at 5:18pm and every 5 minutes after that. If all saved searches are configured like this, they all will get executed exactly at the same time every 5 minutes.

In order to avoid that, configure different starting times for each saved search so they still get executed every 5 minutes but at different times. We can configure “3-59/5 \* \* \* \*” in other saved searches. For example, the operator created a search and saved it at 5:15pm. If Splunk’s 5 minute period is ending at 5:18pm, it will start at 5:21pm (3-minutes later) and every 5-minutes after that.

- b. Another scenario is where each saved search’s action script takes 10-minutes time (at maximum) to execute or it will timeout and exit. All the saved searches mapped with alert actions should also be scheduled to execute after 10-minutes. Otherwise, the system will be overloaded trying to process the new action while the previous action is still running.

## Working with Dashboards

Dashboards are powerful tools that let you visualize CounterACT detection processes and management policies, and drill-down to monitor changes in host properties on endpoints. The app provides the following dashboards based on information reported by CounterACT.

- [Summary Dashboard](#)
- [CounterACT Policy Dashboard](#)
- [Network Insight and Discovery Dashboard](#)
- [Response Dashboard](#)
- [System Overview Dashboard](#)
- [Host Detail View Dashboard](#)

You can modify these standard dashboards, or create custom dashboards or graphs.

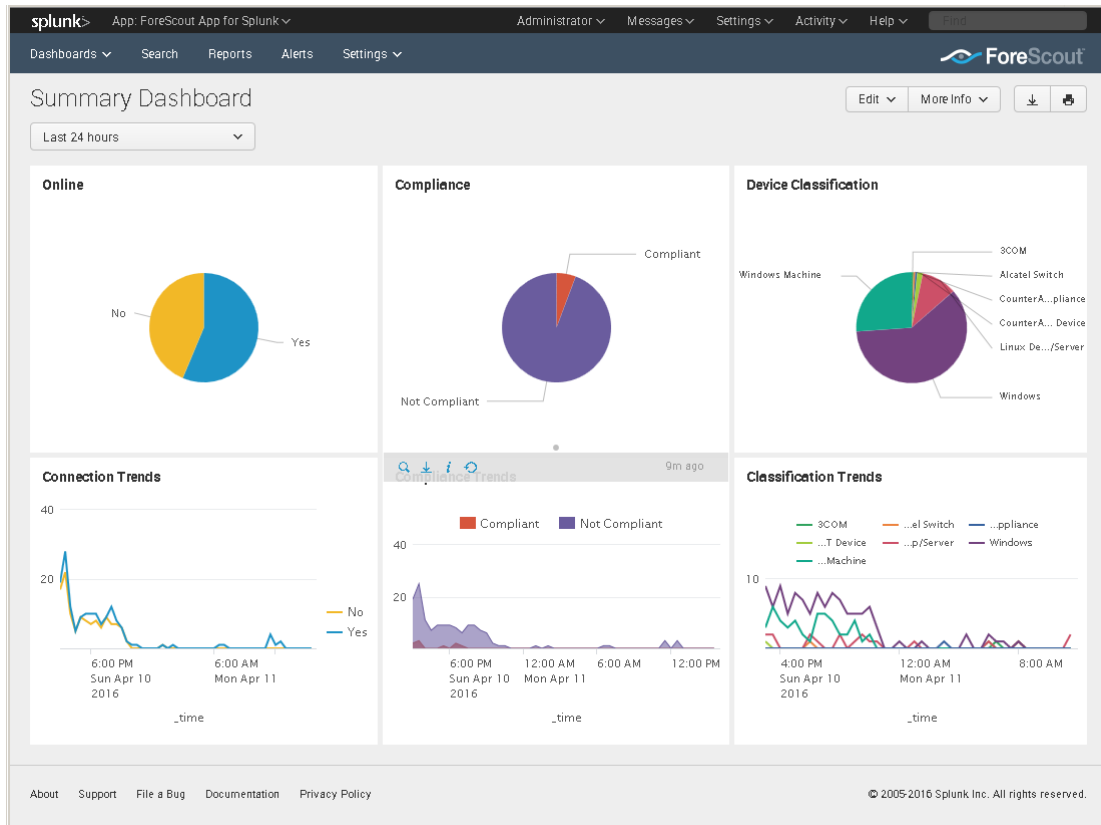
When working with dashboards:

- Remember that Splunk can only display CounterACT host property and policy information that has been sent to Splunk. Define policies in CounterACT that report the information you want to work with in Splunk, and tune reporting frequency to suit your data analysis needs.
- Hover over the graph to view details and percentages.

- Hover at the bottom of the graph and select **Open in Search** to view the Splunk search used to generate the graph.

## Summary Dashboard

The Summary dashboard presents six basic status charts based on endpoint properties reported by CounterACT.



### Online

This panel shows the relative frequency of online and offline status during the time period of the chart, for all endpoints within the reporting scope.

### Connection Trends

This panel tracks the online or offline status of endpoints within the reporting scope over time. The graph shows the variation in the total number of endpoints that are online or offline during the specified time period.

### Compliance

This panel displays the results of compliance policies. The graph shows the relative prevalence of compliant/non-compliant endpoints during the charted period, as a percentage of all endpoints within the reporting scope.

## Compliance Trends

This panel tracks the results of compliance policies over time. The graph shows the number of endpoints that were compliant or non-compliant over the specified period.

## Device Classification

This panel shows the overall results of endpoint classification policies. The graph shows the relative prevalence of different types of endpoint during the charted period, as a percentage of all endpoints within the reporting scope.

## Classification Trends

This panel tracks the results of endpoint classification policies over time. The graph shows changes in the relative number of different endpoint types in the network over the specified time period.

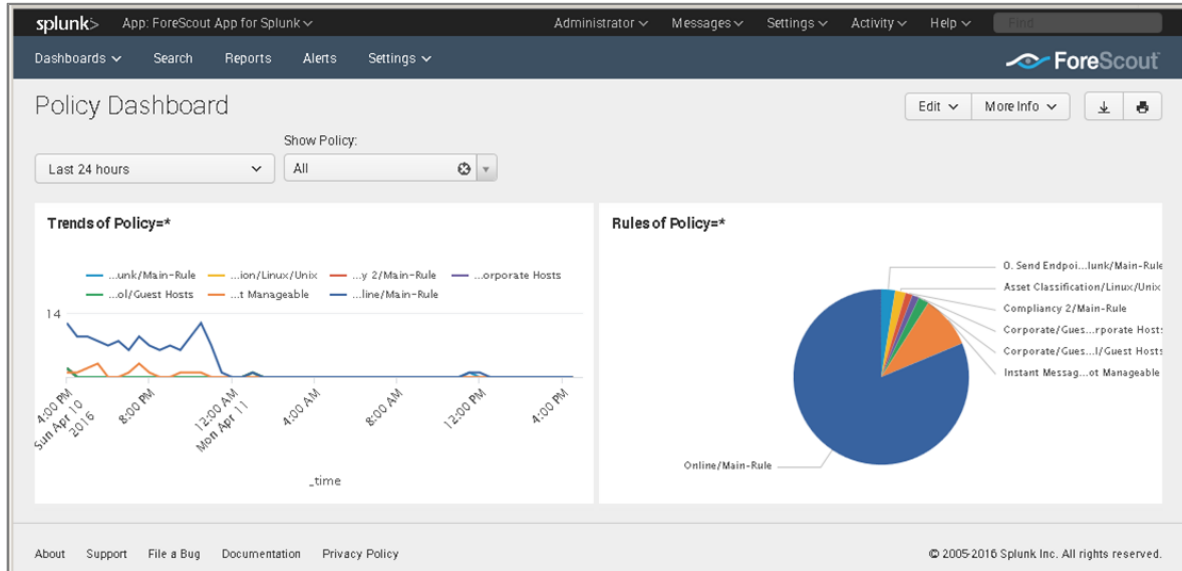
# CounterACT Policy Dashboard

The CounterACT Policy dashboard presents charts that track how CounterACT policies evaluate endpoints.

The **Trends of Policy** graph shows how policy rules evaluate endpoints over time.

The **Rules of Policy** pie chart shows how many endpoints matched each rule of active CounterACT policies during the specified reporting period.

Initially, the graph shows aggregate information for all policies reported to Splunk.



Typically it is more useful to look at how individual policies evaluate endpoints. In the **Show Policy** drop-down, select a CounterACT policy.

## Network Insight and Discovery Dashboard

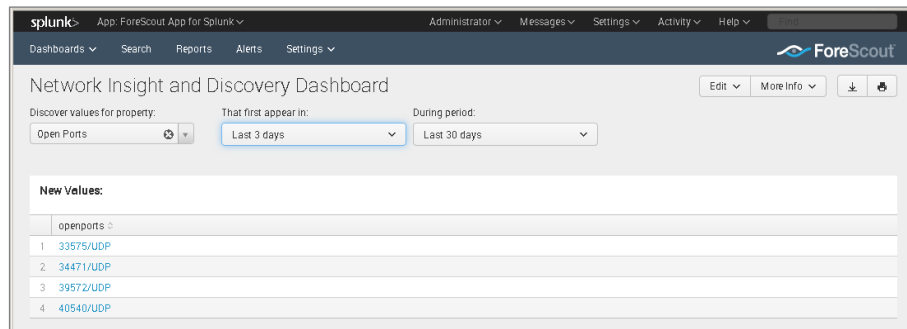
The Network Insight and Discovery dashboard tracks changes in a core set of CounterACT host properties. Use this dashboard to identify anomalous behavior and significant changes in the users, processes, applications, and other metrics associated with endpoints.

### To use the Network Insight and Discovery dashboard:

1. Select the CounterACT host property you wish to view in the Discover Values for Property drop-down.
2. Use the following drop-down fields to specify search criteria:

<b>That first appear in</b>	The search finds new property values that first occur during the period specified in this field. Typically this is the shorter time period specified.
<b>During period</b>	The overall time frame that is searched for new property values. Typically this is the longer time period specified.

The dashboard displays values of the selected property that *first* appear during the interval specified in **That first appear in**  
AND  
Do *not* appear before then within the **During period**.



The dashboard can be used to track the following CounterACT host properties:

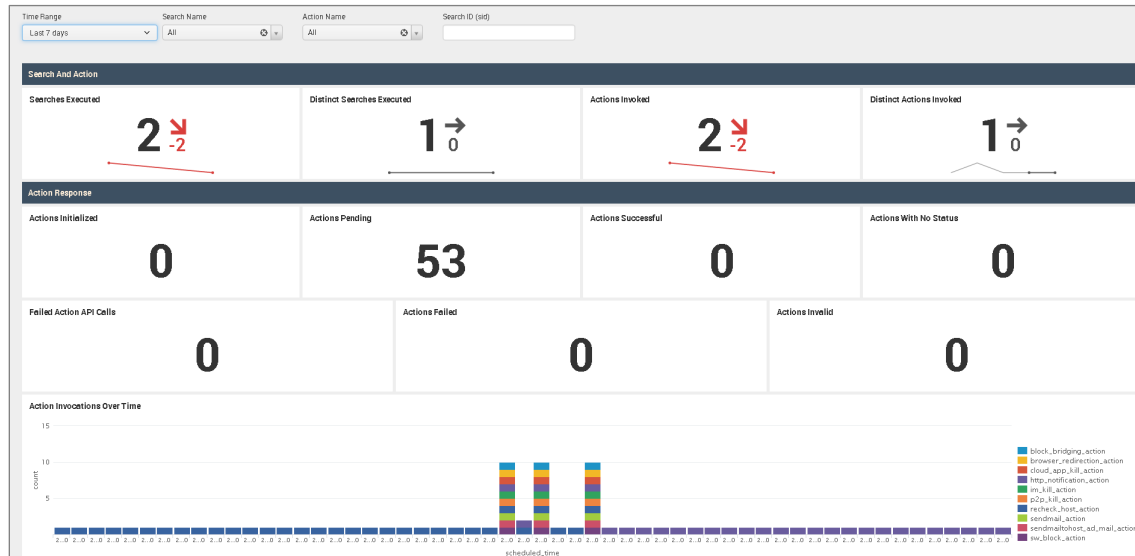
- Instant Messaging Running
- Linux Running Processes
- MAC Running Processes
- Network Function
- Open Ports
- P2P Running
- Switch IP
- Switch Port Name
- Windows Applications Installed
- Windows Processes Running
- Windows Services Installed



- Windows Services Running
- WLAN AP Name

# Response Dashboard

The Response dashboard provides the detailed analysis of Adaptive Response Framework Actions executed by CounterACT for incidents in Splunk Enterprise Security. Refer to [CounterACT Workflow for Adaptive Response](#).



In the Search and Action section, the single-value panels reflect the total count based on the filters applied at the top of the dashboard.

- **Searches Executed** - indicates the number of Saved Searches executed for which CounterACT Alert Actions are mapped.
- **Distinct Searches Executed** - indicates the total number of unique Saved Searches executed for which CounterACT Alert Actions are mapped. If a specific saved search was executed twice, the Searches Executed panel counts both executions of the alert, but the Distinct Searches Executed panel only counts one unique alert execution.
- **Actions Invoked** - indicates the total number of CounterACT Alert Actions invoked. Several alert actions can be mapped to a single saved search. This panel indicates the total number of alert actions executed by CounterACT.
- **Distinct Actions Invoked** - indicates how many unique Alert Actions were executed.

In these panels, the trend is shown beside the actual count. Trend values in green indicate an increase over the last 24 hours. Trend values in red indicate a decrease compared to 24 hours ago.

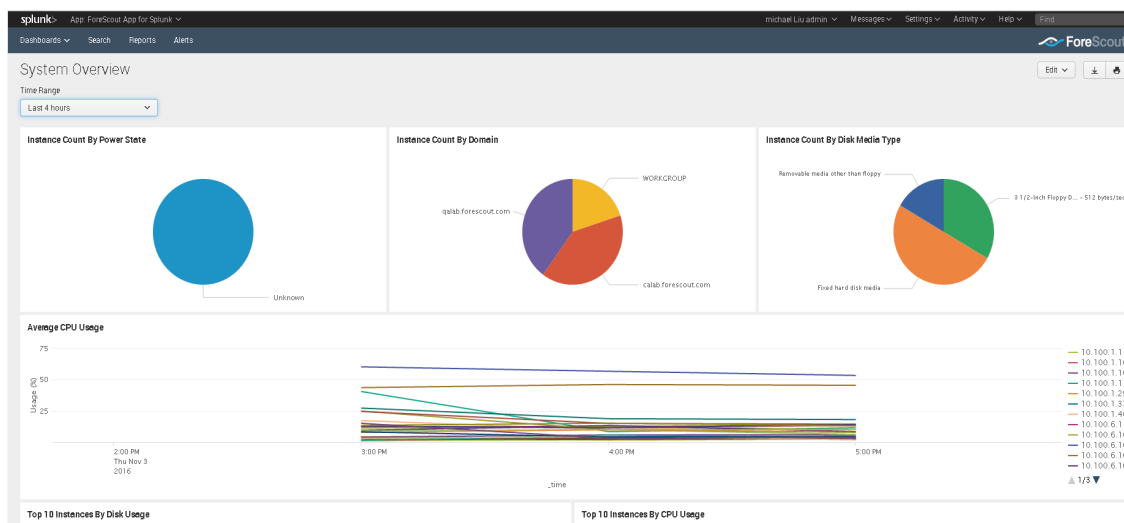
In the Action Response section, the single-value panels reflect the total count of each action status reported to Splunk by CounterACT.

- **Actions Initialized** - Displays the count of Alert Actions for which asynchronous response is received from CounterACT to Splunk with status *init*.
- **Actions Pending** - Displays the count of Alert Actions for which asynchronous response is received from CounterACT to Splunk with status *waiting\_for\_user*.
- **Actions Successful** - Displays the count of Alert Actions for which asynchronous response is received from CounterACT to Splunk with status *success*.
- **Actions with No Status** - Displays the count of Alert Actions for which asynchronous response is received from CounterACT to Splunk with status *no\_status*.
- **Failed Action API Calls** - Displays the count of Alert Actions for which the synchronous response of CounterACT API calls was received with error and the status code was not 200.
- **Actions Failed** - This panel shows the count of Alert Actions for which asynchronous response is received from CounterACT to Splunk with status *failure*.
- **Actions Invalid** - This panel shows the count of Alert Actions for which asynchronous response is received from CounterACT to Splunk with status *invalid*.

The Action Invocations Over Time section displays the count of Alert Actions where the CounterACT API call failed with an error code other than 200.

## System Overview Dashboard

The System Overview dashboard helps administrators track system resources efficiently by providing a summary of endpoint health including details of CPU, memory and disk drives. It presents System Health events reported by the Hardware Inventory Module in CounterACT. For Windows machines, system information also includes details of certificates stored in the device.



## Host Detail View Dashboard

The Host Detail View dashboard provides detailed inventory and performance information for a specific endpoint. This dashboard is also dependent upon the Hardware Inventory module.

Dashboards ▾
Search
Reports
Alerts

ForeScout

Host Detail View

Time Range

IP Address

Last 4 hours ▾

All

Host Information

IP	Name	Manufacturer	Model	OEM String Array	Processor	Power State	Bootup State	Status	Total Physical Memory (MB)
10.0.0.100	QA-HYPER-V	Dell Inc.	PowerEdge R610	Dell System,5[0000]	1	Unknown	Normal boot	OK	5110.08203125
10.0.0.100	NIRG-W8-64BIT	VMware, Inc.	VMware Virtual Platform	[MS_VM_CERT/SHA1 /27d66596a51c48dd3dc7216fd715126e33f59ae7],Welcome to the Virtual Machine	2	Unknown	Normal boot	OK	3071.55078125

Network Information

IP	MAC ADDRESS	Description	Service Name	Gateway	DHCP Enabled
10.0.0.100		Microsoft ISATAP Adapter	tunnel	10.0.0.100	No
10.0.0.100					

Processor Information

IP	Name	Device ID	Architecture	Total CPU Cores
10.0.0.100	Intel(R) Xeon(R) CPU E5620 @ 2.40GHz	CPU0	x64	4
10.0.0.100	Intel(R) Xeon(R) CPU E5-4667 v3 @ 2.00GHz	CPU0	x64	1

Domain Information

IP	Domain	Domain Role	Part of Domain
10.0.0.100	WORKGROUP	Standalone Server	No
10.0.0.100	10.0.0.100.forescout.com	Member Workstation	Yes

Physical Memory Information

No results found.


## Appendix A: Distributed Deployment

For more information about distributed and clustered deployments, see:

<http://docs.splunk.com/Documentation/Splunk/6.6.2/Deploy/Distributedoverview>

**To determine the installation of ForeScout Splunk Apps in a Distributed Splunk Environment:**

App Name	Splunk Search Head Instance	Splunk Indexer Instance	Splunk Forwarder Instance (Universal or Heavy Forwarder)
ForeScout App for Splunk (forescout_app)	Yes		
ForeScout Technology Add-on for Splunk (TA-forescout)	Yes (Setup Required)	Yes (No Setup)	Optional (No Setup)
ForeScout Adaptive Response Add-on for Splunk (TA-forescout_response)	Yes (Will utilize credentials provided in TA-forescout setup)		
Create Index fsctcenter	Yes	Yes	Yes

 *Splunk Cloud Deployment does not allow API calls to external devices (outside Splunk Cloud Infrastructure) directly as a part of Adaptive Response functionality from Splunk Cloud Search Heads. More details on possible ways to do this can be available from Splunk Cloud team.*

## Forwarding Event Data from CounterACT to Splunk

### Possible Communication Channels

Below are the communication channels in which CounterACT can send event data to Splunk

- **HTTP Event Collector (HEC)**

Splunk Enterprise server provides a secured token-based messaging that can be called by the Splunk Module to send event data. HTTP Event Collector needs to be configured in Splunk Data Inputs and is not enabled by default.

It is highly recommended that HTTP Event Collector be used for forwarding event data from CounterACT to the Splunk Enterprise server.

- **Syslog**

TCP/UDP Syslog ports can be configured in Splunk Data Inputs which will listen to event data sent from CounterACT Syslog plugin.

Syslog support is available on all Splunk Enterprise versions including Splunk Universal Forwarders.

📄 *Make sure the index in the Syslog data inputs that is defined on the Splunk Enterprise server uses the same port configured in the ForeScout Extended Module for Splunk.*

- **Simple REST Input**

Splunk provides a built-in Simple REST Input feature with Basic Authentication of which a Splunk hosted REST API can be called by the Splunk Module to send event data. Simple REST Input are enabled by default on Splunk Enterprise.

Simple REST Input support is available on all Splunk Enterprise versions including Splunk Universal Forwarders.

📄 *It is very important to configure only one communication channel to send event data to the Splunk Instance. If multiple channels are configured in CounterACT, duplicate event data will be sent to Splunk - resulting in incorrect statistics displayed in the Splunk App.*

## Forward Event Data to On-premise Distributed Splunk Deployments

Below are the possible ways to forward event data to Splunk from CounterACT:

- Send data directly to Indexers  
ForeScout CounterACT can send event data directly to Splunk Indexers using above mentioned Communication channels.
- Send data to Indexers via Forwarders  
But in some scenarios, we can choose to send event data to Splunk Forwarder and in then Splunk Forwarder can forward all the event data to Splunk Indexers. This can be useful in load balancing situations as Splunk Indexers are generally loaded with processing of Splunk Search queries.

## Forward Event Data to Splunk Cloud Deployments

Below are the possible ways to forward event data to Splunk from CounterACT:


- Send data directly to Splunk Cloud Indexers via HEC  
ForeScout CounterACT can send event data directly to Splunk Indexers deployed on Splunk Cloud using HEC Collector channel. In this case, Splunk Cloud will configure and provide load balancing tools.
- Send data to Splunk Cloud Indexers via on-premise Splunk Forwarders

Forescout CounterACT can send event data to on-premise Splunk Forwarders which can then forward the event data to Splunk Cloud Indexers. In this scenario, there is a pre-defined way how to provide SSL Certificates and Forwarding Configurations to Splunk Forwarders. More details on this can be provided by Splunk Cloud team.

## Appendix B: Upgrade to Splunk Module version 2.8 and ForeScout Apps for Splunk 2.7

This section covers upgrading from Splunk Module 2.5 and 2.7 and ForeScout Apps for Splunk version 2.5, 2.6 or 2.7. This release introduces significant functional and structural changes in both the Splunk Module and ForeScout Apps for Splunk.

- Before upgrading, make sure that you have Splunk Module 2.5 installed and the ForeScout Apps & Add-ons for Splunk version 2.5 or 2.6 in working condition.
- Before upgrading, make sure that you have Splunk Module 2.7 installed and the ForeScout Apps & Add-ons version 2.7 in working condition.

 *Once you have upgraded to Splunk Module version 2.8, you cannot rollback to a previous version.*

**It is recommended to upgrade Forescout Splunk Apps and then upgrade the Forescout Extended Module for Splunk in the following sequence:**

1. On the Splunk Enterprise server, back up the following three ForeScout Splunk App and Add-ons to a secure location:
  - a. ForeScout Technology Add-on for Splunk
  - b. ForeScout App for Splunk
  - c. ForeScout Adaptive Response Add-on for Splunk
2. On Splunkbase, use *Browse More Apps* to find all three ForeScout Splunk Apps v2.8.
3. Select *Load an App* with the *Upgrade App* feature to upgrade them in any order.
4. After all the App and Add-ons are upgraded and configured, restart Splunk by selecting **Settings/SYSTEM > Server Controls > Restart**.
5. On the CounterACT Console, upgrade to CounterACT v8. This includes the ForeScout Extended Module for Splunk to version 2.8. Refer to the *CounterACT Administration Guide* for instructions.
6. In the left pane, Select **Options** and then select **Splunk**. The Splunk configuration pane displays the Splunk Syslog Targets tab.
7. Select each of the channels and then select **Test**.
8. Select the **Splunk HTTPS Targets** tab.

9. Select each of the channels and then select **Test**.
10. Upgrade is now complete.

## Appendix C: Working with CounterACT Data in Splunk

This section describes the structure of data submitted by CounterACT to Splunk, and how this influences your use of CounterACT data in Splunk searches.

### About CounterACT Data Events

CounterACT policies use the **Splunk Send Update from CounterACT** action to regularly report a selected set of host properties to Splunk.

Specify Splunk: Send Update from CounterACT parameters

**Policy Matching** - How each rule of active policies is evaluated for the endpoint.  
**Compliance Status** - Based on active Compliance policies.  
**Host Property values** - Select a subset of CounterACT host properties.

Content Sent | Splunk Server Targets | Trigger | Schedule

☒ Policy Status  
☒ Compliance Status  
☒ Host Properties

☐ All Properties  
☒ Selected Properties

Search

☒ Name ▲

- ☐ Advanced - 802.1X Accounting session ID
- ☐ Advanced - 802.1X RADIUS Log Details
- ☐ Advanced - 802.1X User Login Result
- ☐ Advanced Threat Detection - IOC Scan Stats
- ☐ Advanced Threat Detection - IOCs Detected by CounterACT

Select All  
Clear All

OK Cancel

When this action is applied to an endpoint, CounterACT sends event messages with a data payload. Each time this action is applied to an endpoint, *several* event messages may be sent to Splunk:

- When the **Policy status** option is selected, CounterACT sends *a separate event message* for each endpoint containing policy rules configured for that endpoint in CounterACT.
- When the **Host Properties** option is selected, CounterACT sends *a separate event message* for each endpoint containing host property values for that endpoint information. When the **Compliance Status** option is selected, CounterACT includes Compliance Status host property in the aforementioned event message.



Each event message contains some or all of the following information, as *field:value* pairs:

Field	Description
ip	The IP address of the endpoint for which information is reported.
ctupdate	Identifies the message as a CounterACT update. The value of this attribute indicates the type of data reported by the message: <ul style="list-style-type: none"> <li>Events that report policy information contain the pair <b>ctupdate:policyinfo</b>.</li> <li>Events that report compliance and host properties contain the pair <b>ctupdate:hostinfo</b>.</li> <li>When the <b>Splunk Send Custom Notification</b> action is used, the payload contains the pair <b>ctupdate:notif</b>.</li> </ul>
mac	The MAC address of the endpoint for which information is reported.
ipv6	The IPv6 address of the endpoint for which information is reported.
nbtomain	The NETBIOS Domain of the endpoint for which information is reported.
dnsdomain	The DNS domain of the endpoint for which information is reported, in case the NETBIOS Domain host property is not available for the endpoint.
nbthost	The NETBIOS hostname of the endpoint for which information is reported.
user	The User of the endpoint for which information is reported.
hostname	The DNS Name of the endpoint for which information is reported.
compliance	The Compliance Status of the endpoint for which information is reported.
host_properties	The CounterACT host properties of the endpoint for which information is reported.
policies	The CounterACT policies of the endpoint for which information is reported.

In addition to standard scheduling and recurrence options, this action provides the following optional triggers for reporting to Splunk:

- Independent of the policy recheck schedule, CounterACT can send the current value of all information reported by the action to Splunk at regular intervals.
- CounterACT can send an event message when any property or policy rule reported by the action changes.


See the *ForeScout Extended Module for Splunk Configuration Guide* for more details of action configuration options.

## Considerations When Working with CounterACT Events in Splunk

Consider the following points when you work with CounterACT event data in Splunk:

- Because each property and/or policy rule is reported as a separate event, information from the same endpoint must be correlated. This is most easily achieved using the IP address, which occurs in each event message.

In an environment in which IP addresses are frequently reassigned to other endpoints, it may be possible to use timestamp information to construct a search that isolates data that was associated with a certain IP addresses during a specified time period.

- Timestamps indicate when CounterACT detected/resolved the reported value, not the time of the event message. Applying the **Splunk Send Update from CounterACT** action to endpoints does not necessarily cause properties to be re-evaluated. In particular:
    - Any property that was resolved for an endpoint before the action was applied to the host is reported with the timestamp of its detection/resolution, even though this timestamp predates application of the action and creation of the event message.
    - If a previously reported property is now not resolvable by CounterACT, no new event message is sent to Splunk.
-  *If the endpoint was dropped from the scope of the **Splunk Send Update** action, and then returns to the scope, the last known value is reported again to Splunk.*

## Mapping CounterACT Data to the CIM Model

This section describes mapping of CounterACT host properties to the Common Information Model (CIM) model.

### Certificates

**Tags:** certificate

Splunk Reference:

<https://docs.splunk.com/Documentation/CIM/4.7.0/User/Certificates>

Data Model Field	CounterAct Field Tag
ssl_name	Name
ssl_serial	Serial_Number
ssl_is_valid	Status
ssl_issuer_common_name	CN
ssl_subject_unit	OU
ssl_subject_locality	L
ssl_subject_state	S
ssl_issuer	Issuer
ssl_start_time	Not_Before
ssl_end_time	Not_After

## Compute\_Inventory: CPU

**Tags:** cpu

Splunk Reference:

<http://docs.splunk.com/Documentation/CIM/4.7.0/User/ComputeInventory>

Data Model Field	CounterAct Field Tag
cpu_cores	Number_Of_Cores
family	Family
cpu_load_percent	Load_Percentage

## Compute\_Inventory: Network

**Tags:** network

Splunk Reference:

<http://docs.splunk.com/Documentation/CIM/4.7.0/User/ComputeInventory>

Data Model Field	CounterAct Field Tag
ip	IP_Address
dns	DNS_HostName
mac	MAC_Address

## Compute\_Inventory: Memory

**Tags:** memory

Splunk Reference:

<http://docs.splunk.com/Documentation/CIM/4.7.0/User/ComputeInventory>

Data Model Field	CounterAct Field Tag
mem	Capacity

## Compute\_Inventory: Storage

**Tags:** storage

Splunk Reference:

<http://docs.splunk.com/Documentation/CIM/4.7.0/User/ComputeInventory>

Data Model Field	CounterAct Field Tag
storage	Size__Megabytes_
storage_free	Free_Space__Megabytes_

## Blocked\_Malware

**Tags:** malware,attack

Splunk Reference:

<https://docs.splunk.com/Documentation/CIM/4.7.0/User/Malware>

Data Model Field	CounterAct Field Tag
file_hash	Threat_File_MD5
file_name	Threat_File_Name
sender	host

## Subset of Core Properties

Additionally, the following subset of core properties has been mapped to tags in the CIM model.

CounterACT Property (Name and Tag)	Splunk Tag	Model
IP Address {ip}	dest, dest_ip	All
Windows Processes Running {process_no_ext} Linux Processes Running {linux_process_running} Macintosh Processes Running {mac_process_running}	process	Application State
User {user}	user	All
Windows Services Running {service} Windows Services Installed {service_installed}	service	Application State / Services
NetBIO Domain {nbtomain}	dest_nt_domain	Malware
Malicious Event {malic}	ids_type=host category, signature	Intrusion Detection
Appliance	dvc, dvc_ip	Intrusion Detection

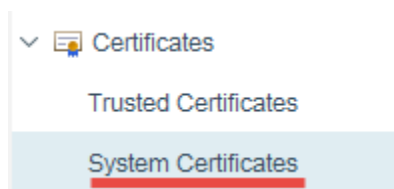
## Appendix D: System Certificate for Web Portal

This section addresses the system certificates for the Splunk web portal on the CounterACT Enterprise Manager. You must install a certificate

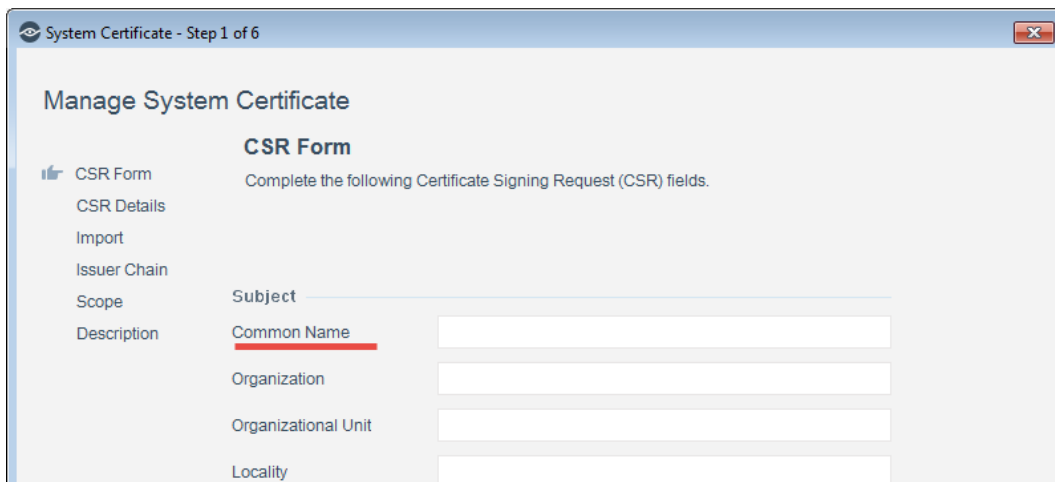
For information on how to install the system certificate for the CounterACT Enterprise Manager, refer to the CounterACT Administration Guide.

### What to Generate:

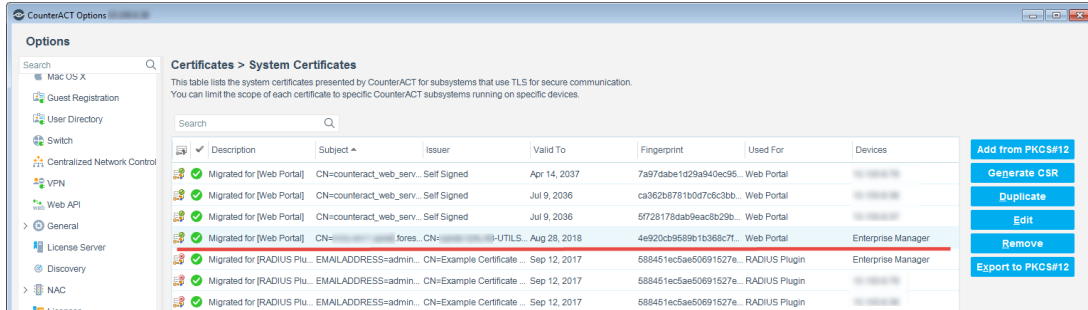
1. Select Options, select Certificates, and then select System Certificates.



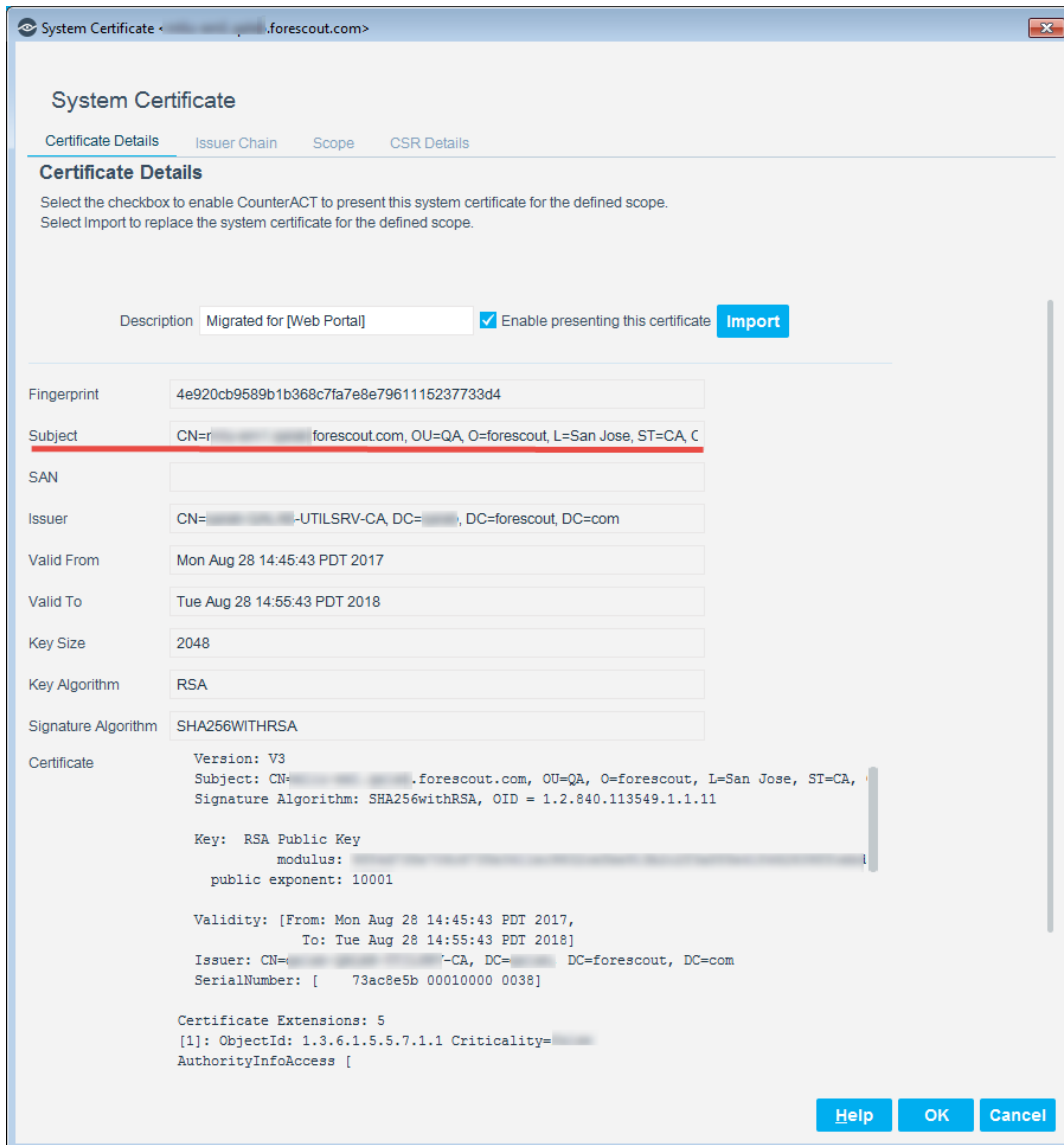
2. In the Certificates > System Certificates pane, select **Generate CSR**.
3. In the System Certificate wizard, enter the **FQDN** or IP address of the CounterACT Enterprise Manager into the *Subject* field. For the Common Name (CN) view, it is best practice to enter the **FQDN**.

A screenshot of a web browser window titled 'System Certificate - Step 1 of 6'. The main content area is titled 'Manage System Certificate' and 'CSR Form'. It instructs the user to 'Complete the following Certificate Signing Request (CSR) fields.' There is a sidebar on the left with links: 'CSR Form' (selected), 'CSR Details', 'Import', 'Issuer Chain', 'Scope', and 'Description'. The main form has several input fields: 'Subject' (with a text input), 'Common Name' (with a text input and a red underline), 'Organization' (with a text input), 'Organizational Unit' (with a text input), and 'Locality' (with a text input).

4. Once the CSR is created, the certificate needs to be submitted to a certificate authority. The CSR is then signed by a trusted Certificate Authority (for example, VeriSign) or by your own Certificate Authority, the certificate needs to be installed on the web portal of the CounterACT Enterprise Manager.



5. Once imported, you can view the certificate by selecting the web portal Enterprise Manager and then selecting **Edit**.



6. The FQDN of the Enterprise Manager selected displays in the *Subject* field and the *Certificate* field is populated.

## Appendix E: Tuning Data Traffic

The data traffic needs to be in agreement with the rate limiting constraints of the ForeScout App for Splunk.

Below is the default rate limiting parameters:

Default Rate Limiting Parameter	Description
<code>config.rate_limit.window.seconds = 3600</code>	Rate limiting timer. After this timer, the Splunk module resets its alerts' data traffic count.
<code>config.rate_limit.window.max_alerts = 15</code>	Maximum number of alert messages accepted by the Splunk Module.
<code>config.message.alerts.max_results = 2000</code>	Maximum number of alert requests that can be bundled in a single alert message.

The above values represent the default parameters that will be used for applying rate limiting to alerts sent to the CounterACT Splunk Module from the ForeScout App for Splunk. These values can be edited on the CounterACT Splunk Module to tune the alert data traffic.

The ForeScout App for Splunk bundles multiple alert requests from a saved search into a single alert message and sends it to the CounterACT Splunk Module. The Module will accept action requests for up to 2000 endpoints in a single message from Splunk. Above 2000 endpoints, the Module will return the following *\*single\** response as a reply to the action request:

```
<?xml version="1.0" encoding="UTF-8"?>
<SPLUNK_ALERTS TYPE="response">
  <STATUS>
    <CODE>400</CODE>
    <MESSAGE>Too many results in one alert message. Discarding this
alert.</MESSAGE>
  </STATUS>
</SPLUNK_ALERTS>
```

The Module only accepts a maximum of 15 alert messages in a one-hour period. If there are more, the following *\*single\** response is sent as a reply to all messages after the first 15 messages:

```
<?xml version="1.0" encoding="UTF-8"?>
<SPLUNK_ALERTS TYPE="response">
  <STATUS>
    <CODE>400</CODE>
    <MESSAGE>Rate limiting condition active on CounterACT. The Splunk
alerts configuration should be reviewed and corrected.</MESSAGE>
  </STATUS>
</SPLUNK_ALERTS>
```

If a single message contains more than 30,000 ( $15 \times 2000 = 30,000$ ) bundled results, then this message alone will send the Module into rate limiting mode for the next one-hour and the reply will be the same as above.

Once the Module enters this mode, it will continue to discard all alert messages with the above response for the next one-hour after which it will recover and start processing alerts again.

When the rate limiting condition is hit for the first time, the Module will also send an email to the CounterACT operator, warning about this condition. The operator needs to check the alert configuration, correct it, and then restart the module.



## Appendix F - Compatibility with CIM Data Models

The ForeScout Technology add-on is developed in a way that data being collected by the add-on will get normalized to CIM data models and its fields. Following section mentions the mapping of counterACT fields to CIM data model fields for user reference.

### CIM Model: Certificates

<b>Event Type</b>	ct_certificate
<b>Search</b>	source=counterACT sourcetype=fsctcenter* ctupdate=hostinfo hwi_certificate=*
<b>Tags</b>	certificate
<b>Splunk Reference</b>	<a href="https://docs.splunk.com/Documentation/CIM/4.7.0/User/Certificates">https://docs.splunk.com/Documentation/CIM/4.7.0/User/Certificates</a>

### Fields

Data Model Field	CounterAct Field
ssl_name	Name
ssl_serial	Serial_Number
ssl_is_valid	Status
ssl_issuer_common_name	CN
ssl_subject_unit	OU
ssl_subject_locality	L
ssl_subject_state	S
ssl_issuer	Issuer
ssl_start_time	Not_Before
ssl_end_time	Not_After

### CIM Model: Compute\_Inventory: CPU

<b>Event Type</b>	ct_hostinfo_cpu
<b>Search</b>	source=counterACT sourcetype=fsctcenter* ctupdate=hostinfo hwi_processor=*

<b>Tags</b>	cpu
<b>Splunk Reference</b>	<a href="https://docs.splunk.com/Documentation/CIM/4.7.0/User/ComputeInventory">https://docs.splunk.com/Documentation/CIM/4.7.0/User/ComputeInventory</a>

### Fields

Data Model Field	CounterAct Field
cpu_cores	Number_Of_Cores
family	Family
cpu_load_percent	Load_Percentage

## CIM Model: Compute\_Inventory: Network

<b>Event Type</b>	ct_hostinfo_network
<b>Search</b>	source=counterACT sourcetype=fscntcenter* ctupdate=hostinfo hwi_network_adapters=*
<b>Tags</b>	network
<b>Splunk Reference</b>	<a href="https://docs.splunk.com/Documentation/CIM/4.7.0/User/ComputeInventory">https://docs.splunk.com/Documentation/CIM/4.7.0/User/ComputeInventory</a>

### Fields

Data Model Field	CounterAct Field
ip	IP_Address
dns	DNS_HostName
mac	MAC_Address

## CIM Model: Compute\_Inventory: Memory

<b>Event Type</b>	ct_hostinfo_memory
<b>Search</b>	source=counterACT sourcetype=fscntcenter* ctupdate=hostinfo hwi_physical_memory=*
<b>Tags</b>	memory

<b>Splunk Reference</b>	<a href="https://docs.splunk.com/Documentation/CIM/4.7.0/User/ComputeInventory">https://docs.splunk.com/Documentation/CIM/4.7.0/User/ComputeInventory</a>
-------------------------	---

### Fields

Data Model Field	Mapped CounterAct Field
mem	Capacity

## CIM Model: Compute\_Inventory: Storage

<b>Event Type</b>	ct_hostinfo_storage
<b>Search</b>	source=counterACT sourcetype=fsctcenter* ctupdate=hostinfo hwi_disk=*
<b>Tags</b>	storage
<b>Splunk Reference</b>	<a href="https://docs.splunk.com/Documentation/CIM/4.7.0/User/ComputeInventory">https://docs.splunk.com/Documentation/CIM/4.7.0/User/ComputeInventory</a>

### Fields

Data Model Field	CounterAct Field
storage	Size__Megabytes_
storage_free	Free_Space__Megabytes_

## CIM Model: Blocked\_Malware

<b>Event Type</b>	ct_malware
<b>Search</b>	source=counterACT sourcetype=fsctcenter* (pan_apt_detected_ioc OR atc_detected_ioc OR fireeye_detected_ioc OR apt_cp_antivirus_ioc)
<b>Tags</b>	malware, attack
<b>Splunk Reference</b>	<a href="https://docs.splunk.com/Documentation/CIM/4.7.0/User/Malware">https://docs.splunk.com/Documentation/CIM/4.7.0/User/Malware</a>

### Fields

Data Model Field	Mapped CounterAct Field
file_hash	Threat_File_MD5
file_name	Threat_File_Name
sender	host

## Legal Notice

© 2018 ForeScout Technologies, Inc. All rights reserved. ForeScout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2018-04-11 13:56