



ForeScout® Extended Module for Splunk®

Configuration Guide

Version 2.8

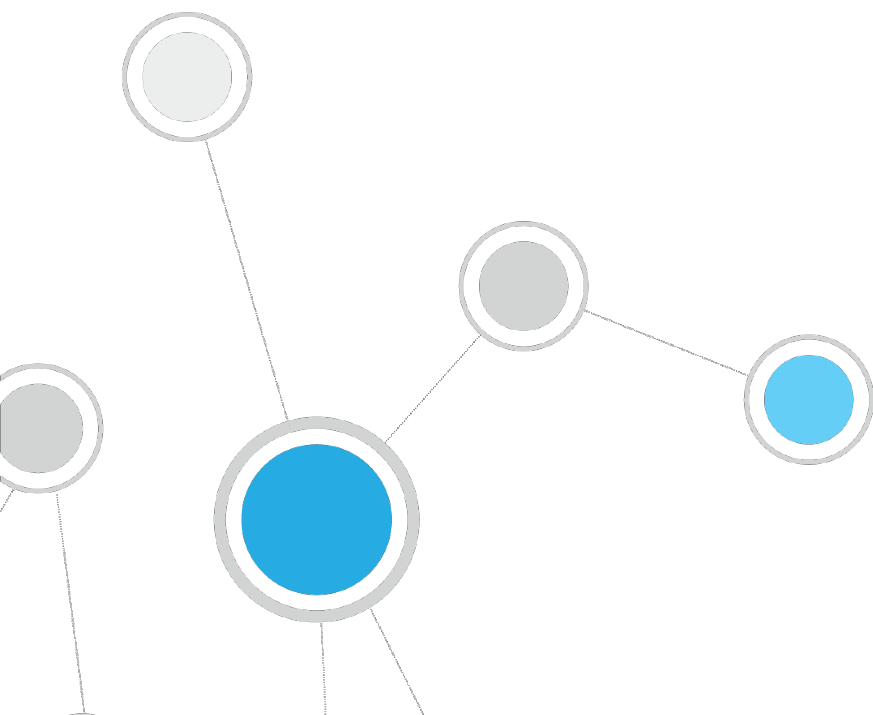


Table of Contents

About Splunk Integration	5
Support for Splunk Enterprise and Splunk Enterprise Security	6
What's New	6
Support for Splunk Cloud	6
Support for Batch Messaging	7
Support for MAC-only Devices and IPv6 Devices	7
New Information is Appended to Every Message	7
Support of Customized Indexes	8
Support for Multiple Channels for each Splunk Target	8
New Test Button with in-depth Results	8
Improved Performance	8
Use Cases	8
Logging	9
Continuous Posture Tracking Based on a Broad Range of CounterACT Data	9
Adaptive Response Actions Triggered by Splunk Data Correlation	9
Splunk Bidirectional Use Cases	10
Additional Splunk Documentation	11
About the ForeScout Extended Module for Splunk	11
ForeScout App for Splunk	12
ForeScout Technology Add-on for Splunk	12
ForeScout Adaptive Response Add-on for Splunk	12
Concepts, Components and Considerations	13
Concepts	13
Components	14
Considerations	15
Splunk Instance Credentials	15
Requirements	15
CounterACT Requirements	15
Supported Vendor Requirements	16
Splunk Cloud Requirements	16
About Support for Dual Stack Environments	16
ForeScout Extended Module License Requirements	16
Per-Appliance Licensing Mode	17
Centralized Licensing Mode	18
More License Information	19
Install the Module	19
Upgrade to Splunk Module version 2.8 and ForeScout Apps for Splunk 2.7	19
Rollback Support	20
Install the ForeScout Extended Module for Splunk	20
Configure the Module	22
Define a new Event Collector	22

Set up Secure Connection Messaging from Splunk Module to the Splunk Enterprise Server	26
Add a Splunk HTTP Target	27
Add a Splunk Syslog Target	34
Test the Module.....	39
Understanding Test Results	41
Run Splunk Policy Templates	41
Send Endpoint and Policy Details to Splunk	42
Batched Messages	42
Run the Template	45
Stage 1 – Add to HTTP Notification Action Group	48
Run the Template	48
Stage 2 - Execute HTTP Notification Action	52
Run the Template	52
Create Custom Splunk Policies	55
Detecting Endpoints – Policy Properties	60
Splunk Alerts	60
Managing Splunk Devices – Policy Actions	61
Splunk: Send Custom Notification Action	61
Splunk: Send Update from CounterACT Action	62
Using the Splunk Module	65
Run Splunk Audit Actions	66
Send Custom Notification to Splunk Enterprise Server Targets	66
Send Update from CounterACT	70
Best Practices	77
CounterACT-to-Splunk Logging	77
Splunk to CounterACT Messaging	77
Splunk Actions on CounterACT	77
What data is sent to Splunk?	77
Appendix A: Default Communication Settings	77
Appendix B - Splunk Cloud Deployments	78
Splunk Cloud vs Splunk Enterprise	78
Deploying Splunk Cloud	79
Types of Splunk Clouds	79
Indexing Requirements for Splunk Cloud Instance	79
Self-service Splunk Cloud	80
REST API	80
HTTP Event Collector	80
Managed Splunk Cloud	82
REST API	84
HTTP Event Collector	84
Set up Secure Connection Messaging from Splunk Module to the Splunk Cloud ..	85

Set up and Configure the ForeScout Technology Add-on for Splunk Cloud	87
Accessing Logs within Splunk Cloud Instance	88
Appendix C: System Certificate for Web Portal.....	89
Additional CounterACT Documentation	91
Documentation Downloads	92
Documentation Portal	92
CounterACT Help Tools.....	93

About Splunk Integration

Splunk® Enterprise data analytics help organizations:

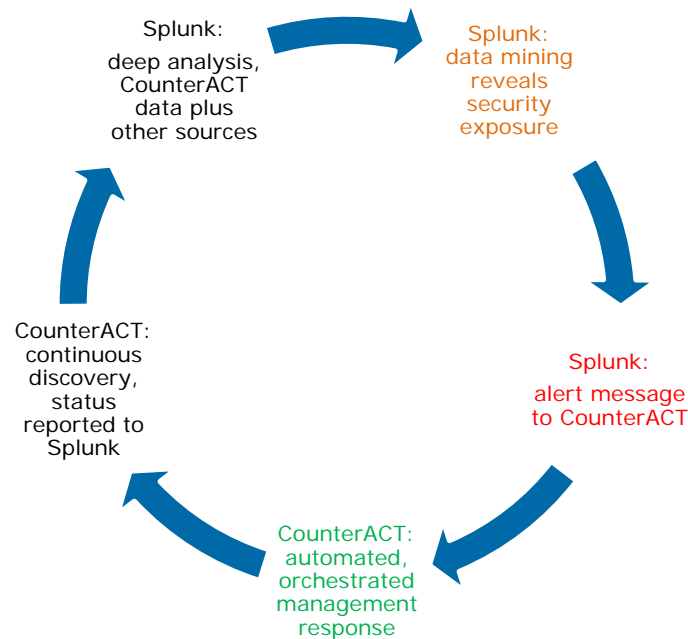
- Leverage the data that their infrastructure and security tools provide
- Understand their security posture
- Pinpoint and investigate anomalies
- Create alerts and reports

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

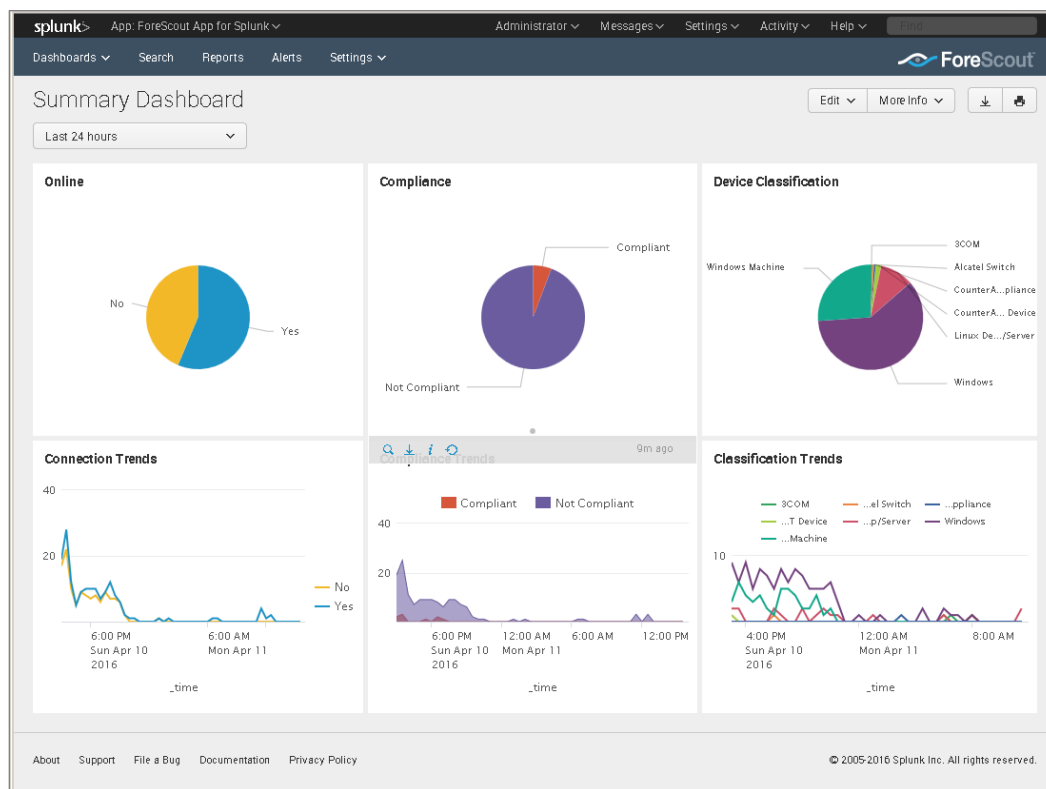
By combining ForeScout CounterACT® dynamic device visibility, access and security capabilities with Splunk Enterprise's data mining capabilities, security managers can:

- 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 host 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 back to Splunk



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



Support for Splunk Enterprise and Splunk Enterprise Security

The ForeScout App & Add-ons for Splunk published on Splunkbase and the ForeScout Extended Module for Splunk (Splunk Module) support the following Splunk versions:

- Splunk Enterprise version 6.4, 6.5, and 6.6.
- Splunk Enterprise Security version 4.5 and 4.7.

What's New

This section addresses what's new in the Splunk Module version 2.8.

Support for Splunk Cloud

ForeScout supports integration with Splunk Cloud™. Splunk Cloud provides the benefits of Splunk Enterprise and if purchased Splunk ES as a cloud service. Splunk Cloud enables you to store, search, analyze, and visualize the machine-generated data that comprise your IT infrastructure or business. Splunk Cloud deployments can be continuously monitored and managed by the Splunk Cloud Operations team.

Forwarders with access to the source data are run to send data to Splunk Cloud. Splunk Cloud then indexes the data and transforms it into searchable "events." After

event processing is complete, you can associate events with knowledge objects to enhance their usefulness.

See [Appendix B - Splunk Cloud Deployments](#).

Support for Batch Messaging

Before Splunk Module 2.8 each property was sent as an individual message to the Splunk Enterprise server. In Splunk Module 2.8, all properties of a host are batched together and sent as a single nested json message. The batched message encapsulates all device properties for each device, thus improving the overall system performance for both the Splunk Module and the Splunk Enterprise server. See [Batched Messages](#).

Support for MAC-only Devices and IPv6 Devices

In Splunk Module version 2.8, IPv6 addresses can be reported as host property inside the *hostinfo* message sent by the Splunk Module. New also in Splunk Module 2.8, IPv6 addresses are sent as part of the identity header in all messages sent by the module. Additionally, CounterACT also reports devices that have only a MAC Address.

New Information is Appended to Every Message

New information is supplied with each update message sent from the Splunk Module to the Splunk Enterprise server. This means when you use the **Send Update from CounterACT** Action, the action submits device properties and its associated data to Splunk. In addition to the specified host properties, each update message sent to Splunk includes the following information for each endpoint:

- MAC Address
- IPv4 Address
- IPv6 Address, when present
- Hostname
- NetBIOS Domain, when present
- DNS Name - For customers that want device domain reported for most endpoints, it is suggested that you add the DNS Name host property in the discovery policy.
- NetBIOS User, when present
- The Tenant ID serves as a differentiator to determine the source of an update message received on the Splunk Enterprise server. It is especially useful when the customer has multiple CounterACT deployments where the appliances sending data to a single Splunk Enterprise server can have overlapping IP addresses.

For more information, see [Add a Splunk HTTP Target](#) and [Add a Splunk Syslog Target](#).

Support of Customized Indexes

The ForeScout Extended Module for Splunk now supports any index of your choice. The default setting is *fsctcenter*, however, you can change it to an index of your own. See [Configure the Module](#).

Support for Multiple Channels for each Splunk Target

In version 2.5.0, if the user configured a new HTTP destination with the same URL as that configured in one of the existing HTTP destinations, then the Splunk Module would raise an error and prevent the user from configuring that HTTP channel.

- a. In version 2.8, for the Event Collector, the user can now configure two or more HTTP channels with same URLs in the following conditions:
 - Same index and same authorization token - rejected
 - Same index and different authorization token - accepted
 - Different index and different authorization token -accepted
 - Different index and same authorization token- accepted
- b. For version 2.8, for the RESTful API, user can now configure two or more HTTP channels with same URLs as long as there are different *Indexes*.
- c. For version 2.8, for RESTful API and Event Collector, TCP and UDP can be used as a form of multi-channel for each Splunk target.

The benefit of this implementation provides greater granularity to the user.

New Test Button with in-depth Results

To ensure your connection to the Splunk Enterprise server, a Test button has been added to the configuration section of the Splunk Module. After a test is run, details of the test display to guide you on troubleshooting your connection difficulties. See [Test the Module](#).

Improved Performance

Due to the reduced number of event forwards from the CounterACT appliance to the Splunk Enterprise server, overall performance has improved:

- Decreased bandwidth usage
- Reduced I/O
- Reduced Memory footprint

Use Cases

This section describes use cases supported by this module. Be sure to review the [Best Practices](#).

To understand how this module helps you achieve these goals, see [About the ForeScout Extended Module for Splunk](#).

Logging

As a real-time appliance, CounterACT relies on SIEM platforms, such as Splunk, for long term data retention. The amount of data that CounterACT can log is expansive, and includes all policy match/un-match events, as well as over 200 individual host properties. The below best practice recommendations are a good foundation with which to build upon.

Audit and Event Logs

Audit logs capture user activity and event logs capture system events. Both of these are supported through the CounterACT Syslog Plugin and can be configured to log them to your Splunk server.

Continuous Posture Tracking Based on a Broad Range of CounterACT Data

Integration with Splunk includes a dedicated ForeScout App for Splunk 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:

- Device compliance status summaries
- Patterns of network access over time
- Trends in CounterACT policies
- Significant changes in device processes and applications
- Device system health information including hardware and certificate information
- 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.

- For more information, see [ForeScout Adaptive Response Add-on for Splunk](#).
- For more information about Adaptive Response Framework, see <http://dev.splunk.com/view/enterprise-security/SP-CAAABFE>

User Behavior Analytics (UBA)

The following minimum CounterACT host properties are considered best practice for capturing UBA, and are initially time-stamped upon device connection. Additionally, in order to capture a timestamp, a separate log should be set up for device disconnect.

- IP address
- MAC address
- Switch IP and port name
- WLAN SSID
- WLAN AP
- User
- Operating System
- Classification group
- Segment name

Policy-based

While all logging to Splunk comes from policy actions, policy-based logs refer to logging events when it is desired to have CounterACT take an access control action on a host. These should occur in the following scenarios:

- On control action, for example, device is moved to quarantine VLAN
- On un-desired policy result match
 - Non-corporate system connect
 - Non-complainant system

Frequency

At a minimum, all of these details should be logged on match/detection, on device disconnect, and every 24 hours of no state change.

Splunk Bidirectional Use Cases

Due to bidirectional communicants between CounterACT and Splunk, CounterACT is able to perform actions on endpoints via Splunk correlation. For example, a device tries to SSH too many Linux servers with “root” account. The event will inform CounterACT to block the endpoint(s) or leverage any other action available via the CounterACT implementation.

Splunk Sizing

Splunk sizing is how much data will be sent to Splunk. Refer to the Splunk sizing tool at <https://splunk-sizing.appspot.com/>.

Additional Splunk Documentation

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

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

To access the ForeScout App & Add-ons for Splunk How-to Guide:

1. Go to <https://splunkbase.splunk.com/app/3381/>
2. Select the **Details** tab and scroll down to access the full *ForeScout App & Add-ons for Splunk How-to Guide*.

About the ForeScout Extended Module for Splunk

The ForeScout Extended Module for Splunk integrates CounterACT and Splunk. This allows you to:

- Use policies and actions provided by the Splunk Module to regularly push device properties and associated data to Splunk:
 - [Send Endpoint and Policy Details to Splunk](#) policy template
 - [Splunk: Send Update from CounterACT Action](#).
- In the ForeScout App for Splunk, view CounterACT data in a dedicated, customizable Splunk dashboard. See the *ForeScout App & Add-ons for Splunk How-to Guide* for details.
- Define CounterACT policies that respond to Splunk alerts:
 - [Run Splunk Policy Templates](#)
- In the Saved Searches bundled with the add-on, configure Splunk to send alerts to CounterACT based on custom search queries. Searches can combine data from multiple data sources.
- The Splunk Module works with ForeScout Technology Add-on for Splunk and ForeScout Adaptive Response Add-on for Splunk to support communication between CounterACT and Splunk. 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 App & Add-ons for Splunk How-to Guide*.

To use the module, you should have a solid understanding of how CounterACT policies work and understand basic Splunk concepts, functionality and terminology.

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:

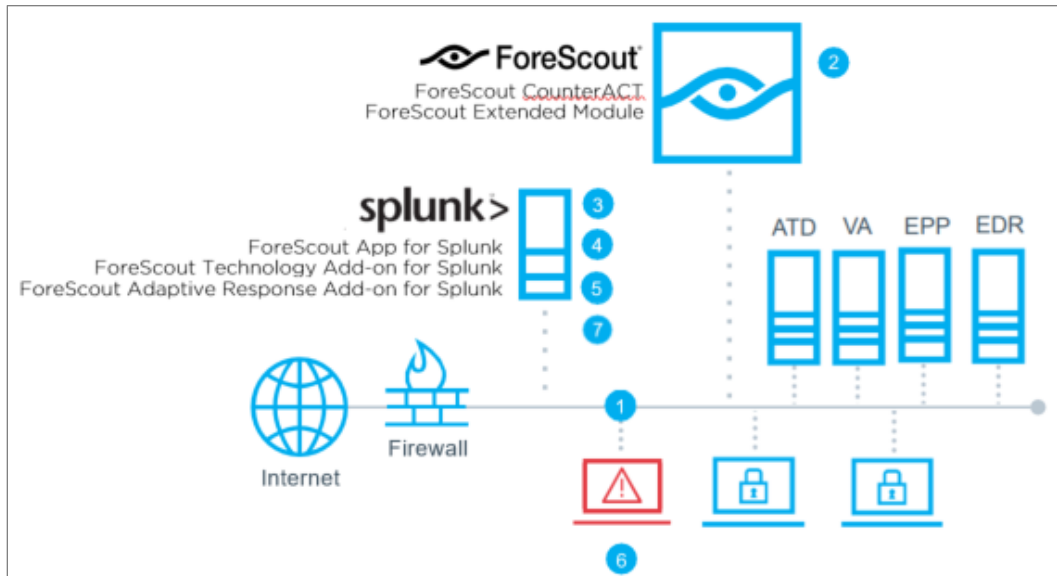
- **Adaptive Response** - TA-forescout_response implements the Adaptive Response framework for ForeScout-Splunk integration.
- **Actions Mapping** - TA-forescout_response stores the CounterACT actions information which are available as *Trigger Actions* in alerts.
- **Sync Response** - This is the synchronous 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.

Concepts, Components and Considerations

This section provides a basic overview of Splunk / CounterACT architecture:

Concepts

How it works:



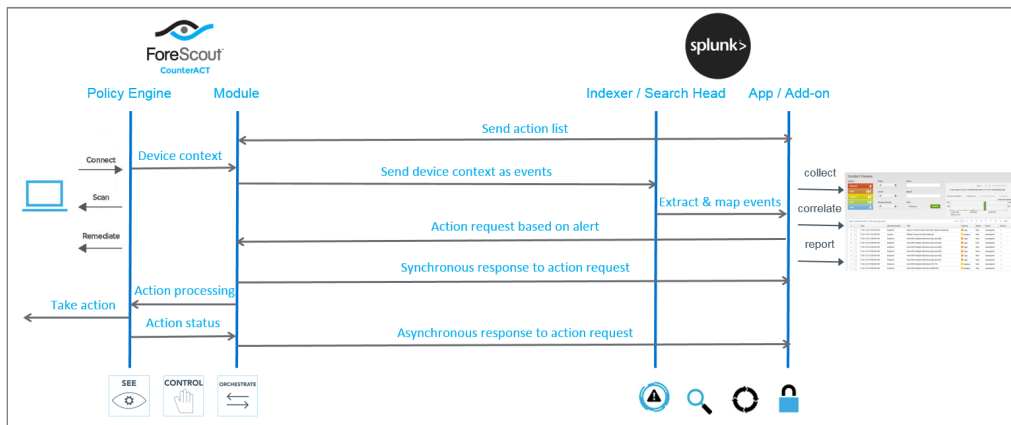
1. CounterACT discovers, classifies and assesses devices as they connect to the network.
2. CounterACT sends real-time, pre-correlated device data, including networking context, in a single message packet to Splunk for long-term storage and easier correlation with other data sources, richer insight and more complete compliance information.
3. ForeScout App for Splunk visualizes CounterACT data for trend analysis, monitoring and reporting.
4. Splunk leverages device context from CounterACT and correlates with other data sources to identify and prioritize incidents.
5. With the ForeScout Adaptive Response Add-on and Splunk Enterprise Security, Splunk operators can initiate actions using CounterACT based on severity of the alert.
6. Through the ForeScout Extended Module for Splunk, CounterACT can automate incident response to Splunk alerts with policy-driven actions on non-compliant, vulnerable or suspicious endpoints and report action status back to Splunk. Actions can include orchestration with other security or management systems if ForeScout Extended Modules for those systems are also utilized.

7. Splunk operators can see the complete alert and response action lifecycle via the Splunk Enterprise Security Alert Mitigation Center or ForeScout App for Splunk Response Action Dashboard within Splunk Enterprise.

Components

Four components are installed to support this integration:

1. The Splunk Module is installed on the CounterACT appliance.
2. The ForeScout Technology Add-on for Splunk is installed on the Splunk Enterprise Server.
3. The ForeScout Adaptive Response Add-on for Splunk is installed on the Splunk Enterprise Server.
4. The ForeScout App for Splunk is installed on the Splunk Enterprise Server.



Results of the integration:

1. The result is comprehensive bi-directional integration – CounterACT can send a dynamic list of device property, policy, and event information to the Splunk Enterprise server. The Splunk Enterprise server can then send alerts and other messages to CounterACT.
2. Splunk search uses data from CounterACT and other sources to detect patterns that indicate threats or incidents.
3. The ForeScout Adaptive Response Add-on for Splunk submits action requests based on alerts generated by Search queries to CounterACT.
4. The Splunk Module policy parses the action requests into incident response actions and initiates on target devices.
5. The Splunk Module sends status of the actions performed back to the Splunk Enterprise server.

Considerations

This section addresses any additional ForeScout Extended Module for Splunk considerations.

It is recommended to review the [Best Practices](#).

Splunk Instance Credentials

You will need to contact your Splunk administrator and get the credentials to connect to the Splunk instance. This is required to configure the ForeScout Extended Module for Splunk. The instructions for creating credentials are listed in the *ForeScout App & Add-ons for Splunk How-to Guide*.

Requirements

This section describes system requirements, including:

- [CounterACT Requirements](#)
- [Supported Vendor Requirements](#)
- [Splunk Cloud Requirements](#)
- [ForeScout Module License Requirements](#)

CounterACT Requirements

The module requires the following CounterACT releases and other CounterACT components:

- The ForeScout App for Splunk interacts with a CounterACT Enterprise Manager running 8.0.
- This module is a component of the ForeScout Extended Module for Splunk and requires a module license.
- An active Maintenance Contract for the licensed module is required.
- Verify that the following policies are active:
 - Classification
 - Compliance

Host information determined by these policies is reported to Splunk and used in standard dashboards of the ForeScout App for Splunk. Similarly, host information determined by other policies categorized as *Classification* or *Compliance* policies is reported to Splunk.

- For CounterACT-Splunk integration, you must also install the **ForeScout App for Splunk** in the applicable Splunk instance(s). See [Install the Module](#).

To categorize policies:

1. Select a policy for categorization from the Console, Policy tab and then select Categorize. The Categorize dialog box opens.
2. Select the category you need.
 - If you plan to send system health and network data, install and enable Hardware Inventory Plugin (v 1.0.2.2, delivered with the Endpoint Module version 1.0).
 - For CounterACT-Splunk integration, you must also install the **ForeScout App for Splunk** in the applicable Splunk instance(s). See the *ForeScout App & Add-ons for Splunk How-to Guide*.
 - This module is a component of the ForeScout Extended Module for Splunk (Splunk Module) and requires a module license. See the *ForeScout App & Add-ons for Splunk How-to Guide*.

Supported Vendor Requirements

- Splunk Enterprise version 6.4, 6.5, 6.6 or 7.0.
- Splunk Enterprise Security version 4.5 or 4.7.

Splunk Cloud Requirements

- Splunk Cloud Enterprise version 6.6.3
- Splunk data integration requires a Splunk Cloud license. Refer to

<https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/User/Datapolicies>

For more information about Splunk Cloud, refer to [Appendix B - Splunk Cloud Deployments](#)

About Support for Dual Stack Environments

CounterACT version 8.0 detects endpoints and interacts with network devices based on both IPv4 and IPv6 addresses. However, **IPv6 addresses are not yet supported by this component**. The functionality described in this document is based only on IPv4 addresses. IPv6-only endpoints are typically ignored or not detected by the properties, actions, and policies provided by this component.

ForeScout Extended Module License Requirements

This ForeScout Extended Module requires a valid license. Licensing requirements differ based on which licensing mode your deployment is operating in:

- [Per-Appliance Licensing Mode](#)
- [Centralized Licensing Mode](#)

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode. Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.

Name	Status	Type
ForeScout CounterACT See	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Control	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Resiliency	Valid	Perpetual
ForeScout Extended Module for Check Point Next...	Valid, Capacity exceeded	Perpetual

Contact your ForeScout representative for any questions about identifying your licensing mode.


Per-Appliance Licensing Mode

When installing the module you are provided with a 90-day demo module license.

If you would like to continue exploring the module before purchasing a permanent license, you can request a demo license extension. Consult with your ForeScout representative before requesting the extension. You will receive email notification and alerts at the Console before the demo period expires.

When the demo period expires, you will be required to purchase a permanent module license. *In order to continue working with the module, you must purchase the license.*

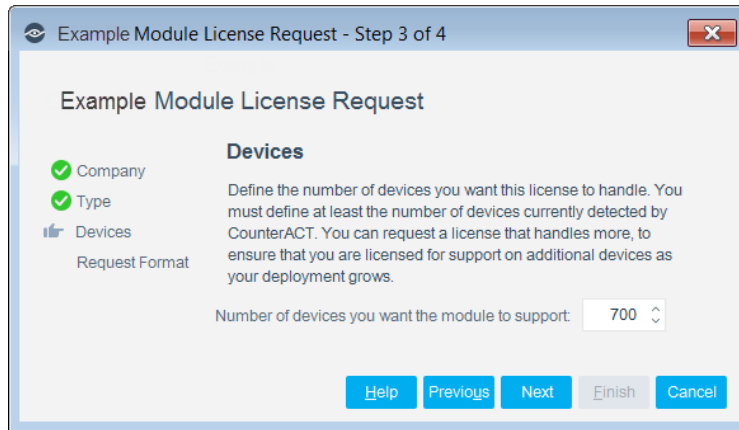
Demo license extension requests and permanent license requests are made from the CounterACT Console.

 *This module may have been previously packaged as a component of an Integration Module which contained additional modules. If you already installed this module as a component of an Integration Module, you can continue to use it as such. Refer to the section about module packaging in the CounterACT Administration Guide for more information.*

Requesting a License

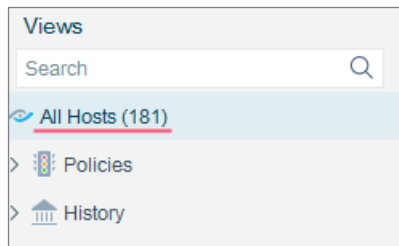
When requesting a demo license extension or permanent license, you are asked to provide the device *capacity* requirements. This is the number of devices that you want this license to handle. You must define at least the number of devices currently detected by CounterACT. You can request a license that handles more to ensure that you are licensed for support on additional devices as your deployment grows.

Enter this number in the **Devices** pane of the Module License Request wizard, in the CounterACT, Console Modules pane.




To view the number of currently detected devices:

1. Select the **Home** tab.
2. In the Views pane, select the **All Hosts** folder. The number in parentheses displayed next to the **All Hosts** folder is the number of devices currently detected.



Centralized Licensing Mode

When you set up your CounterACT deployment, you must activate a license file containing valid licenses for each feature you want to work with in your deployment, including Extended Modules. After the initial license file has been activated, you can update the file to add additional Extended Module licenses or change endpoint capacity for existing Extended Modules. For more information on obtaining Extended Module licenses, contact your ForeScout representative.

 *No demo license is automatically installed during system installation.*

License entitlements are managed in the [ForeScout Customer Portal](#). After an entitlement has been allocated to a deployment, you can activate or update the relevant licenses for the deployment in the Console.

Each Extended Module license has an associated capacity, indicating the number of endpoints the license can handle. The capacity of each Extended Module license varies by module, but does not exceed the capacity of the *See* license.

- Integration Modules, which package together groups of related licensed modules, are not supported when operating in Centralized Licensing Mode. Only Extended Modules, packaging individual licensed modules are supported. The Open Integration Module is an Extended Module even though it packages more than one module.

More License Information

Refer to the *CounterACT Administration Guide* for information on Extended Module licenses. You can also contact your ForeScout representative or license@forescout.com for more information.

Install the Module

This section lists the steps you should take to set up your system when integrating with Splunk.

The Splunk Module, the ForeScout App and the Technology Add-ons for Splunk work together to support communication between CounterACT and Splunk. You must install and configure all components for features to work as described in this document. For example, CounterACT policies and actions provided by the Splunk Module are used to populate Splunk with CounterACT data. As you plan deployment, read this document together with the *ForeScout App & Add-ons for Splunk How-to Guide*.

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.

Rollback Support

Rollback is not available for this module. This means that if you upgrade to this module version and the module does not operate as expected, you cannot roll it back to a previous release.



Install the ForeScout Extended Module for Splunk


This section describes how to download the module from the ForeScout Customer Support site and install it on the CounterACT Console.

 *This module interacts with the ForeScout App for Splunk. If you install only this module, you can send CounterACT information to Splunk.*

To install the module:

1. Navigate to one of the following ForeScout download portals, depending on the licensing mode your deployment is using:
 - [Product Updates Portal](#) - **Per-Appliance Licensing Mode**
 - [Customer Portal, Downloads Page](#) - **Centralized Licensing Mode**To find out which licensing mode your deployment is working with, see [Identifying Your Licensing Mode in the Console](#).
2. Download the module **.fpi** file.
3. Save the file to the machine where the CounterACT Console is installed.
4. Log into the CounterACT Console and select **Options** from the **Tools** menu.

5. Select **Modules**. The Modules pane opens.
 6. Select **Install**. The Open dialog box opens.
 7. Browse to and select the saved module **.fpi** file.
 8. Select **Install**. The Installation screen opens.
 9. Select **I agree to the License Agreement** to confirm that you have read and agree to the terms of the License Agreement, and select **Install**. The installation will not proceed if you do not agree to the license agreement.
-  *The installation will begin immediately after selecting Install, and cannot be interrupted or canceled.*
-  *In modules that contain more than one component, the installation proceeds automatically one component at a time.*
10. When the installation completes, select **Close** to close the window. The installed module is displayed in the Modules pane.

 *Some components are not automatically started following installation.*

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.

Options

Search

VPN

General

Discovery

NAC

Licenses

Lists

Map

Internal Network

Licenses

Activate, update or deactivate your license for CounterACT features and Extended Module


Search

Name ▲	Status	Type
ForeScout CounterACT See	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Control	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Resiliency	Valid	Perpetual
ForeScout Extended Module for Check Point Next...	Valid, Capacity exceeded	Perpetual

Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Configure the Module

Configure the module to ensure that CounterACT can communicate with Splunk instance. Perform this procedure after the ForeScout Extended Module for Splunk is installed on your targeted CounterACT Appliance.

 *If you are using the Splunk Adaptive Alert Response, then a new system certificate for the web portal on the CounterACT Enterprise Manager needs to be installed. See [Appendix C: System Certificate for Web Portal](#).*

To complete configuration of some of these connections, you must perform the following configuration steps on the Splunk instance:

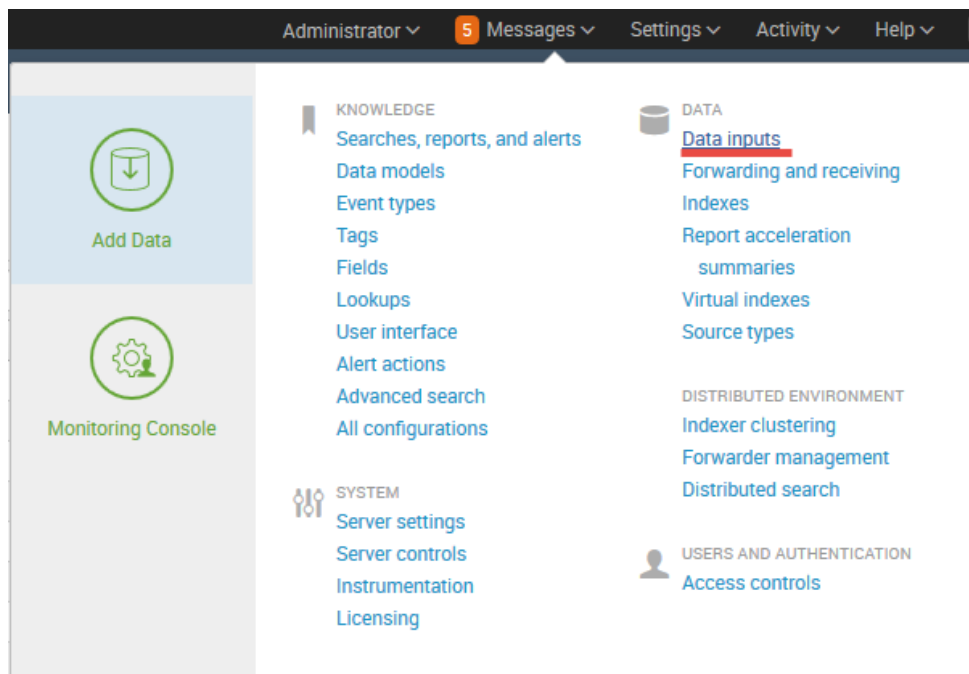
1. The installation of the ForeScout App for Splunk and the two Add-ons are required to be installed first. Refer to the *ForeScout App & Add-ons for Splunk How-to Guide* for more information.
2. Obtain [Splunk Instance Credentials](#) for configuring the HTTP targets on the Splunk Module.
3. [Define a new Event Collector](#). Using Splunk Event Collector messages is the recommended protocol. Event Collector is a proprietary Splunk HTTP(S) channel introduced in Splunk 6.3. Follow the procedure described in this section to use Event Collector Messages.
4. [Set up Secure Connection Messaging from Splunk Module to the Splunk Enterprise Server](#).
5. Add a Splunk Target (optional.) Below are protocols that can be used by CounterACT to send information to Splunk:
 - **Using HTTPS POST messages to the Splunk REST API** - Define server targets as described in [Add a Splunk HTTP Target](#).
 - **Using Syslog messaging** - To use Syslog, define one or more Splunk Enterprise server targets as described in [Add a Splunk Syslog Target](#).
6. On the Splunk Module, [Test the Module](#).

Define a new Event Collector

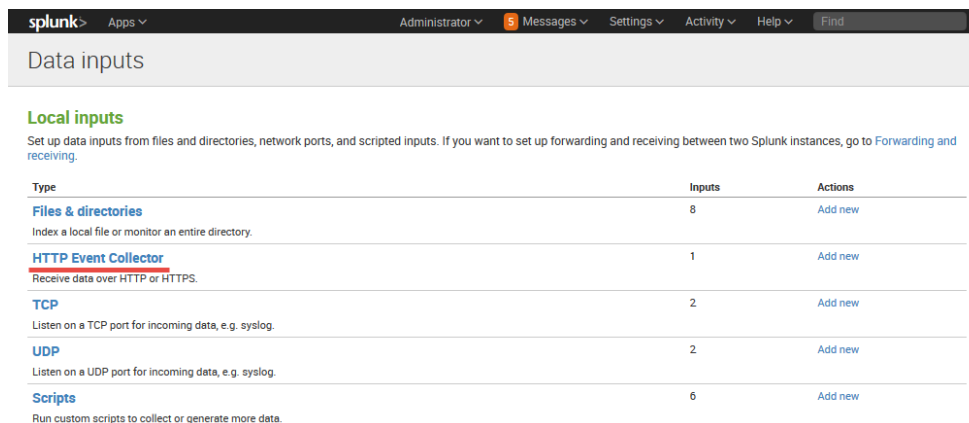
This section covers how to get an Authentication Token. You will need this key for creating a Splunk HTTP Target.

Before you can configure event collectors in the ForeScout Extended Module for Splunk, you will need to first get a token value (key) from the HTTP Event Collector Data Input.

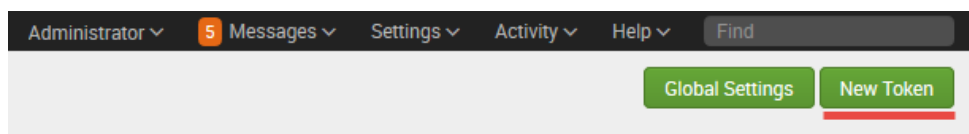
1. In the ForeScout App for Splunk, select **Messages** and then select **Data inputs**.



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. The default setting is *fscntcenter*.

Automatic Select New

fscntcenter_json ▾

Select Allowed Indexes

Available item(s) [add all »](#)

fscntcenter
history
main
summary

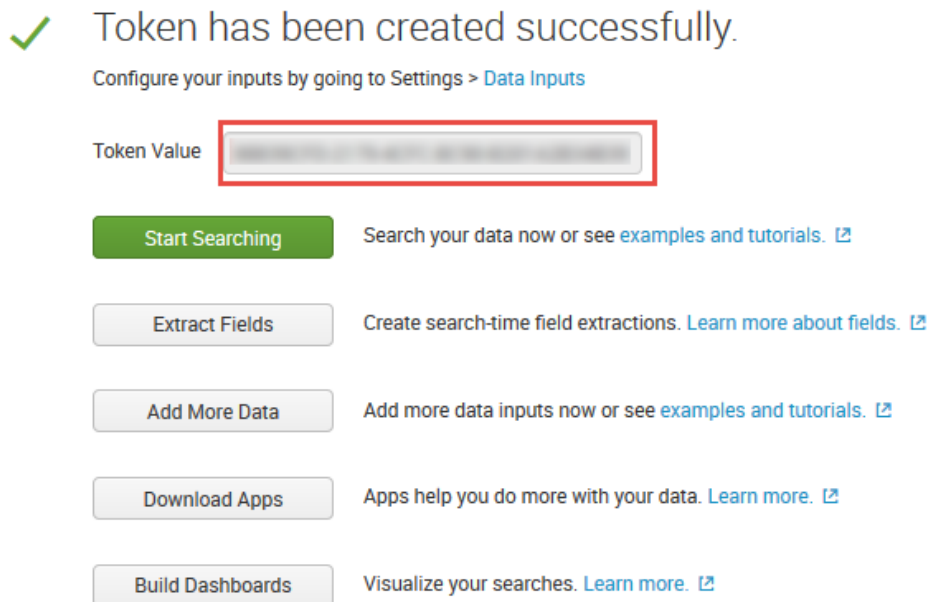
Selected item(s) « [remove all](#)

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.



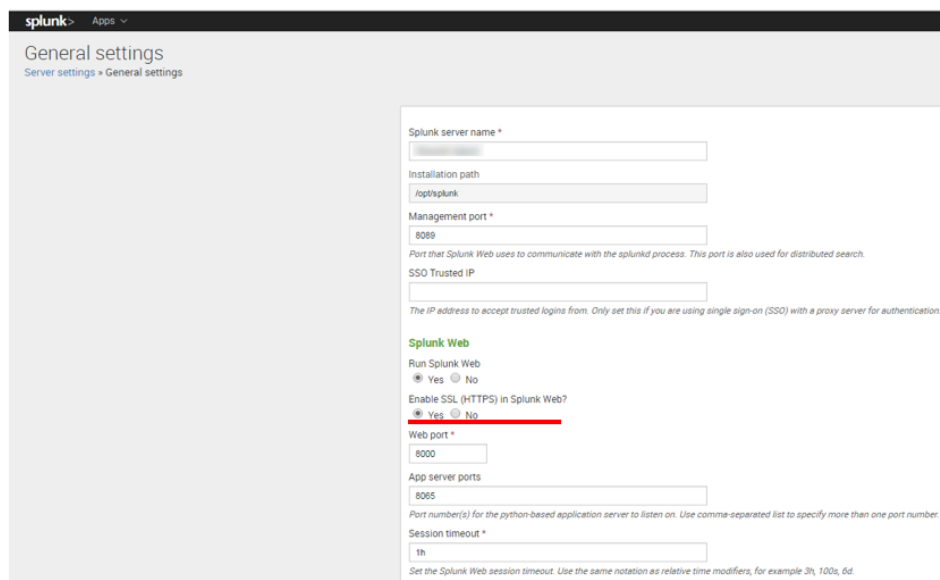
11. Copy this token value and paste it into a Notepad document. Save this Token. The Token Value will be used when you [Add a Splunk HTTP Target](#).

 *Make sure the HTTP Event Collector is enabled - by default, it is disabled.*

Set up Secure Connection Messaging from Splunk Module to the Splunk Enterprise Server

CounterACT Splunk Module updates messages sent to the Splunk Enterprise server via HTTP Event Collector or HTTP REST. It can also use HTTPS. If the Splunk Enterprise server is configured to use SSL (HTTPS) over Splunk Web:

- By default Splunk Enterprise generates a self-signed certificate that it uses for HTTPS messaging. Because this certificate is not signed by any certificate authority, CounterACT does not validate SSL handshakes based on this certificate.



The screenshot shows the 'General settings' page in the Splunk web interface. The 'Splunk Web' section is highlighted with a red box. The 'Run Splunk Web' checkbox is checked. The 'Enable SSL (HTTPS) in Splunk Web?' checkbox is also checked. The 'Web port' is set to 8000. The 'App server ports' are set to 8065. The 'Session timeout' is set to 1h.

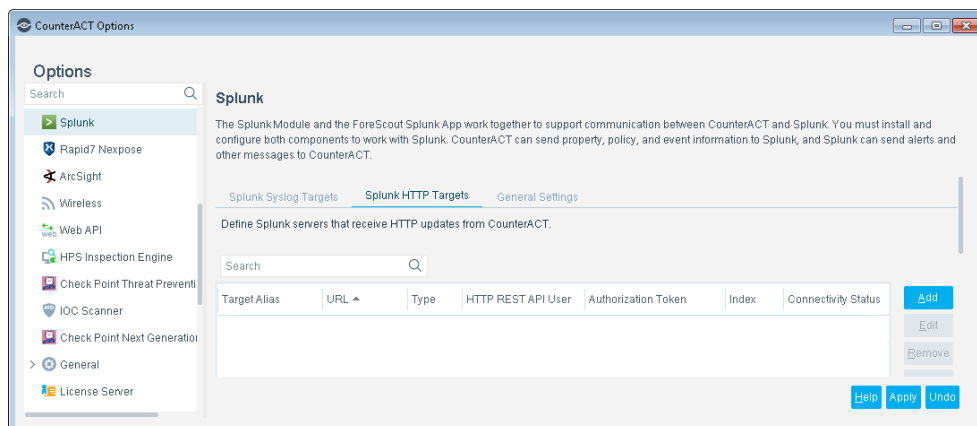
For more information about HTTPS configuration in Splunk, refer to the Splunk knowledge base.

Add a Splunk HTTP Target

(Optional) Use the following procedure to configure the module to send information to Splunk using Event Collector messages or Splunk HTTP REST messages. You can define one or more Splunk Enterprise servers that receive update messages from CounterACT in HTTP POST format.

To configure the module to use HTTP REST messaging:

1. In the CounterACT Console, select **Options** from the **Tools** menu. The Options dialog box opens.
2. Select **Splunk** in the left pane. Select the **Splunk HTTP Targets** tab.



3. Select **Add**. The Add Splunk HTTP Target Details wizard opens.

4. In the Splunk HTTP Type drop down, select one of the following:

- [Event Collector](#)
- [REST API](#)

Event Collector

An Event Collector is a Splunk-specific message type used to report event and endpoint data. The default port in Splunk for these messages is 8089.

a. Enter the following information and then select **Next**.

Splunk HTTP Type	<ul style="list-style-type: none"> ▪ <i>Event Collector</i> - An Event Collector is a Splunk-specific message type used to report event and endpoint data. ▪ REST API
Target Alias	Enter an alias to make it easier for you to select destinations when sending updates to the Splunk Enterprise server.
POST to URL	<p>The target URL that appears in the POST message header. In most cases the URL takes the form of the example shown. Replace <i>my.splunk.com</i> with the IP address of your Splunk Enterprise server.</p> <p>If the Splunk Enterprise server uses a different port from the default, specify the actual port used.</p> <p>See Appendix A: Default Communication Settings.</p>
Index	The index on the Splunk Enterprise server, where the update messages are sent to.

Comment	Optional text that indicates the location or other information that identifies the server.
Authorization Token	In the Splunk App HTTP Event Collector pane, copy the <i>Token Value</i> and paste it in the Authorization Token field.

b. Select **Next**. The Connection Test pane displays.

Add Splunk HTTP Target Details - Step 2 of 2

Add Splunk HTTP Target Details

Connection Test

The connection test establishes communication to the targeted connection using the parameters given below. Each selected test is executed chronologically. A successful test means all information provided to establish communication with the targeted connection was correct. A failed test provides information on what needs addressing before re-testing the connection.

☒ Enable Test Configuration
☒ Check if target is reachable (Check executed via ICMP ping)
☒ Check REST API communication (Server roles are retrieved if successful)
☒ Check data input and index (Check executed via REST API communication)

Management Username:
 Management Password:
 Verify Password:
 Management Port:

[Help](#) [Previous](#) [Next](#) [Finish](#) [Cancel](#)

Enable Test Configuration	Enabled by default, you can un-check the box to disable the testing of the Splunk Syslog Target connection.
Check if target is reachable	Enabled by default, the Splunk Syslog target connection is checked by executing an ICMP ping. De-select if you do not need to find out if the target is reachable.
Check REST API communication	Enabled by default, a check is done to verify if the Splunk Enterprise server's REST API interface is reachable. If it is reachable, this test retrieves and displays the server roles configured on the Splunk Enterprise server.
Check data input and index	<p>Enabled by default, a check is done to verify if the data input configured in the Syslog/HTTP target is:</p> <ul style="list-style-type: none"> Enabled For HTTP Event Collector, it also verifies if the index configured in the target on Splunk Module is also configured in that data inputs settings on the Splunk Enterprise server.

Management Username	The username and password credentials CounterACT uses to access the API on Splunk. Refer to the <i>ForeScout App & Add-ons for Splunk How-to Guide</i> .
Management Password	
Verify Password	Applicable to Event Collector only.
Management Port	Default is set to 8089. See Appendix A: Default Communication Settings .

- c. Select **Finish**. The new HTTP Event Collector target displays in the Splunk pane.

REST API

- a. In the Splunk HTTP Type drop-down, select **REST API**. The fields in the Add Splunk HTTP Target Details pane changes.

Add Splunk HTTP Target Details - Step 1

Add Splunk HTTP Target Details

General

Specify Splunk HTTP Target Details. Please ensure that each target has a unique set of values in the URL, Index and Authorization Token fields.

Splunk HTTP Type: REST API

Target Alias:

POST to URL: e.g. https://my.splunk.com:8089/services/receivers/simple

Index: fscntcenter

Comment:

REST: Username:

REST: Password:

Verify Password:

Buttons: Help, Previous, Next, Finish, Cancel

- b. Enter the following information:

Splunk HTTP Type	<ul style="list-style-type: none"> REST API - select to submit data or queries to the Splunk API. Event Collector
Target Alias	Enter an alias to make it easier for you to select destinations when sending updates to the Splunk Enterprise server.

POST to URL	The target URL that appears in the POST message header. In most cases the URL takes the form of the example shown. Replace <i>my.splunk.com</i> with the IP address of your Splunk Enterprise server. If the Splunk Enterprise server uses a different port from the default (8089), specify the actual port used. See Appendix A: Default Communication Settings .
Index	Enter the index for the HTTP REST API target or keep the default value of <i>fsctcenter</i> .
Comment	Optional text that indicates the location or other information that identifies the server.
REST: Username REST: Password	Enter the credentials CounterACT uses to access the API on Splunk. Enter the credentials of the account created in Splunk for CounterACT. Refer to the <i>ForeScout App & Add-ons for Splunk How-to Guide</i> .
Verify Password	Re-enter the password.

5. Select **Next**. The Connection Test pane displays.

Connection Test

For Splunk HTTP targets, a *test* message is sent to the Splunk Enterprise server (runs on all appliances). Results display success or failure on the basis of the HTTP response received for the HTTP request.

Add Splunk HTTP Target Details - Step 2 of 2

Add Splunk HTTP Target Details

General ☒ Connection Test ☒

Connection Test

The connection test establishes communication to the targeted connection using the parameters given below. Each selected test is executed chronologically. A successful test means all information provided to establish communication with the targeted connection was correct. A failed test provides information on what needs addressing before re-testing the connection.

Enable Test Configuration ☒

Check if target is reachable ☒ (Check executed via ICMP ping)

Check REST API communication ☒ (Server roles are retrieved if successful)

Management Username

Management Password

Verify Password

Management Port


[Help](#) [Previous](#) [Next](#) [Finish](#) [Cancel](#)

6. For REST API, the first three fields in this pane are editable - all other fields are read-only.

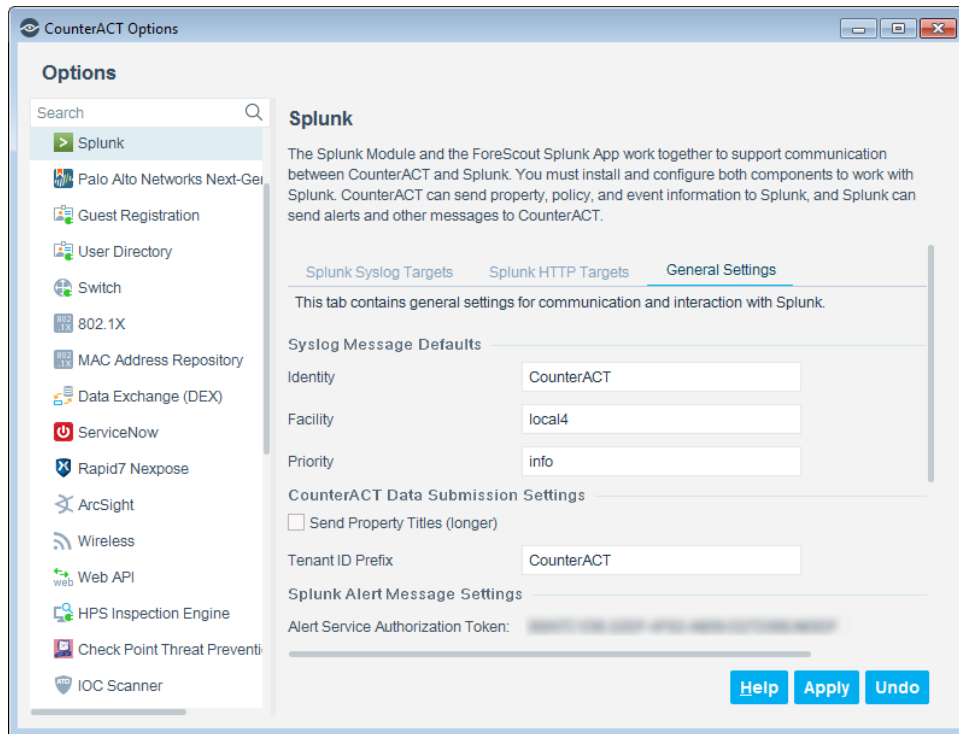
Enable Test Configuration	Enabled by default, you can un-check the box to disable the testing of the Splunk HTTP Target connection.
Check if target is reachable	Enabled by default, the Splunk HTTP target connection is checked by executing an ICMP ping. De-select if you do not want to find out if the target is reachable.
Check REST API communication	Enabled by default, a check is done to verify if the Splunk Enterprise server's REST API interface is reachable. If it is reachable, this test retrieves and displays the server roles configured on the Splunk Enterprise server.
Management Username	(Read-Only) The username and password credentials CounterACT uses to access the API on Splunk. Refer to the <i>ForeScout App & Add-ons for Splunk How-to Guide</i> .
Management Password	
Verify Password	(Read-Only) Applicable to Event Collector only.
Management Port	(Read-Only) Default is set to 8089. See Appendix A: Default Communication Settings .

7. Select **Finish**. The server appears in the Splunk pane, Splunk HTTP Targets tab.
8. Repeat these steps to define additional Event Collector/HTTP targets.

9. To modify Splunk Enterprise server information, select the server, then select **Edit**.

 Verify that data inputs defined on the Splunk Enterprise server use the port and other settings you define here. Refer to the ForeScout App & Add-ons for Splunk How-to Guide.

10. In the Splunk pane, select the **General Settings** tab.



11. The following options and fields are relevant when REST/HTTP messaging is used to report data to Splunk:

Syslog Message Defaults	Identity	Free-text field for identifying the Syslog message. This value overrides default message settings of the Syslog Plugin, but only for messages sent to Splunk.
	Facility	The Syslog message facility that is transmitted as part of the message. This value overrides default message settings of the Syslog Plugin, but only for messages sent to Splunk.
	Priority	The Syslog message severity that is transmitted as part of the message Priority field. This value overrides default message settings of the Syslog Plugin, but only for messages sent to Splunk.

CounterACT Data Submission Settings	Send Property Titles	CounterACT sends host property information to Splunk as Field:Value pairs in JASON format. By default, the Field: label is the internal property tag of each property. Select this option to send two sets of property value information to Splunk: Using the property tag as the Field: label: va_os : Windows 8.1 64-bit Pro Using the property's full name as the Field: label: Windows Version : Windows 8.1 64-bit Pro
	Tenant ID Prefix	Specify the prefix for the Tenant ID value in update messages. The Splunk Module will generate a random suffix (on each appliance) and append it to the Tenant ID prefix value to generate the Tenant ID. The Tenant ID is then sent as part of every update message sent by the Splunk Module to the Splunk Enterprise server.
Splunk Alert Message Settings	Alert Service Authorization Token	This string is used in the HTTP message header of alert messages sent to CounterACT by the ForeScout App for Splunk.

12. In the Splunk pane, select **Apply**. A confirmation dialog box opens.

13. Select **Yes** to save the configuration, and then select **Close**.

14. You are now ready to [Test the Module](#).

Add a Splunk Syslog Target

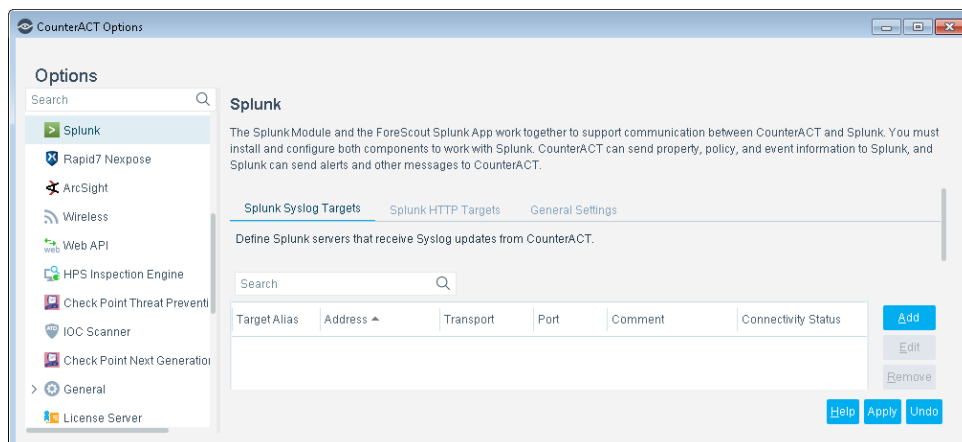
(Optional) Use the following procedure to configure the module to send information to Splunk using Syslog messages instead of Splunk Event Collector messages.

When using a Syslog target, if the message size is greater than 64KB, the Splunk Module will break down a batched update message into multiple messages. For a *hostinfo* message, the module will repeatedly extract one host property from the batched message and send it in a separate message. For a *policyinfo* message, the module will repeatedly extract one policy from the batched message and send it in a separate message. If the message is greater than 64 KB, an error message will be logged in the Module's log file.

 *The Splunk Module does not support secure communication for Syslog Targets.*

To configure Splunk Syslog Targets:

1. In the CounterACT Console, select **Options** from the **Tools** menu. The Options dialog box opens.
2. In the **Options** dialog box, select **Splunk** in the left pane. The Splunk pane opens to the Splunk Syslog Targets tab.



3. Select **Add**. The Add Splunk Syslog Target Details wizard opens.

4. Enter the following information:

Target Alias	Enter an alias to make it easier for you to select destinations when sending updates to the Splunk Enterprise server.
Address	The hostname or IP address of the Splunk Enterprise server.
UDP/TCP	The protocol used for Syslog messaging with the server. <ul style="list-style-type: none"> UDP (default) - select if you are concerned with speed of data messaging. TCP - select if you are concerned with accurate and successful transference of data.

Port	The port on the server that is used for Syslog messaging. If the Splunk Enterprise server uses a different port from the default, specify the actual port used. See Appendix A: Default Communication Settings .
Comment	Optional text that indicates the location or other information that identifies the server.

📄 *Verify that Syslog data inputs defined on the Splunk Enterprise server uses the same port as defined above. Index for Syslog data inputs can only be specified on the Splunk Enterprise Data Inputs Settings. Refer to the ForeScout App & Add-ons for Splunk How-to Guide.*

5. Select **Next**. The Connection Test pane displays.


6. Enter the following information.

Enable Test Configuration	Enabled by default, you can disable the testing of the Splunk Syslog Target connection. When un-checked, all fields in the Connection Test pane become disabled.
Check if target is reachable	Enabled by default, the Splunk Syslog target connection is checked by executing an ICMP ping. De-select if you do not want to find out if the target is reachable.

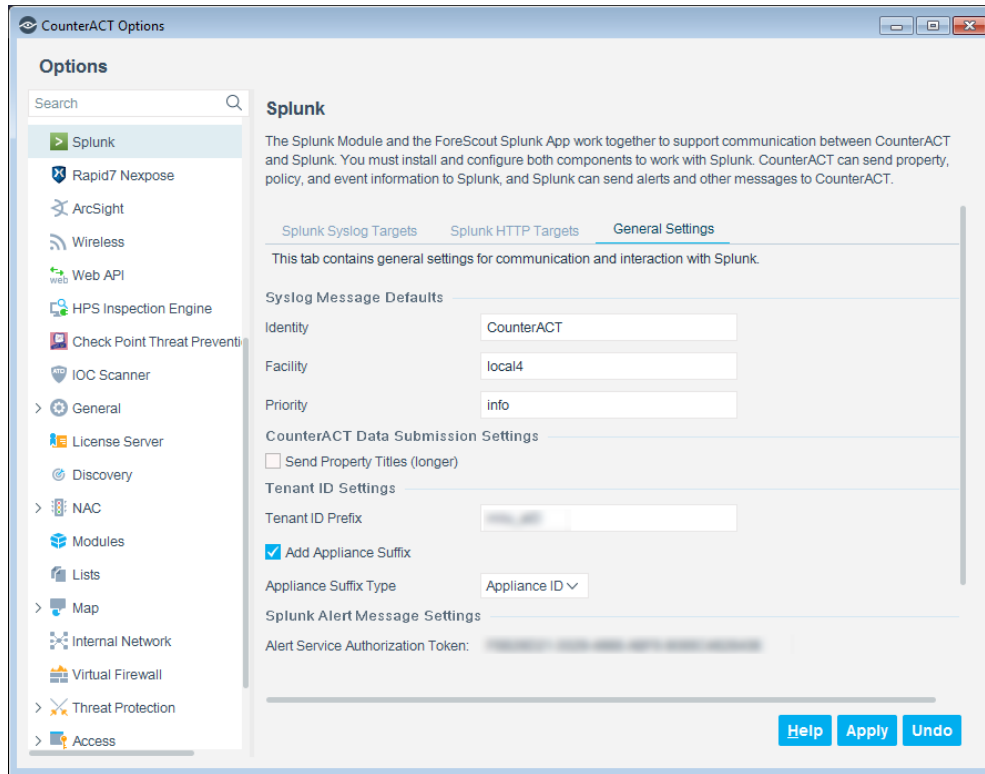
Check REST API communication	Enabled by default, a check is done to verify if the Splunk Enterprise server's REST API interface is reachable. If it is reachable, this test retrieves and displays the server roles configured on the Splunk Enterprise server.
Check data input and index	Enabled by default, a check is done to verify if the data input configured in the Syslog/HTTP target is: <ul style="list-style-type: none"> ▪ Enabled It also displays the indexes configured in that data inputs settings on the Splunk Enterprise server.
HTTP Protocol	<ul style="list-style-type: none"> ▪ HTTP - Select to use a Splunk-specific message to report event and endpoint data. ▪ HTTPS - Select to use an <i>encrypted</i> Splunk-specific message to report event and endpoint data
Management Username	The username and password credentials CounterACT uses to access the API on Splunk. Enter the credentials of the account created in Splunk for CounterACT. Refer to the <i>ForeScout App & Add-ons for Splunk How-to Guide</i> .
Management Password	
Verify Password	Verify the password.
Management Port	Default is set to 8089. If the Splunk Enterprise server uses a different port from the default, specify the actual port used. See Appendix A: Default Communication Settings .

7. Select **Finish.**

- a.** The server appears in the Splunk Syslog Targets tab.
- b.** Repeat these steps to define additional Syslog targets.
- c.** To modify Splunk Enterprise server information, select the server, then select **Edit**.

 *Verify that data inputs defined on the Splunk Enterprise server use the port and other settings you define here. Refer to the ForeScout App & Add-ons for Splunk How-to Guide.*

8. In the Splunk pane, select the **General Settings tab.**



The CounterACT Data Submission Settings and Splunk Alert Message Settings sections are relevant when using Event Collector messaging to report data to Splunk:

Syslog Message defaults	Identity	Free-text field for identifying the Syslog message. This value overrides default message settings of the Syslog Plugin, but only for event messages sent to Splunk.
	Facility	The Syslog message facility that is transmitted as part of the message. This value overrides default message settings of the Syslog Plugin, but only for messages sent to Splunk. For more information, see the <i>CounterACT Syslog Plugin Configuration Guide</i> .
	Priority	The Syslog message severity that is transmitted as part of the message Priority field. This value overrides default message settings of the Syslog Plugin, but only for messages sent to Splunk. For more information, see the <i>CounterACT Syslog Plugin Configuration Guide</i> .

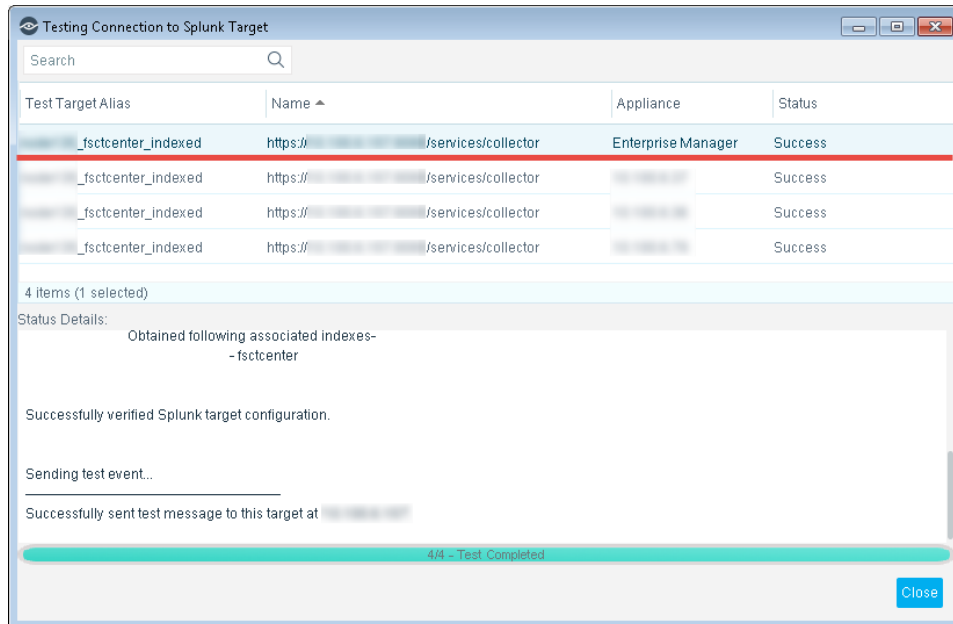
CounterACT Data Submission Settings	Send Property Titles (longer)	CounterACT sends host property information to Splunk as Field:Value pairs in JASON format. By default, the Field: label is the internal property tag of each property. Select this option to send two sets of property value information to Splunk: Using the property tag as the Field: label: va_os : Windows 8.1 64-bit Pro Using the property's full name as the Field: label: Windows Version : Windows 8.1 64-bit Pro
Tenant Settings	Tenant ID Prefix	Specify the prefix for the Tenant ID value in update messages. The user can choose to configure the module to generate a suffix to the aforementioned tenant ID prefix. If the suffix generation is selected, the module will generate a suffix (on each appliance) and append it to the Tenant ID prefix value to generate the Tenant ID. The Tenant ID is then sent as part of every update message sent by the Splunk Module to the Splunk Enterprise server. In the configuration wizard, the user enables/disables the Tenant ID suffix generation and specifies the type of suffix value in the Tenant ID.
	Add Appliance Suffix	Select the checkbox to enable/disable the Tenant ID suffix generation on each CounterACT appliance.
	Add Appliance Suffix Type	This configuration can only be done if the <i>Add Appliance Suffix</i> checkbox is selected. This field allows the user to control the nature of the Tenant ID suffix generated. Depending on user selection, the Tenant ID suffix corresponding to each CounterACT appliance can be: <ul style="list-style-type: none"> ▪ GUID ▪ Appliance IP address ▪ Appliance ID (a ForeScout-generated Node identifier)
Splunk Alert Message Settings	Alert Service Authorization Token	This string is used in the HTTP message header of alert messages sent to CounterACT by the ForeScout App for Splunk.

9. In the Splunk pane, select **Apply**. A confirmation dialog box opens.
10. Select **Yes** to save the configuration, and then select **Close**.
11. You are now ready to [Test the Module](#).

Test the Module

You can run an optional test to check the network connection to a Splunk Syslog target and/or a Splunk HTTP target (for Splunk Cloud). To test the Splunk Module configurations:

1. In the Options pane, select **Splunk**.
2. Select an item in the Splunk Syslog Targets tab or the Splunk HTTP Targets tab and then select **Test**.
3. Using configured settings, CounterACT attempts to connect with the Splunk Syslog / HTTP target.
4. The test results display.
5. Select one of the appliances shown in the test results to view the Status Details listed in the bottom half of the screen.










Checking for reachability	This check is done to verify if the Splunk Enterprise server can be reached via ICMP.
Checking for Splunk server roles	This check is done to verify if the Splunk Enterprise server's REST API interface is reachable. If it is reachable, this test retrieves and displays server roles configured on the Splunk Enterprise server.
Checking data inputs configuration	<p>This check is done to verify if the data input configured in the Syslog/HTTP target is:</p> <ul style="list-style-type: none"> ▪ Enabled ▪ For HTTP Event Collector and Syslog TCP and Syslog UDP targets, it also verifies if the index configured in the target on Splunk Module is also configured in that data inputs settings on the Splunk Enterprise server.

6. Review [Understanding Test Results](#).
7. Select **Close**. If necessary, make appropriate changes to the Splunk Enterprise and/or CounterACT configuration and re-test.

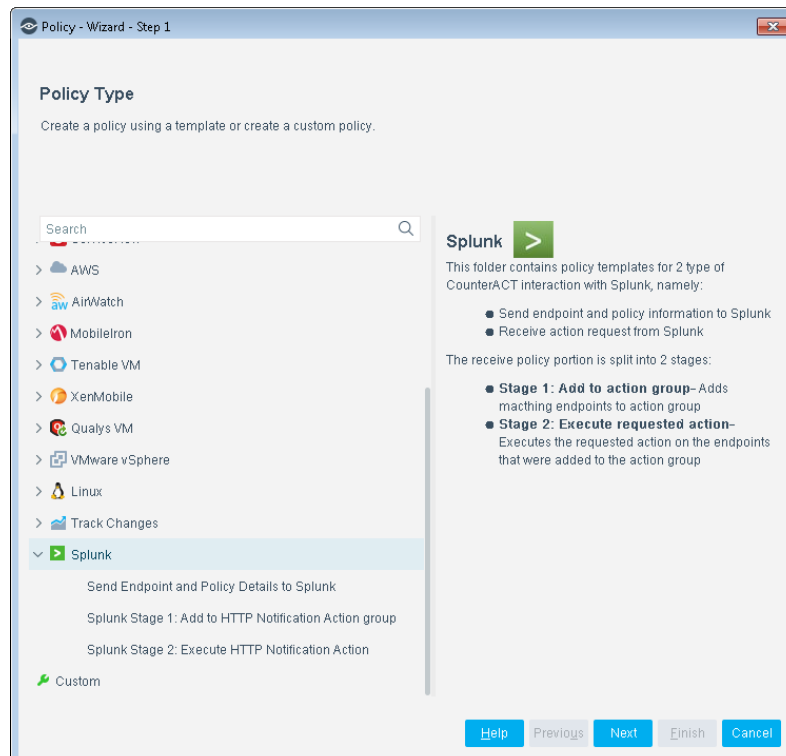
Understanding Test Results

Read this section to understand the various test states and their icons.

State / Icon	Definition
	New Splunk target or no test has been attempted yet on this Splunk target.
	Test failed on the Splunk target.
	Connectivity status expired.
	Test message successfully sent from the Splunk Module to the Splunk Enterprise server.
	Splunk test alert was received after a test message was sent successfully.
	Splunk test alert was received, but no test message sent for this target.
	Test message could not be sent on some appliances.

Run Splunk Policy Templates

This module provides the following policy templates used to detect, manage and remediate endpoints based on the Splunk integration.



Before applying the templates, it is recommended that you have a basic understanding of CounterACT policies before working with the templates. See the CounterACT Templates and Policy Management chapters of the CounterACT Administration Guide.

- The [Send Endpoint and Policy Details to Splunk](#) template generates a policy that sends endpoint and policy information to Splunk.
- The following templates provide an example of group-based handling of action request messages received from Splunk.
- Splunk [Stage 1 – Add to HTTP Notification Action Group](#) template generates a policy that detects messages that request the HTTP Notification action, and places them in the Splunk HTTP Notification group. Use this as a reference and follow the correct action group based on the action requested from Splunk.
- Splunk [Stage 2 - Execute HTTP Notification Action](#) template generates a policy that executes the HTTP Notification action for endpoints in the HTTP Notification Action Group.

Send Endpoint and Policy Details to Splunk

This section addresses batched messages and setting up a policy to send endpoint and policy details to the Splunk Enterprise server.

Batched Messages

Create policies based on this template to send endpoint properties, classification, and policy information to the Splunk Enterprise server. This information is sent as batched messages and you can view the message sent to the Splunk Enterprise server using Splunk's Search and Reporting app or the ForeScout App for Splunk search capability.

Below is an example search results for "index=fscntcenter". Notice there are several (batched) messages.

The screenshot shows the Splunk Search & Reporting interface. The search bar contains 'index=fscntcenter' and the search is filtered for 'Last 4 hours'. The results show 20,676 events. The interface includes a timeline visualization at the top and a list view of the search results below. The list view shows three events, each with a timestamp and a JSON payload. The first event is at 1/19/18 5:00:24.000 AM, the second at 1/19/18 5:00:17.000 AM, and the third at 1/19/18 5:00:15.000 AM. Each event contains a JSON object with fields like 'ctupdate', 'dnsdomain', 'host_properties', 'ip', 'mac', and 'tenant_id'. The 'tenant_id' is 'CounterACT_39FF80E8-D957-4B39-BD58-102E7A9BDAC4' for the first two events. The third event only shows 'ctupdate' and 'host_properties'.

i	Time	Event
>	1/19/18 5:00:24.000 AM	{ [-] ctupdate: hostinfo dnsdomain: .forescout.com host_properties: { [+] } ip: mac: tenant_id: CounterACT_39FF80E8-D957-4B39-BD58-102E7A9BDAC4 } Show as raw text host = source = CounterACT sourcetype = fscntcenter_json
>	1/19/18 5:00:17.000 AM	{ [-] ctupdate: hostinfo dnsdomain: .forescout.com host_properties: { [+] } ip: mac: tenant_id: CounterACT_39FF80E8-D957-4B39-BD58-102E7A9BDAC4 } Show as raw text host = source = CounterACT sourcetype = fscntcenter_json
>	1/19/18 5:00:15.000 AM	{ [-] ctupdate: hostinfo host_properties: { [+] }

Selecting one of the messages, you can expand the message to display it in full.

The screenshot shows the Splunk search results for the query `index=fsctcenter`. The search returned 24,174 events. The selected event is a JSON object with the following structure:

```

{
  "ctupdate": "hostinfo",
  "host_properties": {
    "adm": [
      {
        "since": "1516330498",
        "value": "Authentication Server: Microsoft-DS"
      }
    ],
    "auth_login": [
      {
        "since": "1516330498",
        "value": "Authentication Server: Microsoft-DS"
      }
    ],
    "auth_login_adv": [
      {
        "since": "1516330498",
        "value": "Authentication Server: Microsoft-DS"
      }
    ]
  },
  "ip": "192.168.1.1",
  "mac": "08:00:27:00:00:00",
  "nbtomain": "Microsoft-DS",
  "nbthost": "W7-648-01",
  "tenant_id": "CounterACT_39FF80E8-D957-4B39-BD58-102E7A9BDAC4",
  "user": "administrator"
}

```

The event is displayed in a table with columns for Time and Event. The event is shown in a raw text format. The search results are paginated, showing 20 results per page.

A single message contains multiple host properties or policies for a particular endpoint.

The screenshot shows the 'Policy Wizard - Step 1' dialog box. The 'Policy Type' section is active, showing a search bar and a list of policy types. The 'Send Endpoint and Policy Details to Splunk' policy type is selected. The dialog also includes a description of the policy type and buttons for 'Help', 'Previous', 'Next', 'Finish', and 'Cancel'.

Run the Template

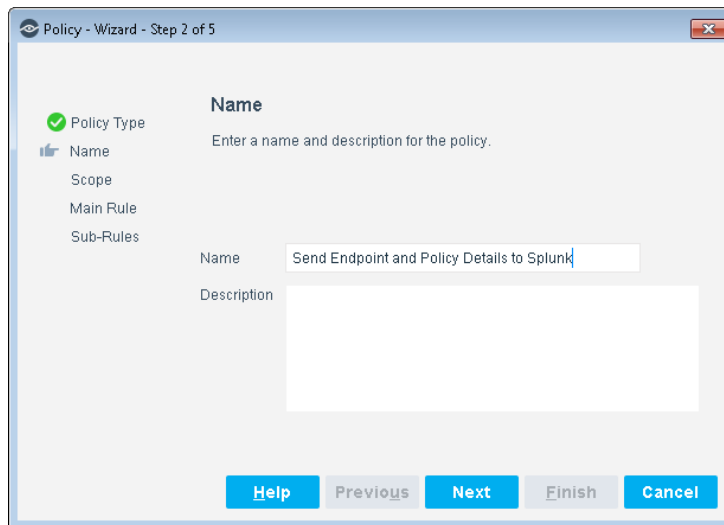
This section describes how to create a policy from the policy template. For details about how the policy works, see [Run Splunk Policy Templates](#).

To run the template:

1. Log in to the CounterACT Console and select the **Policy** tab.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **Splunk** folder and select **Send Endpoint and Policy Details to Splunk**.
4. Select **Next**. The **Name** pane of the Policy Wizard opens.

Name the Policy

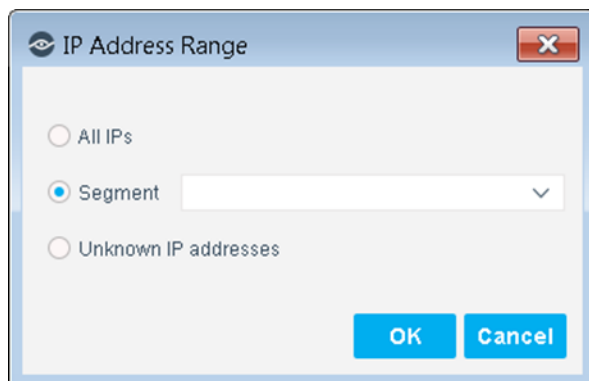
The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.



5. Define a unique name for the policy you are creating based on this template, and enter a description.
 - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as `My_Compliance_Policy`.
 - Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
 - Ensure that the name indicates whether the policy criteria must be met or not met.
 - Avoid having another policy with a similar name.
6. Select **Next**. The Scope pane and IP Address Range dialog box opens.

Define which Hosts will be Inspected - Policy Scope

7. Use The IP Address Range dialog box to define which endpoints are inspected.



The following options are available:

- **All IPs:** Include all IP addresses in the Internal Network.
 - **Segment:** Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope page.
 - **Unknown IP addresses:** Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.
8. Select **OK**. The added range appears in the Scope pane.
 9. Select **Next**. The Main Rule pane opens. See [How Devices are Detected and Handled](#) for details of default policy logic.
 10. Select **Next**. The Sub-rules pane opens. See [How Devices are Detected and Handled](#) for details of default policy logic.
 11. Select **Finish**. The policy is created.

How Devices are Detected and Handled

This section describes the main rule and sub-rules of the policy created by the template. Policy rules instruct CounterACT how to detect and handled hosts defined in the policy scope.

Policy: "Send Endpoint and Policy Details to Splunk"

Name
 Name: Send Endpoint and Policy Details to Splunk [Edit]
 Description: None.

Scope
 IP Ranges: All IPs [Edit]
 Filter by Group: None.
 Exceptions: None.

Main Rule

Conditions	Actions	Re-check
No Conditions		Every 8 hours, All ad...

[Edit]

Sub-Rules

Name	Conditions	Actions
No items to display		

[Add] [Edit] [Remove] [Duplicate] [Up] [Down]

[Help] [OK] [Cancel]

Endpoints that match the Main Rule are included in policy sub-rule inspection. When *endpoints do not match the Main Rule, policy evaluation ends. Sub-rules are not evaluated for these endpoints.*

Sub-rules are evaluated in order until a match is found. When an endpoint matches the conditions of a sub-rule, the actions of that sub-rule are applied to the endpoint and policy evaluation ends. If the host does not match the conditions of the sub-rule, evaluation moves to the next sub-rule.

Main Rule

The main rule of this policy applies no filtering conditions: it includes all endpoints detected by CounterACT within the specified policy scope.

The [Splunk: Send Update from CounterACT Action](#) can send the following information to Splunk for each detected endpoint:

- Selected host properties – by default, the policy sends all host properties.
- Compliance policy status – by default, the policy sends information for all active Compliance policies.
- General policy status – by default, the policy sends all active policy information to Splunk.

For details about specifying the information that is sent to Splunk and for other action options, see [Splunk: Send Update from CounterACT Action](#).

Sub-Rules

There are no sub-rules in this policy.

Stage 1 – Add to HTTP Notification Action Group

Create policies based on this template to detect messages that request the HTTP Notification action, and place them in the Splunk HTTP Notification group. Use this as a reference and follow the correct action group based on the action requested from Splunk.

Run the Template

This section describes how to create a policy from the policy template. See [How Devices are Detected and Handled](#) for details of default policy logic.

To run the template:

1. Log in to the CounterACT Console and select the **Policy** tab.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **Splunk** folder and select the Execute HTTP Notification Action Group template.
4. Select **Next**. The **Name** pane of the policy creation wizard opens.

Name the Policy

The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

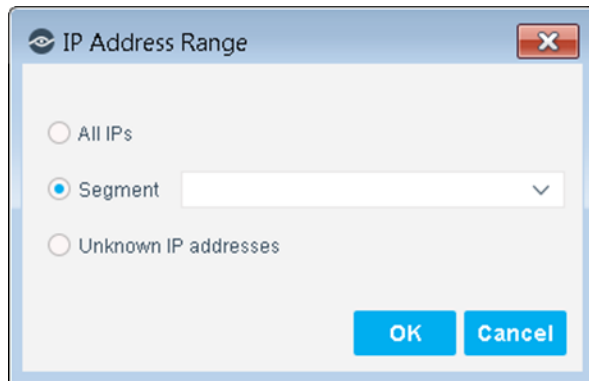
The screenshot shows a window titled "Policy - Wizard - Step 2 of 5". On the left is a sidebar with a tree view containing: "Policy Type" (with a green checkmark icon), "Name" (with a folder icon), "Scope", "Main Rule", and "Sub-Rules". The main area is titled "Name" and contains the instruction "Enter a name and description for the policy." Below this are two text input fields: "Name" and "Description". The "Name" field contains the text "Splunk Stage 1: Add to HTTP Notification Action grou". At the bottom of the window are five buttons: "Help", "Previous", "Next", "Finish", and "Cancel".

5. Define a unique name for the policy you are creating based on this template, and enter a description.

- Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
 - Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
 - Ensure that the name indicates whether the policy criteria must be met or not met.
 - Avoid having another policy with a similar name.
6. Select **Next**. The Scope pane and IP Address Range dialog box opens.

Define which Hosts will be Inspected - Policy Scope

7. Use The IP Address Range dialog box to define which endpoints are inspected.



The following options are available:

- **All IPs**: Include all IP addresses in the Internal Network.
 - **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope page.
 - **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.
8. Select **OK**. The added range appears in the Scope pane.
9. Select **Next**. The Main Rule pane opens. See [How Devices are Detected and Handled](#) for details of default policy logic.
10. Select **Finish**. The policy is created.

How Devices are Detected and Handled

This section describes the main rule and sub-rules of the policy created by the template. Policy rules instruct CounterACT how to detect and handled hosts defined in the policy scope.

Endpoints that match the Main Rule are included in policy sub-rule inspection. When *endpoints do not match the Main Rule, policy evaluation ends. Sub-rules are not evaluated for these endpoints.*

Sub-rules are evaluated in order until a match is found. When an endpoint matches the conditions of a sub-rule, the actions of that sub-rule are applied to the endpoint

and *policy evaluation ends*. If the host does not match the conditions of the sub-rule, evaluation moves to the next sub-rule.

Main Rule

The main rule captures all Splunk action requests associated with a specific action group.

Sub-Rules

The first sub-rule of the policy adds an endpoint to HTTP Notification Action group when an HTTP Notification Action request is received from Splunk. The endpoint is part of the group for a day (default.)

The second sub-rule detects all other endpoints that do not match the action request within a day (default).

To define the action:

1. Select **Splunk Alerts** from the Sub-rules, Condition dialog box.
2. Select **Edit**.
3. Select **Splunk Alert Action Group** and then select **Meets the following criteria**.
4. Use the drop-downs to specify the criteria for meeting the Action Group alert.
5. Select **Splunk Alert Action** and then select **Meets the following criteria**.

The screenshot shows the 'Condition' tab of the ForeScout Configuration Wizard. The left sidebar lists various configuration categories, with 'Splunk Alerts' selected. The main panel is titled 'Splunk Alerts: Indicates information for alert messages received from Splunk for an endpoint.' It contains two sections: 'Splunk Alert Action Group' and 'Splunk Alert Action'.

Splunk Alert Action Group

- ☒ **Splunk Alert Action Group**
Select the Action Group contained in the Alert. Valid values can be one of: [manage, notify, remediate, restrict]
- ☒ Meets the following criteria
☐ Does not meet the following criteria
- Matches:
- ☐ Match case

Splunk Alert Action

Actions are grouped by 'Splunk Alert Action Group'. Each action is prefixed with the action group it belongs to. Make sure to select entry that have prefix matching the value entered in 'Splunk Alert Action Group' field. Prefix would be one of 'manage', 'notify', 'remediate' or 'restrict'. Note: When selecting multiple entries, correct status is sent back to Splunk only for actions requested from Splunk.

- ☒ Meets the following criteria
☐ Does not meet the following criteria

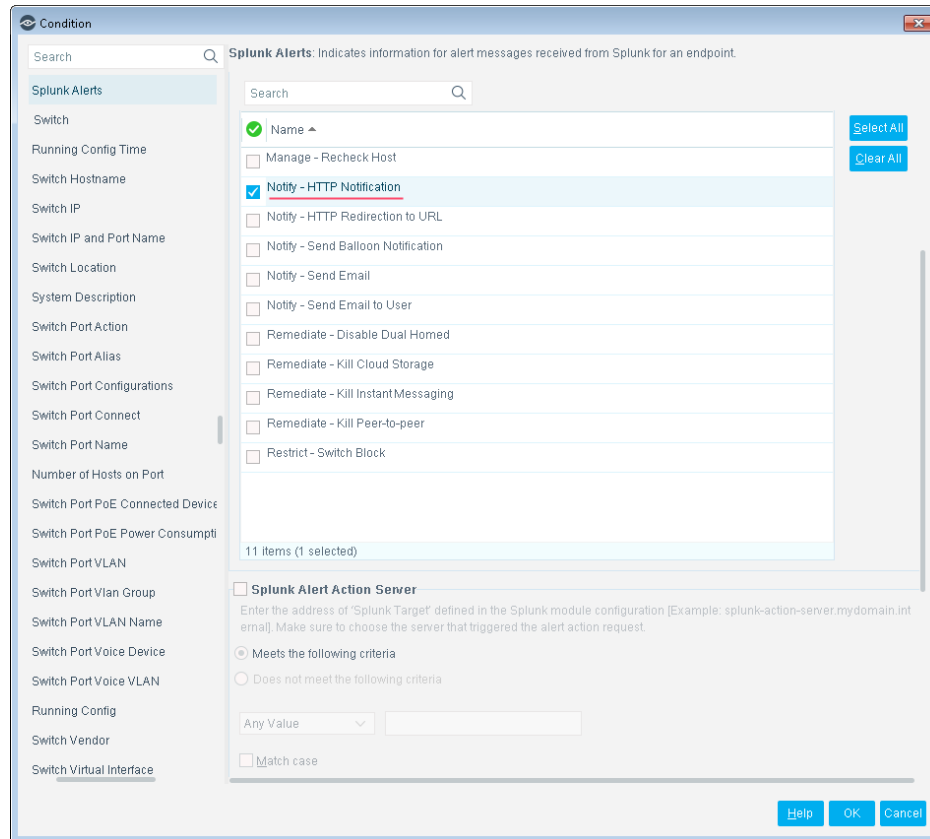
Search:

<input checked="" type="checkbox"/> Name
<input type="checkbox"/> Manage - Recheck Host
<input type="checkbox"/> Notify - HTTP Notification
<input type="checkbox"/> Notify - HTTP Redirection to URL
<input type="checkbox"/> Notify - Send Balloon Notification
<input type="checkbox"/> Notify - Send Email
<input type="checkbox"/> Notify - Send Email to User
<input type="checkbox"/> Remediate - Disable Dual Homed
<input type="checkbox"/> Remediate - Kill Cloud Storage
<input type="checkbox"/> Remediate - Kill Instant Messaging

Buttons:

Buttons:

6. Select Notify – HTTP Notification and then select OK.



Stage 2 - Execute HTTP Notification Action

Create policies based on this template to instruct CounterACT how to handle action request alerts sent to CounterACT from Splunk. The policy detects endpoints for which Splunk has requested the HTTP Notification action and then adds these endpoints to the Splunk HTTP Notification Alerts group.

To support Splunk action request alert messages, create a companion policy based on this template. The policy will then add endpoints to the Splunk HTTP Notification Alerts group when Splunk alert messages request this action for the endpoint.

To implement other actions requested by Splunk, create and modify policies based on this template.

Run the Template

This section describes how to create a policy from the policy template. See [How Devices are Detected and Handled](#) for details of default policy logic.

To run the template:

1. Log in to the CounterACT Console and select the **Policy** tab.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **Splunk** folder and select the Execute HTTP Notification Action template.

4. Select **Next**. The **Name** pane of the policy creation wizard opens.

Name the Policy

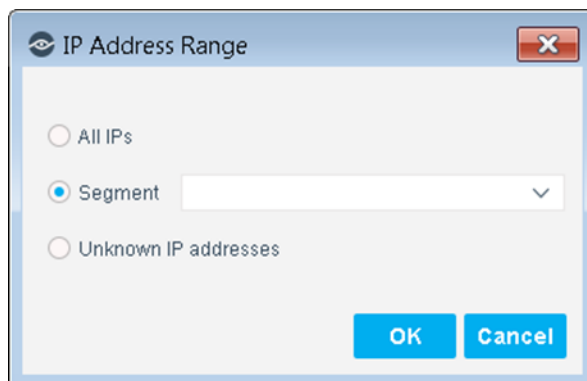
The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

The screenshot shows a window titled "Policy - Wizard - Step 2 of 5". On the left is a sidebar with a tree view containing "Policy Type" (checked with a green icon), "Name" (selected with a blue icon), "Scope", "Main Rule", and "Sub-Rules". The main area is titled "Name" and contains the instruction "Enter a name and description for the policy." Below this are two text input fields: "Name" (containing "Splunk Stage 2: Execute HTTP Notification Action") and "Description" (empty). At the bottom right are five buttons: "Help", "Previous", "Next", "Finish", and "Cancel".

5. Define a unique name for the policy you are creating based on this template, and enter a description.
 - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
 - Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
 - Ensure that the name indicates whether the policy criteria must be met or not met.
 - Avoid having another policy with a similar name.
6. Select **Next**. The Scope pane and IP Address Range dialog box opens.

Define which Hosts will be Inspected - Policy Scope

7. Use The IP Address Range dialog box to define which endpoints are inspected.

The screenshot shows a dialog box titled "IP Address Range". It has three radio button options: "All IPs", "Segment" (which is selected), and "Unknown IP addresses". The "Segment" option is followed by a dropdown menu. At the bottom right are two buttons: "OK" and "Cancel".

The following options are available:

- **All IPs:** Include all IP addresses in the Internal Network.
 - **Segment:** Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope page.
 - **Unknown IP addresses:** Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.
8. Select **OK**. The added range appears in the Scope pane.
 9. Select **Next**. The Main Rule pane opens. See [How Devices are Detected and Handled](#) for details of default policy logic.
 10. Select **Finish**. The policy is created.

The CounterACT 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 following action status values displayed in the Dashboard are reported by CounterACT.

Success	The action completed without failure.
Failure	The action completed with a failure, or timed out.
Pending	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.
Init	The action is in Initializing state, and not yet complete.
No Status	No status can be reported for one of the following reasons: <ul style="list-style-type: none"> ▪ No active policy detects the relevant Splunk Last Alert property, or applies the requested action. ▪ The endpoint has been deleted from CounterACT. ▪ Even though the IP address of the endpoint is within CounterACT's network scope, the endpoint has not been detected by CounterACT. ▪ Scheduled CounterACT data purges clear action data before reports are generated.
Invalid	<ul style="list-style-type: none"> ▪ The endpoint IP is outside the network scope defined in CounterACT. ▪ An unspecified internal error occurred.

Note that:

- 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.

How Devices are Detected and Handled

This section describes the main rule and sub-rules of the policy created by the template. Policy rules instruct CounterACT how to detect and handled hosts defined in the policy scope.

Endpoints that match the Main Rule are included in policy sub-rule inspection. When *endpoints do not match the Main Rule, policy evaluation ends. Sub-rules are not evaluated for these endpoints.*

Sub-rules are evaluated in order until a match is found. When an endpoint matches the conditions of a sub-rule, the actions of that sub-rule are applied to the endpoint and *policy evaluation ends*. If the host does not match the conditions of the sub-rule, evaluation moves to the next sub-rule.

Main Rule

The main rule looks for an endpoint that is part of a specific group and when it finds a match, applies a defined action. The conditions defined in the Criteria section are re-checked every 8 hours (default.)

The screenshot shows the 'Policy - Wizard - Step 4 of 5' window. On the left, a progress bar indicates that 'Policy Type', 'Name', and 'Scope' are completed, and 'Main Rule' is the current step. The main area is titled 'Main Rule' and contains the following sections:

- Condition:** A host matches this rule if it meets the following condition:
 - Dropdown: All criteria are True
 - Criteria list: Member of Group - HTTP Notification Action
 - Buttons: Add, Edit, Remove
- Actions:** Actions are applied to hosts matching the above condition.

Ena...	Action	Details
<input type="checkbox"/>	HTTP Notification	HTTP Notif...

 Buttons: Add, Edit, Remove

At the bottom, there are navigation buttons: Help, Previous, Next, Finish, and Cancel.

Sub-Rules

There are no sub-rules in this policy.

Create Custom Splunk Policies

You may need to create a custom policy to capture Splunk action requests supported by this integration but not covered in the policy templates provided with this module. In addition to the bundled CounterACT properties and actions available for detecting

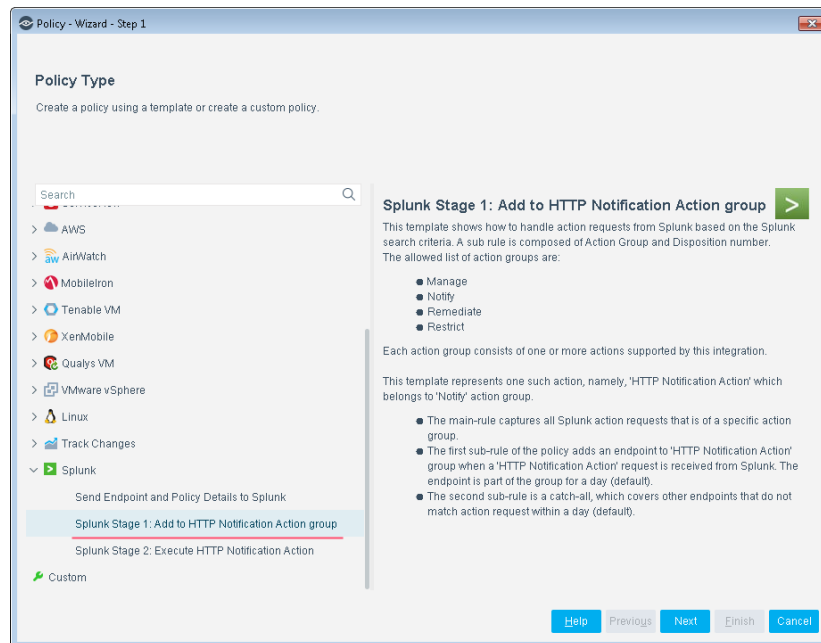
and handling endpoints, you can work with properties and actions provided by this module to create custom policies.

To ensure all conditional properties for responding to an action requests are adequately fulfilled, it is best to create this custom policy out of Stage 1 and Stage 2 policy templates provided with CounterACT.

For more information about working with policies, select **Help** from the Policy Wizard.

To create a custom Splunk Stage 1 policy:

1. Log in to the CounterACT Console.
2. On the Console toolbar, select the **Policy** tab. The Policy Manager opens.
3. Select **Add** to create a policy.
4. Select **Splunk Stage 1: Add to HTTP Notification Action Group** template and select **Next**.



5. Change the name of the policy to a custom name and then select **Next**.
6. Select an appropriate scope and then select **Next**.
7. Edit the main rule to specify the desired Splunk Alert Action Group. Select **Next**. The Add to Switch Block Action group dialog box displays.

Policy - Wizard - Step 4 of 5

☒ Policy Type
☒ Name
☒ Scope
☒ Main Rule
☐ Sub-Rules

Main Rule

Use this screen to review policy sub-rule definitions.
Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Condition

A host matches this rule if it meets the following condition:

All criteria are True

Criteria	Add	Edit	Remove
Splunk Alerts - Splunk Alert Action Group: Matches notify Within the last 1 day			

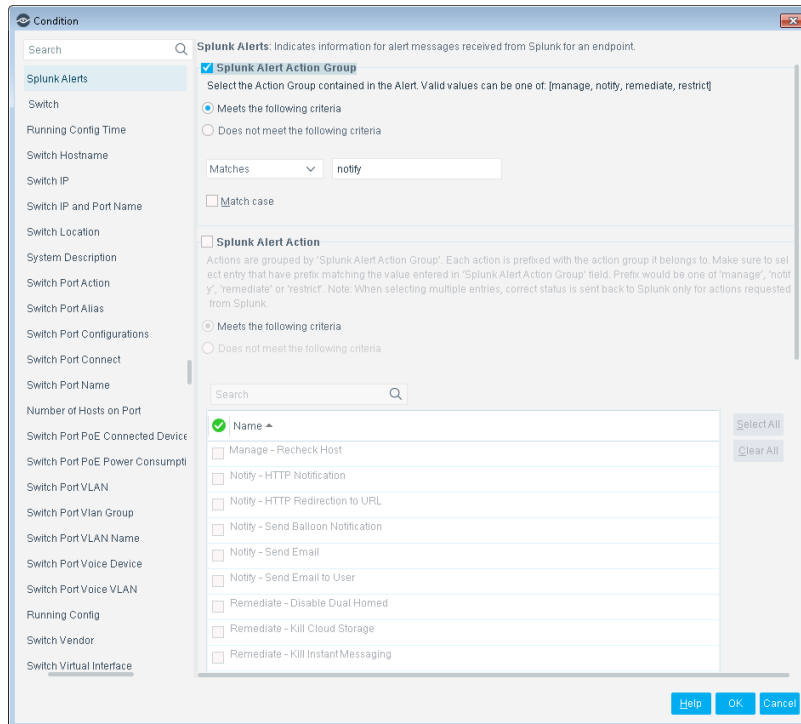
Actions

Actions are applied to hosts matching the above condition.

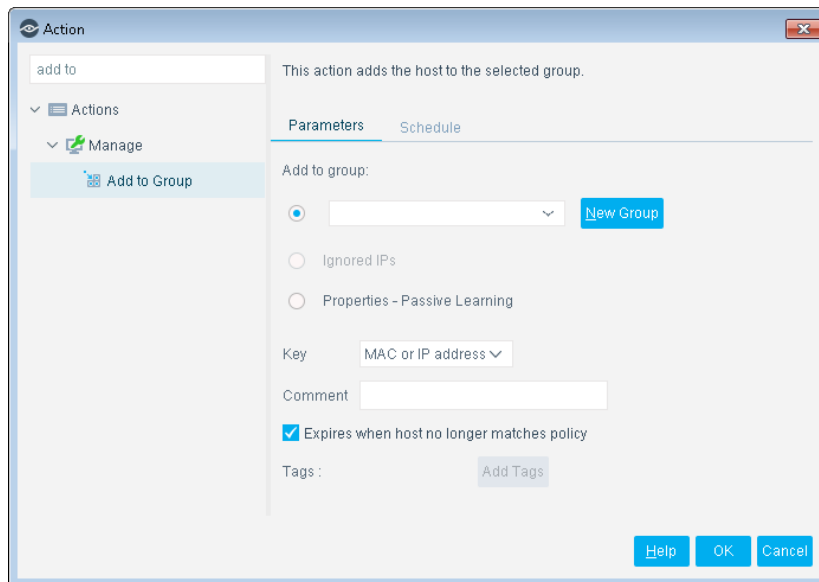
Enable	Action	Details	Add	Edit	Remove
No items to display					

Help Previous Next Finish Cancel

8. In the Condition section, **Edit** the first Sub-Rule and give it a custom name.
9. In the Actions section, **Add** or **Edit** the desired Splunk Alert Action. The Splunk Alert Action Group should be the same as the one specified in the main rule.
10. Select **OK**. The Condition pane displays.



11. In the Splunk Alert Action section, select the **Splunk Alert Action** that is to be associated with the custom policy. Select **OK**. The Action dialog box displays.

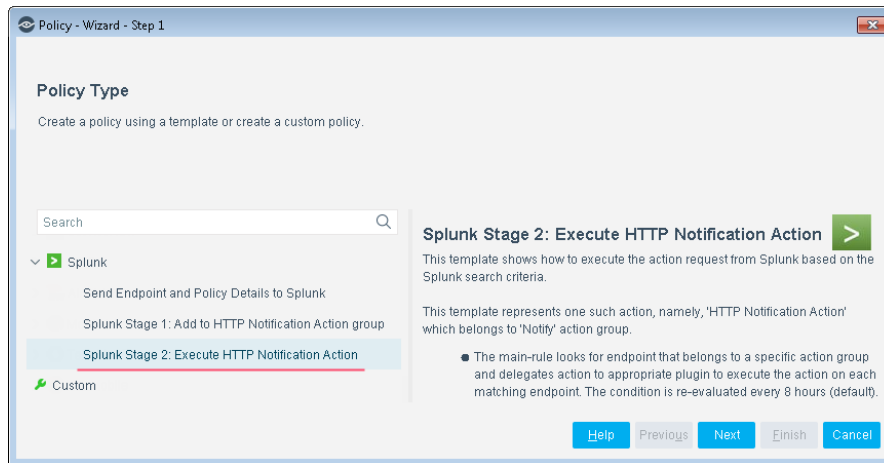


12. The second sub-rule does not need to be edited. Select **Finish**.

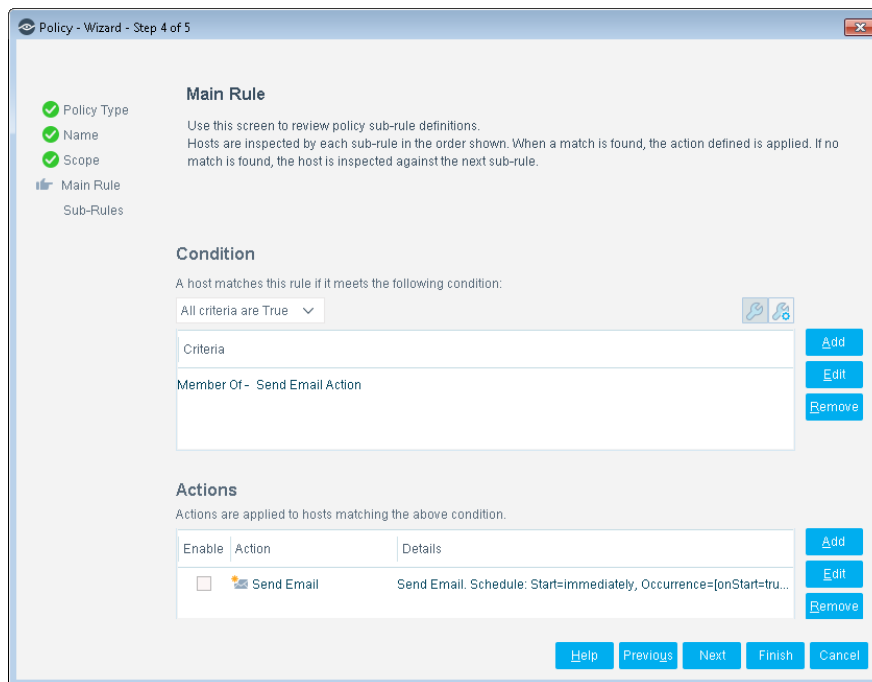
To create a custom Splunk Stage 2 policy:

1. Log in to the CounterACT Console.
2. On the Console toolbar, select the **Policy** tab. The Policy Manager opens.

3. Select **Add** to create a policy. The Policy Wizard displays.
4. Select Splunk Stage 2: Execute HTTP Notification Action template and select **Next**.



5. Change the name of the policy to a custom name and then select **Next**.
6. Select an appropriate scope and then select **Next**. The Condition dialog box displays.



7. In the Condition section, select the "Member of Group" item and **Edit** the main rule condition to specify the group from the Stage 1 policy template.
8. In the Actions section, **Add** or **Edit** the Action in the main-rule to the action for the custom policy.
9. Select **OK**.

Detecting Endpoints – Policy Properties

As part of the custom policy you created, the endpoints need to be configured.

Splunk Alerts

Splunk alerts messages are sent to CounterACT to request an action to an endpoint.

There are three aspects for every Splunk alert check: Splunk Alert Action Group, Splunk Alert Action, and Splunk Alert Action Server.

To configure Splunk alerts:

1. In the ForeScout Splunk App, search for “Splunk Alerts”. Select it. The Condition pane displays the configurations for Splunk Alerts.
2. The **Splunk Alert Action Group** field maps to an action group in CounterACT. In the Condition pane, select the Action Group values.

Condition

Search

Splunk Alerts: Indicates information for alert messages received from Splunk for an endpoint.

☒ **Splunk Alert Action Group**

Select the Action Group contained in the Alert. Valid values can be one of: [manage, notify, remediate, restrict]

☒ Meets the following criteria

☐ Does not meet the following criteria

Matches

☐ Match case

☐ **Splunk Alert Action**

Actions are grouped by "Splunk Alert Action Group". Each action is prefixed with the action group it belongs to. Make sure to select entry that have prefix matching the value entered in "Splunk Alert Action Group" field. Prefix would be one of 'manage', 'notify', 'remediate' or 'restrict'. Note: When selecting multiple entries, correct status is sent back to Splunk only for actions requested from Splunk.

☒ Meets the following criteria

☐ Does not meet the following criteria

Search

☒ Name ^

☐ Manage - Recheck Host

☐ Notify - HTTP Notification

☐ Notify - HTTP Redirection to URL

☐ Notify - Send Balloon Notification

☐ Notify - Send Email

☐ Notify - Send Email to User

☐ Remediate - Disable Dual Homed

☐ Remediate - Kill Cloud Storage

☐ Remediate - Kill Instant Messaging

Select All

Clear All

Help OK Cancel

3. The **Splunk Alert Action** field maps the action(s) the selected group. If the group meets or does not meet the selected criteria, a request for action (alert) will be sent to CounterACT.
4. The **Splunk Alert Action Server** – Enter the IP address of the server that triggers the alert action request.
5. Select **OK**.

Managing Splunk Devices – Policy Actions

This section describes the actions that are made available when the Splunk module is installed.

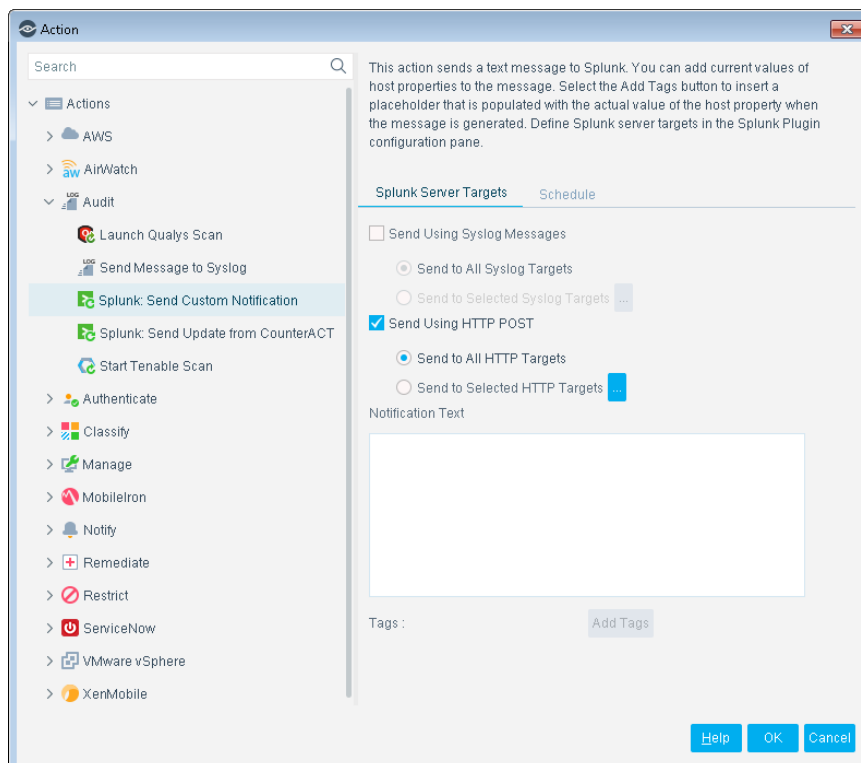
To access Splunk actions:

1. Navigate to the Actions tree from the Policy Actions dialog box.
2. Expand the Audit folder in the Actions tree.
3. The following actions are available:
 - [Splunk: Send Custom Notification Action](#)
 - [Splunk: Send Update from CounterACT Action](#)

Splunk: Send Custom Notification Action

Use this action to send a text message to one or more Splunk Enterprise servers. This message can include varied information, such as:

- Standard event or error strings that are reported by other components of your security environment.
- Information not included in regular updates of host property and policy information that CounterACT sends to Splunk. For example: add this action to policies that apply or remove the **Switch Block** action to track port blocking in Splunk.



To use this action:

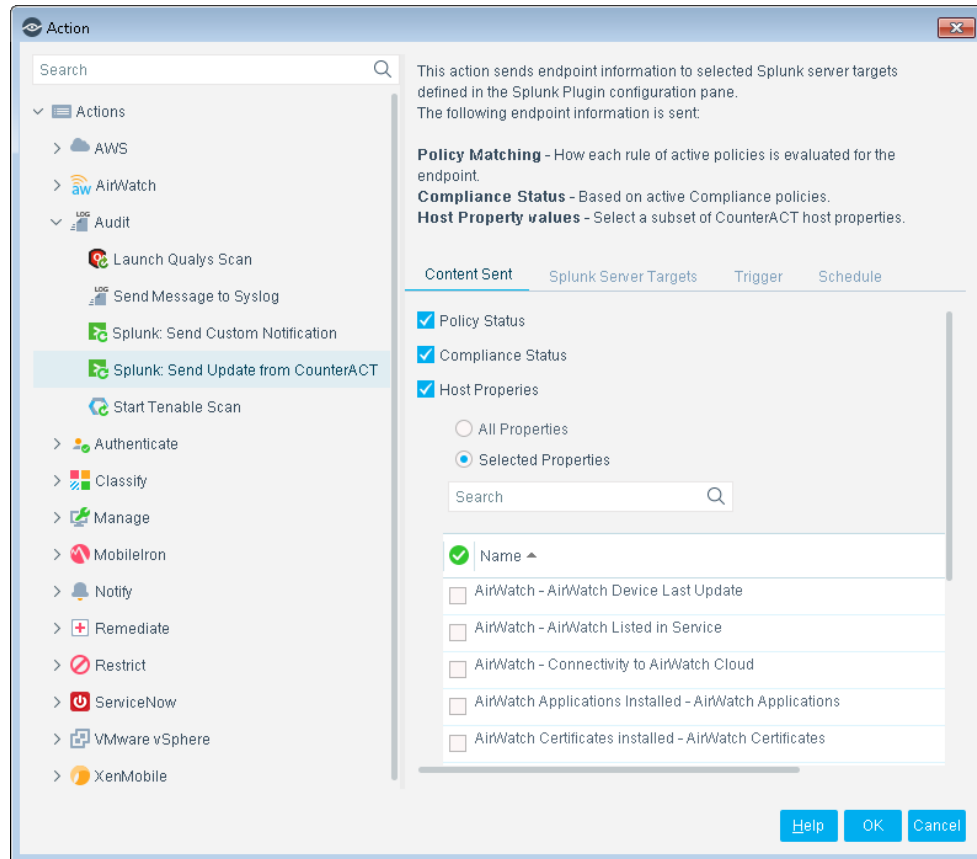
1. Select the **Send Using Syslog Messages** and/or the **Send using HTTP POST** options to determine how CounterACT submits the message to Splunk.
2. For each message type you selected, do one of the following:
 - Select the **Send to All...** option to send the message to all Splunk Enterprise server targets defined in CounterACT.
 - Select the **Send to Selected...** option to send the message to a subset of Splunk Enterprise server targets defined in CounterACT.
3. Compose the message text. You can use property tags to include endpoint-specific or user-specific values in this field. See the *CounterACT Administration Guide* for details.
4. Use the options of the Schedule tab to specify when the action is applied, to delay application of the action, or to specify repeat application of the action.

Splunk: Send Update from CounterACT Action

When sending update messages from the ForeScout Splunk Module to the Splunk Enterprise server, the update messages contains the IP Address, MAC Address, NetBIOS Host, NetBIOS Domain and Username. If none of these parameters are available, the fields are removed from the update message. If, for a given device, one or more of these attributes cannot be resolved, then the update messages will contain only the ones that have been successfully resolved.

This action submits endpoint data to Splunk. This action is the primary method used for transmitting data from CounterACT to Splunk.

Typically action and policy schedule settings are configured to regularly update Splunk with data for all endpoints detected by CounterACT. For example, see the [Send Endpoint and Policy Details to Splunk](#) policy template provided with the module.



Content Sent Tab

Specify the data that is included in the message sent to Splunk.

- Select the **Policy Status** option to include the most recent results of policy-based evaluation of the endpoint. CounterACT reports whether the endpoint matches each rule of all active policies.
- Select the **Compliance Status** option to include the aggregate Compliance status of the endpoint, based on the Compliance properties.
- Select the **Host Properties** option to include host property values for the endpoint. Do one of the following:

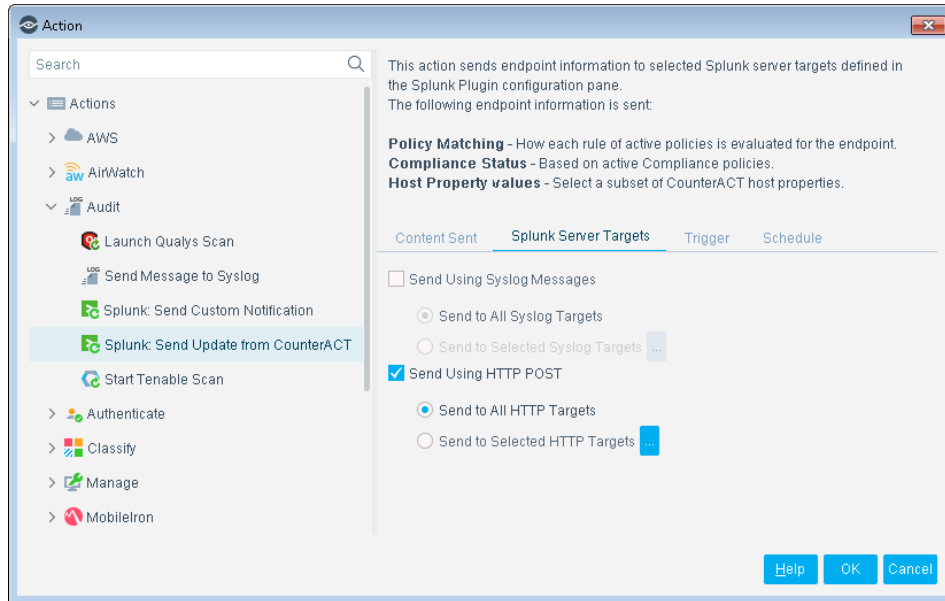
Select the **All Properties** option to include all host property values.

Select the **Selected Properties** option and select properties you want to include. Use the Search field to quickly locate properties.

By default, the Field: label is the internal property tag of each property. You can configure the module to use the full name of each property as the Field: label. See [Configure the Module](#).

Splunk Server Target Tab

Select the **Send Using Syslog Messages** and/or the **Send using HTTP POST** options to determine how CounterACT submits the message to Splunk.

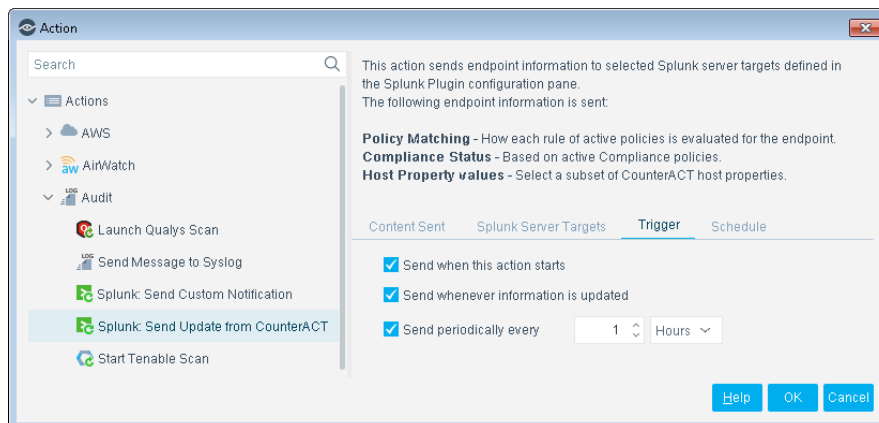


For each message type you selected, do one of the following:

- Select the **Send to All...** option to send the message to all Splunk Enterprise server targets defined in CounterACT.
- Select the **Send to Selected...** option to send the message to a subset of Splunk Enterprise server targets defined in CounterACT.

Trigger Tab

Specify one or more triggers that send the specified information to Splunk.



- Select the **Send when this action starts** option to send a message when the endpoint matches the conditions of a policy rule that invokes this action.

- Select the **Send whenever information is updated** option to send a message when the specified information changes. For example, if a previously compliant endpoint no longer satisfies Compliance policies, the message is sent.
- Select the **Send periodically** option to repeatedly send the message at the time interval you specify, with updated information. Messages are sent periodically as long as the endpoint satisfies the conditions of the policy rule that invokes this action.

Schedule Tab

Use the options of the Schedule tab to specify when the action is applied, to delay application of the action, or to specify repeat application of the action.


Using the Splunk Module

Once the Splunk Module and the ForeScout App for Splunk has been configured, you can view and manage the devices from Asset Inventory view in the CounterACT Console. This provides activity information, accurate at the time of the poll, on endpoints based on certain instances' properties. The Asset Inventory lets you:

- Complement a device-specific view of the organizational network with an activity-specific view
- View endpoints that were detected with specific attributes
- Incorporate inventory detections into policies

To access the inventory:

1. Log in to the CounterACT Console and select the **Asset Inventory** tab.
2. In the Views pane, expand the **Splunk** folder.

 *If you did not configure to show the property in the Asset Inventory tab, your Splunk properties will not display in the Views pane of the Asset Inventory tab.*

3. In the left pane, select the **Splunk** icon to expand it and then select any of the items in the list to view its properties.
4. Check that the properties match the configuration requirements.

To access the Home tab:

1. In the CounterACT Console, select the **Home** tab.
2. In the Views tree, expand **Policies** and then select **Splunk**.
3. Select an item in the Detections pane. The Profile, Compliance and All policies tabs display the information related to the selected host.

Refer to *Working on the Console>Working with Inventory Detections* in the *CounterACT Administration Guide* or the Console Online Help for information about working with the CounterACT Inventory.

Run Splunk Audit Actions

There are two types of Audit actions that can be sent from the CounterACT Console:

- [Send Custom Notification to Splunk Enterprise Server Targets](#)
- [Send Update from CounterACT](#)

Send Custom Notification to Splunk Enterprise Server Targets

Use this action to send a text message to one or more Splunk Enterprise servers. This message can include varied information, such as:

- Standard event or error strings that are reported by other components of your security environment.
- Information not included in regular updates of host property and policy information that CounterACT sends to Splunk. For example: add this action to policies that apply or remove the **Switch Block** action to track port blocking in Splunk.

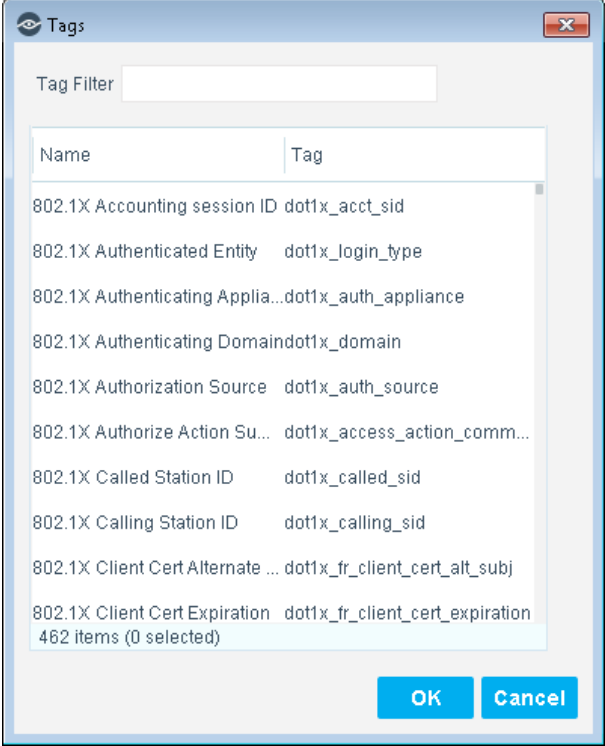
To send a customized notification to Splunk Enterprise server targets:

1. In the CounterACT Console, Home tab, right-click on an **IP address**.
2. Select **Audit** and then select **Splunk: Send Custom Notification**.
3. The Specify Splunk: Send Custom Notification parameters dialog box opens to the Splunk Server Targets tab.

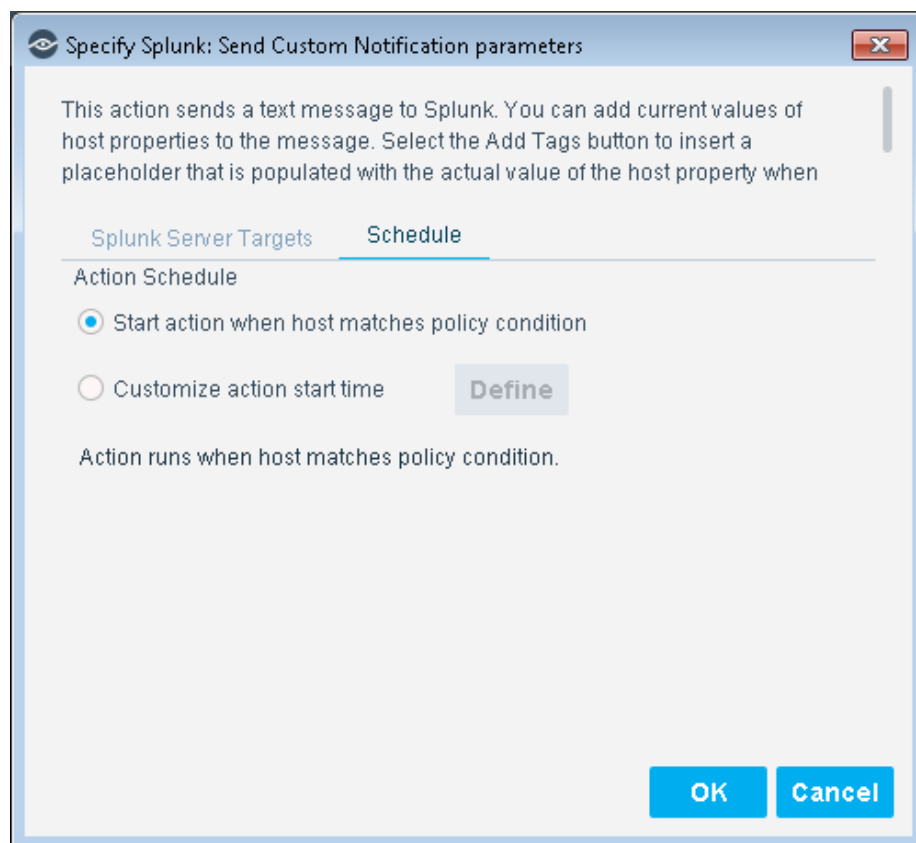
This action sends a text message to Splunk. You can add current values of host properties to the message. Select the **Add Tags** button to insert a placeholder that is populated with the actual value of the host property when the message is generated. See [Configure the Module](#) to define Splunk Enterprise server targets in the Splunk Module configuration pane.

In the Splunk Server Targets tab, enter your configurations.

Send Using Syslog Messages	<ul style="list-style-type: none"> ▪ Send to All Syslog Targets - Select the checkbox to send a notification to all Splunk Syslog targets. These are all targets that display in the Splunk Syslog Targets tab of the Splunk configuration pane. ▪ Send to Selected Syslog Targets - Select the checkbox and then select More. A dialog box opens. Select the target(s) and then select OK.
-----------------------------------	---

Send Using HTTP POST	<ul style="list-style-type: none"> ▪ Send to All HTTP Targets (default) - Select the checkbox to send a notification to all Splunk HTTP targets. These are all targets that display in the Splunk HTTP Targets tab of the Splunk configuration pane. ▪ Send to Selected HTTP Targets - Select the checkbox and then select More. A dialog box opens. Select the target(s) and then select OK.
Notification Text	<p>Compose the message text. You can use property tags to include endpoint-specific or user-specific values in this field. See the <i>CounterACT Administration Guide</i> for details.</p> <ul style="list-style-type: none"> ▪ Select Add Tags. The Tags dialog box opens.  <ul style="list-style-type: none"> ▪ Hold the Ctrl key down and select the tags for the notification text and then select OK. ▪ The Notification Text field populates with the selected tags.

4. Select the **Schedule** tab to specify when the action is applied, to delay application of the action, or to specify repeat application of the action.



- a. Accept the default of **Start action when host matches policy condition**. This option sends an update message immediately upon discovering a specific policy criterion.
- b. Alternately, select **Customize action start time** or select the **Define** button. The Action Scheduler dialog box opens.

Action Scheduler

Start

☒ Immediately (on policy match)

☐ Wait for Seconds

☐ On ... at

Activity pattern

☒ Constantly

☐ Scheduled

Duration

☒ No end date

☐ End after Seconds

☐ End on ... at

5. Use the options of the Action Scheduler tab to specify when the action is applied, to delay application of the action, or to specify repeat application of the action.
6. When finished, select **OK**.
7. Select **OK** in the Specify Splunk: Sent Custom Notification parameters dialog box.
8. In the CounterACT Console, Home tab, an icon displays in the Action column. This represents the active Custom Notification to Splunk Enterprise server.

Send Update from CounterACT

This action sends endpoint information to selected Splunk Enterprise server targets defined in the Splunk Module configuration pane.

The following endpoint information is sent:

- **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.

To send an update to CounterACT:

1. In the CounterACT Console, Home tab, right-click on an **IP address**.
2. Select **Audit** and then select **Splunk: Send Update from CounterACT**.
3. The Specify Splunk: Send Update from CounterACT parameters dialog box opens to the Content Sent tab.

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

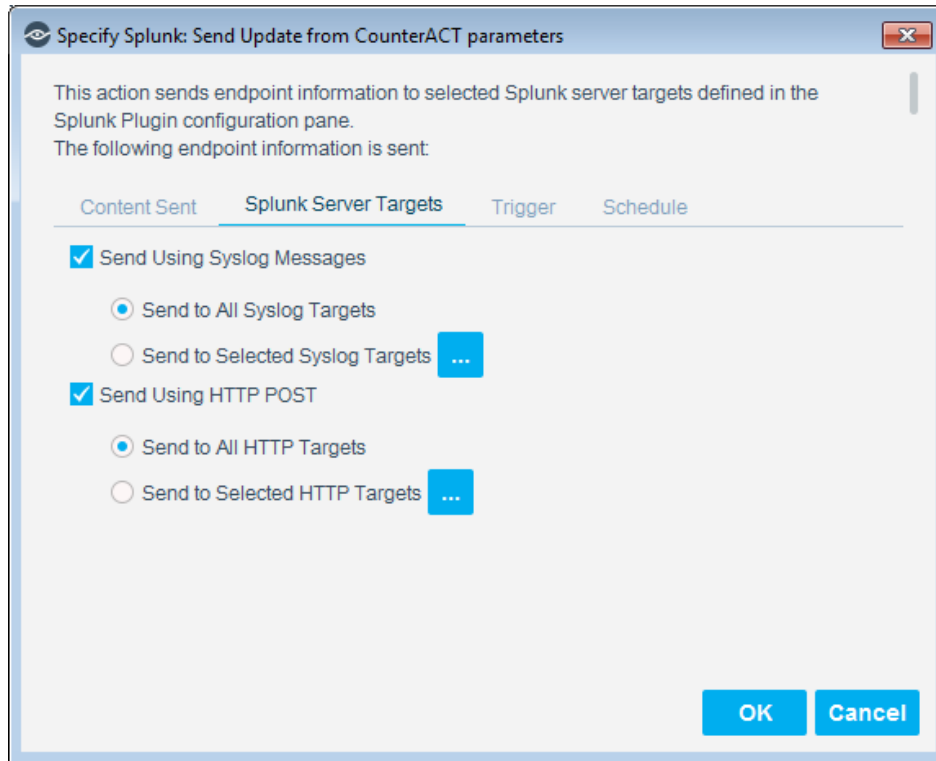
Select All
Clear All

OK Cancel

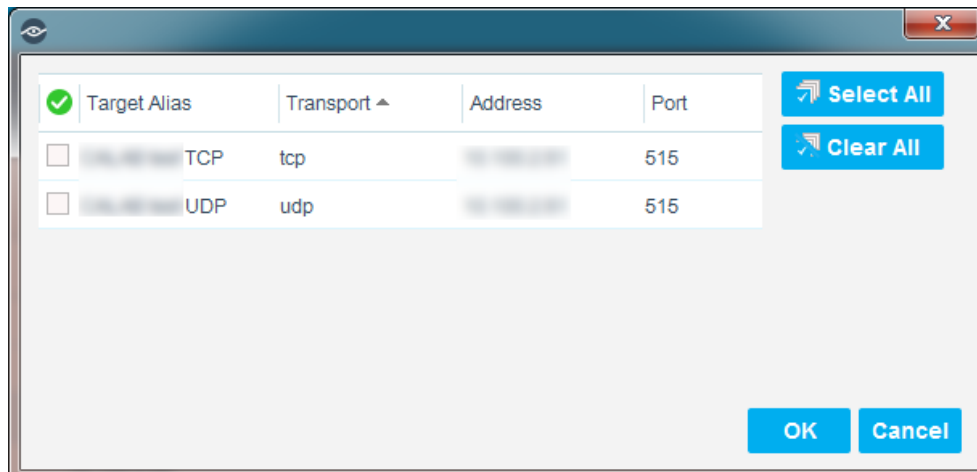
4. You can use the default settings and simply select specific boxes in the Host Properties Name field or you can use the Select All button.
5. Alternately, set your own customized settings.
6. Select the **Splunk Server Targets** tab.

Send Using Syslog Messages


- a. Select the Splunk Server Targets tab.
- b. Select **Send Using Syslog Messages** if you want to send an update using Syslog messaging.



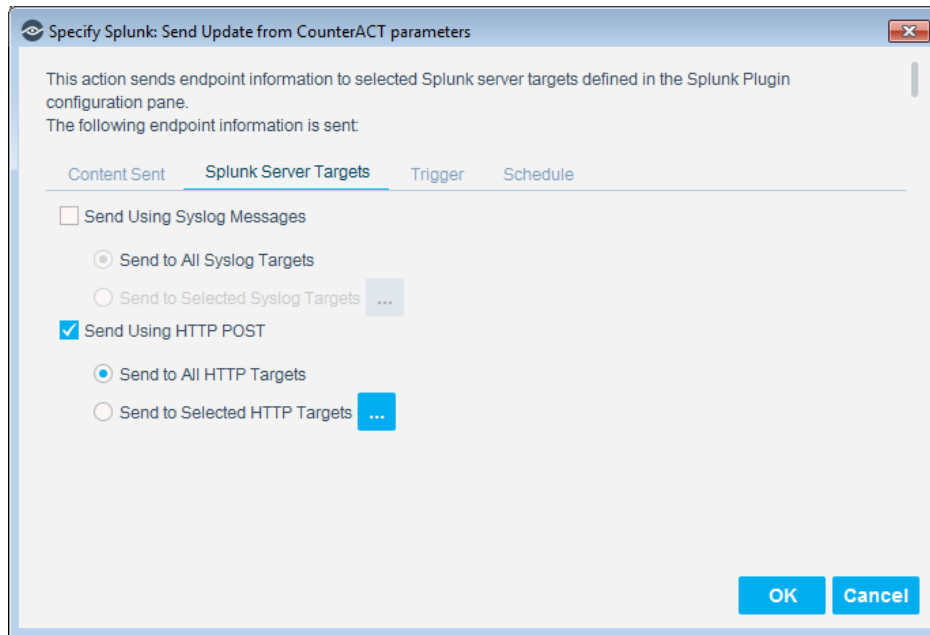
- c. Accept the default of **Send to All Syslog Targets**. This option sends the message to all Splunk Enterprise server targets defined in CounterACT.
- d. Alternately, select **Send to Selected Syslog Targets**. The targets dialog box opens.



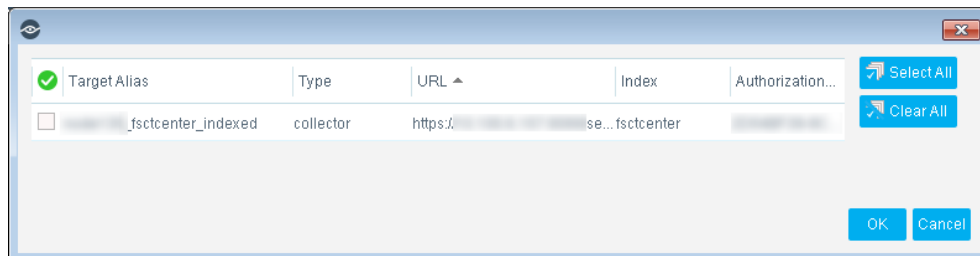
- e. This option sends an update message to a subset of Splunk Enterprise server targets defined in CounterACT. Select one or more addresses and then select **OK**.

 For details on configuring two or more HTTP channels with the same URL, see [Support for Multiple Channels for each Splunk Target](#)

Send Using HTTP POST



- a. Select the **Splunk Server Targets** tab.
- b. You can accept the default of **Send Using HTTP POST** to all HTTP Targets.
- c. Alternately, you can select **Send to Selected HTTP Targets**. The targets dialog box opens.

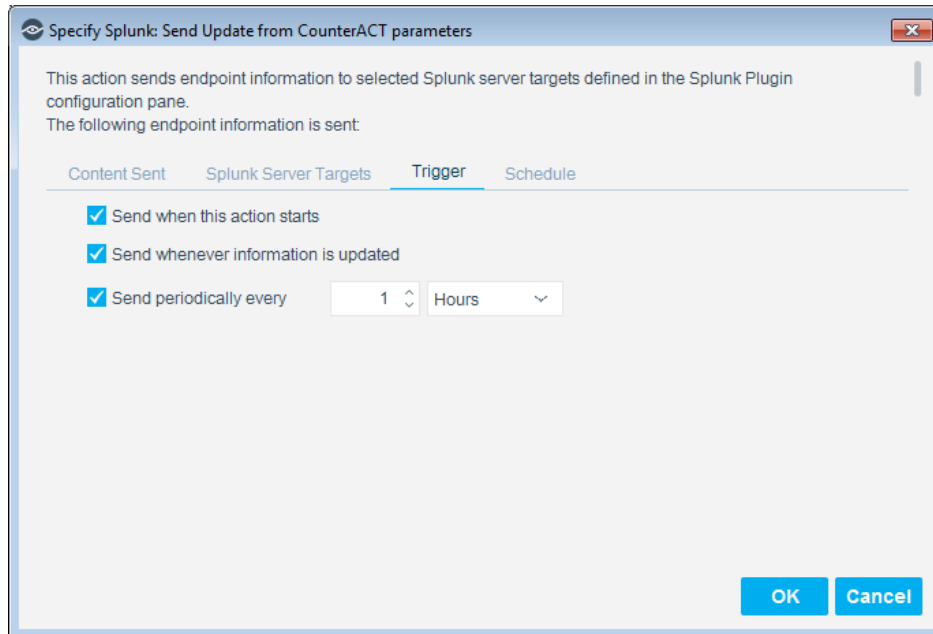


- d. This option sends an update message to a subset of Splunk HTTP targets defined in CounterACT. Select one or more URLs and then select **OK**.

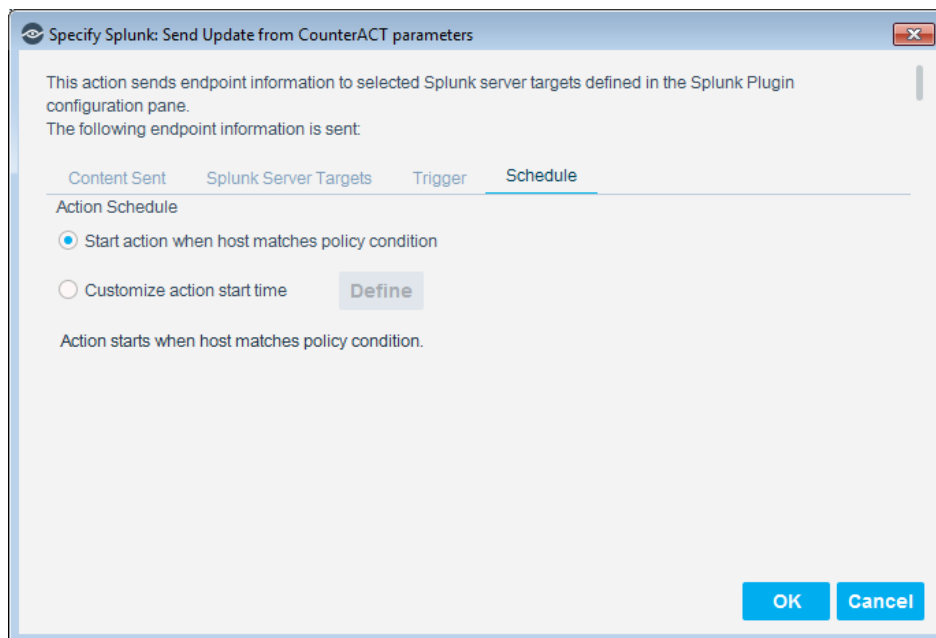
For details on configuring two or more HTTP channels with the same URL, see [Support for Multiple Channels for each Splunk Target](#).

In version 2.5.0, if the user configured a new HTTP destination with the same URL as that configured in one of the existing HTTP destinations, then the Splunk Module would raise an error and prevent the user from configuring that HTTP destination. In version 2.8, the user can now configure two HTTP targets with same URLs as long as either the Index or the Authorization Token fields are different.

7. In the Specify Splunk: Send Update from CounterACT parameters dialog box, select the **Trigger** tab.



- a. Select the **Send when this action starts** option to send an update message when the endpoint matches the conditions of a policy rule that invokes this action.
 - b. Select the **Send whenever information is updated** option to send an update message when the specified information changes. For example, if a previously compliant endpoint no longer satisfies Compliance policies, the update message is sent.
 - c. Select the **Send periodically** option to repeatedly send the update message at the time interval you specify. This is a good option if you want regular updates with updated information provided. Update messages are sent periodically as long as the endpoint satisfies the conditions of the policy rule that invokes this action.
8. Select the **Schedule** tab.



9. Accept the default of **Start action when host matches policy condition**. This option sends an update message immediately upon discovering a specific policy criterion.
10. Alternately, select **Customize action start time** or select the **Define** button. The Action Scheduler dialog box opens.

Action Scheduler

Start

☒ Immediately (on policy match)

☐ Wait for Seconds

☐ On at

Activity pattern

☒ Constantly

☐ Scheduled **Define**

Duration

☒ No end date

☐ End after Seconds

☐ End on at

Help OK Cancel

11. Use the options of the Action Scheduler tab to specify when the action is applied, to delay application of the action, or to specify repeat application of the action.
12. When finished, select **OK**.
13. In the Specify Splunk: Send Custom Notification parameters dialog box, select **OK**.
14. In the CounterACT Console, Home tab, hover the mouse over the green icon in the Action field of the selected IP address. The Send Update from CounterACT information displays.

Function	Network Function	Actions
Splunk: Send Update from CounterACT Action triggered by: CounterACT operator Action Status: Success - Action performed; Success		
Press 'F2' for focus		

Best Practices

This section covers the best practices for using the Splunk Extended Module.

CounterACT-to-Splunk Logging

A best practice for logging to Splunk from CounterACT is to use the Event Collector. The Event Collector is a token-based, encrypted HTTP messaging service. See [Define a new Event Collector](#).

Splunk to CounterACT Messaging

Splunk messaging to CounterACT must be sent to the Enterprise Manager (EM). The EM then determines which appliance needs the message and disseminates. It is best practice to use both an EM, a Recovery Enterprise Manager (REM), and have a load balancer sent to the REM when the EM is down.

Splunk Actions on CounterACT

Splunk can automate actions on CounterACT and allow the Splunk Administrator to take manual actions. Automatic actions are based on Splunk-driven use case, while manual actions can be taken on any host-based on non-automated use cases. Actions on CounterACT can control actions such as *VLAN changes*, *Apply ACL on Endpoint* as well as any other action available on the CounterACT implementation.

What data is sent to Splunk?

Best practice is to deploy a policy with the *Splunk Send Updates from CounterACT* action. This action by default sends all Policy Statuses, Compliance Statuses and Host Properties to Splunk.

It is also recommended to fine tune policies to reduce the number of properties and reduce duplicate properties, for example, the MAC address can be sent in various formats.

Appendix A: Default Communication Settings


The following table lists default settings for the communication between Splunk and CounterACT.

Name	Direction	Protocol	Port	To customize
REST	To Splunk	HTTPS	8089	Enter custom port/URL in the POST to URL field when you Configure the Module .
Event Collector	To Splunk	HTTPS	8088	
Syslog	To Splunk	TCP/UDP	515	<ol style="list-style-type: none"> 1. In Splunk: clone the Data Input, and customize port. 2. In CounterACT: customize Port and TCP/UDP fields when you Configure the Module.

Name	Direction	Protocol	Port	To customize
Alert API	To CounterACT	HTTP	80	In Splunk: edit the URL of the built in alerts.

Appendix B - Splunk Cloud Deployments

This section covers information relating to Splunk Cloud.

-  You will need a Splunk Cloud license for how much data you are allowed to retain in the Splunk Cloud. This is used for indexing your daily data retention. For more information, see [Indexing Requirements for Splunk Cloud Instance](#).

Splunk Cloud vs Splunk Enterprise

There are a few differences between Splunk Cloud and Splunk Enterprise.

Splunk Cloud	Splunk Enterprise
Security – The security of the cloud deployment is managed and controlled by the Splunk Cloud team. There are more layers of security with Splunk Cloud.	Security – Access and security of your Splunk deployment is locally managed and maintained by each customer.
CLI access - There is no command line interface (CLI). Many administrative tasks can be performed using the web browser, for example, managing indexes. Other tasks must be performed by Splunk Cloud Support.	CLI access - see the <i>ForeScout App & Add-ons for Splunk How-to Guide</i>
<ul style="list-style-type: none"> ▪ Managed Splunk Cloud - the apps must be installed by Splunk Cloud Support. ▪ Self-Service Splunk Cloud - you can install the apps See Deploying Splunk Cloud .	N/A
TCP and UDP data cannot be sent directly to Splunk Cloud. You must use an on-premises forwarder to send such data. The default port for the forwarder to Splunk Cloud are ports 9997 or 9998; make sure the port on the firewall is open to Splunk Cloud. Refer to Splunk documentation.	Splunk Enterprise allows direct monitoring of TCP and UDP . See Add a Splunk Syslog Target .
HTTP Event Collector (HEC) - For Managed Splunk Cloud deployments, HEC must be enabled by Splunk Support	HTTP Event Collector (HEC) - see Define a new Event Collector .

Deploying Splunk Cloud

This section covers the setup and deployment of Splunk Cloud.

Types of Splunk Clouds

To determine whether your Splunk Cloud deployment is self-service or managed, look at the format of the URL for connecting to Splunk Cloud:

Self-service Splunk Cloud This is purchased directly from the Splunk web site. For installation, see Self-service Splunk Cloud .	https://prd-*.cloud.splunk.com
Managed Splunk Cloud Managed Splunk Cloud means you need to work with Splunk Sales to obtain your Splunk Cloud deployment. For installation, see Managed Splunk Cloud .	https://*.splunkcloud.com

For more information, refer to <https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/User/TypesofSplunkClouddeployment>

Indexing Requirements for Splunk Cloud Instance

As part of your Splunk Cloud Instance, you will need to:

- Determine the maximum size of your data to be held in the Splunk Cloud.
- Determine the maximum age of events (data retention)

New Index [X]

Index Name:

Max Size of Entire Index: GB ▾
Maximum target size of entire index.

Retention (days):

For more information, see: <https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/User/Datapolicies>

Self-service Splunk Cloud

1. In the Splunk home page, browse to the **Apps** page and select the **Browse more apps** button.
2. There are three ForeScout apps that need to be installed:
 - a. ForeScout Technology Add-on for Splunk
 - b. ForeScout App for Splunk
 - c. ForeScout Adaptive Response Add-on for Splunk
3. Select each ForeScout app and then select the **Install** button.

REST API

For self-service deployment, Splunk Support uses a dedicated user and sends you credentials that enable you to access the REST API.

 *You cannot use SAML authentication with REST API.*


1. You will need to get the deployment name and credentials from Splunk Cloud Support.
2. Open the port 8089 **on the firewall** from the CounterACT appliance to Splunk Cloud.
3. To access REST API, use this URL:
`https://input-<deployment-name>.cloud.splunk.com:8089`

HTTP Event Collector

Define the URL for the HTTP Event Collector

Self-service HTTP Event Collector

For self-service HTTP Event Collector deployment, use the URL to access the Splunk Cloud Instance, for example:

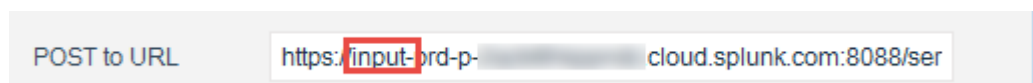


The red square is to be replaced with the unique ID assigned to your deployment, for example:

HEC API Access

 *Make sure that port 8088 **on the firewall** is open from the CounterACT appliance to Splunk Cloud.*

For the HEC API access, you need to add the **input-** as a prefix to the URL.



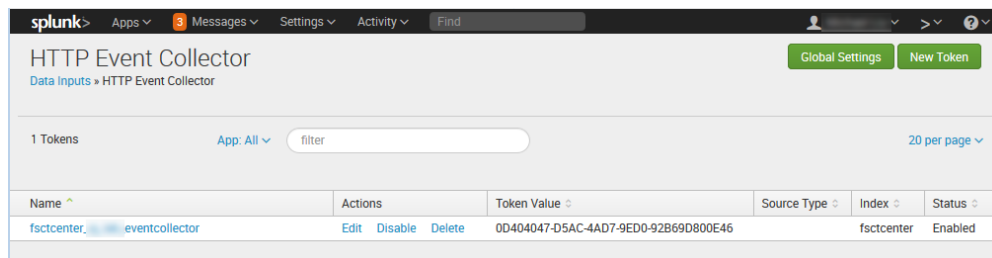
`https://input-prd-p-XXXXXXX.cloud.splunk.com:8088/services/collector`

XXXXXX = the unique ID for the Splunk Cloud Instance.

Create HTTP Event Collector as a Data Input

Next create a HTTP Event Collector data input on the Splunk Web UI.

1. Select **Settings**, and then select **Data Inputs**.
2. The Data inputs page displays. In the HTTP Event Collector row, select **Add new**.
3. Enter the information into the Add Data section. This will create a token. Save this token.



Create Splunk HTTP Target in the Splunk Extended Module

1. Go to the Splunk Extended Module, select **Options**, select **Splunk** and then select the **Splunk HTTP Targets** tab.
2. Select **Add**.
3. In the POST to URL field, paste the URL of the Instance with the *input-* prefix.
4. In the Authorization Token field, paste the token value from the Splunk HTTP Event Collector page.

Add Splunk HTTP Target Details - Step 1

Add Splunk HTTP Target Details

General

Specify Splunk HTTP Target Details. Please ensure that each target has a unique set of values in the URL, Index and Authorization Token fields.

Splunk HTTP Type: Event Collector ▼

Target Alias: Splunk_Cloud_2_Event_Collector

POST to URL: https://input-prd-p-...cloud.splunk.com:8088/ser

Index: fsccenter

Comment:

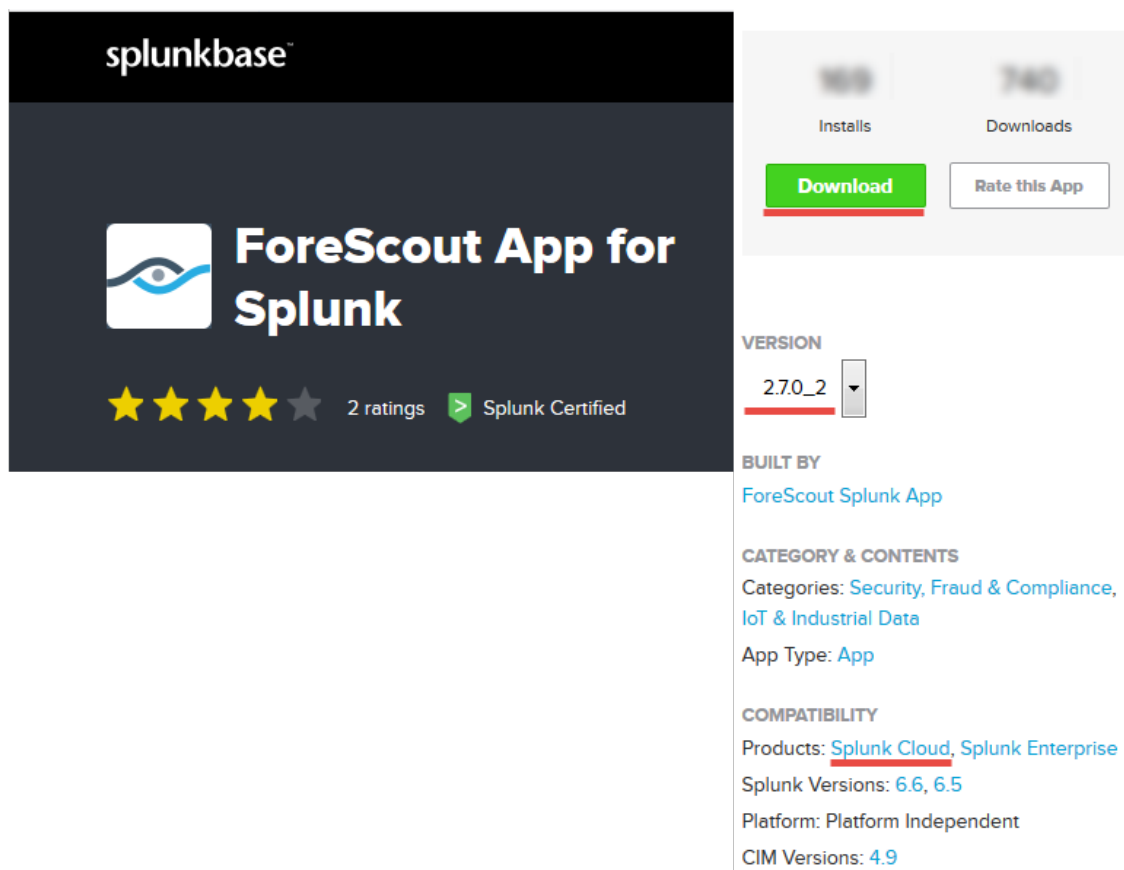
Authorization Token: 0D404047-D5AC-4AD7-9ED0-92B69D800E46

[Help](#) [Previous](#) [Next](#) [Finish](#) [Cancel](#)

5. Finish the Add Splunk HTTP Target wizard. For instructions, see [Event Collector](#).

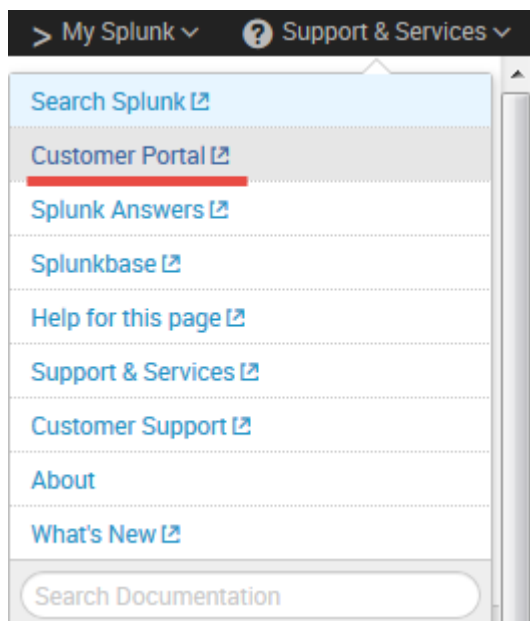
Managed Splunk Cloud

1. On the Splunk App page, select the **Manage Apps** icon in the left pane.
2. The Apps page displays. Select **Browse more apps** button.
3. In the search field, enter *ForeScout* and run the search.
4. Under the ForeScout Apps for Splunk, select the **View on Splunkbase** link.
5. The ForeScout Apps for Splunk installation page displays.
6. Select **2.7.0_2** in the version field and then select **Download**.



The screenshot shows the Splunkbase interface for the 'ForeScout App for Splunk'. The app card on the left features the Splunkbase logo, the app name 'ForeScout App for Splunk', a 4-star rating (2 ratings), and a 'Splunk Certified' badge. To the right, statistics show 159 installs and 740 downloads, with a green 'Download' button and a 'Rate this App' button. Below these, the 'VERSION' is listed as 2.7.0_2. The 'BUILT BY' section identifies the creator as 'ForeScout Splunk App'. The 'CATEGORY & CONTENTS' section lists categories like 'Security, Fraud & Compliance' and 'IoT & Industrial Data', and the app type as 'App'. The 'COMPATIBILITY' section lists supported products ('Splunk Cloud', 'Splunk Enterprise'), Splunk versions ('6.6', '6.5'), platform ('Platform Independent'), and CIM versions ('4.9').

7. Save the files to the local server.
8. In the Splunk home page, select **Support & Services** and then select **Customer Portal**.



- Open a Splunk support ticket requesting installation of the app on your Splunk Cloud deployment.

Submit a Case

Our support contracts offer different response times and case handling based on case priority levels.

- P1 = A Splunk installation is inaccessible or the majority of its functionality is unusable.
- P2 = One or more key features of a Splunk installation are unusable.
- P3 = All configuration issues and any other case where a feature is not operating as documented.
- P4 = All enhancement requests.

Customers with an Enterprise license can select the priority for initial response. When the case is received, We may change the priority based on our own analysis.

Select Entitlement

Select Deployment

Splunk installation is? A Splunk installation is inaccessible or the majority of its functionality is unusable.

Subject Install ForeScout App

What Product are you having trouble with? Splunk Cloud Version Cloud

Add

What OS are you using? Other

What OS Version are you using?

I need help with... Apps

Feature / Component / App Other App

Deployment Type Splunk Cloud

What is the impact...

Problem Description

- Make the selections according to the screen image above.

- Submit the ticket.

REST API

For managed deployment, Splunk Support has to have open port 8089 **on the firewall** for REST API access.

You cannot use SAML authentication with REST API.

To access REST API, use this URL:

`https://<deployment-name>.cloud.splunk.com:8089`

HTTP Event Collector

Define the URL for the HTTP Event Collector

Self-service HTTP Event Collector

For self-service HTTP Event Collector deployment, use the URL to access the Splunk Cloud Instance, for example:

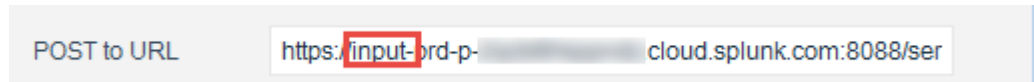
`https://prd-p- .cloud.splunk.com/en-US/manager/launcher/http-eventcollector`

The red square is to be replaced with the unique ID assigned to your deployment, for example:

HEC API Access

- Make sure that port 8088 **on the firewall** is open from the CounterACT appliance to Splunk Cloud.

For the HEC API access, you need to add the **input-** as a prefix to the URL.



`https://input-prd-p-XXXXXXXX.cloud.splunk.com:8088/services/collector`

XXXXXXXX = the unique ID for the Splunk Cloud Instance.

Create HTTP Event Collector as a Data Input

You will need to create a Splunk Support ticket to request HTTP event collection to be enabled. You will need to provide the following information to Splunk Support:

- Name for data input
- Name for target index
- Source type to be applied to the data
- Amount of data per day that you expect to receive, and any details about your intended usage that will help Splunk Support estimate the number of HTTP connections per hour

Splunk Support will provide you with the Authorization Token required for sending HTTP events to Splunk Cloud.

For more information, see

<https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/User/AdddatausingHTTPeventcollector>

Set up Secure Connection Messaging from Splunk Module to the Splunk Cloud

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

To enable HTTPS communication:

- Open port 443 on the firewall** from the Splunk Cloud to the CounterACT Enterprise Manager or the stand-alone CounterACT appliance.
- In CounterACT, operators must use the 'fstool cert' utility to create a Certificate Signing Request (CSR) using the following steps:
 - Use 'fstool cert gen' to generate the certificate request.
 - Answer the questions required for certificate generating. Below is an example.

- 📄 To create the server-side certificate, test.forescout.com was used as the FQDN in the DNS name of the Enterprise Manager field. The FQDN used by CounterACT needs to be recognized by Splunk Cloud.

```
[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'.
3. Get the CSR signed by a trusted Certificate Authority (for example, VeriSign).
4. Once the certificates are installed on the CounterACT appliance using **`fstool cert import`** CLI and confirmed by **`fstool cert test`** CLI.
5. Open a Splunk Support ticket and request that the CounterACT Public Key Certificate is appended to the cacert.pem file at the following location:
`$SPLUNK_HOME/lib/python2.7/site-packages/requests/cacert.pem`

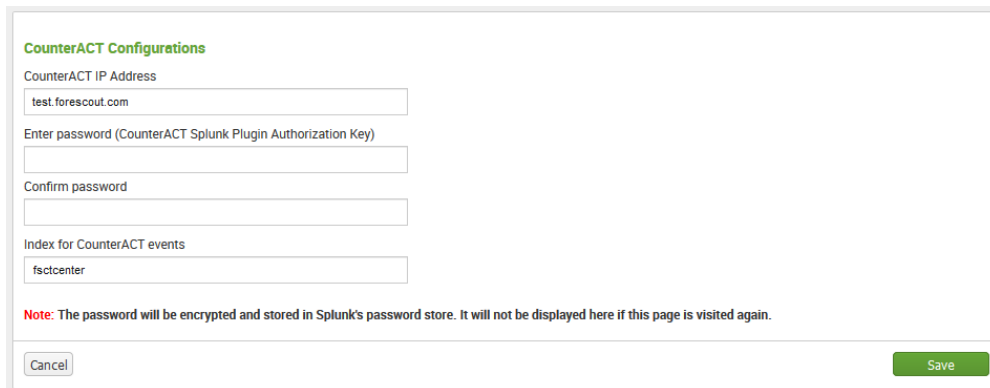
- 📄 **This step is very important, if you do not open a support ticket, the Adaptive Response alerts will not work.**

Set up and Configure the ForeScout Technology Add-on for Splunk Cloud

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 Cloud:

1. **Login** to the Splunk Cloud Instance.
2. 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
test.forescout.com


Enter password (CounterACT Splunk Plugin Authorization Key)

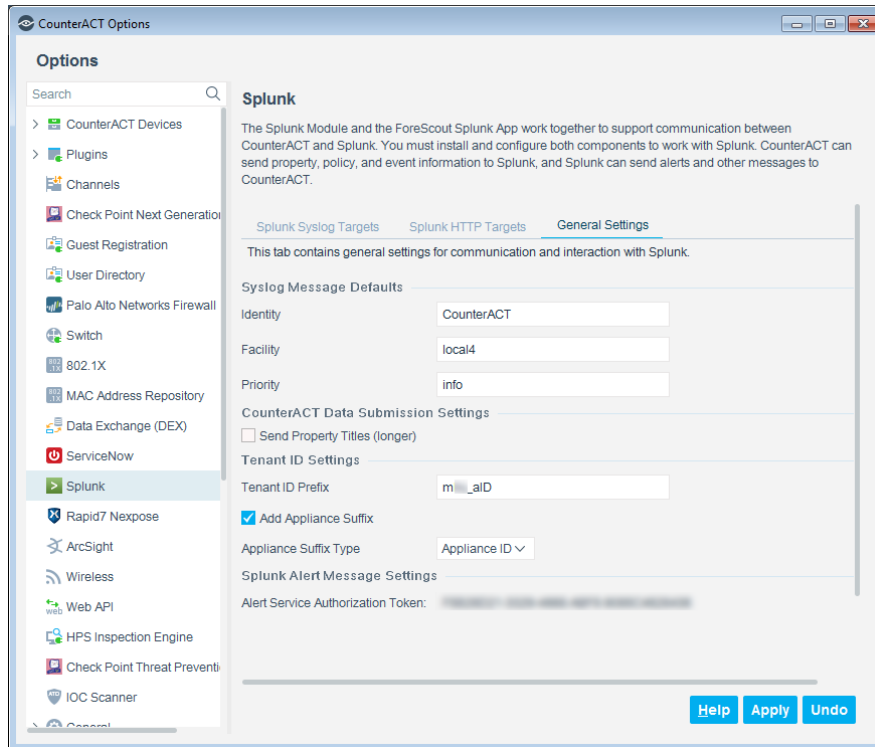
Confirm password

Index for CounterACT events
fctcenter

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.

Cancel Save

3. In the CounterACT IP Address or Hostname field, enter the **FQDN** of the CounterACT Enterprise Manager or standalone CounterACT appliance of 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.*
4. 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.



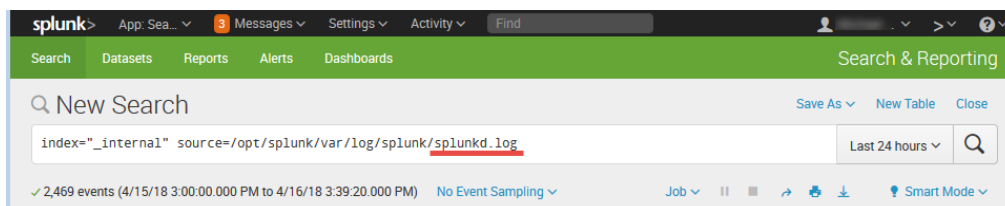
5. Select **Save**.
6. In Splunk Instance, select Settings and then select Server controls.
7. Select **Restart Splunk**.

Accessing Logs within Splunk Cloud Instance

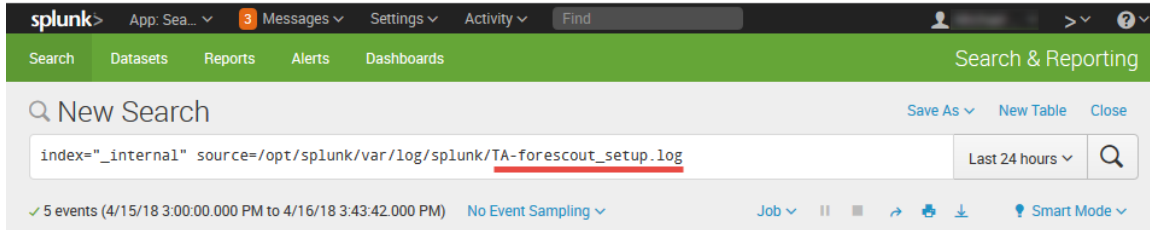
Because CLI is not provided on the Splunk Cloud, you will need to access your logs via the search function.

Below are example searches for:

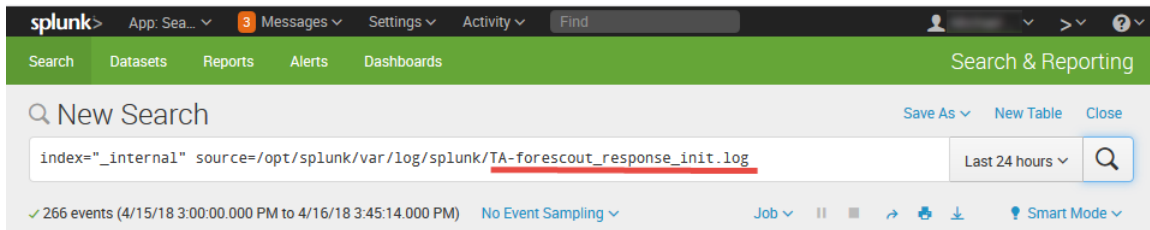
- Splunkd log
- TA-forescout_setup log
- TA-forescout_response_init log



Splunkd log



TA-forescout_setup log



TA-forescout_response_init log

Appendix C: 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

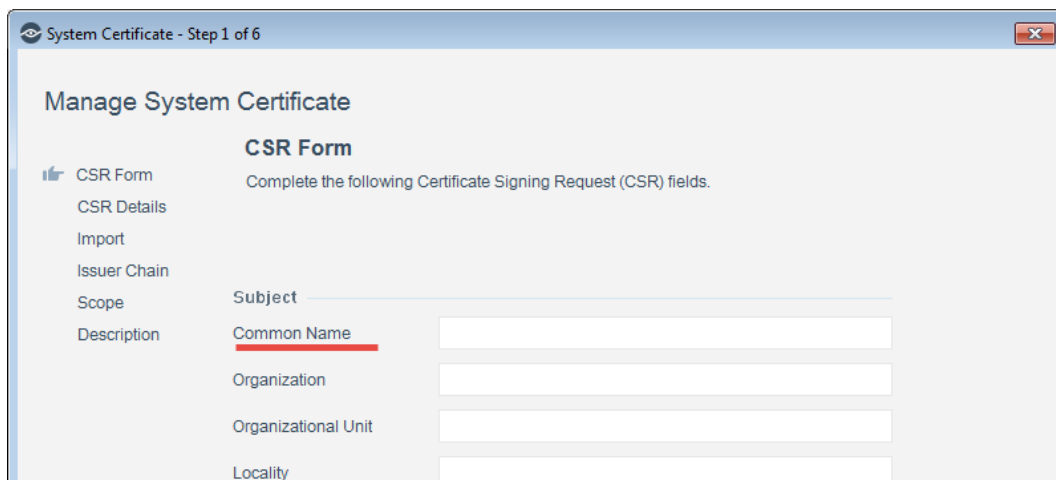
For information on how to install the system certificate for the CounterACT Enterprise Manager, refer to the CounterACT Administration Guide.

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**.



System Certificate - Step 1 of 6

Manage System Certificate

CSR Form
Complete the following Certificate Signing Request (CSR) fields.

CSR Details

Import

Issuer Chain

Scope

Description

Subject

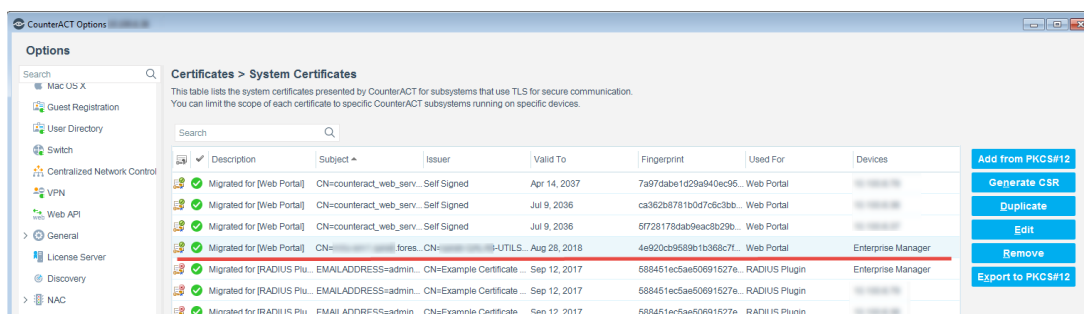
Common Name

Organization

Organizational Unit

Locality

- 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.



Options

Certificates > System Certificates

This table lists the system certificates presented by CounterACT for subsystems that use TLS for secure communication. You can limit the scope of each certificate to specific CounterACT subsystems running on specific devices.

Description	Subject	Issuer	Valid To	Fingerprint	Used For	Devices
Migrated for [Web Portal]	CN=counteract_web_serv...	Self Signed	Apr 14, 2037	7a97dabe1d29a940ec95...	Web Portal	
Migrated for [Web Portal]	CN=counteract_web_serv...	Self Signed	Jul 9, 2036	ca362b8781bd07c5c3bb...	Web Portal	
Migrated for [Web Portal]	CN=counteract_web_serv...	Self Signed	Jul 9, 2036	5f728178dab9eac2b29b...	Web Portal	
Migrated for [Web Portal]	CN=fore...-CN=fore...-CN=fore...-CN=fore...-CN=fore...	Self Signed	Aug 28, 2018	4e920cd9589b1b368c7f...	Web Portal	Enterprise Manager
Migrated for [RADIUS Plu...]	EMAILADDRESS=admin... CN=Example Certificate	Self Signed	Sep 12, 2017	588451ec5ae50691527e...	RADIUS Plugin	Enterprise Manager
Migrated for [RADIUS Plu...]	EMAILADDRESS=admin... CN=Example Certificate	Self Signed	Sep 12, 2017	588451ec5ae50691527e...	RADIUS Plugin	
Migrated for [RADIUS Plu...]	EMAILADDRESS=admin... CN=Example Certificate	Self Signed	Sep 12, 2017	588451ec5ae50691527e...	RADIUS Plugin	

Buttons: Add from PKCS#12, Generate CSR, Duplicate, Edit, Remove, Export to PKCS#12

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

System Certificate

Certificate Details | Issuer Chain | Scope | CSR Details

Certificate Details

Select the checkbox to enable CounterACT to present this system certificate for the defined scope.
Select Import to replace the system certificate for the defined scope.

Description: Migrated for [Web Portal] ☒ Enable presenting this certificate **Import**

Fingerprint: 4e920cb9589b1b368c7fa7e8e7961115237733d4

Subject: CN=r[redacted]forescout.com, OU=QA, O=forescout, L=San Jose, ST=CA, C

SAN:

Issuer: CN=[redacted]-UTILSRV-CA, DC=[redacted], DC=forescout, DC=com

Valid From: Mon Aug 28 14:45:43 PDT 2017

Valid To: Tue Aug 28 14:55:43 PDT 2018

Key Size: 2048

Key Algorithm: RSA

Signature Algorithm: SHA256WITHRSA

Certificate:

```
Version: V3
Subject: CN=[redacted]forescout.com, OU=QA, O=forescout, L=San Jose, ST=CA, C
Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

Key: RSA Public Key
modulus: [redacted]
public exponent: 10001

Validity: [From: Mon Aug 28 14:45:43 PDT 2017,
To: Tue Aug 28 14:55:43 PDT 2018]
Issuer: CN=[redacted]-CA, DC=[redacted] DC=forescout, DC=com
SerialNumber: [ 73ac8e5b 00010000 0038]

Certificate Extensions: 5
[1]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=[redacted]
AuthorityInfoAccess [
```

Help OK Cancel

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

Additional CounterACT Documentation


For information about other CounterACT features and modules, refer to the following resources:

- [Documentation Downloads](#)
- [Documentation Portal](#)
- [CounterACT Help Tools](#)

Documentation Downloads

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** - [Product Updates Portal](#)
- **Centralized Licensing Mode** - [Customer Portal](#)

 Software downloads are also available from these portals.

To learn which licensing mode your deployment is using, see [Identifying Your Licensing Mode in the Console](#).

Product Updates Portal

The Product Updates Portal provides links to CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

1. Go to <https://updates.forescout.com/support/index.php?url=counteract>.
2. Select the CounterACT version you want to discover.

Customer Portal


The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:

1. Go to <https://forescout.force.com/support/>.
2. Select **Downloads** or **Documentation**.

Documentation Portal

The ForeScout Documentation Portal is a searchable, web-based library containing information about CounterACT tools, features, functionality and integrations.

 If your deployment is using Centralized Licensing Mode, you may not have credentials to access this portal.

To access the Documentation Portal:

1. Go to www.forescout.com/docportal.
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

CounterACT Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons

Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with.

CounterACT Administration Guide

Select **CounterACT Help** from the **Help** menu.

Plugin Help Files

1. After the plugin is installed, select **Options** from the **Tools** menu and then select **Modules**.
2. Select the plugin and then select **Help**.

Documentation Portal

Select **Documentation Portal** from the **Help** menu.

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options** > **Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.

Options		
<div>Search</div> <div> <div>VPN</div> <div>General</div> <div>Discovery</div> <div>NAC</div> <div>Licenses</div> <div>Lists</div> <div>Map</div> <div>Internal Network</div> </div>		
Licenses		
<div>Activate, update or deactivate your license for CounterACT features and Extended Module</div> <div>Search</div>		
Name ▲	Status	Type
ForeScout CounterACT See	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Control	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Resiliency	Valid	Perpetual
ForeScout Extended Module for Check Point Next...	Valid, Capacity exceeded	Perpetual

Contact your ForeScout representative if you have any questions about identifying your licensing mode.

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.

2018-06-22 16:32