ForeScout

ForeScout App for Splunk

How-to Guide

Version 2.0.0

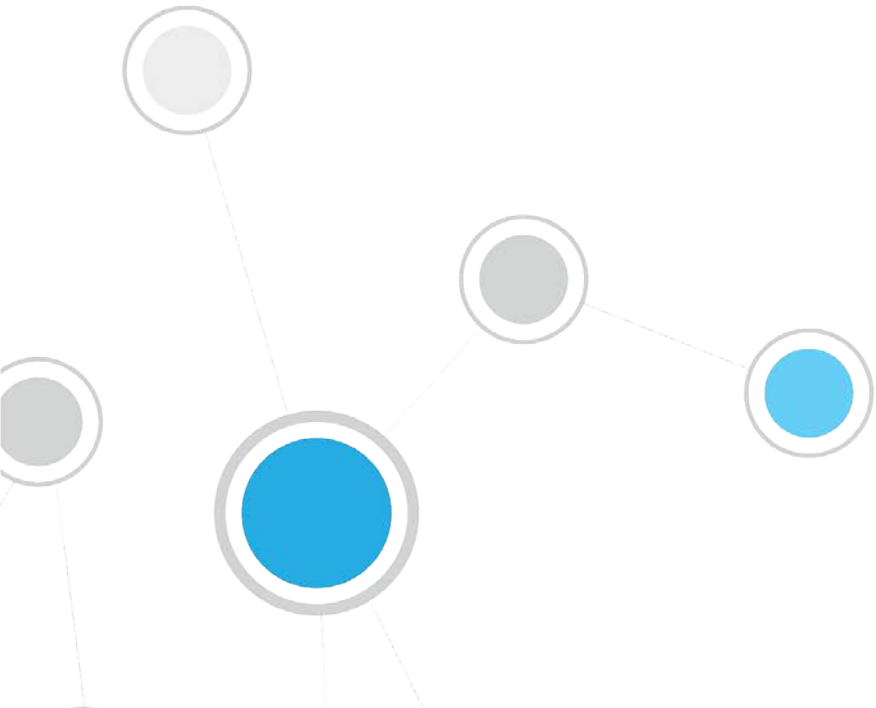


Table of Contents

About Splunk Integration

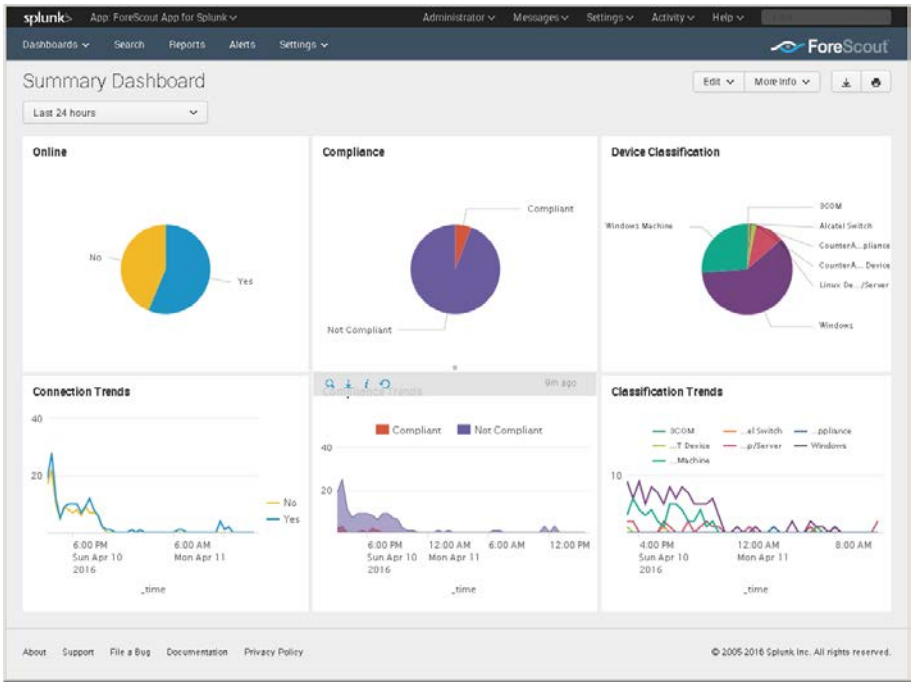
Splunk Enterprise data analytics help organizations leverage the data that their infrastructure and security tools provide, to understand their security posture, pinpoint and investigate risks, and create alerts and reports.

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

Combining ForeScout dynamic endpoint 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, and respond more quickly to mitigate a range of security issues.

Integration is fully bi-directional – CounterACT sends property, policy, and event information to Splunk, and Splunk sends alerts and notification messages to CounterACT.

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



Use Cases

This section describes important use cases supported by this plugin. To understand how this plugin helps you achieve these goals, see About This App.

- Data Mining and Trend Analysis of CounterACT Data
- Continuous Posture Tracking Based on a Broad Range of CounterACT Data
- Response Actions Triggered by Splunk Data Correlation

Data Mining and Trend Analysis of CounterACT Data

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

Continuous Posture Tracking Based on a Broad Range of CounterACT Data

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

- Endpoint compliance status summaries
- Patterns of network access over time
- Trends in CounterACT policies
- Significant changes in endpoint processes and applications

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

Response Actions Triggered by Splunk Data Correlation

The results of Splunk's intuitive search and reporting tools can generate notification messages which are sent to CounterACT. Based on alert data received from Splunk, CounterACT policies can automatically apply remediation actions, isolate breached systems, or invoke additional management steps such as security scans.

For example, if Splunk determines that a set of endpoints have a material security issue, CounterACT can automatically initiate remediation that targets the specific problem identified by Splunk.

Additional Splunk Documentation

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

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

About This App

This app works with the Splunk Plugin to integrate CounterACT and Splunk so that you can:

- View data from CounterACT in a dedicated, customizable Splunk dashboard. See Working with Dashboards.

- Use Splunk search queries to perform data mining and trend analysis on CounterACT data, and to enrich these searches with data from other information sources. See Working with Searches.

  In CounterACT, define policies that send CounterACT data to Splunk. This data populates the dashboard and is available to Splunk search tools. Refer to the *Splunk Plugin Configuration Guide*.

- Configure Splunk to send alerts to CounterACT based on custom search or report results. Searches can combine data from multiple sources. See Working with Alerts.

  In CounterACT, you can define policies that detect and respond to alerts sent by Splunk. Refer to the *Splunk Plugin Configuration Guide*.

The Splunk Plugin and the ForeScout App for Splunk work together 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 Plugin are used to populate Splunk with CounterACT data. Read this document together with the *Splunk Plugin Configuration Guide*.

Supported Splunk Versions

This release supports Splunk Enterprise version 6.3.x and 6.4.

Before You Begin

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

In the CounterACT Console	On the Splunk Server
1. Review the *Splunk Plugin Configuration Guide* and this *How-to Guide*. **2.** Choose protocol(s) for CounterACT messaging to Splunk. See Configure the App.	
3. Verify that CounterACT requirements are met. **4.** Install the Splunk Plugin.	
	5. Verify that the Splunk server contains a user with the required permissions to work with the ForeScout App. **6.** Download and Install the ForeScout App for Splunk.
Required for configuration: **Enterprise Manager IP** **HTTPS Authorization Token (from Splunk Plugin configuration pane)**	**7.** Configure Splunk Communication with CounterACT

In the CounterACT Console	On the Splunk Server
	8. Configure Splunk to receive messages from CounterACT: - Verify and Configure Data Inputs for Syslog Messaging - Configure Splunk REST API Credentials for CounterACT - Configure a Data Input for Event Collector Messages
9. Configure the Splunk Plugin.	**Required for configuration:** **Splunk Server IP** **Custom Port/Protocol** **REST API Credentials** **Event Collector Authorization Token (from Data Inputs)**
10. Create a CounterACT policy that sends information to Splunk. **11.** Tune the frequency of data reporting based on your network conditions and the volume of data you want to work with in Splunk.	

Download and Install the ForeScout App for Splunk

If a Beta version of this release is installed in your environment, uninstall the Beta release before you install this release.

To download and install the app:

1. Do one of the following:
   - Install the app from Splunkbase at:
     https://splunkbase.splunk.com/app/3130/
   - Download the file **`SplunkforCounterACT.spl`** from Splunkbase, or acquire it from your ForeScout representative. In Splunk, select **Apps>Manage apps>install from file**. Browse to the app package you downloaded, and upload the package to your Splunk instance.

   The ForeScout app appears in your Splunk console homepage view, and is listed under the Apps menu.

Configure the App

Perform the procedures in this section after the Splunk Plugin is installed in CounterACT and the ForeScout App is installed on the Splunk Server. To complete

configuration of some of these connections, you must perform parallel configuration steps in the Splunk plugin.

- When you first install the app, you are prompted to Configure Splunk Communication with CounterACT. These settings allow the app to *send* alert messages to CounterACT.
- You must configure the app to *receive* data from CounterACT. The following protocols can be used by CounterACT to send information to Splunk:
  - Using Syslog messaging. To configure the app, see Verify and Configure Data Inputs for Syslog Messaging.
  - Using one of these HTTP message types:

    HTTPS messages to the Splunk REST API. To configure the app, see Configure Splunk REST API Credentials for CounterACT.

    Splunk Event Collector messages. To configure the app, see Configure a Data Input for Event Collector Messages from CounterACT.

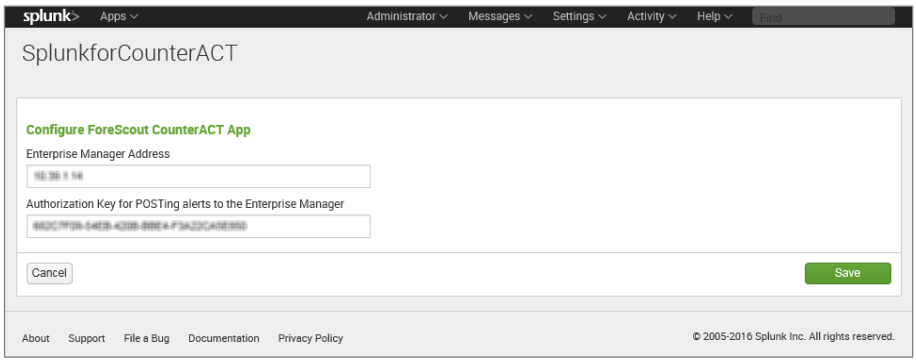
The server targets you define in the Splunk Plugin in CounterACT must use the port, authorization token, and other settings of the data inputs defined on the Splunk server.

Configure Splunk Communication with CounterACT

This procedure lets the ForeScout App for Splunk send alerts to the Splunk Plugin on CounterACT.

To configure Splunk communication with CounterACT:

1. In the Splunk console window, select **Apps>Manage apps.**
2. In the Apps table, find the *ForeScout App*. In the Actions column, select **Set up**. The SplunkforCounterACT page appears.



3. In the **Enterprise Manager Address** field, enter the IP address of the Enterprise Manager or standalone CounterACT Appliance in your environment.
4. In the **Authorization Key** field, enter the string in the **Alert Service Authorization Token** field of the Splunk Plugin configuration pane. Refer to the *Splunk Plugin Configuration Guide* for details.

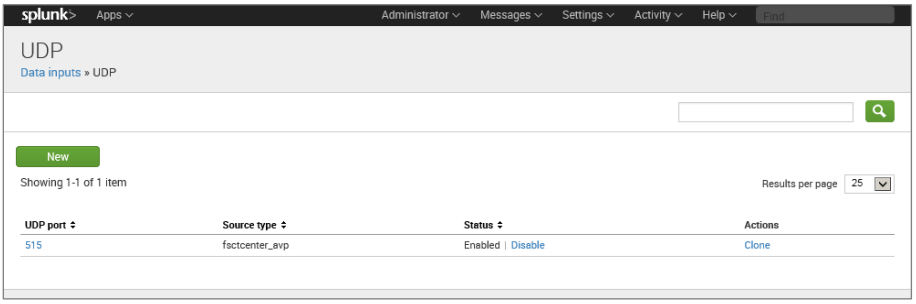
5. Select **Save**.

Verify and Configure Data Inputs for Syslog Messaging

When the ForeScout App is installed it automatically creates data inputs for Syslog messaging from CounterACT. If your implementation uses non-standard ports or other settings, you may need to modify these data inputs.

To verify data inputs:

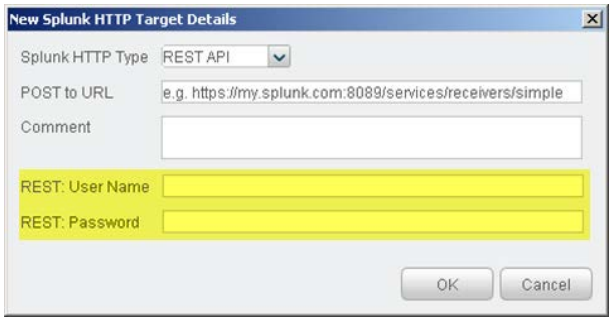
1. In the Splunk console, select **Settings>DATA>Data inputs**. The Data Inputs page appears.
2. In the Local Inputs section, select **TCP** or **UDP** and locate the data input whose *Source type* is **`fsctcenter_avp.`** To support Syslog communication, the app creates TCP and UDP inputs using port 515.
3. To modify this default port, clone the data input and modify the port. Verify that the data input *Status* is **`Enabled`** after modification.



Configure Splunk REST API Credentials for CounterACT

To send CounterACT data to Splunk using the Splunk REST API, CounterACT must have Splunk user account credentials that provide access to the API. Use an existing account, or create an account unique to CounterACT.

Specify this account's credentials when you define the REST API source in the Splunk Plugin. Refer to the *Splunk Plugin Configuration Guide*.



Configure a Data Input for Event Collector Messages from CounterACT

When you use the proprietary Splunk Event Collector format for HTTPS messaging from CounterACT, follow this procedure to create a corresponding Splunk data input.

To create a data input for Event Collector messaging:

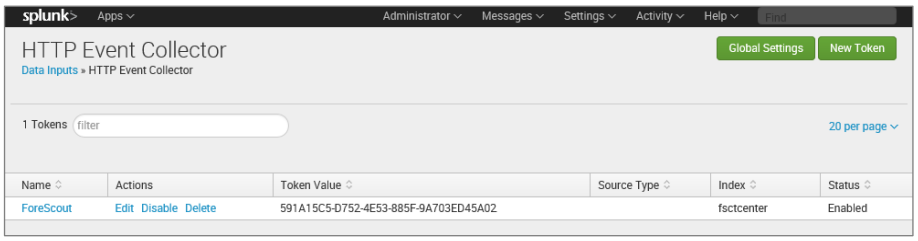
1. In the Splunk console, select **Settings>DATA>Data inputs**. The Data Inputs page appears.
2. In the Local Inputs section, locate the HTTP Event Collector entry. In the Actions column, select **Add New**. The Add Data wizard appears.
3. Define a HTTP Event Collector data input with the following settings:

   Name: ForeScout

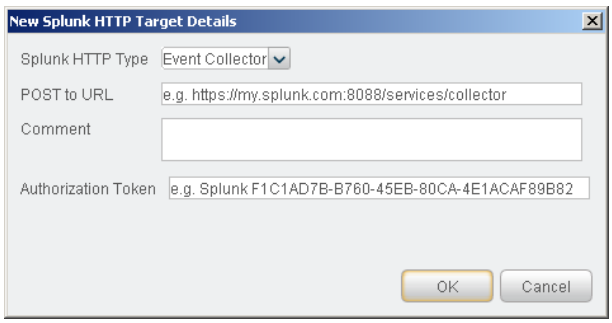
   Source: CounterACT

   Source Type: fsctcenter_json

   Default Index: fsctcenter



*Copy the **Token Value** and use it to configure HTTP Event Collector settings in CounterACT. Refer to the* Splunk Plugin Configuration Guide.



Working with Dashboards

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

- Summary Dashboard
- CounterACT Policy Dashboard
- Network Insight and Discovery Dashboard

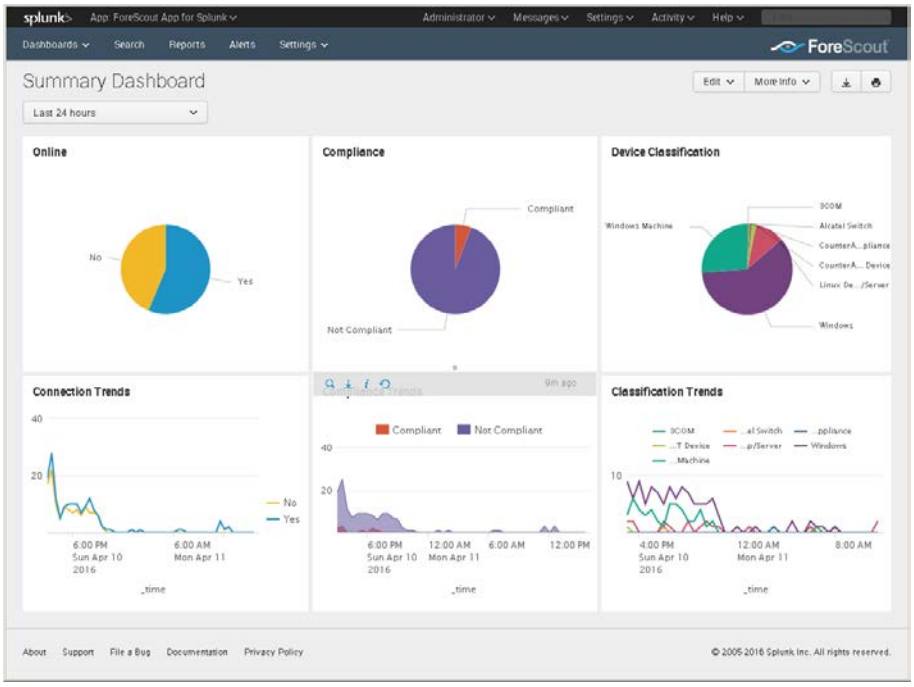
You can modify these standard dashboards, or create custom dashboards or graphs.

When working with dashboards:

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

Summary Dashboard

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



Online

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

Connection Trends

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

Compliance

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

Compliance Trends

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

Device Classification

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

Classification Trends

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

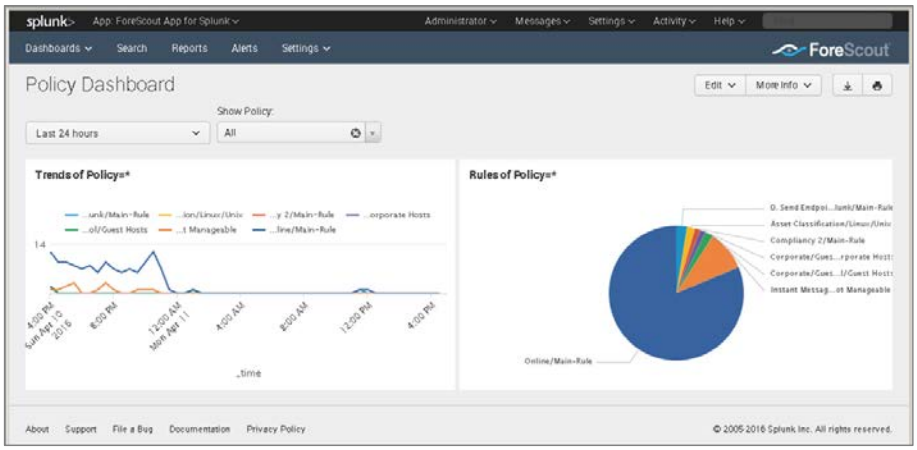
CounterACT Policy Dashboard

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

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

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

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



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

Network Insight and Discovery Dashboard

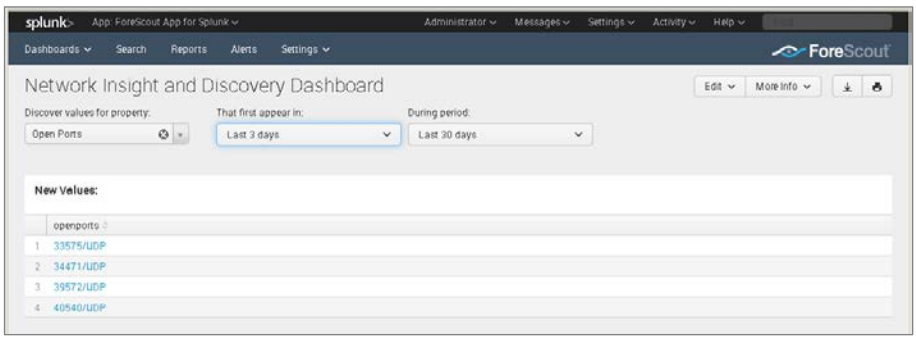
The Network Insight and Discovery dashboard tracks changes in a core set of CounterACT host properties. Use this dashboard to identify anomalous behavior and significant changes in the users, processes, applications, and other metrics associated with endpoints.

To use the Network Insight and Discovery dashboard:

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

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

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



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

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

Working with Searches

As a starting point for creating your own searches that include CounterACT data, examine the searches used to generate the dashboards provided with the ForeScout App. To examine macros referenced by these searches, select **Settings>KNOWLEDGE>Advanced search** and select **Search macros.**

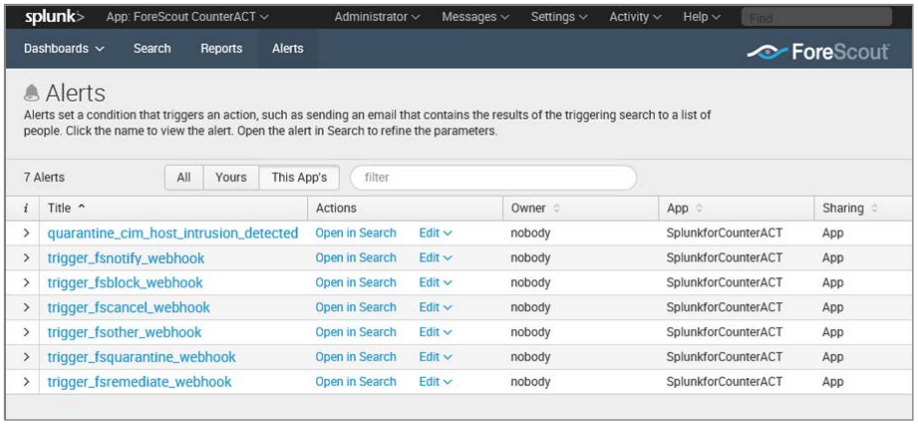
> *Not all CounterACT host properties are mapped to the CIM model. See Mapping CounterACT Data to the CIM Model for details.*

Working with Alerts

The app provides the following predefined alerts. These alerts are parsed by the Splunk Plugin to populate the **Splunk Alerts** and **Splunk Last Alert** host properties. CounterACT management policies examine these properties to respond to Splunk alerts.

Title	Description
quarantine_cim_host_intrusion_detected	Sends an alert with disposition Quarantine {3} to CounterACT based on a search of CIM typed data
trigger_fsnotify_webhook	Sends an alert with disposition Notify {1} to CounterACT
trigger_fsblock_webhook	Sends an alert with disposition Block {4}to CounterACT
trigger_fscancel_webhook	Sends an alert with disposition Cancel {0} to CounterACT

Title	Description
trigger_fsother_webhook	Sends an alert with disposition Other {5} to CounterACT
trigger_fsquarantine_webhook	Sends an alert with disposition Quarantine {3} to CounterACT
trigger_fsremediate_webhook	Sends an alert with disposition Remediate {2} to CounterACT



Read this section carefully before you try to use your own searches with these alerts.

By default, port 80 is used to send alerts to CounterACT. To use another port for alert messaging, edit the port configured in these predefined alerts as described in Change the Port Used for Alerts.

Targeting Endpoints in Alerts Sent to CounterACT

The alert messages sent to CounterACT must reference a specified endpoint. Typically CounterACT acts in response to the message by applying management or remediation actions to the endpoint. The IP address is used to specify the endpoint. This leads to the following considerations:

Mapping Search Terms to IP Addresses

The results array contained in the alert message payload must contain a Field:Value pair that CounterACT can parse to yield an IP address. CounterACT recognizes the following CIM tags as containing IP address information:

- **dest**
- **dest_host**
- **dest_ip**
- **dest_name**

In addition, CounterACT recognizes the label **ip** although it is not a CIM tag. When IP address information is in result fields not recognized by CounterACT, use the

following command in your search to label IP information so that CounterACT can parse it:

eval ip = <*IP_info*>

Where <*IP_info*> is an expression or field that resolves to an endpoint IP address.

CounterACT evaluates the fields in the following order:

- **ip**
- **dest_ip**
- **dest_host**
- **dest_name**
- **dest**

The first IP address found is used to identify the endpoint to which the alert applies. If an endpoint with this IP address does not exist in CounterACT, the alert is discarded.

Generating an Alert Message for each Endpoint

Typically a search returns more than one matching endpoint. Splunk must send these results to CounterACT as individual messages, each for a single endpoint, like most host information is reported to CounterACT. The trigger conditions for the alerts provided all use the **Trigger | Once | For each result** logic to ensure that an alert message is generated for each endpoint found by the search. It is recommended to retain this logic.

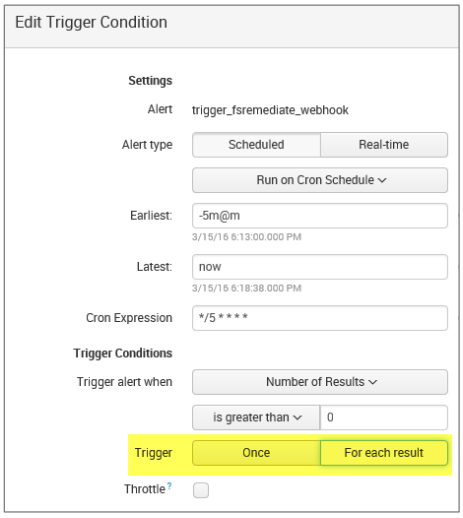
The default time expressions are:

Earliest | -5m@m

and

Cron Expression | */5**

Combined, these expressions cause Splunk to process alerts at five minute intervals. This approximates real-time alert behavior, while avoiding the processing overhead of real-time alerts.



Insert a Search in an Alert

Typically, Splunk searches are saved directly as Alerts with editable actions. To apply the actions of these predefined alerts to the results of your Splunk search, a different approach is required: clone and edit the alert that provides the desired action, and then paste your search logic into the clone.

To insert a search in an alert:

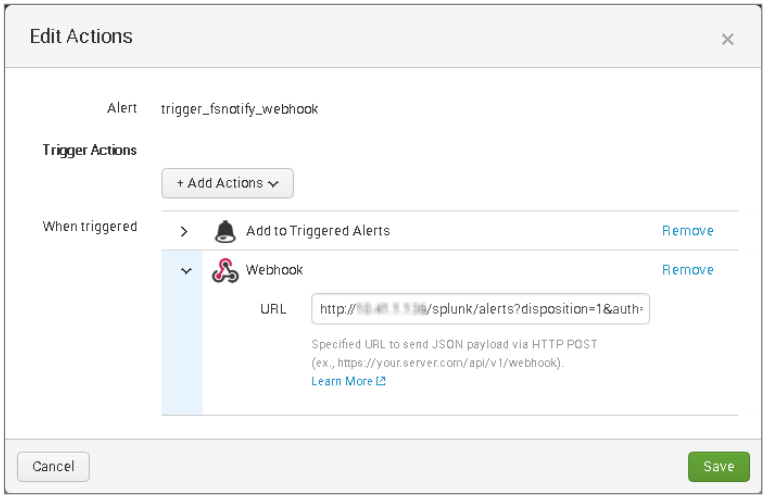
1. Compose and test your search. Select and copy the search.
2. In the App, select Alerts view.
3. Locate the alert that sends the type of message you want. In the Actions column, select **Edit>Clone**. The Clone Alert dialog appears.
4. Edit the alert's name and permissions. Select **Clone Alert**.
5. The Alert has been cloned dialog appears. Select **Open in Search**.
6. Replace your search with the default search of the alert.
7. Select **Save** and save the alert.
8. (Optional) By default, port 80 is used to send alerts to CounterACT. If you are using a port different from the default port, edit this setting in the clone as described in Change the Port Used for Alerts.

Change the Port Used for Alerts

By default, port 80 is used to send alerts to CounterACT. To use another port for alert messaging, edit this setting in the predefined alerts provided with this app.

To change the port used for alert messaging:

1. In the Alerts view, select one of the predefined alerts provided with the app, or a cloned copy.
2. Select **Edit > Edit Actions**. The Edit Actions dialog appears.



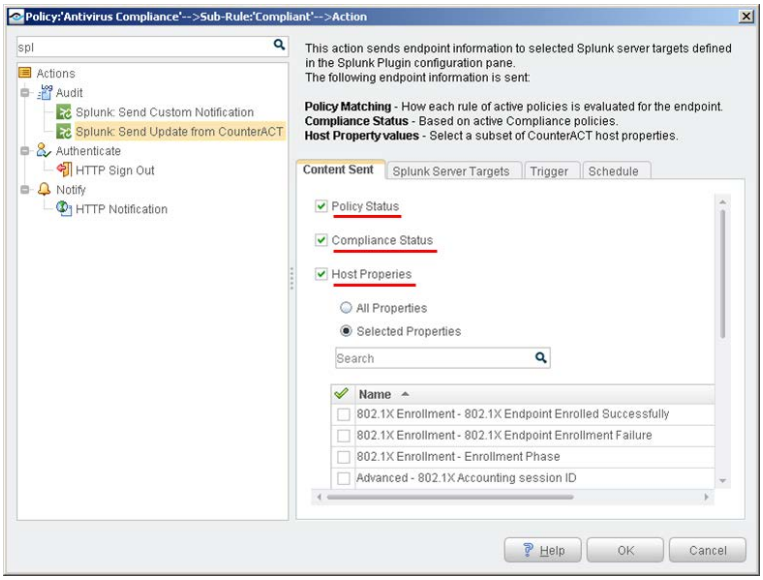
3. In the **URL** field, enter the full URL to the target CounterACT device that accepts alert notifications from Splunk. The string you enter overrides defaults used for this messaging, for example:
   - Specify a port in the URL string, using standard **`/host:port/`** syntax.
   - To use secure HTTP, use the **`https://`** prefix in the URL string.

Appendix A: Working with CounterACT Data in Splunk

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

About CounterACT Data Events

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



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

- When the **Policy status** option is selected, CounterACT sends *a separate event message* for each policy rule that is reported to Splunk.
- When the **Host Properties** option is selected, CounterACT sends *a separate event message* for each host property that is reported to Splunk. Similarly, when the **Compliance Status** option is selected, CounterACT sends an event message with the value of the *Compliance Status* host property.

Each event message contains the following additional information, as field:value pairs:

Field	Description
ip	The IP address of the endpoint for which information is reported.
Since	A timestamp that indicates when the data reported was first detected/resolved by CounterACT. This value is mapped to the _time field in Splunk.

Field	Description
ctupdate	Identifies the message as a CounterACT update. The value of this attribute indicates the type of data reported by the message: ▪ Events that report policy information contain the pair **`ctupdate:policyinfo`**. ▪ Events that report compliance and host properties contain the pair **`ctupdate:hostinfo`**. ▪ When the **Splunk Send Custom Notification** action is used, the payload contains the pair **`ctupdate:notif`** .

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

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

See the *Splunk Plugin Configuration Guide* for more details of action configuration options.

Considerations When Working with CounterACT Events in Splunk

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

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

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

- Timestamps indicate when CounterACT detected/resolved the reported value, not the time of the event message. Applying the **Splunk Send Update from CounterACT** action to endpoints does not necessarily cause properties to be re-evaluated. In particular:

  – Any property that was resolved for an endpoint before the action was applied to the host is reported with the timestamp of its detection/resolution, even though this timestamp predates application of the action and creation of the event message.

  – If a previously reported property is now not resolvable by CounterACT, no new event message is sent to Splunk.

  *If the endpoint was dropped from the scope of the **Splunk Send Update** action, and then returns to the scope, the last known value is reported again to Splunk.*

Mapping CounterACT Data to the CIM Model

Due to the extensive range of data that can be reported by CounterACT host properties, this release of the ForeScout App does not include a Technology Add-on that fully maps CounterACT properties to tags in the CIM model.

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

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

Legal Notice

2016-07-28 12:53