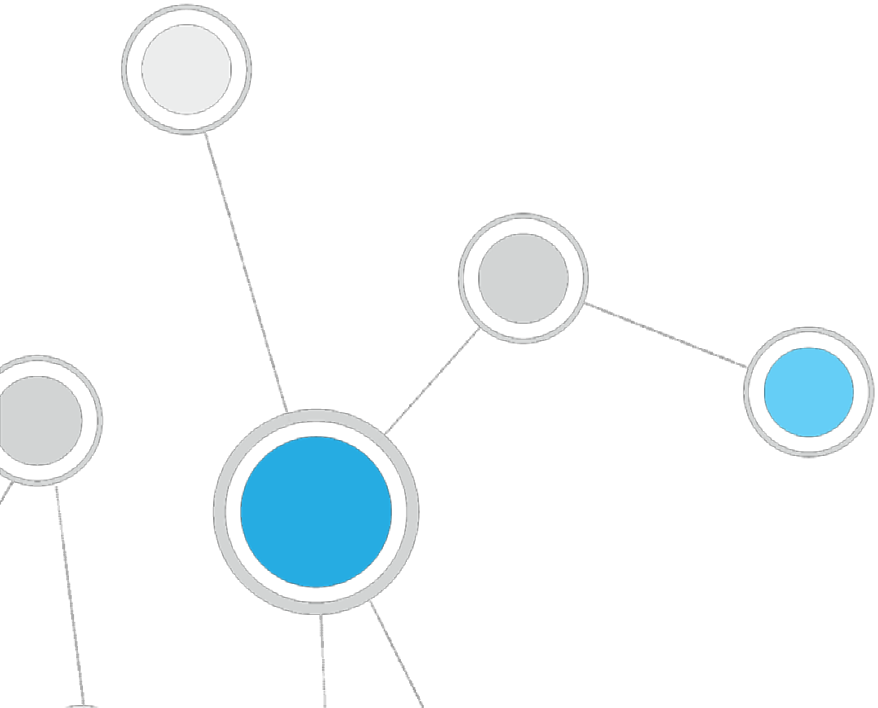
# ForeScout App for Splunk

## How-to Guide

**Version 2.5.0**



# Table of Contents

# About Splunk Integration

Splunk Enterprise data analytics help organizations:

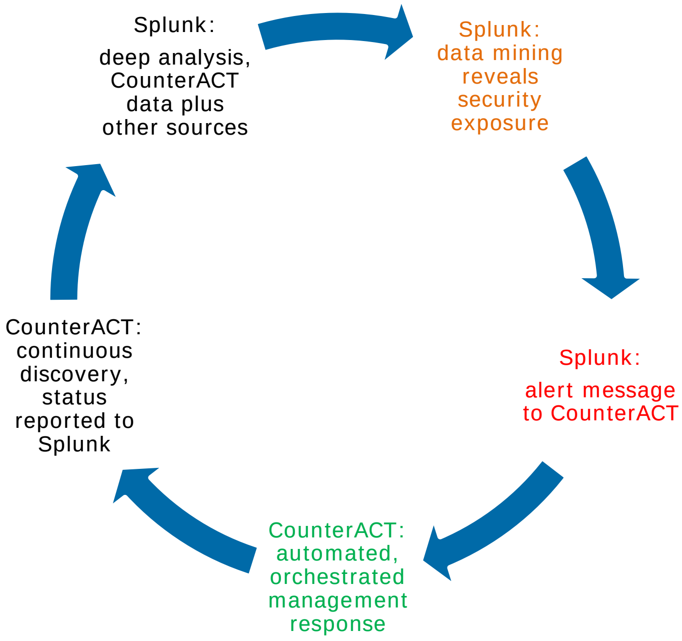
- Leverage the data that their infrastructure and security tools provide
- Understand their security posture
- Pinpoint and investigate risks
- Create alerts and reports.

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 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
- 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 action requests to CounterACT.


Splunk:
deep analysis, CounterACT data plus other sources
Splunk: data mining reveals security exposure
Splunk:
alert message to CounterACT
CounterACT: automated, orchestrated management response
CounterACT: continuous discovery, status reported to Splunk

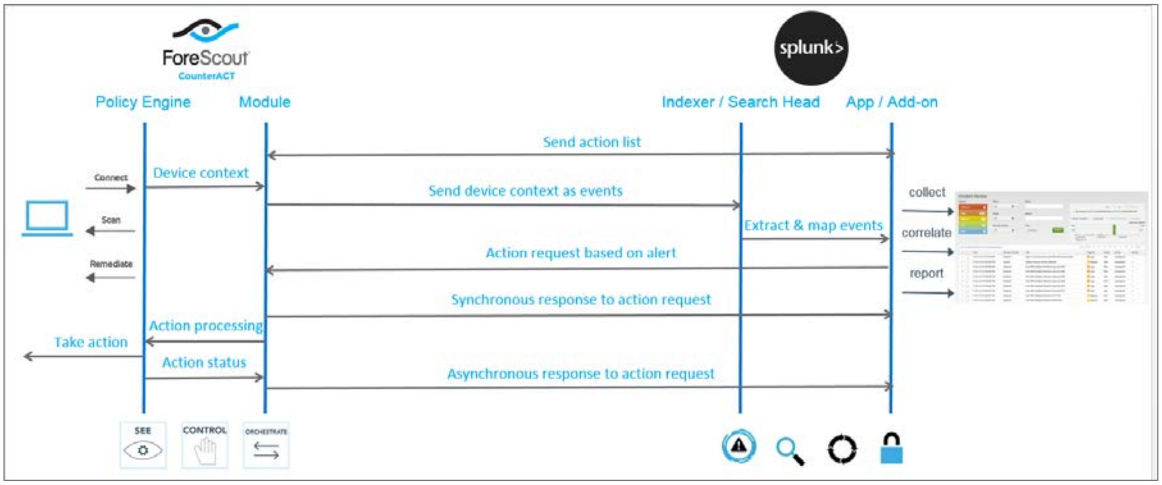
The result is enhanced threat insight, automated control, and greater operational efficiency.

## Support for Splunk Adaptive Response

Splunk's Adaptive Response framework describes a complete action flow, which includes requesting an action be applied to an endpoint, and tracking the status of the action taken.

This integration supports the Splunk Adaptive Response framework as follows:

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



# Use Cases

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

The ForeScout App for Splunk works with the Splunk Plugin to integrate CounterACT and Splunk so that you can:

- 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 Correlation Searches and Saved 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 *CounterACT™ Splunk Module Configuration Guide*.

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

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

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

The Splunk Module 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 Module are used to populate Splunk with CounterACT data. Read this document together with the *CounterACT™ Splunk Module Configuration Guide*.

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

## Supported Splunk Versions

This release supports Splunk Enterprise version 6.4.x and 6.5. Additionally, it also works with Splunk Enterprise Security App 4.5.

# New Options for ForeScout App for Splunk

Version 2.5 of the ForeScout App for Splunk has been split into three apps: Technology Add-on, Technology Add-on Adaptive Response and the ForeScout App for Splunk. Users may choose to install and use the Technology Add-on and Technology Add-on Adaptive Response with or without the ForeScout App for Splunk.

Additionally, this app works in Splunk Enterprise or Splunk Enterprise Security App 4.5.

| App Module | Description |
|---|---|
| **ForeScout Adaptive Response Add-on for Splunk** (TA-forescout_response)<br>**v2.5.0** | Module for Splunk Enterprise Security Suite (ESS) app for executing Modular Alert Actions on CounterACT. It leverages Adaptive Response Framework solution provided by Splunk through the Splunk Enterprise Security Suite (ESS). |
| **ForeScout App for Splunk (Forescout_app)**<br>**v2.5.0** | A visualization app containing dashboards to monitor CounterACT endpoints using event data provided by CounterACT to Splunk. It also contains dashboards to monitor Modular Alert Actions in case of non-ESS environments. |
| **ForeScout Technology Add-on for Splunk (TA-forescout)**<br>**v2.5.0** | Data collector app that maintains credentials for CounterACT Appliance communications and provides field extraction configurations for all CounterACT events. |

## Requirements

This section describes system requirements, including:

- Splunk Requirements
- CounterACT Requirements
- Networking and Communication Protocol Requirements

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

## Splunk Requirements

To integrate CounterACT with a Splunk environment that runs Splunk Enterprise Security:

- Splunk Components 6.4.x or 6.5.x
  - Version 4.5 of the Enterprise Security App should be installed.
- Splunk Processing Capacity
- Splunk System Configuration
- Splunk User Permissions

To integrate CounterACT with a Splunk environment that **does not** run Splunk Enterprise Security:

- Splunk Components
- Splunk Processing Capacity
  - Non-Windows platforms – 2x six-core, 2+ GHz CPU
  - Windows platforms - 2x six-core, 2+ GHz CPU
  - Splunk System Configuration
  - Non-Windows platforms – 12GB RAM, Redundant Array of Independent Disks (RAID) 0 or 1+0, with a 64 bit OS installed.
  - Windows platforms - 12GB RAM, RAID 0 or 1+0, with a 64-bit OS installed.
- Splunk User Permissions

## CounterACT Requirements

The ForeScout for Splunk interacts with an Enterprise Manager running 7.0.0 and above. The following components must be installed:

- Service Pack 2.2.0 or above ( SP 2.3.2 recommended)
- In case you want to receive endpoint classification and compliance information, verify that the following policies are active on CounterACT:
  - 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.

In case, you plan to send system health and network data, make sure to also install and enable Hardware Inventory Plugin (v 1.0.1) and NetFlow Plugin (v 1.1.0). ForeScout Module

## Networking and Communication Protocol Requirements

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

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

| **Communication** | **Recommended** | **Alternative** |
|---|---|---|
| Retrieve Action Info<br>The ForeScout App for Splunk polls CounterACT's action_info API to retrieve a list of available actions. | REST API<br>Default port: 80 | REST API on HTTPS |
| Ongoing Data Reporting<br>CounterACT sends endpoint data to Splunk. This is the protocol used by the Splunk Module in CounterACT to implement the **Splunk: Send Update from CounterACT** action. | Event Collector<br>Default port: 8088 | Syslog (port 515/TCP/UDP)<br>RESTful API HTTPS (8089)<br>Syslog may not support data tags and json embedded format. |
| Splunk Action Request<br>▪ Splunk sends alerts to CounterACT's alert API.<br>▪ The alert API confirms receipt of alert message (Synchronous response - see CounterACT Response to Alert Messages). | REST API<br>Default port: 80 | REST API on HTTPS |
| Splunk Action Final Status<br>CounterACT reports the status of actions requested by Splunk (Asynchronous response - see CounterACT Response to Alert Messages). | Event Collector<br>Default port: 8088 | Syslog (port 515/TCP/UDP)<br>RESTful API HTTPS (8089)<br>Syslog may not support data tags and json embedded format. |

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

## About Certificates for Secured Messaging

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

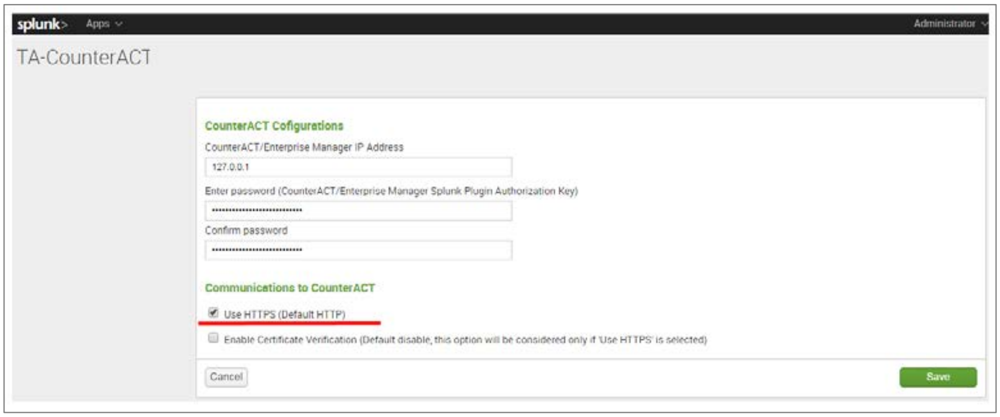
- EventCollector and REST API messaging from CounterACT to Splunk do not require HTTPS, but can support it.
- Splunk alert messages sent to CounterACT's alert API do not require HTTPS, but can support it.

## Secured Messaging from ForeScout Splunk App to CounterACT Splunk Module

The alerts forwarded by the ForeScout Splunk App to CounterACT Splunk Module can be sent over HTTPS.

**To enable HTTPS communication:**

1. In the ForeScout Splunk App, go to **Settings > General Settings > Server Settings**. The CounterACT Configurations page displays (see below.)



TA-CounterACT

CounterACT Cofigurations

CounterACT/Enterprise Manager IP Address: 127.0.0.1

Enter password (CounterACT/Enterprise Manager Splunk Plugin Authorization Key): ••••••••••••••••••••••••

Confirm password: ••••••••••••••••••••••••

Communications to CounterACT

☑ Use HTTPS (Default HTTP)

☐ Enable Certificate Verification (Default disable, this option will be considered only if 'Use HTTPS' is selected)

2. In CounterACT, operators must not use the default self-signed web-portal certificate, instead, they need to procure their own certificate. Use ‘fstool cert’ utility to create a Certificate Signing Request (CSR) using the following steps:
    a. Use ‘fstool  cert gen’ to generate the certificate request.
    b. A number of questions are asked. Free text is expected as answers.
    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) or by the customer's own Certificate Authority.
4. If using a self-signed certificate, once the certificates are installed on the CounterACT appliance, the CounterACT Public Key Certificate must be appended to the cacert.pem file at the following location:

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

Please refer to the CounterACT Splunk Module Configuration Guide for instructions on secured messaging from CounterACT Splunk Module to ForeScout App for Splunk.

# Installation and Configuration

This section describes installation scenarios and procedures for the ForeScout App.

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

1. Review the Splunk Plugin Configuration Guide and this How-to Guide.
2. Verify that Requirements are met.
3. Download App Files
4. Create a Data Index for CounterACT
5. Install and Configure the ForeScout Technology Add-on
6. Install the CounterACT Adaptive Response Add-on

7. Install the ForeScout App for Splunk. If you are working with Splunk Enterprise Security, you may omit this component.
8. (Optional) test and tune the frequency of data reporting based on your network conditions and the volume of data you want to work with in Splunk.

## Download App Files

The ForeScout App for Splunk consists of the following components:

| Component | Description | File |
|---|---|---|
| **Forescout Technology Add-on for Splunk** (TA-forescout) | Handles data collection from CounterACT. | **`TA-forescout.tar.gz`** |
| **Forescout Adaptive Response Add-on for Splunk** (TA-forescout_response) | Supports Adaptive Response action calls to CounterACT. | **`TA-forescout_response.tar.gz`** |
| **ForeScout App for Splunk** (forescout_app) | A visualization App containing dashboards to monitor endpoints using data provided by CounterACT. | **`forescout_app.tar.gz`** |

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

## Create a Data Index for CounterACT

Follow the procedure described in the Splunk knowledge base to create an index that identifies information sent to Splunk by CounterACT. The index should have the name **`fsctcenter`**.

http://docs.splunk.com/Documentation/Splunk/6.4.3/Indexer/Setupmultipleindexes

## Install and Configure the ForeScout Technology Add-on for Splunk

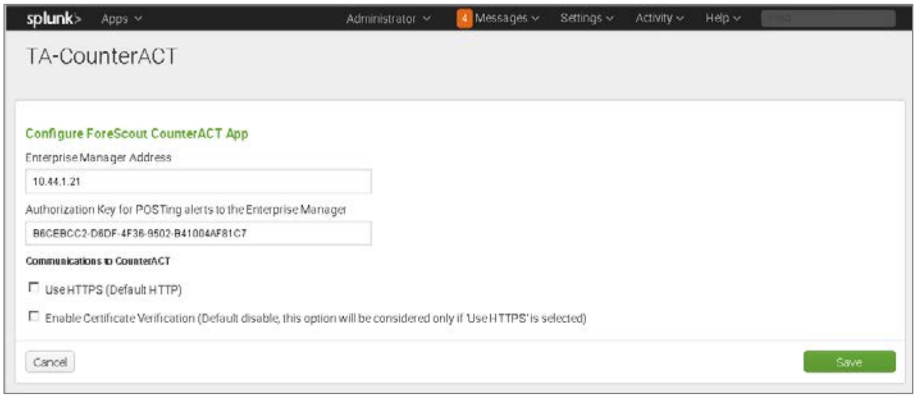
The ForeScout Technology Add-on for Splunk supports data communication between CounterACT and the Splunk App.

**To install and configure the add-on:**

1. Log in to Splunk as an Admin user.
2. In the Apps pane on the left of the Splunk window, select the Apps utility menu.
3. Select **Manage Apps > Install from file**.
4. Browse to the ForeScout App files and select **`TA-CounterACT.tar.gz`**.

To complete installation, you are prompted to restart.

5. After restart, log in to Splunk and return to the Manage Apps menu. Locate the **`TA-CounterACT` app** and select **Set up**. The configuration page for the app displays.



TA-CounterACT

Configure ForeScout CounterACT App

Enterprise Manager Address: 10.44.1.21

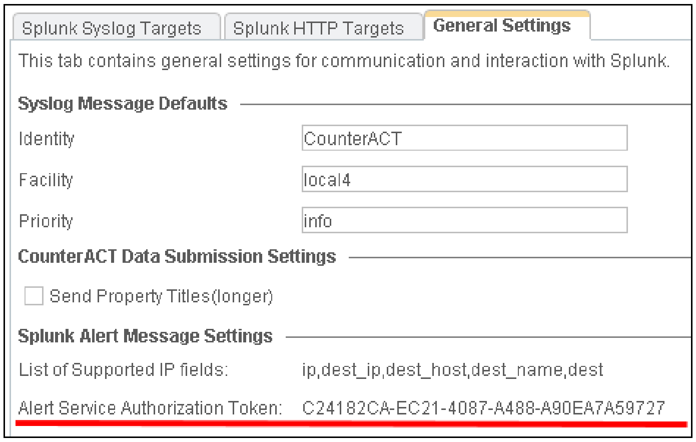
Authorization Key for POSTing alerts to the Enterprise Manager: B6CEBCC2-D6DF-4F36-9502-B41004AF81C7

Communications to CounterACT

□ Use HTTPS (Default HTTP)

□ Enable Certificate Verification (Default disable, this option will be considered only if 'Use HTTPS' is selected)

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



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

Syslog Message Defaults

Identity: CounterACT

Facility: local4

Priority: info

CounterACT Data Submission Settings

□ Send Property Titles(longer)

Splunk Alert Message Settings

List of Supported IP fields: ip,dest_ip,dest_host,dest_name,dest

Alert Service Authorization Token: C24182CA-EC21-4087-A488-A90EA7A59727

   c. (Optional) Perform additional certificate-related configuration steps to enable HTTPS communication between CounterACT and Splunk. See About Certificates for Secured Hypertext Messaging.
   d. Select **Save**.

**To create a data input for Event Collector messaging:**

🗎 *It is recommended to use Event Collector protocol for data messaging. If you want to use other supported protocols, see Configuration Procedures.*

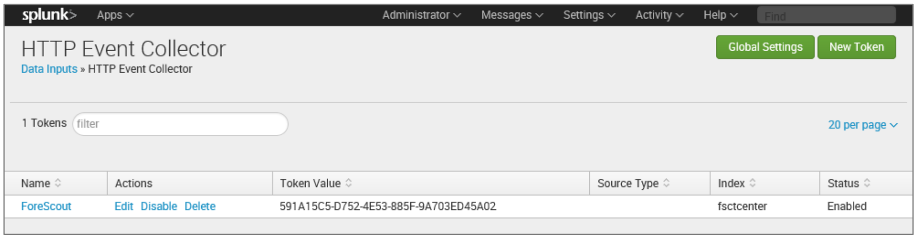
1. In the Splunk console, select **Settings>DATA>Data inputs**. The Data Inputs page appears.
2. In the Local Inputs section, locate the HTTP Event Collector entry. In the Actions column, select **Add New**. The Add Data wizard appears.
3. Define a HTTP Event Collector data input with the following settings:

   **Name**: ForeScout

   **Source**: CounterACT

   **Source Type**: fsctcenter_json

   **Default Index**: fsctcenter



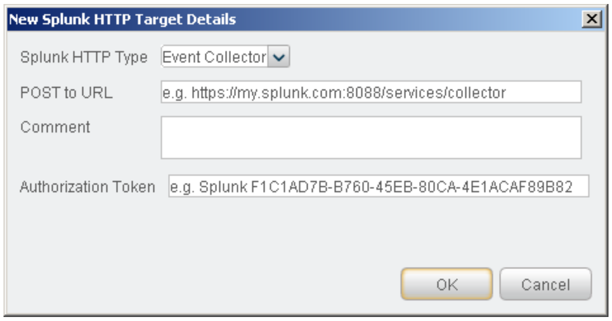
HTTP Event Collector

Data Inputs » HTTP Event Collector

1 Tokens

| Name | Actions | Token Value | Source Type | Index | Status |
|---|---|---|---|---|---|
| ForeScout | Edit Disable Delete | 591A15C5-D752-4E53-885F-9A703ED45A02 | | fsctcenter | Enabled |

*Copy the* ***Token Value*** *from the new Splunk HTTP Target Details diaplog box and use it to configure HTTP Event Collector settings in CounterACT. Refer to the* Splunk Plugin Configuration Guide*.*



New Splunk HTTP Target Details

Splunk HTTP Type: Event Collector

POST to URL: e.g. https://my.splunk.com:8088/services/collector

Comment:

Authorization Token: e.g. Splunk F1C1AD7B-B760-45EB-80CA-4E1ACAF89B82

# Install the CounterACT Adaptive Response Add-on for Splunk

This add-on supports Adaptive Response action calls to CounterACT.

**To install and configure the add-on:**

1. Go to splunkbase.splunk.com and search for the name of the Add-on.
2. In the App Results page, select the app and download.

   No configuration or restart is required for this add-on.

# 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 the version 2.5.x release.*

**To install and configure the add-on:**

1. Go to splunkbase.splunk.com and search for the name of the Add-on.
2. In the App Results page, select the app and download.

   No configuration or restart is required for this add-on.

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

# Configuration Procedures

When your implementation uses non-standard ports or protocols for communication, you may need to perform the procedures in this section.

- Verify and Configure Data Inputs for Syslog Messaging
- Configure Splunk REST API Credentials for CounterACT

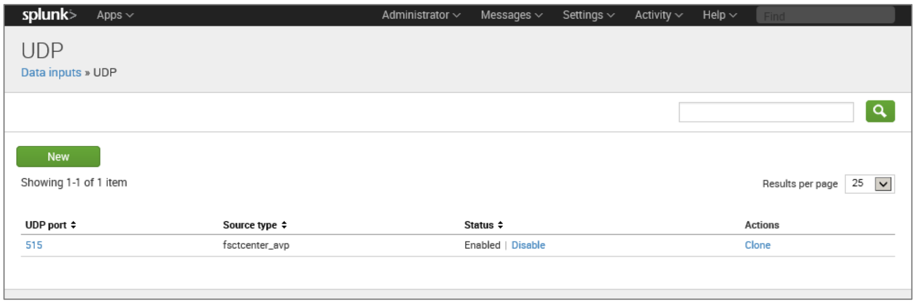
## Verify and Configure Data Inputs for Syslog Messaging

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.

🗎 *If you choose to submit CounterACT data to Splunk using Syslog instead of the Event Collector protocol, data typing/tagging information is sometimes not transmitted. As a result, you may not be able to use data tags to filter information in Splunk.*

**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.



UDP

Data inputs » UDP

Showing 1-1 of 1 item

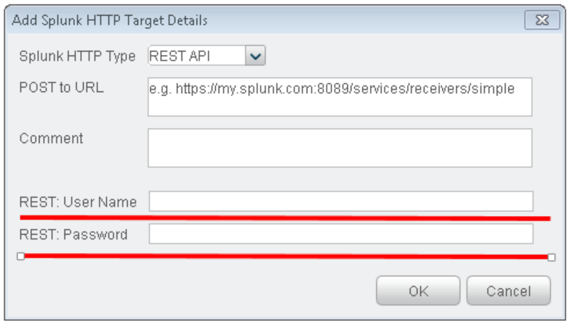
Results per page 25

| UDP port | Source type | Status | Actions |
|---|---|---|---|
| 515 | fsctcenter_avp | Enabled \| Disable | Clone |

## Configure Splunk REST API Credentials for CounterACT (Optional)

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*.


Add Splunk HTTP Target Details

Splunk HTTP Type: REST API

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

Comment:

REST: User Name:

REST: Password:

# Splunk Roles for CounterACT

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

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

### counteract_admin

Users with this role can:

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

- Enable/disable saved searches

### counteract_user

Users with this role can:

- Create Dashboard
- View Dashboards
- Search on all indexes

User with this role cannot:

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

# CounterACT Workflow for Adaptive Response

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

- ***CounterACT alert action list***: the CounterACT Adaptive Response add-on initializes and maintains a list of actions by polling CounterACT's action_info API. The frequency of update polling can be configured. This list represents the actions that CounterACT can apply to an endpoint based on Splunk alerts.
- ***CounterACT events***: the rich stream of endpoint information that Splunk receives from CounterACT can be combined with information from other sources in searches that identify suspect endpoints or network events of concern.
- ***CounterACT alerts (saved search)***: The add-on provides predefined searches that mine standard endpoint properties reported by CounterACT to Splunk.
- ***CounterACT Alert API***: Splunk sends action requests to CounterACT through a REST API interface.
- ***CounterACT action response***:

– *Synchronous response* - CounterACT acknowledges the action request, and initiates policy-based implementation of the action.

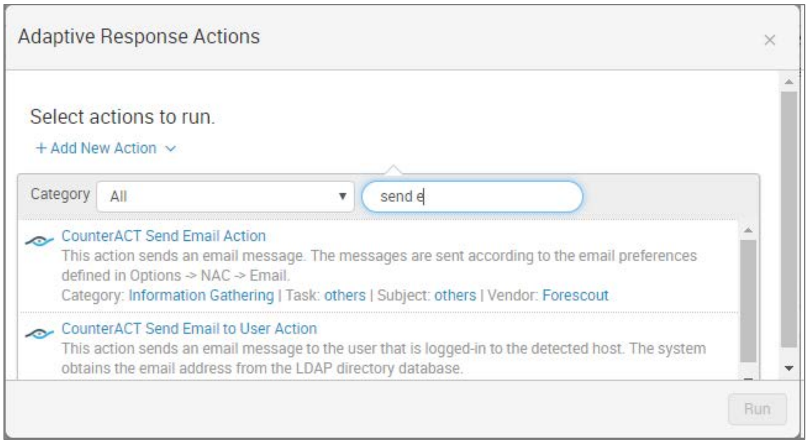
– *Asynchronous response* - CounterACT reports the status of the requested action 8 hours after the request is received (configurable).

See CounterACT Response to Alert Messages.

In addition, the ForeScout App provides a dashboard that tracks actions requested by Splunk. See Modular Action Center Dashboard.

### With Splunk Enterprise Security

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



Select actions to run.

CounterACT Send Email Action
This action sends an email message. The messages are sent according to the email preferences defined in Options -> NAC -> Email.
Category: Information Gathering | Task: others | Subject: others | Vendor: Forescout

CounterACT Send Email to User Action
This action sends an email message to the user that is logged-in to the detected host. The system obtains the email address from the LDAP directory database.

### In Splunk Enterprise Environments without Enterprise Security

Saved searches provided with the ForeScout App for Splunk identify endpoints of interest based on various data feeds including CounterACT endpoint data. Alerts that invoke CounterACT actions can be attached to these or other scheduled searches. The result is ongoing, automatic application of CounterACT actions to endpoints identified by periodic searches.

## Correlation Searches and Saved Searches

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

- trigger_apt_cp_threatemulation_ioc_notification

  Search based on CounterACT Malware Activity that applies the CounterACT HTTP Notificiation action`

- trigger_apt_cp_antivirus_ioc_notification

  Search based on CounterACT Malicious File Download that applies the CounterACT Send Message to Syslog action.

- trigger_dot1x_action_failure_notification

  Search based on CounterACT Authentication Failure Exceeding Threshold that applies the Send Email action

- trigger_dot1x_action_failure_email

  Search based on CounterACT Authentication Failures that applies the Send Email action

- es_trigger_apt_cp_threatemulation_ioc_notification

  Enterprise Security Correlation Search based on CounterACT Malware Activity

- es_trigger_apt_cp_antivirus_ioc_notification

  Enterprise Security Correlation Search Based on CounterACT Malicious File Download

- es_trigger_dot1x_action_failure_notification

Enterprise Security Correlation Search based on CounterACT Authentication Failure Exceeding Threshold

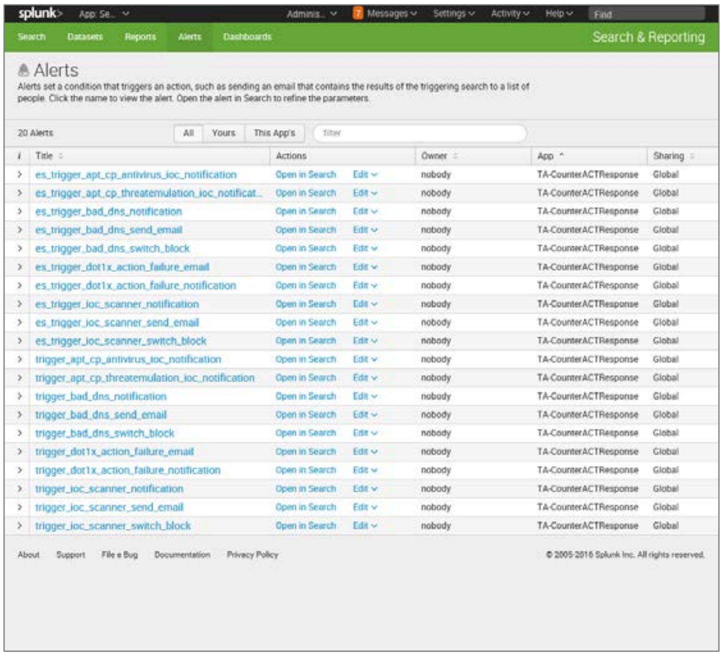
- es_trigger_dot1x_action_failure_email

Enterprise Security Correlation Search based on CounterACT Authentication Failures

# Alerts

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

On the Alerts page, the default Saved Searches are listed.



Alerts

Alerts set a condition that triggers an action, such as sending an email that contains the results of the triggering search to a list of people. Click the name to view the alert. Open the alert in Search to refine the parameters.

20 Alerts

| i | Title | Actions | | Owner | App | Sharing |
|---|---|---|---|---|---|---|
| > | es_trigger_apt_cp_antivirus_ioc_notification | Open in Search | Edit | nobody | TA-CounterACTResponse | Global |
| > | es_trigger_apt_cp_threatemulation_ioc_notificat... | Open in Search | Edit | nobody | TA-CounterACTResponse | Global |
| > | es_trigger_bad_dns_notification | Open in Search | Edit | nobody | TA-CounterACTResponse | Global |
| > | es_trigger_bad_dns_send_email | Open in Search | Edit | nobody | TA-CounterACTResponse | Global |
| > | es_trigger_bad_dns_switch_block | Open in Search | Edit | nobody | TA-CounterACTResponse | Global |
| > | es_trigger_dot1x_action_failure_email | Open in Search | Edit | nobody | TA-CounterACTResponse | Global |
| > | es_trigger_dot1x_action_failure_notification | Open in Search | Edit | nobody | TA-CounterACTResponse | Global |
| > | es_trigger_ioc_scanner_notification | Open in Search | Edit | nobody | TA-CounterACTResponse | Global |
| > | es_trigger_ioc_scanner_send_email | Open in Search | Edit | nobody | TA-CounterACTResponse | Global |
| > | es_trigger_ioc_scanner_switch_block | Open in Search | Edit | nobody | TA-CounterACTResponse | Global |
| > | trigger_apt_cp_antivirus_ioc_notification | Open in Search | Edit | nobody | TA-CounterACTResponse | Global |
| > | trigger_apt_cp_threatemulation_ioc_notification | Open in Search | Edit | nobody | TA-CounterACTResponse | Global |
| > | trigger_bad_dns_notification | Open in Search | Edit | nobody | TA-CounterACTResponse | Global |
| > | trigger_bad_dns_send_email | Open in Search | Edit | nobody | TA-CounterACTResponse | Global |
| > | trigger_bad_dns_switch_block | Open in Search | Edit | nobody | TA-CounterACTResponse | Global |
| > | trigger_dot1x_action_failure_email | Open in Search | Edit | nobody | TA-CounterACTResponse | Global |
| > | trigger_dot1x_action_failure_notification | Open in Search | Edit | nobody | TA-CounterACTResponse | Global |
| > | trigger_ioc_scanner_notification | Open in Search | Edit | nobody | TA-CounterACTResponse | Global |
| > | trigger_ioc_scanner_send_email | Open in Search | Edit | nobody | TA-CounterACTResponse | Global |
| > | trigger_ioc_scanner_switch_block | Open in Search | Edit | nobody | TA-CounterACTResponse | Global |

© 2005-2016 Splunk Inc. All rights reserved.

## Configuring your Alerts

This section provides an example of the default alert. When you are creating your alert, you will need to fill in the Search Description, Search Name, Search Query, Action Name, API call to CounterACT, and Sample log/event fields.

**To create an Alert:**

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

Sample Alert configurations are shown below.

**Search Description:** Search for CounterACT Authentication Failure Exceeding Threshold

**Search Name:** trigger_dot1x_action_failure_notification

**Search Query:** index=fsctcenter sourcetype=fsctcenter_json source=counterACT dot1x_update_authentication_props "Logon Failure"| join type=inner max=0 username [search index=fsctcenter sourcetype=fsctcenter_json source=counterACT dot1x_set_fr_properties | eval NAS3IpAddress=if(field="NAS3IpAddress",value,null)| stats latest(NAS3IpAddress) as ip by username]| eventstats count as eventcount by username,ip| dedup username ip| WHERE eventcount>10

**Action Name:** sendmail_action

**API call to counterACT:**
http://<em_ip>/splunk/alerts?disposition=3&action_group=notify&auth=CounterACT%20<token>

**Sample log/event:** main::dot1x_update_authentication_props:1799:[fr-update]::0:<601912435557|usr=601912435557>Logon Failure: Rejected user 601912435557:

## Customizing your own Alerts

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

### Index

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

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

| Index Name | Created in App/Manual | Purpose/Type of event data |
|---|---|---|
| | | related information are stored in this index. |
| _introspection | Available as part of Splunk framework. | All the Splunk Performance related metrics are logged here |

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

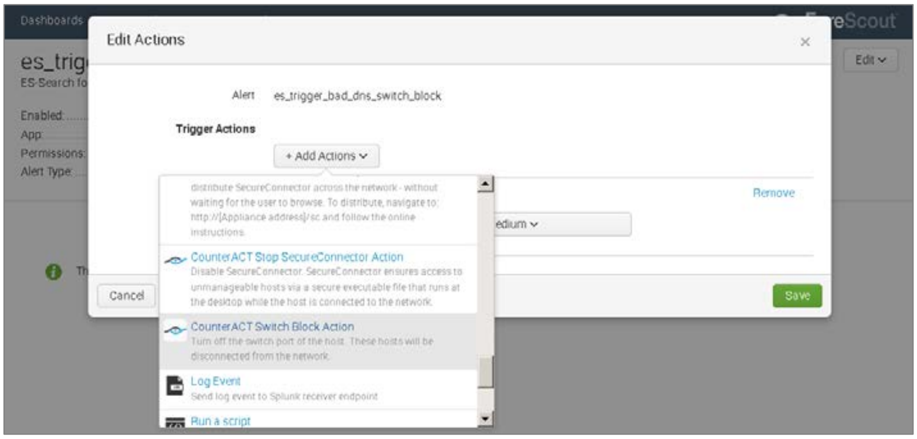
### Source and Sourcetype

Source and Sourcetype are default Splunk fields to categorize and parse indexed data in a proper way. Below is the table which shows how the CounterACT related event data is distributed in these fields.
Please read more about the default fields at:
http://docs.splunk.com/Documentation/Splunk/6.4.3/Data/Aboutdefaultfields

| Index Name | Source | Sourcetype | Purpose/Type of event data |
|---|---|---|---|
| fsctcenter | CounterACT | fsctcenter_avp | This contains all the event data sent from CounterACT to Splunk using Syslog/UDP ports |
| fsctcenter | CounterACT | fsctcenter_json | This contains all the event data sent from CounterACT to Splunk using either REST API or HEC Collector |
| fsctcenter | modactions | counteract_alerts | All the Adaptive Response Framework Alert Action related logs are written in this category. This will also have the Alert Action API call responses. |
| fsctcenter | modactions | counteract_orig_event | The original events from index=fsctcenter which triggered any Modular Alert Action are stored here with their corresponding Splunk |

| Index Name | Source | Sourcetype | Purpose/Type of event data |
|---|---|---|---|
| | | | search_id and row_id of the event results. |
| _internal | /opt/splunk/var/log/splunk/scheduler.log | scheduler | All the Saved Search and their execution time related information are stored here. |

When you save a search, you can define alert messages that request one or more of these actions.



Alert es_trigger_bad_dns_switch_block

distribute SecureConnector across the network - without waiting for the user to browse. To distribute, navigate to: http://[Appliance address]/sc and follow the online instructions.

CounterACT Stop SecureConnector Action
Disable SecureConnector. SecureConnector ensures access to unmanageable hosts via a secure executable file that runs at the desktop while the host is connected to the network.

CounterACT Switch Block Action
Turn off the switch port of the host. These hosts will be disconnected from the network.

Log Event
Send log event to Splunk receiver endpoint

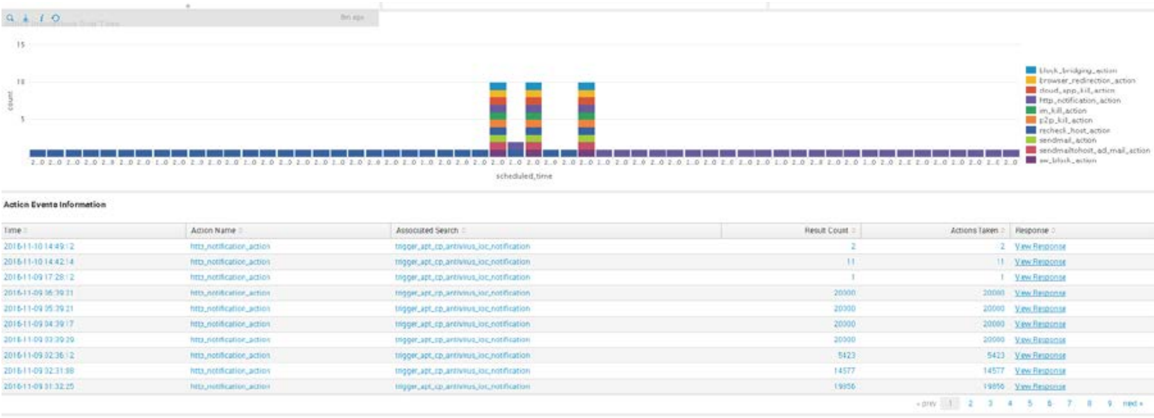
Run a script

When the saved search runs, the alert message tells CounterACT to apply the action to endpoints that match the search.

## CounterACT Response to Alert Messages

When CounterACT receives a Splunk alert message:

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



Action Events Information

| Time | Action Name | Associated Search | Result Count | Actions Taken | Response |
|---|---|---|---|---|---|
| 2016-11-10 14:49:12 | http_notification_action | trigger_apt_cp_antivirus_ioc_notification | 2 | 2 | View Response |
| 2016-11-10 14:42:14 | http_notification_action | trigger_apt_cp_antivirus_ioc_notification | 11 | 11 | View Response |
| 2016-11-09 17:28:12 | http_notification_action | trigger_apt_cp_antivirus_ioc_notification | 1 | 1 | View Response |
| 2016-11-09 06:39:11 | http_notification_action | trigger_apt_cp_antivirus_ioc_notification | 20000 | 20000 | View Response |
| 2016-11-09 05:39:21 | http_notification_action | trigger_apt_cp_antivirus_ioc_notification | 20000 | 20000 | View Response |
| 2016-11-09 04:39:17 | http_notification_action | trigger_apt_cp_antivirus_ioc_notification | 20000 | 20000 | View Response |
| 2016-11-09 03:39:29 | http_notification_action | trigger_apt_cp_antivirus_ioc_notification | 20000 | 20000 | View Response |
| 2016-11-09 02:36:12 | http_notification_action | trigger_apt_cp_antivirus_ioc_notification | 5423 | 5423 | View Response |
| 2016-11-09 02:31:58 | http_notification_action | trigger_apt_cp_antivirus_ioc_notification | 14577 | 14577 | View Response |
| 2016-11-09 01:32:25 | http_notification_action | trigger_apt_cp_antivirus_ioc_notification | 19956 | 19956 | View Response |

The CounterACT Splunk Plugin 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 8 hours after the alert message is received. The report interval is configurable. Refer to the CounterACT Splunk Module Configuration Guide for details. If an alert requested several actions, a report is generated for each action, identifying its alert message.

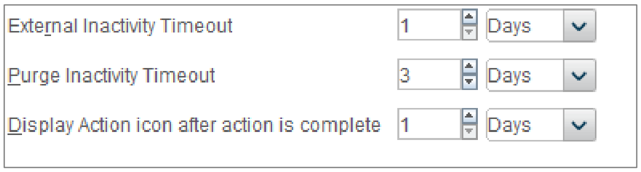
To yield significant action status values:

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

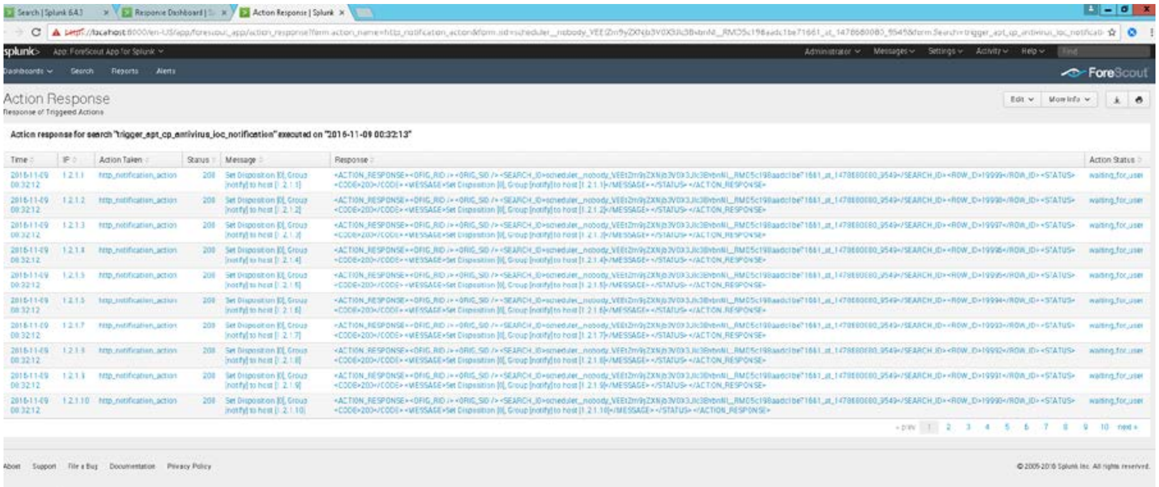
In other situations, error status values are returned.

The following action status values are reported by CounterACT.

| Value | Description |
|---|---|
| **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. |

| Value | Description |
|---|---|
| **No Status** | No status can be reported for one of the following reasons:<br>▪ No active policy detects the relevant Splunk Last Alert property, or applies the requested action.<br>▪ The endpoint has been deleted from CounterACT.<br>▪ Even though the IP address of the endpoint is within CounterACT's network scope, the endpoint has not been detected by CounterACT.<br>▪ Scheduled CounterACT data purges clear action data before reports are generated.<br><br>External Inactivity Timeout 1 Days<br>Purge Inactivity Timeout 3 Days<br>Display Action icon after action is complete 1 Days |
| **Invalid** | ▪ The endpoint IP is outside the network scope defined in CounterACT.<br>▪ An unspecified internal error occurred. |

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



Search | Splunk 6.4.1
Response Dashboard | S
Action Response | Splunk
https://localhost:8000/en-US/app/forescout_app/action_response?form.action_name=http_notification_action&form.sid=scheduler__nobody_VEE1Zm9pZXNjb3V0X3Jlc3BvbnNl__RMD5c198aadc1be71661_at_1478680080_9549&form.search=trigger_apt_cp_antivirus_ioc_notification
splunk>
App: ForeScout App for Splunk
Administrator
Messages
Settings
Activity
Help
Find
Dashboards
Search
Reports
Alerts
ForeScout
Edit
More Info

Action Response

Response of Triggeed Actions

Action response for search "trigger_apt_cp_antivirus_ioc_notification" executed on "2016-11-09 00:32:13"

| Time | IP | Action Taken | Status | Message | Response | Action Status |
|---|---|---|---|---|---|---|
| 2016-11-09 00:32:12 | 1.2.1.1 | http_notification_action | 200 | Set Disposition [0], Group [notify] to host [1.2.1.1] | <ACTION_RESPONSE><ORIG_RID /><ORIG_SID /><SEARCH_ID>scheduler__nobody_VEE1Zm9pZXNjb3V0X3Jlc3BvbnNl__RMD5c198aadc1be71661_at_1478680080_9549</SEARCH_ID><ROW_ID>19999</ROW_ID><STATUS><CODE>200</CODE><MESSAGE>Set Disposition [0], Group [notify] to host [1.2.1.1]</MESSAGE></STATUS></ACTION_RESPONSE> | waiting_for_user |
| 2016-11-09 00:32:12 | 1.2.1.2 | http_notification_action | 200 | Set Disposition [0], Group [notify] to host [1.2.1.2] | <ACTION_RESPONSE><ORIG_RID /><ORIG_SID /><SEARCH_ID>scheduler__nobody_VEE1Zm9pZXNjb3V0X3Jlc3BvbnNl__RMD5c198aadc1be71661_at_1478680080_9549</SEARCH_ID><ROW_ID>19998</ROW_ID><STATUS><CODE>200</CODE><MESSAGE>Set Disposition [0], Group [notify] to host [1.2.1.2]</MESSAGE></STATUS></ACTION_RESPONSE> | waiting_for_user |
| 2016-11-09 00:32:12 | 1.2.1.3 | http_notification_action | 200 | Set Disposition [0], Group [notify] to host [1.2.1.3] | <ACTION_RESPONSE><ORIG_RID /><ORIG_SID /><SEARCH_ID>scheduler__nobody_VEE1Zm9pZXNjb3V0X3Jlc3BvbnNl__RMD5c198aadc1be71661_at_1478680080_9549</SEARCH_ID><ROW_ID>19997</ROW_ID><STATUS><CODE>200</CODE><MESSAGE>Set Disposition [0], Group [notify] to host [1.2.1.3]</MESSAGE></STATUS></ACTION_RESPONSE> | waiting_for_user |
| 2016-11-09 00:32:12 | 1.2.1.4 | http_notification_action | 200 | Set Disposition [0], Group [notify] to host [1.2.1.4] | <ACTION_RESPONSE><ORIG_RID /><ORIG_SID /><SEARCH_ID>scheduler__nobody_VEE1Zm9pZXNjb3V0X3Jlc3BvbnNl__RMD5c198aadc1be71661_at_1478680080_9549</SEARCH_ID><ROW_ID>19996</ROW_ID><STATUS><CODE>200</CODE><MESSAGE>Set Disposition [0], Group [notify] to host [1.2.1.4]</MESSAGE></STATUS></ACTION_RESPONSE> | waiting_for_user |
| 2016-11-09 00:32:12 | 1.2.1.5 | http_notification_action | 200 | Set Disposition [0], Group [notify] to host [1.2.1.5] | <ACTION_RESPONSE><ORIG_RID /><ORIG_SID /><SEARCH_ID>scheduler__nobody_VEE1Zm9pZXNjb3V0X3Jlc3BvbnNl__RMD5c198aadc1be71661_at_1478680080_9549</SEARCH_ID><ROW_ID>19995</ROW_ID><STATUS><CODE>200</CODE><MESSAGE>Set Disposition [0], Group [notify] to host [1.2.1.5]</MESSAGE></STATUS></ACTION_RESPONSE> | waiting_for_user |
| 2016-11-09 00:32:12 | 1.2.1.6 | http_notification_action | 200 | Set Disposition [0], Group [notify] to host [1.2.1.6] | <ACTION_RESPONSE><ORIG_RID /><ORIG_SID /><SEARCH_ID>scheduler__nobody_VEE1Zm9pZXNjb3V0X3Jlc3BvbnNl__RMD5c198aadc1be71661_at_1478680080_9549</SEARCH_ID><ROW_ID>19994</ROW_ID><STATUS><CODE>200</CODE><MESSAGE>Set Disposition [0], Group [notify] to host [1.2.1.6]</MESSAGE></STATUS></ACTION_RESPONSE> | waiting_for_user |
| 2016-11-09 00:32:12 | 1.2.1.7 | http_notification_action | 200 | Set Disposition [0], Group [notify] to host [1.2.1.7] | <ACTION_RESPONSE><ORIG_RID /><ORIG_SID /><SEARCH_ID>scheduler__nobody_VEE1Zm9pZXNjb3V0X3Jlc3BvbnNl__RMD5c198aadc1be71661_at_1478680080_9549</SEARCH_ID><ROW_ID>19993</ROW_ID><STATUS><CODE>200</CODE><MESSAGE>Set Disposition [0], Group [notify] to host [1.2.1.7]</MESSAGE></STATUS></ACTION_RESPONSE> | waiting_for_user |
| 2016-11-09 00:32:12 | 1.2.1.8 | http_notification_action | 200 | Set Disposition [0], Group [notify] to host [1.2.1.8] | <ACTION_RESPONSE><ORIG_RID /><ORIG_SID /><SEARCH_ID>scheduler__nobody_VEE1Zm9pZXNjb3V0X3Jlc3BvbnNl__RMD5c198aadc1be71661_at_1478680080_9549</SEARCH_ID><ROW_ID>19992</ROW_ID><STATUS><CODE>200</CODE><MESSAGE>Set Disposition [0], Group [notify] to host [1.2.1.8]</MESSAGE></STATUS></ACTION_RESPONSE> | waiting_for_user |
| 2016-11-09 00:32:12 | 1.2.1.9 | http_notification_action | 200 | Set Disposition [0], Group [notify] to host [1.2.1.9] | <ACTION_RESPONSE><ORIG_RID /><ORIG_SID /><SEARCH_ID>scheduler__nobody_VEE1Zm9pZXNjb3V0X3Jlc3BvbnNl__RMD5c198aadc1be71661_at_1478680080_9549</SEARCH_ID><ROW_ID>19991</ROW_ID><STATUS><CODE>200</CODE><MESSAGE>Set Disposition [0], Group [notify] to host [1.2.1.9]</MESSAGE></STATUS></ACTION_RESPONSE> | waiting_for_user |
| 2016-11-09 00:32:12 | 1.2.1.10 | http_notification_action | 200 | Set Disposition [0], Group [notify] to host [1.2.1.10] | <ACTION_RESPONSE><ORIG_RID /><ORIG_SID /><SEARCH_ID>scheduler__nobody_VEE1Zm9pZXNjb3V0X3Jlc3BvbnNl__RMD5c198aadc1be71661_at_1478680080_9549</SEARCH_ID><ROW_ID>19990</ROW_ID><STATUS><CODE>200</CODE><MESSAGE>Set Disposition [0], Group [notify] to host [1.2.1.10]</MESSAGE></STATUS></ACTION_RESPONSE> | waiting_for_user |

« prev 1 2 3 4 5 6 7 8 9 10 next »
About
Support
File a Bug
Documentation
Privacy Policy
© 2005-2016 Splunk Inc. All rights reserved.

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

Note that:

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

# Targeting Endpoints in Alerts Sent to CounterACT

A list of actions provided by CounterACT are specified in the Splunk search or manually added by the Splunk user and triggered. The alert messages sent to CounterACT must reference a specified endpoint. Typically CounterACT acts in response to the Splunk alert message by applying the requested action on the endpoint. IP address is used to identify an 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 Splunk's CIM (Common Information Model) tag. When IP address information is in result fields not recognized by CounterACT, use the following command in your Splunk 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.

For Compatibility with CIM Data Models, refer to Appendix C.

# Best Practices for Scheduling Saved Searches

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

- Configure offsets in the Cron Schedule parameter.

All Cron expressions are evaluated based on an internal clock maintained by the Splunk framework. When searches are configured with a simple time period expression in the Cron interval, all searches with the same interval tend to be launched nearly simultaneously based on the internal clock.

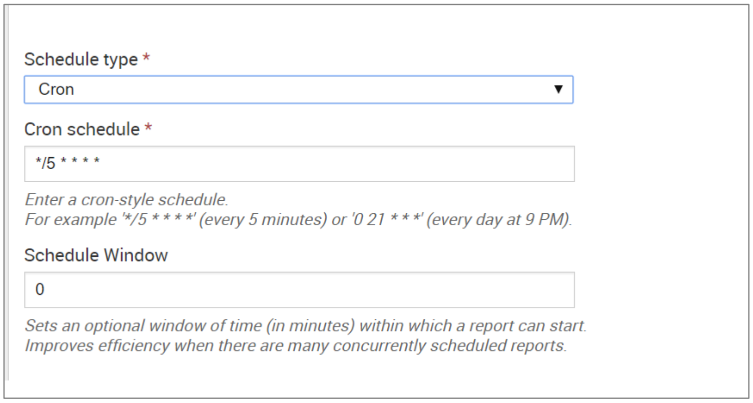
It is recommended to configure Cron expressions that offset the start of search launch in relation to the internal clock. For example, the following expression configures the search to repeat every 5 minutes, but delays search launch by 3 minutes relative to the internal clock.

```
3-59/5 * * * *
```

  - The repeat interval should exceed evaluation time. For example, if the action script attached to a search times out after 10 minutes, the search should repeat at a greater interval than 10 minutes.

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

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



Schedule type *

Cron

Cron schedule *

*/5 * * * *

*Enter a cron-style schedule.*
*For example '*/5 * * * *' (every 5 minutes) or '0 21 * * *' (every day at 9 PM).*

Schedule Window

0

*Sets an optional window of time (in minutes) within which a report can start.*
*Improves efficiency when there are many concurrently scheduled reports.*

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

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

# Working with Dashboards

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

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

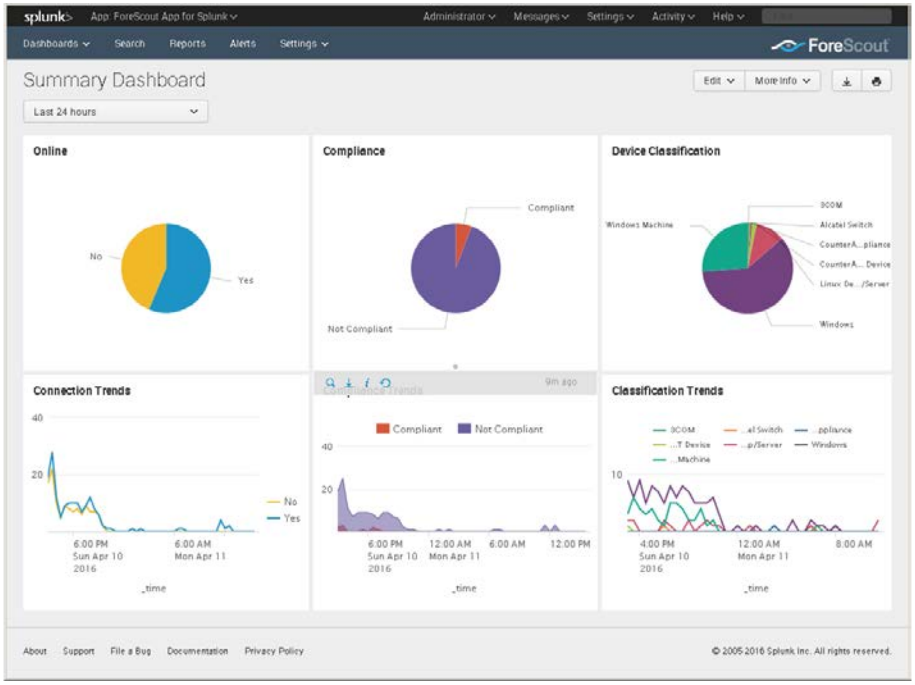
You can modify these standard dashboards, or create custom dashboards or graphs.

When working with dashboards:

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

## Summary Dashboard

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



### Online

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

### Connection Trends

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

### Compliance

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

### Compliance Trends

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

### Device Classification

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

### Classification Trends

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

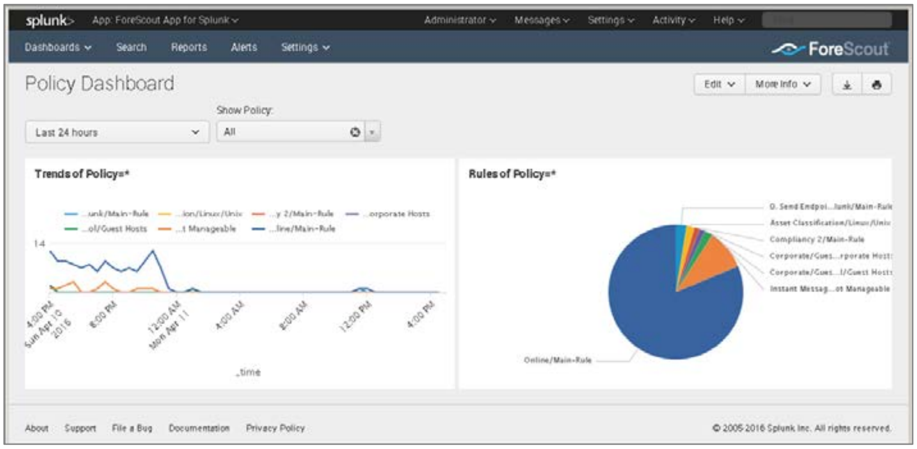
## CounterACT Policy Dashboard

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

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

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

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



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

## Network Insight and Discovery Dashboard

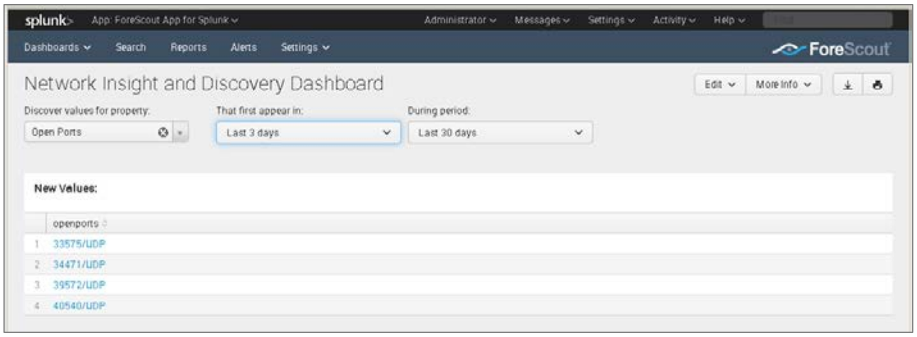
The Network Insight and Discovery dashboard tracks changes in a core set of CounterACT host properties. Use this dashboard to identify anomalous behavior and significant changes in the users, processes, applications, and other metrics associated with endpoints.

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

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

| | |
|---|---|
| **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**.



Network Insight and Discovery Dashboard

Discover values for property: Open Ports

That first appear in: Last 3 days

During period: Last 30 days

New Values:

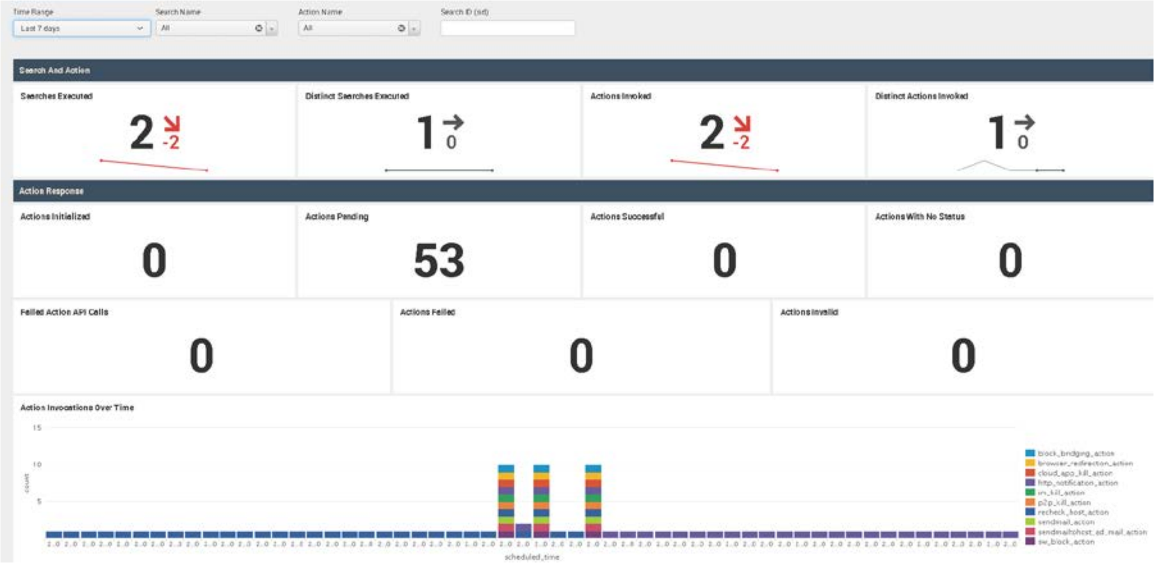
|  | openports |
|---|---|
| 1 | 33575/UDP |
| 2 | 34471/UDP |
| 3 | 39572/UDP |
| 4 | 40540/UDP |

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

## Modular Action Center Dashboard

The Modular Action Center dashboard provides the detailed analysis of Adaptive Response Framework Modular Actions executed by CounterACT for incidents in Splunk Enterprise Security. Refer to CounterACT Integration to Support Adaptive Response CounterACT Workflow for Adaptive Response.



Time Range: Last 7 days
Search Name: All
Action Name: All
Search ID (sid):

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

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

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

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

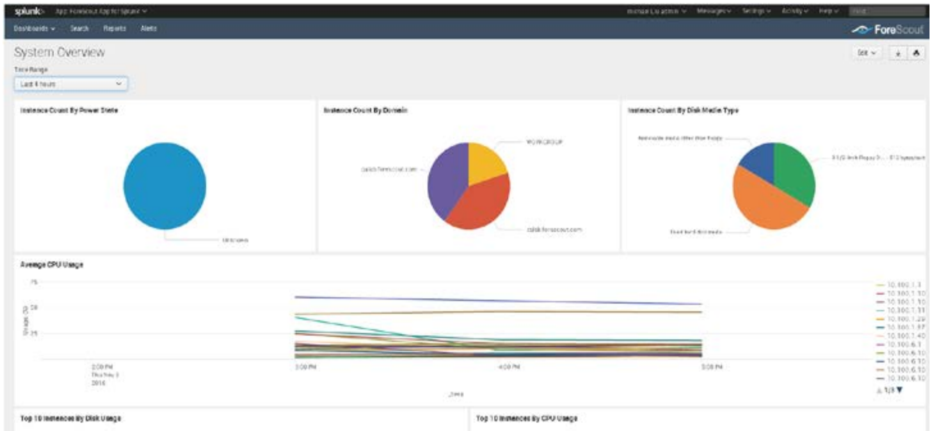
- **Actions Initialized** - Displays the count of Alert Actions for which asynchronous response is received from Counter ACT to Splunk with status “init”.
- **Actions Pending** - Displays the count of Alert Actions for which asynchronous response is received from Counter ACT to Splunk with status “waiting_for_user”.
- **Actions Successful** - Displays the count of Alert Actions for which asynchronous response is received from Counter ACT to Splunk with status “success”.

- **Actions with No Status** - Displays the count of Alert Actions for which asynchronous response is received from Counter ACT to Splunk with status “no_status”.
- **Failed Action API Calls** - Displays the count of Alert Actions for which the synchronous response of CounterACT API calls was received with error and the status code was not 200.
- **Actions Failed** - This panel shows the count of Alert Actions for which asynchronous response is received from Counter ACT to Splunk with status “failure”.
- **Actions Invalid** - This panel shows the count of Alert Actions for which asynchronous response is received from Counter ACT to Splunk with status “invalid”.

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

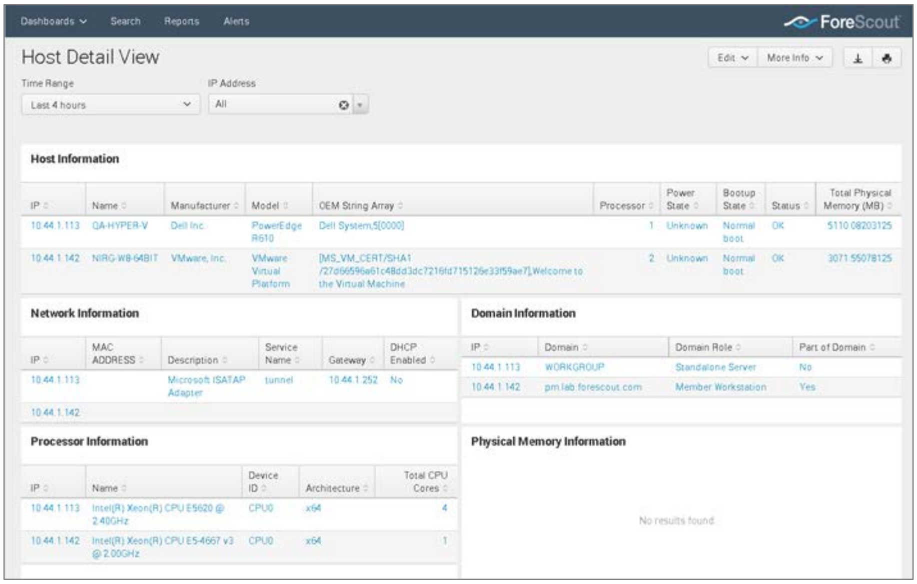
## System Overview Dashboard

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



## Host Detail View Dashboard

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



Host Detail View

Time Range: Last 4 hours

IP Address: All

**Host Information**

| IP | Name | Manufacturer | Model | OEM String Array | Processor | Power State | Bootup State | Status | Total Physical Memory (MB) |
|---|---|---|---|---|---|---|---|---|---|
| 10.44.1.113 | QA-HYPER-V | Dell Inc. | PowerEdge R610 | Dell System,5[0000] | 1 | Unknown | Normal boot | OK | 5110.08203125 |
| 10.44.1.142 | NIRG-WB-64BIT | VMware, Inc. | VMware Virtual Platform | [MS_VM_CERT/SHA1 /27d66596a61c48dd3dc7216fd715126e33f59ae7],Welcome to the Virtual Machine | 2 | Unknown | Normal boot | OK | 3071.55078125 |

**Network Information**

| IP | MAC ADDRESS | Description | Service Name | Gateway | DHCP Enabled |
|---|---|---|---|---|---|
| 10.44.1.113 | | Microsoft ISATAP Adapter | tunnel | 10.44.1.252 | No |
| 10.44.1.142 | | | | | |

**Domain Information**

| IP | Domain | Domain Role | Part of Domain |
|---|---|---|---|
| 10.44.1.113 | WORKGROUP | Standalone Server | No |
| 10.44.1.142 | pm.lab.forescout.com | Member Workstation | Yes |

**Processor Information**

| IP | Name | Device ID | Architecture | Total CPU Cores |
|---|---|---|---|---|
| 10.44.1.113 | Intel(R) Xeon(R) CPU E5620 @ 2.40GHz | CPU0 | x64 | 4 |
| 10.44.1.142 | Intel(R) Xeon(R) CPU E5-4667 v3 @ 2.00GHz | CPU0 | x64 | 1 |

**Physical Memory Information**

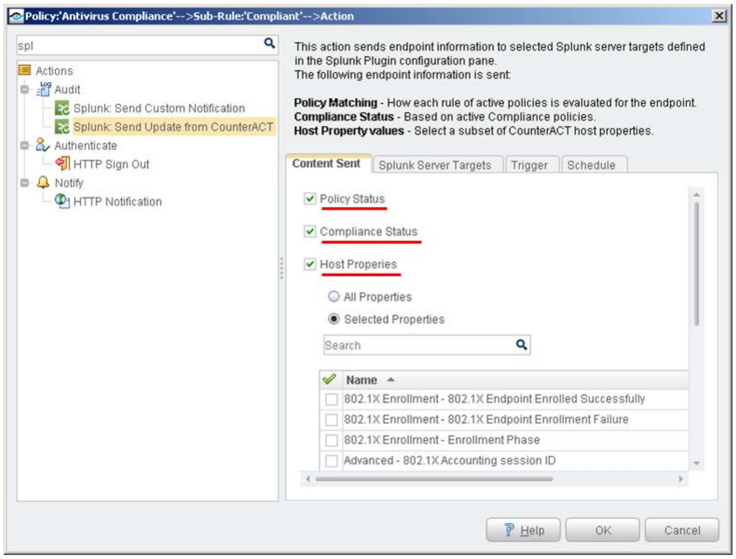
No results found.

# 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.



Policy:'Antivirus Compliance'-->Sub-Rule:'Compliant'-->Action

spl

- Actions
  - Audit
    - Splunk: Send Custom Notification
    - Splunk: Send Update from CounterACT
  - Authenticate
    - HTTP Sign Out
  - Notify
    - HTTP Notification

This action sends endpoint information to selected Splunk server targets defined in the Splunk Plugin 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.

Content Sent | Splunk Server Targets | Trigger | Schedule

☑ Policy Status

☑ Compliance Status

☑ Host Properies

○ All Properties

● Selected Properties

Search

| ✓ | Name |
|---|---|
| □ | 802.1X Enrollment - 802.1X Endpoint Enrolled Successfully |
| □ | 802.1X Enrollment - 802.1X Endpoint Enrollment Failure |
| □ | 802.1X Enrollment - Enrollment Phase |
| □ | Advanced - 802.1X Accounting session ID |

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:<br>▪ Events that report policy information contain the pair **`ctupdate:policyinfo`**.<br>▪ Events that report compliance and host properties contain the pair **`ctupdate:hostinfo`**.<br>▪ 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 CounterACT Splunk Module Configuration Guide for more details of action configuration options.

## Considerations When Working with CounterACT Events in Splunk

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

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

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

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

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

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

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

# Mapping CounterACT Data to the CIM Model

This section describes mapping of CounterACT host properties to the CIM model.

## Certificates

***Tags:*** certificate

Splunk Reference:
http://docs.splunk.com/Documentation/CIM/4.5.0/User/Certificates

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

## Compute_Inventory: CPU

***Tags:*** cpu

Splunk Reference:
http://docs.splunk.com/Documentation/CIM/4.5.0/User/ComputeInventory

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

## Compute_Inventory: Network

***Tags:*** network

Splunk Reference:
http://docs.splunk.com/Documentation/CIM/4.5.0/User/ComputeInventory

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

## Compute_Inventory: Memory

***Tags:*** memory

Splunk Reference:
http://docs.splunk.com/Documentation/CIM/4.5.0/User/ComputeInventory

| Data Model Field | CounterAct Field Tag |
|---|---|
| mem | Capacity |

## Compute_Inventory: Storage

***Tags:*** storage

Splunk Reference:
http://docs.splunk.com/Documentation/CIM/4.5.0/User/ComputeInventory

| Data Model Field | CounterAct Field Tag |
|---|---|
| storage | Size__Megabytes_ |
| storage_free | Free_Space__Megabytes_ |

## Blocked_Malware

***Tags:*** malware,attack

Splunk Reference: http://docs.splunk.com/Documentation/CIM/4.5.0/User/Malware

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

## Subset of Core Properties

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

| CounterACT Property (Name and Tag) | Splunk Tag | Model |
|---|---|---|
| IP Address {ip} | dest, dest_ip | All |
| Windows Processes Running {process_no_ext}<br>Linux Processes Running {linux_process_running}<br>Macintosh Processes Running {mac_process_running} | process | Application State |
| User {user} | user | All |

| CounterACT Property (Name and Tag) | Splunk Tag | Model |
|---|---|---|
| Windows Services Running {service}<br>Windows Services Installed {service_installed} | service | Application State / Services |
| NetBIO Domain {nbtdomain} | dest_nt_domain | Malware |
| Malicious Event {malic} | ids_type=host<br>category, signature | Intrusion Detection |
| Appliance | dvc, dvc_ip | Intrusion Detection |

# Appendix B: Tuning Data Traffic

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

Below are the default rate limiting parameters:

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

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

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

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

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

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

```
</SPLUNK_ALERTS>
```

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

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

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

# Appendix C - Compatibility with CIM Data Models

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

*CIM Model:* Certificates
*eventtype:* ct_certificate
*Search:* source=counterACT sourcetype=fsctcenter* ctupdate=hostinfo hwi_certificate=*
*tags:* certificate
*Splunk Reference*:
http://docs.splunk.com/Documentation/CIM/4.5.0/User/Certificates

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

*CIM Model:* Compute_Inventory: CPU
*eventtype:* ct_hostinfo_cpu
*Search:* source=counterACT sourcetype=fsctcenter* ctupdate=hostinfo hwi_processor=*
*tags:* cpu
*Splunk Reference:*
http://docs.splunk.com/Documentation/CIM/4.5.0/User/ComputeInventory

| **Data Model Field** | **CounterAct Field** |
|---|---|
| cpu_cores | Number_Of_Cores |

| | |
|---|---|
| family | Family |
| cpu_load_percent | Load_Percentage |

**CIM Model:** Compute_Inventory: Network
**eventtype:** ct_hostinfo_network
**Search**: source=counterACT sourcetype=fsctcenter* ctupdate=hostinfo hwi_network_adapters=*
**tags:** network
**Splunk Reference**:
http://docs.splunk.com/Documentation/CIM/4.5.0/User/ComputeInventory

| **Data Model Field** | **CounterAct Field** |
|---|---|
| ip | IP_Address |
| dns | DNS_HostName |
| mac | MAC_Address |

**CIM Model:** Compute_Inventory: Memory
**eventtype:** ct_hostinfo_memory
**Search**: source=counterACT sourcetype=fsctcenter* ctupdate=hostinfo hwi_physical_memory=*
**tags:** memory
**Splunk Reference**:
http://docs.splunk.com/Documentation/CIM/4.5.0/User/ComputeInventory

| **Data Model Field** | **Mapped CounterAct Field** |
|---|---|
| mem | Capacity |

**CIM Model:** Compute_Inventory: Storage
**eventtype:** ct_hostinfo_storage
**Search**: source=counterACT sourcetype=fsctcenter* ctupdate=hostinfo hwi_disk=*
**tags:** storage
**Splunk Reference**:
http://docs.splunk.com/Documentation/CIM/4.5.0/User/ComputeInventory

| **Data Model Field** | **CounterAct Field** |
|---|---|
| storage | Size__Megabytes_ |
| **storage_free** | Free_Space__Megabytes_ |

**CIM Model:** Blocked_Malware
**eventtype:** ct_malware
**Search**: source=counterACT sourcetype=fsctcenter* (pan_apt_detected_ioc OR atc_detected_ioc OR fireeye_detected_ioc OR apt_cp_antivirus_ioc)
**tags:** malware,attack
**Splunk Reference**:
http://docs.splunk.com/Documentation/CIM/4.5.0/User/Malware

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

# Legal Notice

These products are based on software developed by ForeScout. The products described in this document are protected by U.S. patents #6,363,489, #8,254,286, #8,590,004, #8,639,800 and #9,027,079 and may be protected by other U.S. patents and foreign patents.

Redistribution and use in source and binary forms are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials and other materials related to such distribution and use acknowledge that the software was developed by ForeScout.

Unless there is a valid written agreement signed by you and ForeScout that governs the below ForeScout products and services:

- If you have purchased any ForeScout products, your use of such products is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you have purchased any ForeScout support service (“ActiveCare”), your use of ActiveCare is subject to your acceptance of the terms set forth at http://www.forescout.com/activecare-maintenance-and-support-policy/;
- If you have purchased any ForeScout Professional Services, the provision of such services is subject to your acceptance of the terms set forth at http://www.forescout.com/professional-services-agreement/;
- If you are evaluating ForeScout’s products, your evaluation is subject to your acceptance of the applicable terms set forth below:
  - If you have requested a General Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/evaluation-license/.
  - If you have requested an Early Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/early-availability-agreement/.
  - If you have requested a Beta Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/beta-test-agreement/.
  - If you have purchased any ForeScout Not For Resale licenses, such license is subject to your acceptance of the terms set forth at http://www.forescout.com/nfr-license/.

Send comments and questions about this document to: documentation@forescout.com

2016-11-10 17:58