Forescout

App & Add-on for Splunk

How-to Guide

Version 2.9.1

Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

https://www.forescout.com/support/

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the Resources page on the Forescout website for additional technical documentation: https://www.forescout.com/company/resources/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at https://www.forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2019-12-20 08:13

Table of Contents

About Splunk Integration **6**
Support for Splunk Adaptive Response 7

What's New **7**
Support for IPv6 7

Use Cases **8**
Data Mining and Trend Analysis of Forescout Platform Data 8
Continuous Posture Tracking Based on a Broad Range of Forescout Platform Data 8
Adaptive Response Actions Triggered by Splunk Data Correlation 9
Additional Splunk Documentation 9

About Forescout App and Add-ons for Splunk **9**
Forescout App for Splunk 10
Forescout Technology Add-on for Splunk 10
Forescout Adaptive Response Add-on for Splunk 10

About Forescout eyeExtend for Splunk **11**
Support for Batch Messaging 11

Requirements **12**
External Systems Connections 12
Install the Forescout Platform 13
Install Forescout eyeExtend for Splunk 13
Splunk Requirements 13
Forescout App for Splunk Enterprise (on-premise) Communication Requirements 14
About Certificates for Secured Messaging 15
Secured Messaging from Forescout Adaptive Response Add-On 15

Installation and Configuration **15**
Create a Data Index for the Forescout Platform 16
Obtain an Authorization Token 16
Install the Forescout Apps for Splunk 19
Upgrade to eyeExtend for Splunk 2.9.1 and Foresout Apps for Splunk 2.9.1 .. 19
Install the Forescout Apps for Splunk 20
Post-Installation Check for Adaptive Response Add-on in Splunk Cloud Deployment 22
Set Up the Forescout Technology Add-on for Splunk 22
Splunk Roles for the Forescout Platform 24

Forescout Platform Workflow for Adaptive Response **24**
Correlation Searches and Saved Searches 26
Alerts 28

Configuring your Alerts 29
How to create an Alert with Trigger Actions 31
Customizing your own Alerts 33
Forescout Platform Response to Alert Messages 34
Targeting Devices in Alerts Sent to the Forescout Platform 36
Best Practices for Scheduling Saved Searches 37

Working with Dashboards 38
Summary Dashboard 39
Forescout Policy Dashboard 40
Network Insight and Discovery Dashboard 40
Response Dashboard 41
System Overview Dashboard 43
Host Detail View Dashboard 43

Appendix A: Distributed Deployment 44
Forwarding Event Data from the Forescout Platform to Splunk 45
Possible Communication Channels 45
Forward Event Data to On-premise Distributed Splunk Deployments 45
Forward Event Data to Splunk Cloud Deployments 46

Appendix B: Splunk Cloud Deployments 47
Splunk Cloud vs Splunk Enterprise 47
Deploying Splunk Cloud 48
Types of Splunk Clouds 48
Indexing Requirements for Splunk Cloud Instance 48
Self-service Splunk Cloud 49
REST API 49
HTTP Event Collector 49
Managed Splunk Cloud 52
REST API 53
HTTP Event Collector 53
Set up Secure Connection Messaging to the Splunk Cloud 56
Set up the Forescout Technology Add-on for Splunk Cloud 57
Accessing Logs within Splunk Cloud Instance 58

Appendix C: Working with Forescout Platform Data in Splunk 59
About Forescout Platform Data Events 59
Considerations When Working with Forescout Platform Events in Splunk 61
Mapping Forescout Platform Data to the CIM Model 61
Certificates 61
Compute_Inventory: CPU 62
Compute_Inventory: Network 62
Compute_Inventory: Memory 62
Compute_Inventory: Storage 62
Blocked_Malware 63
Subset of Core Properties 63

Appendix D: System Certificate for Web Portal 64

Appendix E: Default Rate Limiting 66

Appendix F: Compatibility with CIM Data Models 67

CIM Model: Certificates 67
CIM Model: Compute_Inventory: CPU 68
CIM Model: Compute_Inventory: Network 68
CIM Model: Compute_Inventory: Memory 68
CIM Model: Compute_Inventory: Storage 69
CIM Model: Blocked_Malware 69

About Splunk Integration

Splunk® Enterprise data analytics help organizations:

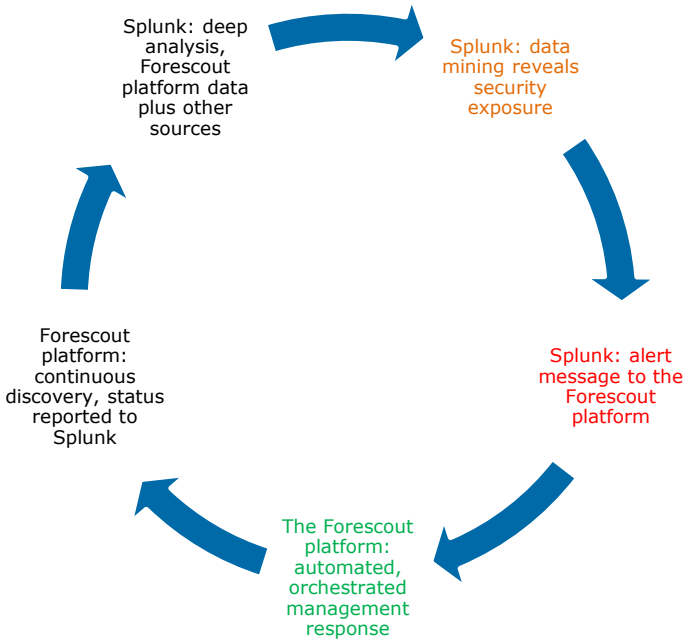
- Leverage the data that their infrastructure and security tools provide
- Understand their security posture
- Pinpoint and investigate anomalies
- Create alerts and reports

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

By combining the Forescout platform's dynamic device visibility, access, and security capabilities with Splunk Enterprise's data mining capabilities, security managers can:

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

This integration is fully bi-directional. The Forescout platform sends host property, policy, and event information to Splunk, Splunk sends alerts and action requests to the Forescout platform, the Forescout platform responds to action requests through policy and sends action status back to Splunk.



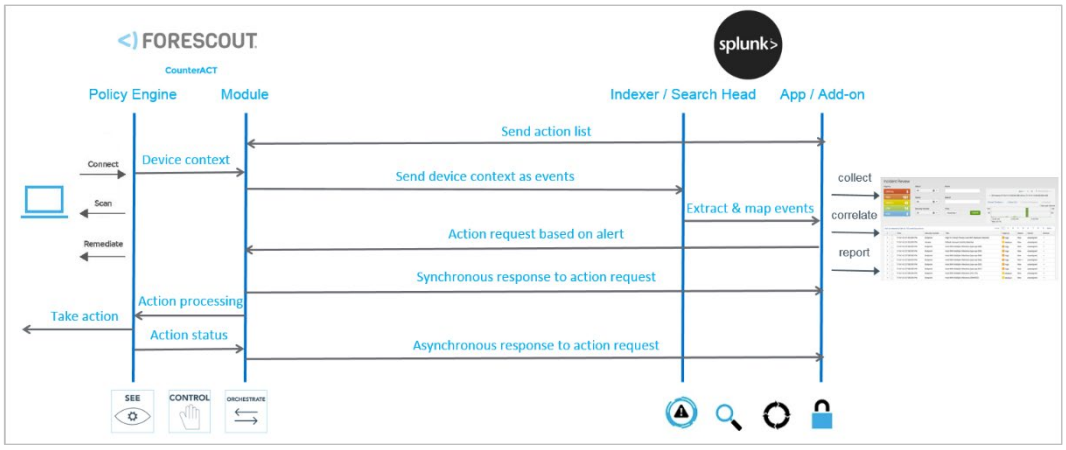
The result is enhanced threat insight, quicker incident response, automated control, and greater operational efficiency.

Support for Splunk Adaptive Response

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

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

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



What's New

This section describes what's new in Forescout eyeExtend for Splunk version 2.9.1 and Forescout Apps for Splunk version 2.9.1.

Support for IPv6

In the device configuration of Forescout eyeExtend for Splunk, IPv6 addresses are supported for HTTP targets (Event Collector and REST API) and Syslog targets (TCP and UDP).

In Forescout Apps, IPv6 addresses are supported in the CounterACT configuration of the Forescout Technology Add-on for Splunk (TA-forescout) for a standalone CounterACT® Appliance or an Enterprise Manager.

In events sent from eyeExtend for Splunk to the Splunk server, endpoints can contain IPv6 addresses or IPv6-only addresses, with or without MAC addresses.

Adaptive Response action alerts apply to endpoints with IPv6 addresses or IPv6-only addresses, with or without MAC addresses.

Refer to https://docs.splunk.com/Documentation/Splunk/7.2.4/Admin/ConfigureSplunkforIPv6 for details on how to configure Splunk for IPv6.

Use Cases

This section describes use cases supported by the Forescout Splunk App. To understand how this App helps you achieve these goals, see:

- About Forescout App and Add-ons for Splunk.
- Data Mining and Trend Analysis of Forescout Platform Data
- Continuous Posture Tracking Based on a Broad Range of Forescout Platform Data
- Adaptive Response Actions Triggered by Splunk Data Correlation

Data Mining and Trend Analysis of Forescout Platform Data

Spunk's strength is storing and indexing data over long periods of time. To complement the Forescout platform'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 Forescout Platform Data

Integration with Splunk includes a dedicated Forescout App for Splunk with custom dashboards that let you quickly monitor the current operational/security posture. The Forescout platform reports a wide range of data to Splunk, and the dashboards display real-time metrics derived from this information, such as:

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

Experienced Splunk users can customize the searches and dashboards provided with the Forescout App or they can combine Forescout platform information with other data sources in the Splunk environment.

Adaptive Response Actions Triggered by Splunk Data Correlation

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

Additional Splunk Documentation

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

https://docs.splunk.com/Documentation/Splunk/7.2.4

About Forescout App and Add-ons for Splunk

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

The Forescout has published three Apps:

- Forescout App for Splunk
- Forescout Technology Add-on for Splunk
- Forescout Adaptive Response Add-on for Splunk

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

> *Forescout eyeExtend for Splunk needs to be deployed on the CounterACT Appliance. You also need to read the* Forescout eyeExtend for Splunk Configuration Guide*.*

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

Forescout App for Splunk

The Forescout App for Splunk lets you view Forescout platform data in a dedicated, customizable Splunk dashboard. This bi-directional interaction with Splunk lets you quickly monitor the current operational/security posture.

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

Forescout Technology Add-on for Splunk

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

- ***Configurations***: The add-on presents a setup page that lets information be stored, such as the Forescout platform credentials needed to send alerts to Forescout eyeExtend for Splunk on the Forescout platform. It also displays the index name to which Forescout eyeExtend for Splunk sends its update messages.
- ***Authentication***: The add-on stores credentials entered on the setup page. These credentials are used for authentication when communicating with the Forescout platform.
- ***Field Extraction***: The add-on defines any field extraction rules needed to extract events from properties received from the Forescout platform.

Forescout Adaptive Response Add-on for Splunk

The Forescout Adaptive Response Add-on for Splunk (TA-forescout_response) consists of:

- ***Adaptive Response***: The add-on implements the Adaptive Response framework for the Forescout platform's integration with Splunk.
- ***Actions Mapping***: The add-on stores the Forescout platform actions information which is available as *Trigger Actions* in alerts.
- ***Sync Response***: This is the synchronous response sent by Forescout eyeExtend for Splunk on the Forescout platform, once it receives an alert sent by the Forescout App for Splunk. It contains information indicating if the alert was correctly received and applied to the endpoint included in the alert.
- ***Async Response***: This is the asynchronous response sent by Forescout eyeExtend for Splunk on the Forescout platform containing the outcome of the action that was executed on an endpoint because of an alert sent by the Forescout App for Splunk.

About Forescout eyeExtend for Splunk

Forescout eyeExtend for Splunk and the Forescout Apps work together to support communications between the Forescout platform and Splunk.

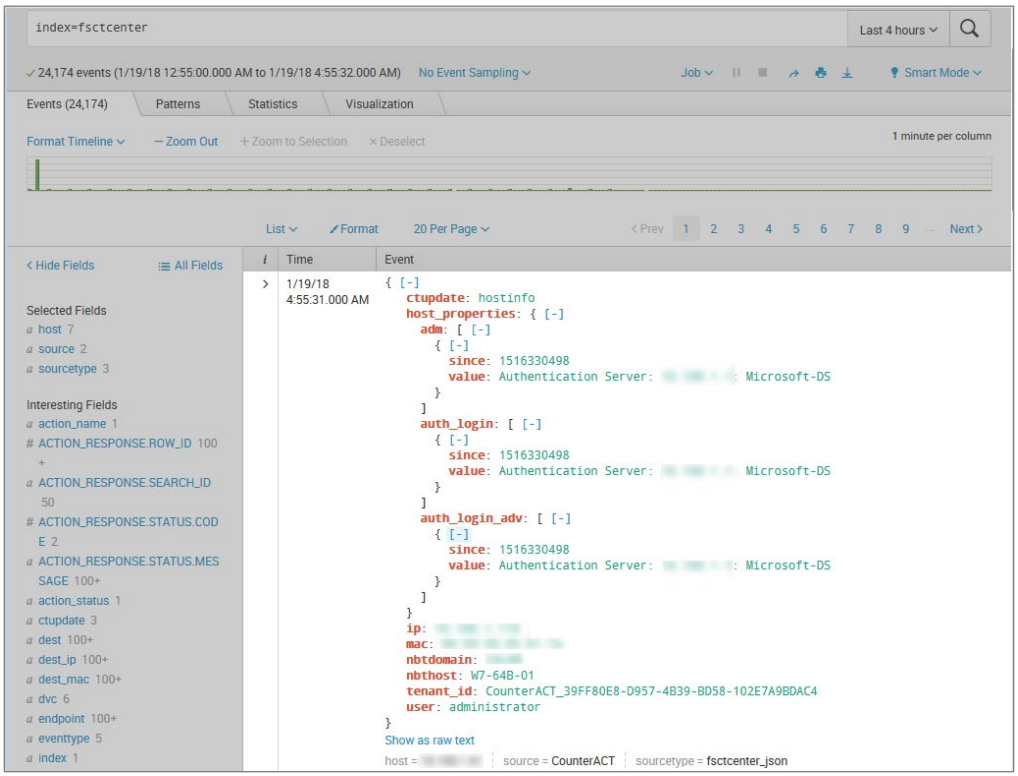
- Use Splunk search queries to search and filter information in Splunk. See Correlation Searches and Saved Searches.
- Configure to have alerts processed and have request for action messages sent from Splunk Enterprise server to Forescout eyeExtend for Splunk.
- See Alerts.

  In the Forescout platform, you can define policies that respond to alerts sent by Splunk. Refer to the *Forescout eyeExtend for Splunk Configuration Guide*.
- View data from the Forescout platform in a dedicated, customizable Splunk dashboard. See Working with Dashboards.

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

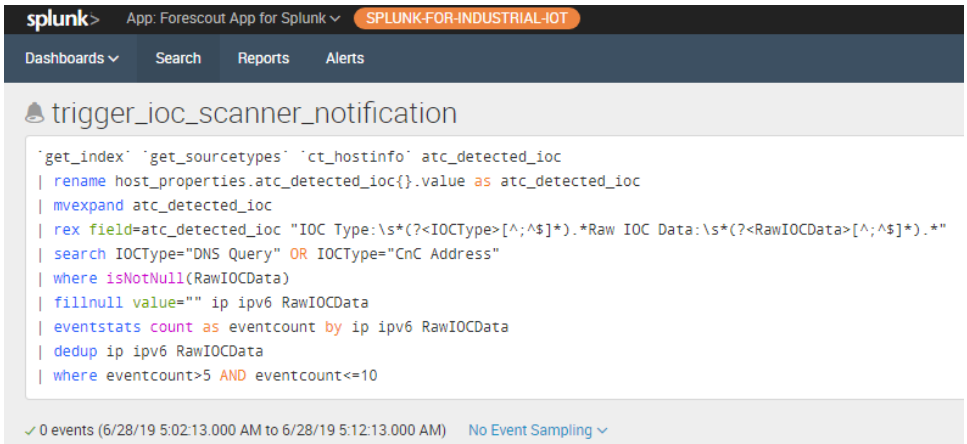
Support for Batch Messaging

Batched messages are part of Forescout eyeExtend for Splunk. The saved searches and dashboard aspect in the Forescout App for Splunk was enhanced.



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

For the relevant search, select Open in Search link. In this example, the trigger_ioc_scanner_notification search was selected.



The information that comprises the search query is displayed.

For configuring these batched messages, refer to the *Forescout eyeExtend for Splunk Configuration Guide*.

Requirements

This section describes system requirements, including:

- External Systems Connections
- Splunk Requirements
- Forescout App for Splunk Enterprise (on-premise) Communication Requirements

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

External Systems Connections

This section covers the Forescout platform-related installation and configuration.

Install the Forescout Platform

The Forescout platform is required to be installed and configured in order to get data into Splunk. Contact your Forescout representative for more details.

Install Forescout eyeExtend for Splunk

Forescout eyeExtend for Splunk is required to be installed and configured in order to get data into Splunk. Contact your Forescout representative for more details.

After installing Forescout eyeExtend for Splunk, you will need to do the following:

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

For more information on how to use Forescout eyeExtend for Splunk, refer to the *Forescout eyeExtend for Splunk Configuration Guide*.

Splunk Requirements

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

- Create an account on Splunkbase
- Splunk Enterprise version 7.0 or 7.2
- Splunk Enterprise Security version 5.2
- Common Information Model (CIM) 4.12
- For information about hardware/software vendor models and operating system versions that are validated for integration with Forescout components, refer to the Forescout Compatibility Matrix.
- Splunk Processing Capacity, refer to: https://docs.splunk.com/Documentation/Splunk/7.2.4/Capacity/Referencehardware
- Splunk System Configuration, refer to: https://docs.splunk.com/Documentation/Splunk/7.2.4/Deploy/Deploymentcharacteristics
- Splunk User Permissions, refer to: https://docs.splunk.com/Documentation/Splunk/7.2.4/Admin/Aboutusersandroles

To integrate the Forescout platform with a Splunk environment that ***does not*** run Splunk Enterprise Security, refer to the Splunk deployment guides for details:

https://docs.splunk.com/Documentation/Splunk/7.2.4/Installation/SystemRequirements

Splunk Cloud Requirements

- Splunk Cloud Enterprise version 7.2

- Splunk data integration requires a Splunk Cloud license. Refer to:

https://docs.splunk.com/Documentation/SplunkCloud/7.2.4/User/Datapolicies

For more information about Splunk Cloud, see Appendix B: Splunk Cloud Deployments.

Forescout App for Splunk Enterprise (on-premise) Communication Requirements

The integration of the Forescout platform with Splunk is based on the following data sharing/messaging interactions.

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

Communication	Recommended	Alternative
Retrieve Action Info The Forescout App for Splunk polls the Forescout platform's action_info API to retrieve a list of available actions.	REST API Default port: 443	REST API on HTTP
Ongoing Data Reporting The Forescout platform sends endpoint data to Splunk. This is the protocol used by Forescout eyeExtend for Splunk in the Forescout platform to implement the **Splunk: Send Update from CounterACT** action.	Event Collector Default port: 8088	Syslog (port 515 TCP/UDP) RESTful API HTTPS (port 8089)
Splunk Action Request ▪ Splunk sends alerts to the Forescout platform's alert API. ▪ The alert API confirms receipt of alert message (Synchronous response. See Forescout Platform Response to Alert Messages).	REST API Default port: 443	REST API on HTTP
Splunk Action Final Status The Forescout platform reports the status of actions requested by Splunk (Asynchronous response. See Forescout Platform Response to Alert Messages).	Event Collector Default port: 8088	Syslog (port 515 TCP/UDP) RESTful API HTTPS (port 8089)

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

About Certificates for Secured Messaging

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

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

Secured Messaging from Forescout Adaptive Response Add-On

The alerts forwarded by the Forescout Adaptive Response Add-On to Forescout eyeExtend for Splunk are sent over via HTTPS.

To enable HTTPS communication using Forescout eyeExtend for Splunk:

1. Operators must not use the default self-signed web-portal certificate; instead, they need to procure their own certificate. See Appendix D: System Certificate for Web Portal.
2. Once the certificates are installed on the CounterACT Appliance, the Forescout platform 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`

   Refer to the *Forescout eyeExtend for Splunk Configuration Guide* for instructions on secured messaging from Forescout eyeExtend for Splunk to Forescout Adaptive Response Add-On for Splunk.

Installation and Configuration

This section describes installation scenarios and procedures for the Forescout App and Add-ons. For installation of Forescout Splunk App and Add-ons in a distributed Splunk environment, see Appendix A: Distributed Deployment. For installation and configuration of Splunk Cloud, see Appendix B: Splunk Cloud Deployments.

Perform the following steps to work with the dashboard. For steps performed in the Console, refer to the *Forescout* eye*Extend for Splunk Configuration Guide*.

1. Review the *Forescout eyeExtend for Splunk Configuration Guide* and this *How-to Guide*.
2. Verify that Requirements are met.
3. Create an account on Splunkbase.
4. Create a Data Index for the Forescout Platform.
5. Install the Forescout Apps for Splunk.
6. Set Up the Forescout Technology Add-on for Splunk.

7. Splunk Roles for the Forescout Platform.
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.

Create a Data Index for the Forescout Platform

Follow the procedure described in the Splunk knowledge base to create an index that identifies information sent to Splunk by the Forescout platform:

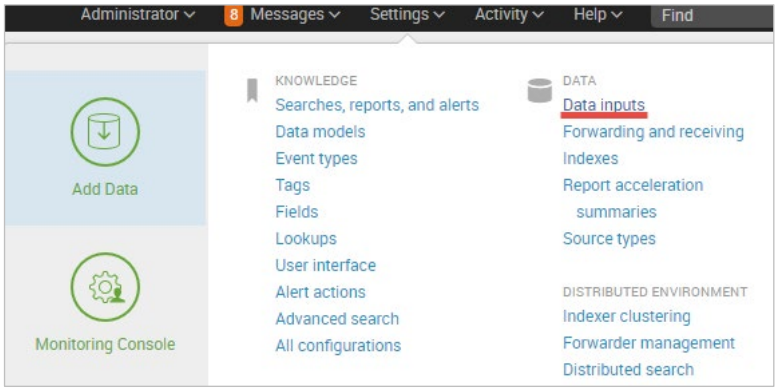
https://docs.splunk.com/Documentation/Splunk/7.2.4/Indexer/Setupmultipleindexes

Obtain an Authorization Token

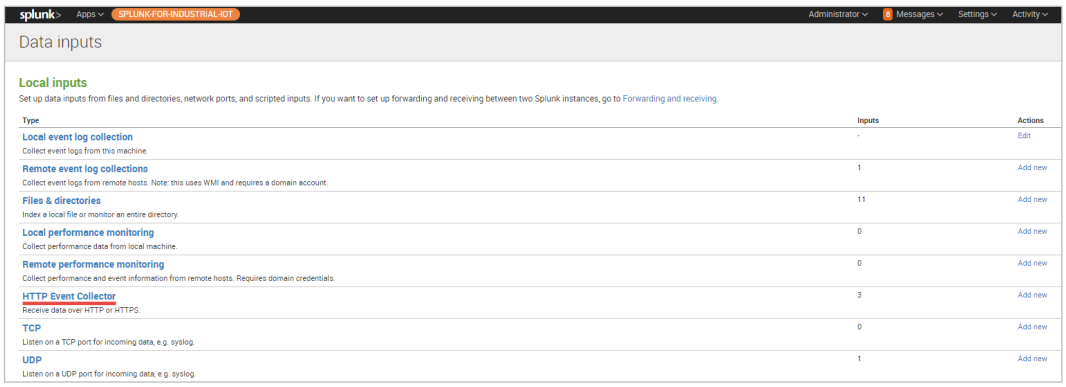
You will need to get a token value (key) from the Forescout App for Splunk so that event collectors can be created.

To obtain an authorization token to define an event collector:

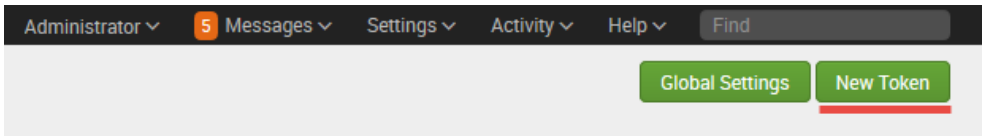
1. In the Forescout App for Splunk, select **Settings** and then select **Data inputs**.



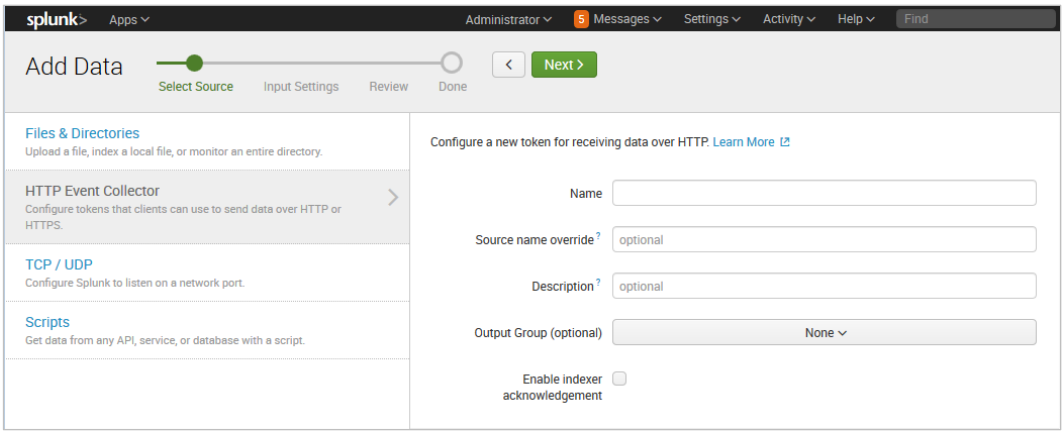
The Data Inputs page opens.



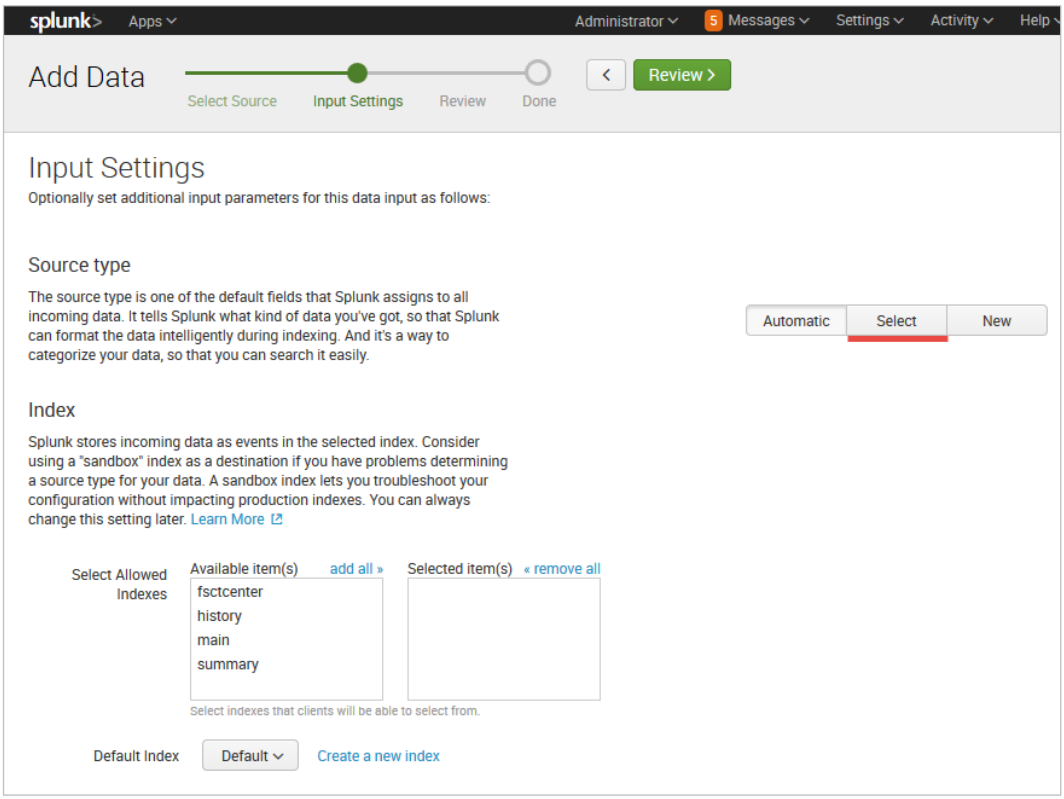
2. Select **HTTP Event Collector**.



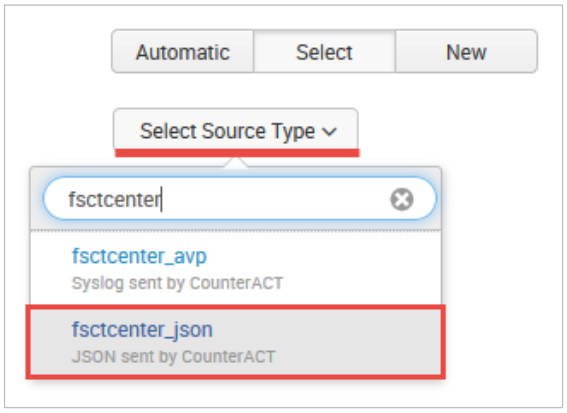
3. Select **New Token**. The Add Data page opens to the Select Source pane.



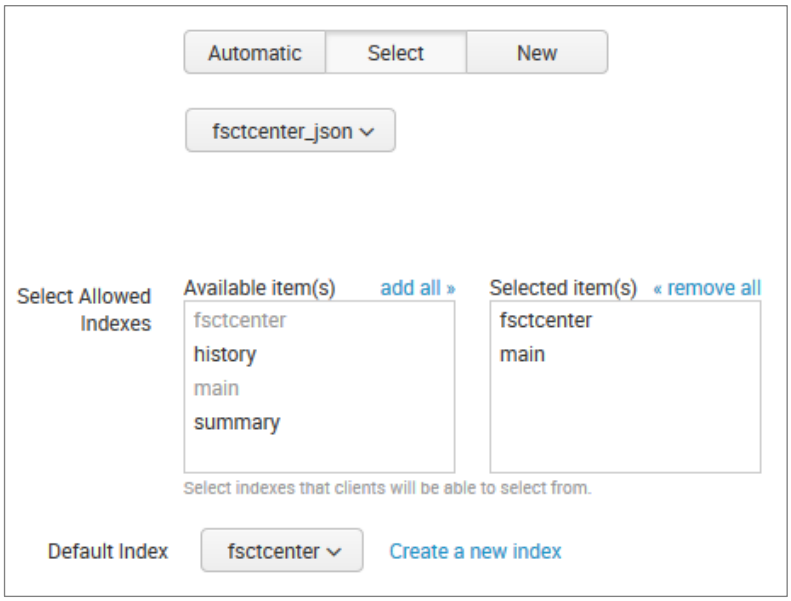
4. Enter the Name of the Event Collector and select **Next**.



5. In the Source type section, select **Select**.

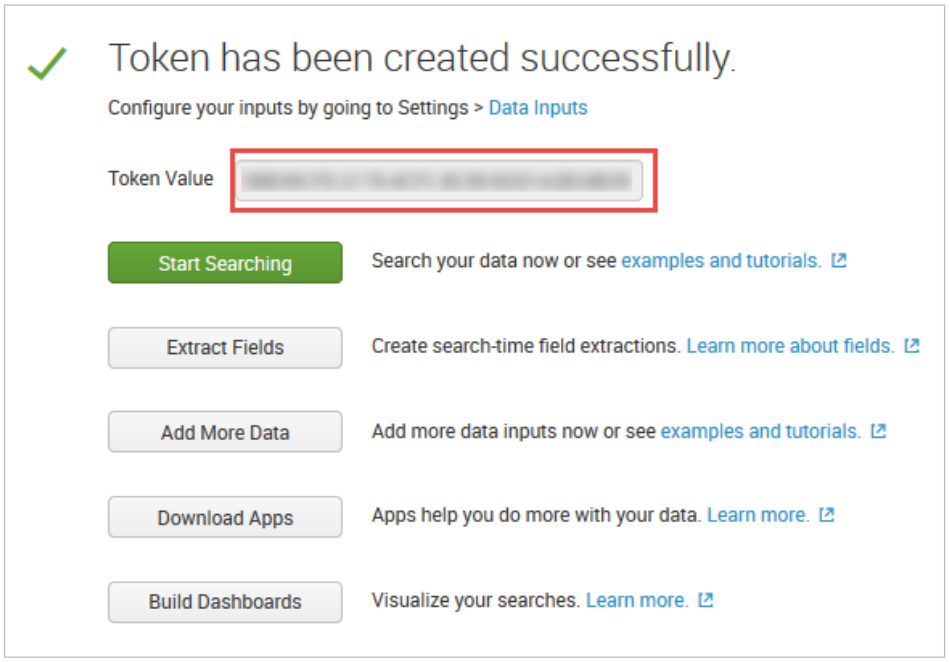


6. Select **Select Source Type** and enter *fsctcenter* in the search field. Then select **fsctcenter_json** from the drop-down menu.
7. In the Index section of the Input Settings page, select one or more allowed indexes. The default setting is *fsctcenter*.



8. At the top of the Add Data pane, select **Review**. Check your settings.

9. Select **Submit**. The new token value is created.



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

Install the Forescout Apps for Splunk

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

Upgrade to eyeExtend for Splunk 2.9.1 and Foresout Apps for Splunk 2.9.1

This section describes how to upgrade from prior versions of Forescout eyeExtend for Splunk and Forescout Apps & Add-ons for Splunk.

Before upgrading, make sure that you have Forescout eyeExtend for Splunk 2.7, 2.8, or 2.9 installed and the Forescout Apps & Add-ons for Splunk version 2.7 in working condition.

Rollback is not available for this module. If you upgrade to Forescout eyeExtend for Splunk version 2.9.1 and the module does not operate as expected, you cannot roll back to a previous release.

It is recommended you upgrade Forescout Splunk Apps and then upgrade Forescout eyeExtend for Splunk in the following sequence:

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

- Forescout App for Splunk
- Forescout Adaptive Response Add-on for Splunk

2. On Splunkbase, use **Browse More Apps** to find all three Forescout Splunk Apps version 2.9.1.
3. Select **Load an App** with the **Upgrade App** feature to upgrade them in any order.
4. After all the App and Add-ons are upgraded and configured, restart Splunk by selecting **Settings > SYSTEM > Server controls > Restart Splunk**.
5. In the Console, upgrade Forescout version 8.1. This includes upgrading Forescout eyeExtend for Splunk to version 2.9.1. Refer to the *Forescout Administration Guide* for instructions.
6. In the left pane, select **Options** and then select **Splunk**. The Splunk configuration pane opens to the Splunk Syslog Targets tab.
7. Select each of the channels and then select **Test**.
8. Select the Splunk HTTPS Targets tab.
9. Select each of the channels and then select **Test**.

   The upgrade is complete.

Install the Forescout Apps for Splunk

The Forescout App for Splunk consists of the following components.

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

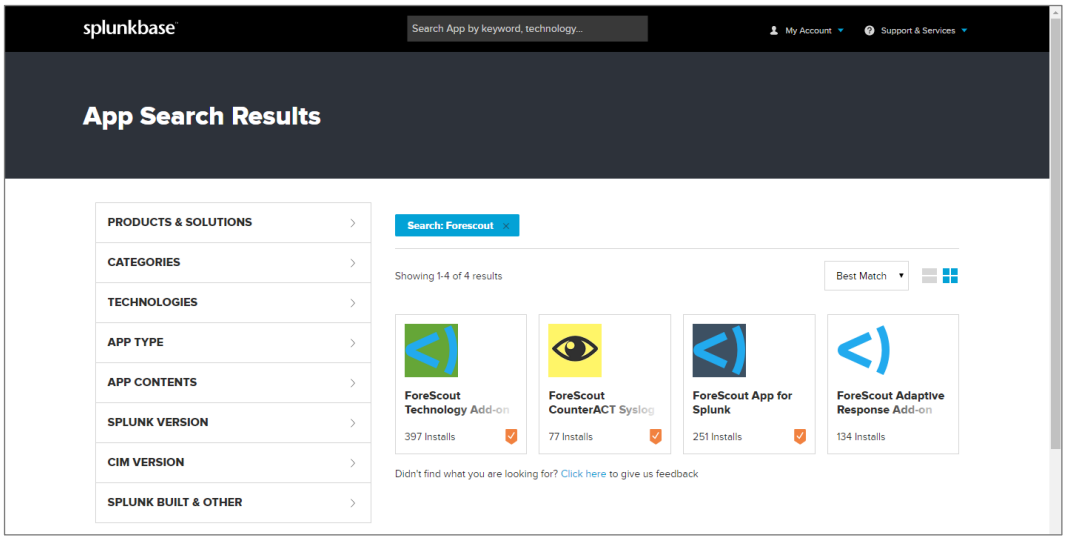
Install Order	Component	Description	File
1.	**Forescout App for Splunk (forescout_app)** **See** About Forescout App and Add-ons for Splunk	A visualization App containing dashboards to monitor endpoints using data provided by the Forescout platform.	`forescout_app.tar.gz`
2.	**Forescout Adaptive Response Add-on for Splunk (TA-forescout_response)** **See** Forescout Adaptive Response Add-on for Splunk	Supports Adaptive Response action calls to the Forescout platform.	`TA-forescout_response.tar.gz`

Install Order	Component	Description	File
3.	**Forescout Technology Add-on for Splunk (TA-forescout)** **See** Forescout Technology Add-on for Splunk	Handles data collection from the Forescout platform.	`TA-forescout.tar.gz`
4.	**Restart**	Restart the Splunk service.	N/A

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

To install and configure each App:

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



4. **Login** to the Splunk Enterprise server.
5. Go to the Splunk/Apps page and select **Install app from file**.
6. **Upload** each of the above apps.

The Apps are displayed in your Splunk console homepage view and are listed under the Apps menu.

Post-Installation Check for Adaptive Response Add-on in Splunk Cloud Deployment

If you installed the Forescout Adaptive Response Add-on for Splunk in a Splunk cloud deployment, check that the inputs.conf file exists in the following folder:

/opt/splunk/etc/apps/TA-forescout_response/default/inputs.conf

If the inputs.conf file exists in the folder, there is no further action.

If the file is not there, perform the following procedure to add the file and its contents. See Create inputs.conf File and Contents.

If you do not have access to the folder, open a support ticket to do the post-installation check and/or to add the file and its contents. See Create inputs.conf File and Contents.

Create inputs.conf File and Contents

To create the inputs.conf file and its contents:

1. Using an editor such as vi or Notepad, create a file called inputs.conf.
2. Add the following lines to the file:

   ```
   [script://$SPLUNK_HOME/etc/apps/TA-forescout_response/bin/ta_forescout_response_init.py]
   disabled = False
   interval = 14400
   passAuth = admin
   ```

3. Save the file in the folder:

   /opt/splunk/etc/apps/TA-forescout_response/default/

4. Restart Splunk.

Set Up the Forescout Technology Add-on for Splunk

The Forescout Technology Add-on for Splunk supports data communication between the Forescout platform and the Forescout App for Splunk. The best practice is to install it from Splunkbase.

To set up the Technology Add-on for Splunk:

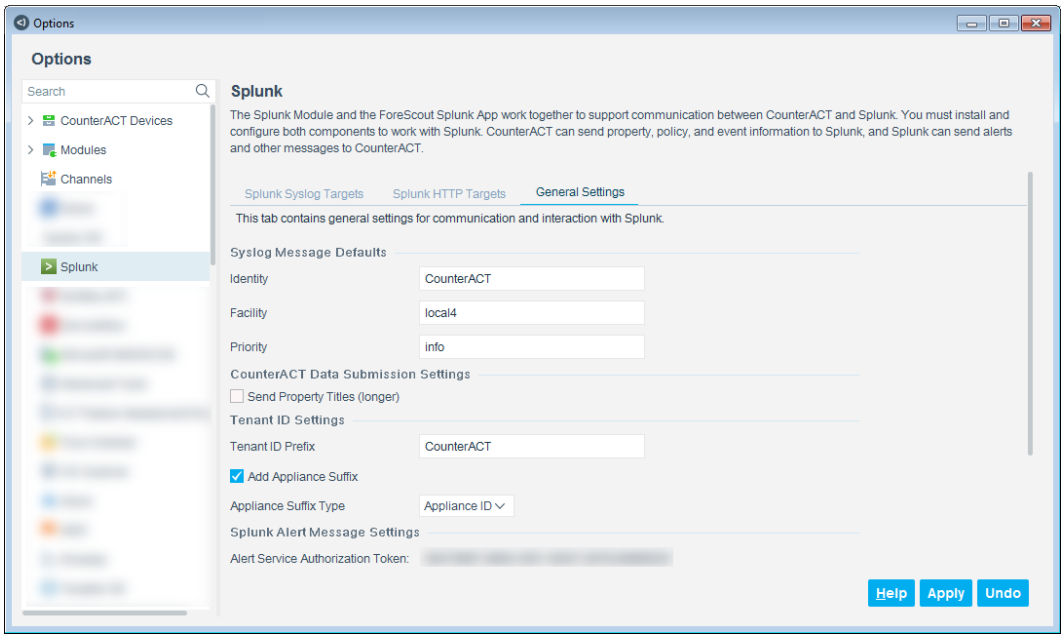
1. **Login** to the Splunk Enterprise server.

2. Go to the Splunk/Apps page and within the Forescout Technology Add-on for Splunk row, select **Set up**.

3. In the CounterACT IP Address or Hostname field, enter the Fully Qualified Domain Name (FQDN), or IPv4 or IPv6 address of the Enterprise Manager or standalone CounterACT Appliance of your environment.

   If you are configuring the Forescout Technology Add-on for Splunk with the FQDN, specify it in all lowercase characters.

4. In the Enter password field, enter the **Alert Service Authorization Token**. You can get this token from the General Settings pane of the Forescout eyeExtend for Splunk configuration. See Obtain an Authorization Token for details. Confirm the password.



5. Select **Save**.
6. **Restart** the Splunk Enterprise server.

Splunk Roles for the Forescout Platform

The following 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 indexes
- Enable/disable saved searches

counteract_user

Users with this role can:

- Create Dashboards
- View Dashboards
- Search on all indexes

User with this role cannot:

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

Forescout Platform Workflow for Adaptive Response

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

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

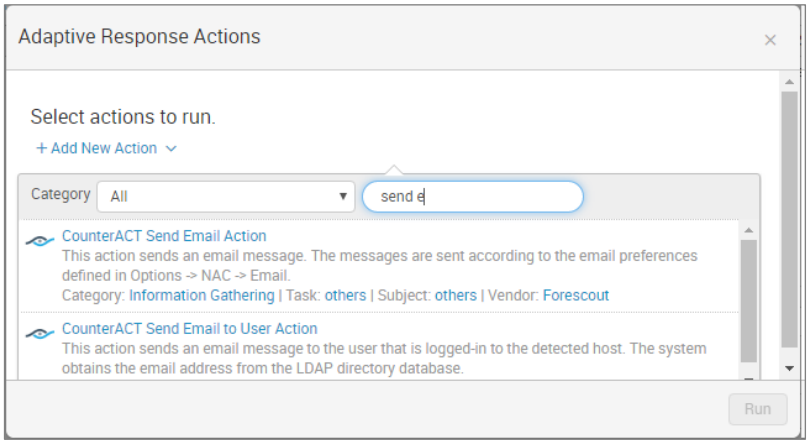
- ***Forescout platform alerts (saved search)***: The add-on provides predefined searches that mine standard endpoint properties reported by the Forescout platform to Splunk.
- ***Forescout platform Alert API***: Splunk sends action requests to the Forescout platform through a REST API interface.
- ***Forescout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

    See Forescout Platform Response to Alert Messages.

    In addition, the Forescout App provides a dashboard that tracks actions requested by Splunk. See Response Dashboard.

With Splunk Enterprise Security

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

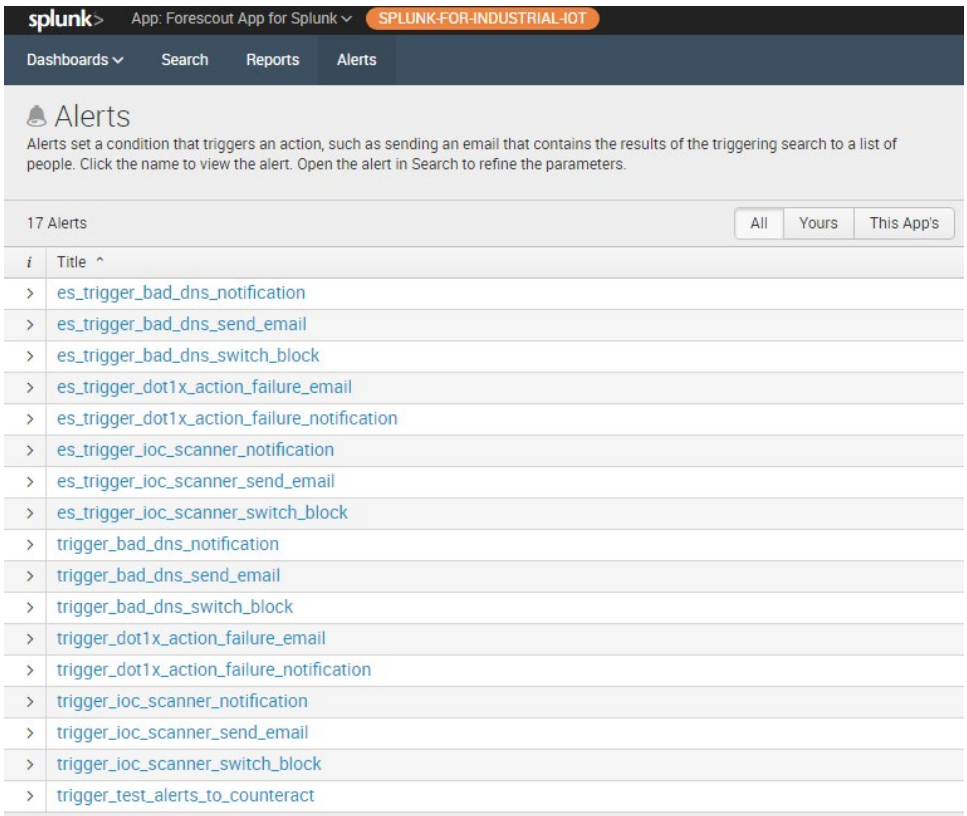


In Splunk Enterprise Environments without Enterprise Security

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

Correlation Searches and Saved Searches

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



The default saved searches are defined below:

Saved Search	**Purpose**
es_trigger_bad_dns_notification	Enterprise Security Correlation Search based on the Forescout platform's Bad DNS Activity and applies the Forescout platform *HTTP Notification* action.
es_trigger_bad_dns_send_email	Enterprise Security Correlation Search based on the Forescout platform's Bad DNS Activity that applies the Forescout platform *Send Email* action.
es_trigger_bad_dns_switch_block	Enterprise Security Correlation Search based on the Forescout platform's Bad DNS Activity that applies the Forescout platform *Switch Block*.
es_trigger_dot1x_action_failure_email	Enterprise Security Correlation Search based on the Forescout platform's Authentication Failures that applies the Forescout platform *Send Email* action.

Saved Search	Purpose
es_trigger_dot1x_action_failure_notification	Enterprise Security Correlation Search based on the Forescout platform's Authentication Failure Exceeding Threshold that applies the Forescout platform *HTTP Notification* action.
es_trigger_ioc_scanner_notification	Enterprise Security Correlation Search based on the Forescout platform's IOC Scanner Activity that applies the Forescout platform *HTTP Notification* action.
es_trigger_ioc_scanner_send_email	Enterprise Security Correlation Search based on the Forescout platform's IOC Scanner Activity that applies the Forescout platform *Send Email* action.
es_trigger_ioc_scanner_switch_block	Enterprise Security Correlation Search based on the Forescout platform's IOC Scanner Activity that applies the Forescout platform *Switch Block*.
trigger_bad_dns_notification	Saved Search based on the Forescout platform's Bad DNS Activity and that applies the Forescout platform *HTTP Notification* action.
trigger_bad_dns_send_email	Saved Search based on the Forescout platform's Bad DNS Activity that applies the Forescout platform *Send Email* action.
trigger_bad_dns_switch_block	Saved Search based on the Forescout platform's Bad DNS Activity that applies the Forescout platform *Switch Block.*
trigger_dot1x_action_failure_email	Saved Search based on the Forescout platform's Authentication Failures that applies the Forescout platform *Send Email* action.
trigger_dot1x_action_failure_notification	Saved Search based on the Forescout platform's Authentication Failures that applies the Forescout platform *HTTP Notification* action.
trigger_ioc_scanner_notification	Saved Search based on the Forescout platform's IOC Scanner Activity and that applies the Forescout platform *HTTP Notification* action.
trigger_ioc_scanner_send_email	Saved Search based on the Forescout platform's IOC Scanner Activity that applies the Forescout platform *Send Email* action.
trigger_ioc_scanner_switch_block	Saved Search based on the Forescout platform's IOC Scanner Activity that applies the Forescout platform *Switch Block*.

Saved Search	Purpose
trigger_test_alerts_to_counteract	Searches for test events from the Forescout platform and replies with a test alert message. See Alerts for more information.

Alerts

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

To view an alert:

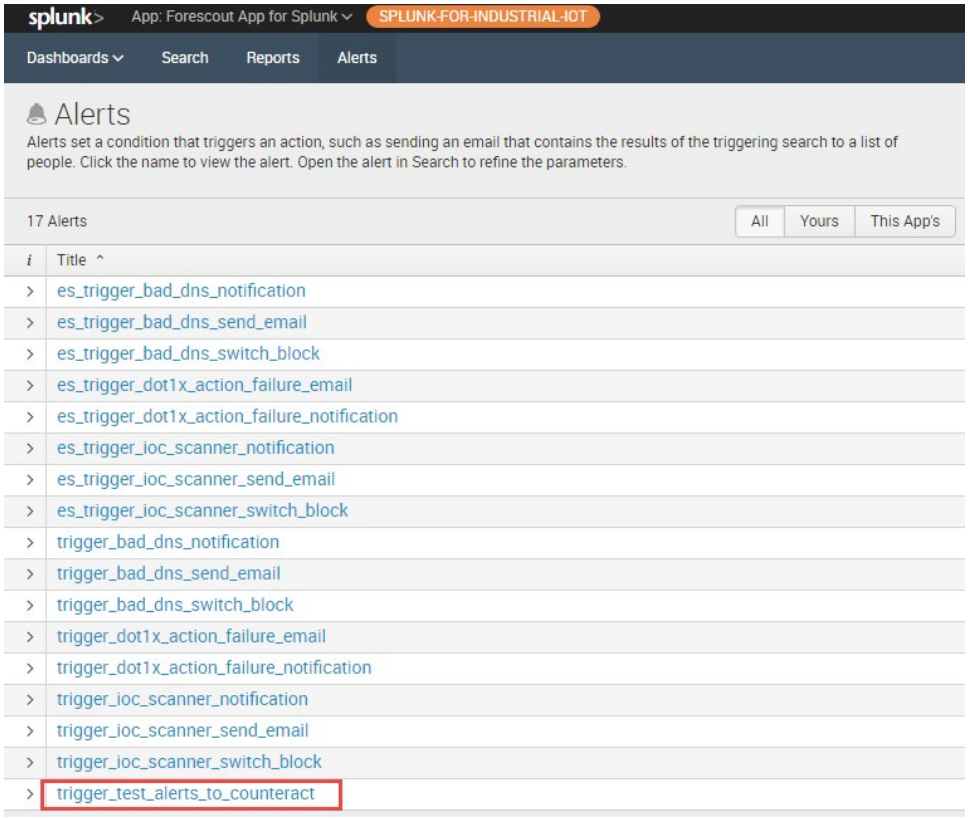
- In the left corner, select **App Search and Reporting**. In the Alerts page, the default Saved Searches are displayed.

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

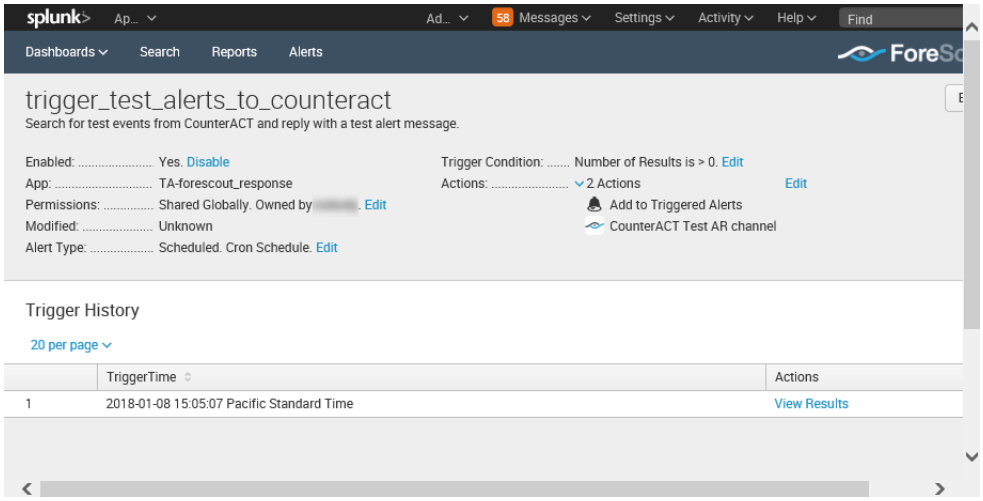
To view the contents of an alert / saved search:

You can optionally view the details of a saved search and see what it contains. We will use the *trigger_test_alerts_to_counteract* alert as an example.

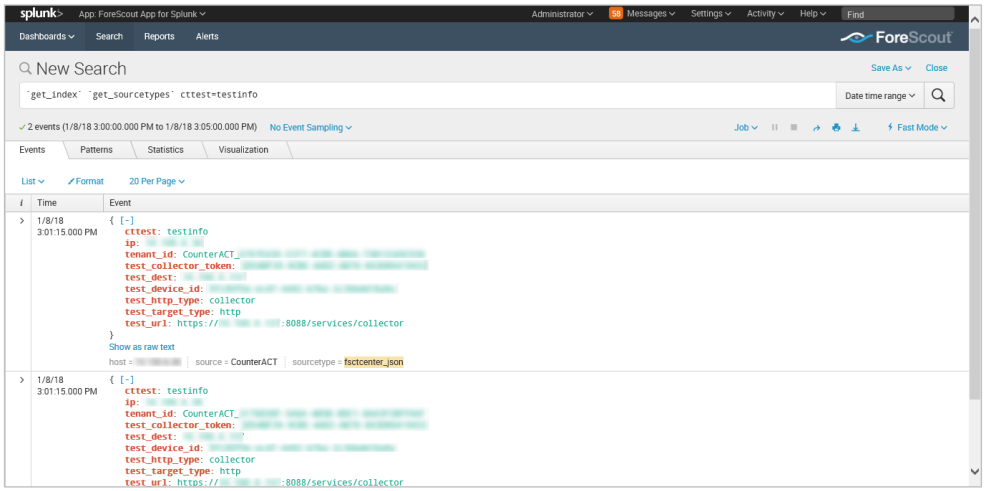
1. In the Alerts page, select **trigger_test_alerts_to_counteract**.



2. The trigger_test_alerts_to_counteract page opens. Select the **View Results** link.



3. The event details of the search results are displayed.



4. You can view information such as, IP address and target device details. These are configured in Forescout eyeExtend for Splunk. Refer to the *Forescout eyeExtend for Splunk Configuration Guide* for more information.

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 the Forescout platform, 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 Bad DNS Activity

   Search Name:

   trigger_bad_dns_notification

   Search Query:

```
`get_index` `get_sourcetypes` `ct_hostinfo` dnsniff_event
| rename host_properties.dnsniff_event{}.value as dnsniff_event
| mvexpand dnsniff_event
| rex field=dnsniff_event "DNS Query
Type:\s*(?<DNSQueryType>[^;^$]*);DNS Query/Response: Query;DNS Zone:
;DNS Addresses.*"
| search DNSQueryType="A"
| fillnull value="" ip ipv6
| eventstats count as eventcount by ip, ipv6
| dedup ip ipv6
| where eventcount>5 AND eventcount<=10
```

   Action Name:

   HTTP Notification Action

   API call to the Forescout platform:

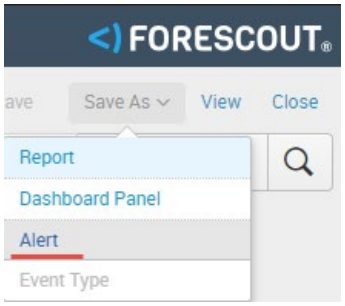
   http://<em_ip>/splunk/alerts?disposition=3&action_group=notify&auth=CounterACT%20<token>

   Sample log/event:

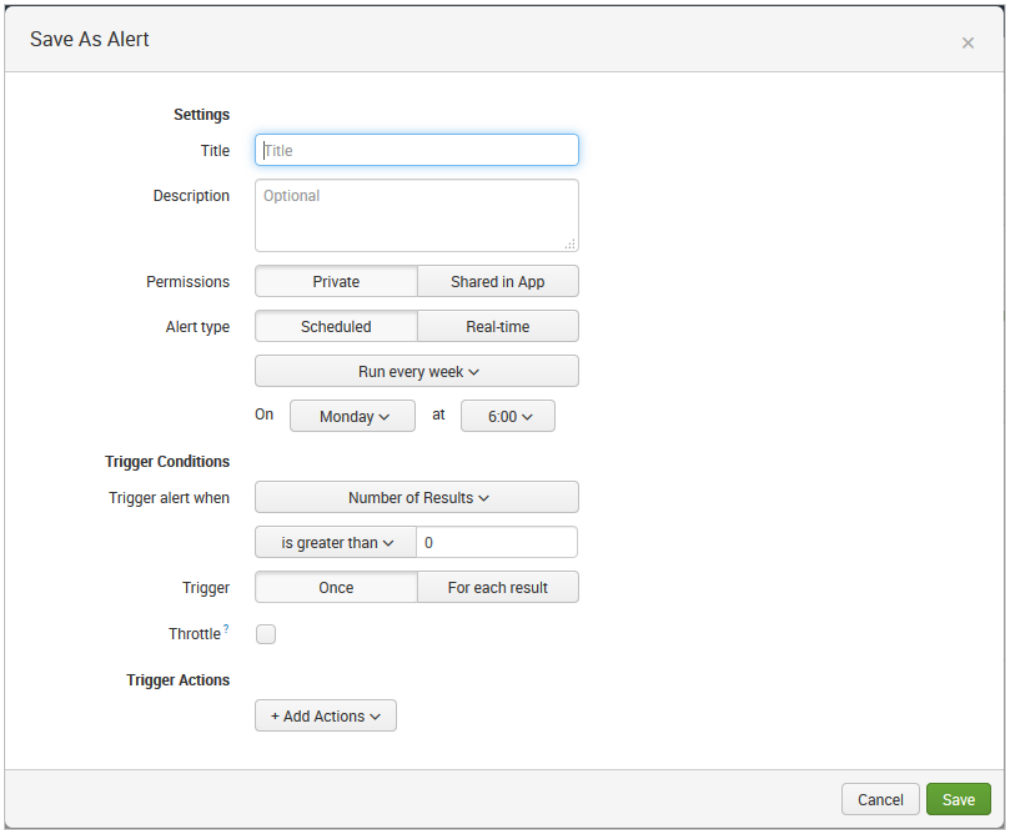

```
> 1/24/18 12:38:53.000 AM
{ [-]
  ctupdate: hostinfo
  dnsdomain: calab.forescout.com
  host_properties: { [-]
    dnsniff_event: [ [-]
      { [-]
        since: 1516747030
        value: DNS Name: [redacted].in-addr.arpa;DNS Query Type: PTR;DNS Query/Response: Query;DNS Zone: ;DNS Addresses: ;DNS Server Address: [redacted];DNS Monitoring Tag:  policy
      }
      { [-]
        since: 1516747030
        value: DNS Name: [redacted].in-addr.arpa;DNS Query Type: PTR;DNS Query/Response: Response;DNS Zone: 10.in-addr.arpa. IN SOA fs0.forescout.com. hostmaster.forescout.com. [redacted];;DNS
Addresses:  ;DNS Server Address: [redacted];DNS Monitoring Tag:  policy
      }
      { [-]
        since: 1516747119
        value: DNS Name: [redacted].in-addr.arpa;DNS Query Type: PTR;DNS Query/Response: Query;DNS Zone: ;DNS Addresses: ;DNS Server Address: [redacted];DNS Monitoring Tag:  policy
      }
      { [-]
        since: 1516747119
        value: DNS Name: [redacted].in-addr.arpa;DNS Query Type: PTR;DNS Query/Response: Response;DNS Zone: 10.in-addr.arpa. IN SOA fs0.forescout.com. hostmaster.forescout.com. [redacted];DNS
Addresses:  ;DNS Server Address: [redacted];DNS Monitoring Tag:  policy
      }
      { [-]
        since: 1516747129
        value: DNS Name: [redacted].in-addr.arpa;DNS Query Type: PTR;DNS Query/Response: Query;DNS Zone: ;DNS Addresses: ;DNS Server Address: [redacted];DNS Monitoring Tag:  policy
      }
      { [-]
        since: 1516747129
        value: DNS Name: [redacted].in-addr.arpa;DNS Query Type: PTR;DNS Query/Response: Response;DNS Zone: 10.in-addr.arpa. IN SOA fs0.forescout.com. hostmaster.forescout.com. [redacted];;DNS
Addresses:  ;DNS Server Address: [redacted];DNS Monitoring Tag:  policy
      }
      { [-]
        since: 1516747059
        value: DNS Name: [redacted].in-addr.arpa;DNS Query Type: PTR;DNS Query/Response: Query;DNS Zone: ;DNS Addresses: ;DNS Server Address: [redacted];DNS Monitoring Tag:  policy
      }
      { [-]
        since: 1516747059
        value: DNS Name: [redacted].in-addr.arpa;DNS Query Type: PTR;DNS Query/Response: Response;DNS Zone: 10.in-addr.arpa. IN SOA fs0.forescout.com. hostmaster.forescout.com. [redacted];;DNS
Addresses:  ;DNS Server Address: [redacted];DNS Monitoring Tag:  policy
      }
      { [-]
        since: 1516747052
        value: DNS Name: [redacted].in-addr.arpa;DNS Query Type: PTR;DNS Query/Response: Query;DNS Zone: ;DNS Addresses: ;DNS Server Address: [redacted];DNS Monitoring Tag:  policy
      }
```

How to create an Alert with Trigger Actions

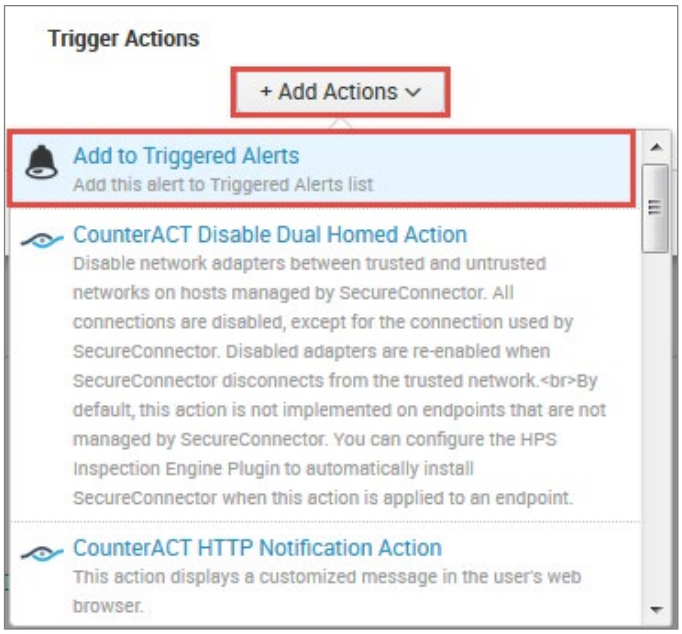
1. In the Forescout App for Splunk, run a search.
2. Under the Forescout logo, select **Save As** and then select **Alert**.



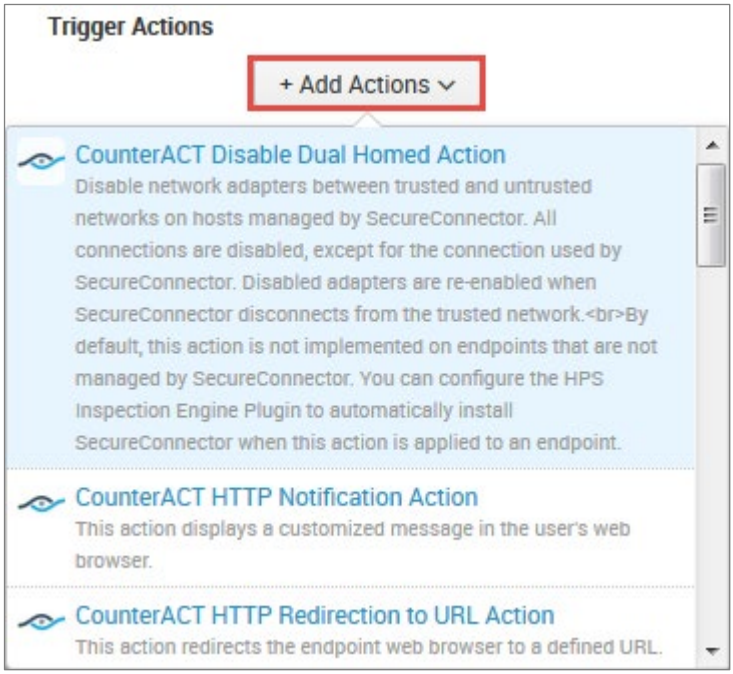
3. The Save As Alert dialog box opens.



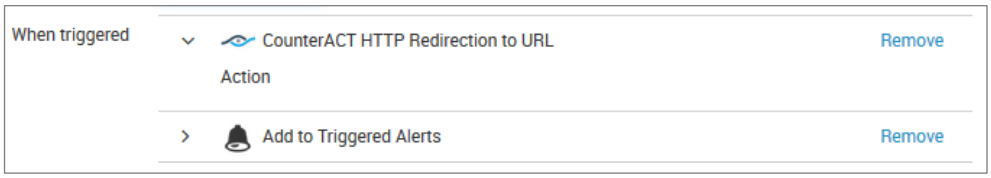
4. Define the schedule and trigger conditions.
5. In the Trigger Actions section, select **Add Actions** and then select **Add to Triggered Alerts**. This step is always required when you want to save a new Alert.



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



7. At the bottom of the Saved As Alert dialog box, the triggered alert setting is displayed.



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

For more information on configuring alert trigger conditions, refer to: https://docs.splunk.com/Documentation/SplunkCloud/7.2.4/Alert/AlertTriggerConditions

Customizing your own Alerts

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

Index

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

Index Name	Created in App/Manual	Purpose/Type of event data
fsctcenter (or name of your choice)	Should be created Manually.	All the event data forwarded from the Forescout platform to Splunk using any of the Channels viz. Syslog/UDP, REST API or HTTP Event Collector is stored in this index. 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 execution time-related information are stored in this index.
_introspection	Available as part of Splunk framework.	All the Splunk Performance-related metrics are logged here.

These indexes are used in various dashboards of the Forescout 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. The following table shows how the Forescout platform-related event data is distributed in these fields.

You can read more about the default fields at:

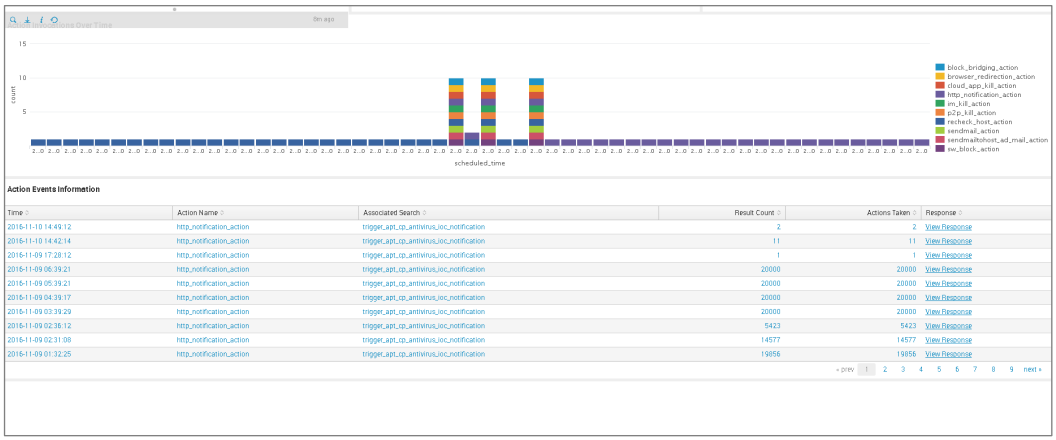
https://docs.splunk.com/Documentation/Splunk/7.2.4/Data/Aboutdefaultfields

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

Forescout Platform Response to Alert Messages

When the Forescout platform receives a Splunk alert message:

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



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

To yield significant action status values:

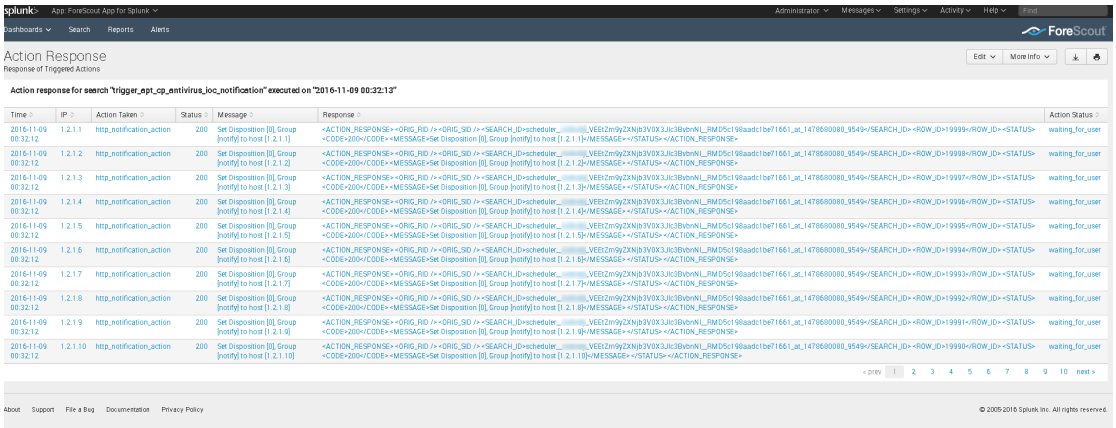
- Endpoints must exist in the Forescout platform when the report is generated.
- There should be an active Forescout platform policy that detects the Splunk Alert property that is updated by the alert message, and apply the action requested by the alert.

In other situations, error status values are returned.

The following action status values are reported by the Forescout platform.

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.
No Status	No status can be reported for one of the following reasons: ▪ No active policy detects the relevant Splunk Last Alert property, or applies the requested action. ▪ The endpoint has been deleted from the Forescout platform. ▪ Even though the IP address of the endpoint is within the Forescout platform's network scope, the endpoint has not been detected by the Forescout platform. ▪ Scheduled Forescout platform data purges clear action data before reports are generated.
Invalid	▪ The endpoint IP is outside the network scope defined in the Forescout platform. ▪ An unspecified internal error occurred.

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



The screenshot above shows the alert details given from Splunk to the Forescout platform. 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 the following:

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

Targeting Devices in Alerts Sent to the Forescout Platform

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

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.

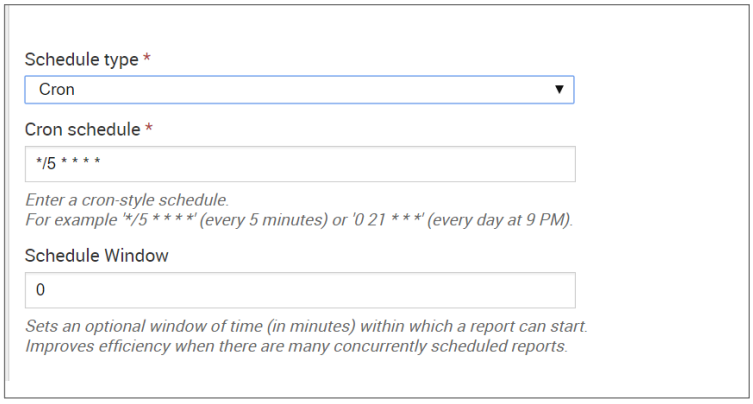
- It is recommended to configure Cron expressions that offset the start of search launch in relation to the internal clock. For example, the following expression configures the search to repeat every 5 minutes, but delays search launch by 3 minutes relative to the internal clock.

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



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

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 Forescout platform 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 the Forescout platform.

- Summary Dashboard
- Forescout Policy Dashboard
- Network Insight and Discovery Dashboard
- Response Dashboard
- System Overview Dashboard
- Host Detail View Dashboard

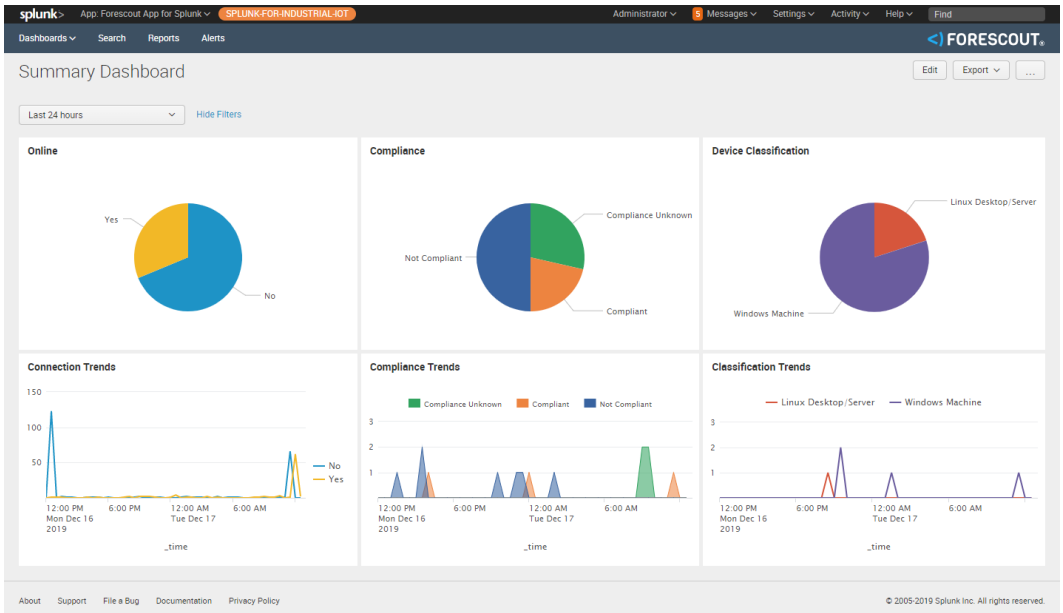
You can modify these standard dashboards or create custom dashboards or graphs.

When working with dashboards:

- Remember that Splunk can only display Forescout platform host property and policy information that has been sent to Splunk. Define policies in the Forescout platform 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 the Forescout platform.



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 endpoints 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.

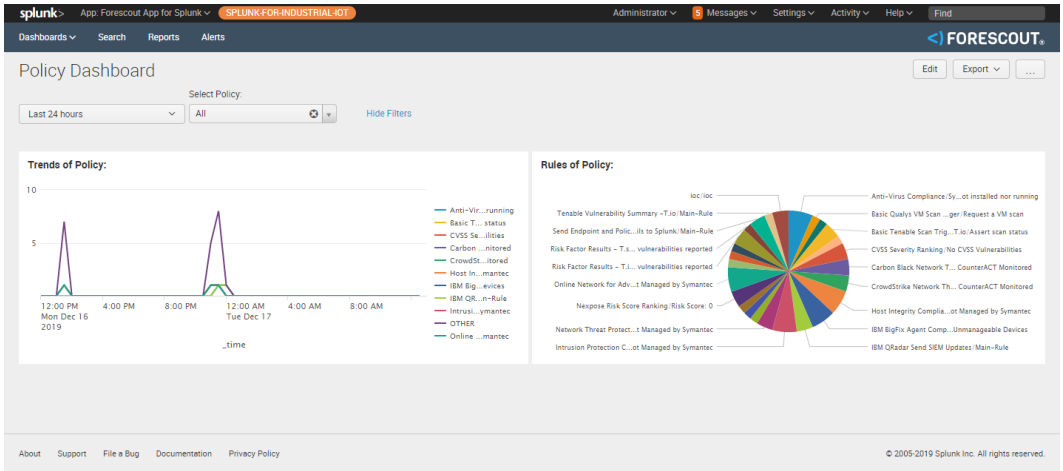
Forescout Policy Dashboard

The Forescout Policy dashboard presents charts that track how Forescout platform 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 Forescout platform 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 Forescout platform policy.

Network Insight and Discovery Dashboard

The Network Insight and Discovery dashboard tracks changes in a core set of Forescout platform 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:

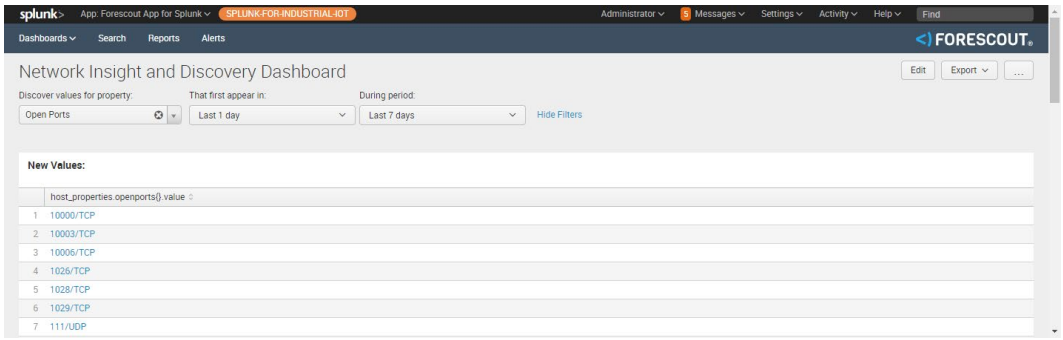
1. Select the Forescout platform host property you wish to view in the Discover Values for Property drop-down.
2. Use the following drop-down fields to specify search criteria:

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**.

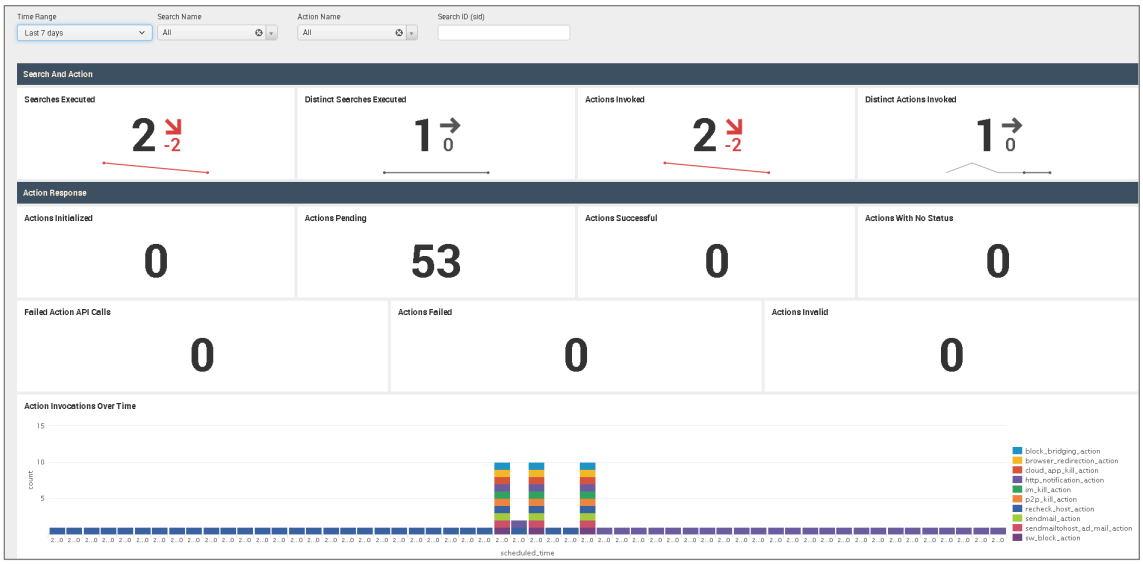


The dashboard can be used to track the following Forescout platform host properties:

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

Response Dashboard

The Response dashboard provides the detailed analysis of Adaptive Response Framework Actions executed by the Forescout platform for incidents in Splunk Enterprise Security. See Forescout Platform Workflow for Adaptive Response.



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

- **Searches Executed**: Indicates the number of Saved Searches executed for which Forescout platform Alert Actions are mapped.
- **Distinct Searches Executed**: Indicates the total number of unique Saved Searches executed for which Forescout platform 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 Forescout platform 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 the Forescout platform.
- **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 the Forescout platform.

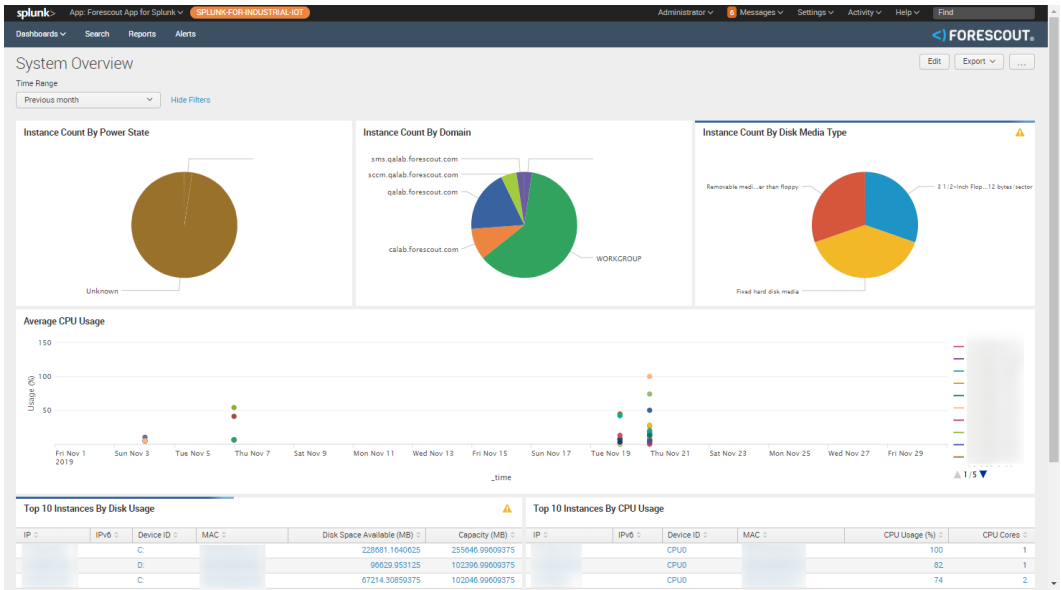
- **Actions Initialized**: Displays the count of Alert Actions for which asynchronous response is received from the Forescout platform to Splunk with status *init*.
- **Actions Pending**: Displays the count of Alert Actions for which asynchronous response is received from the Forescout platform to Splunk with status *waiting_for_user*.
- **Actions Successful**: Displays the count of Alert Actions for which asynchronous response is received from the Forescout platform to Splunk with status *success*.

- **Actions with No Status**: Displays the count of Alert Actions for which asynchronous response is received from the Forescout platform to Splunk with status *no_status*.
- **Failed Action API Calls**: Displays the count of Alert Actions for which the synchronous response of Forescout platform API calls was received with error and the status code was not 200.
- **Actions Failed**: Displays the count of Alert Actions for which asynchronous response is received from the Forescout platform to Splunk with status *failure*.
- **Actions Invalid**: Displays the count of Alert Actions for which asynchronous response is received from the Forescout platform to Splunk with status *invalid*.

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

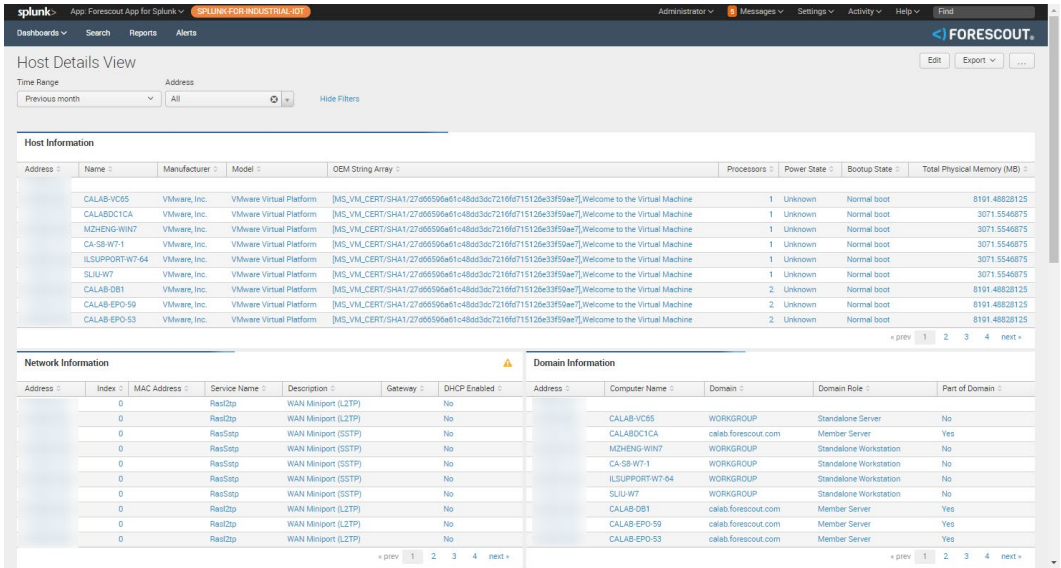
System Overview Dashboard

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 the Forescout platform. 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.



Appendix A: Distributed Deployment

For more information about distributed and clustered deployments, refer to:

https://docs.splunk.com/Documentation/Splunk/7.2.4/Deploy/Distributedoverview

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

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

Forwarding Event Data from the Forescout Platform to Splunk

Possible Communication Channels

Below are the communication channels in which the Forescout platform can send event data to Splunk:

- ***HTTP Event Collector (HEC)***

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

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

- ***Syslog***

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

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

  Make sure the index in the Syslog data inputs that is defined on the Splunk Enterprise server uses the same port configured in Forescout eyeExtend for Splunk.

- ***Simple REST Input***

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

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

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

Forward Event Data to On-premise Distributed Splunk Deployments

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

- Send data directly to Indexers

  The Forescout platform can send event data directly to Splunk Indexers using above mentioned Communication channels.

- Send data to Indexers via Forwarders

  But in some scenarios, we can choose to send event data to Splunk Forwarder and then Splunk Forwarder can forward all the event data to Splunk Indexers. This can be useful in load balancing situations as Splunk Indexers are generally loaded with processing of Splunk Search queries.

Forward Event Data to Splunk Cloud Deployments

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

- Send data directly to Splunk Cloud Indexers via HTTP Event Collector

  The Forescout platform can send event data directly to Splunk Indexers deployed on Splunk Cloud using HTTP Event Collector channel. In this case, Splunk Cloud will configure and provide load balancing tools.

- Send data to Splunk Cloud Indexers via on-premise Splunk Forwarders

  The Forescout platform can send event data to on-premise Splunk Forwarders which can then forward the event data to Splunk Cloud Indexers.

Appendix B: Splunk Cloud Deployments

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

Forwarders with access to the source data are run to send data to Splunk Cloud. Splunk Cloud then indexes the data and transforms it into searchable "events." After event processing is complete, you can associate events with knowledge objects to enhance their usefulness.

You will need a Splunk Cloud license for how much data you can retain in the Splunk Cloud. This is used for indexing your daily data retention. For more information, see Indexing Requirements for Splunk Cloud Instance.

Splunk Cloud vs Splunk Enterprise

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

Splunk Cloud	Splunk Enterprise
Security: The security of the cloud deployment is managed and controlled by the Splunk Cloud team. There are more layers of security with Splunk Cloud.	***Security***: Access and security of your Splunk deployment is locally managed and maintained by each customer.
CLI access: There is no command line interface (CLI). Many administrative tasks can be performed using the web browser, for example, managing indexes. Other tasks must be performed by Splunk Cloud Support.	***CLI access***: Refer to the *Forescout App & Add-ons for Splunk How-to Guide*.
▪ ***Managed Splunk Cloud***: The apps must be installed by Splunk Cloud Support. ▪ ***Self-Service Splunk Cloud***: You can install the apps. See Deploying Splunk Cloud.	N/A
TCP and UDP data cannot be sent directly to Splunk Cloud. You must use an on-premises forwarder to send such data. The default port for the forwarder to Splunk Cloud are ports 9997 or 9998. Make sure the port ***on the firewall*** is open to Splunk Cloud. Refer to Splunk documentation.	Splunk Enterprise allows direct monitoring of ***TCP and UDP***. Refer to the *Forescout eyeExtend for Splunk Configuration Guide*.

Splunk Cloud	Splunk Enterprise
HTTP Event Collector (HEC): For Managed Splunk Cloud deployments, HEC must be enabled by Splunk Support.	***HTTP Event Collector (HEC)***: Refer to the *Forescout eyeExtend for Splunk Configuration Guide*.

Deploying Splunk Cloud

This section covers the setup and deployment of Splunk Cloud.

Types of Splunk Clouds

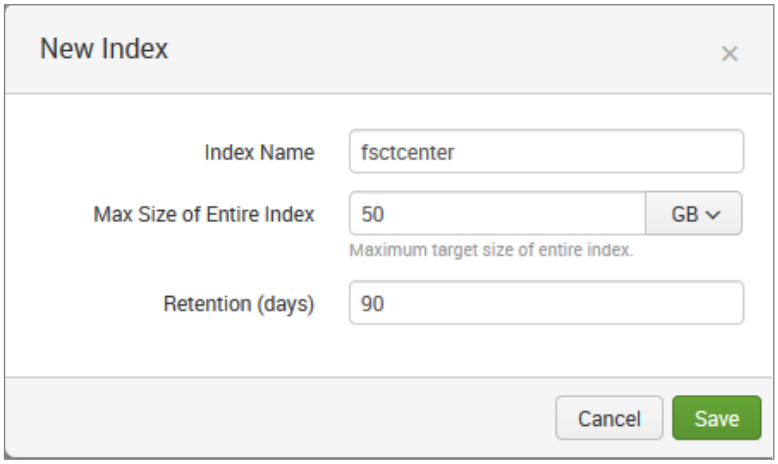
To determine whether your Splunk Cloud deployment is self-service or managed, look at the format of the URL for connecting to Splunk Cloud:

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

Indexing Requirements for Splunk Cloud Instance

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

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



For more information, refer to:

https://docs.splunk.com/Documentation/SplunkCloud/7.2.4/User/Datapolicies

Self-service Splunk Cloud

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

REST API

There is a limitation to use REST API on Splunk Cloud deployments. Refer to "REST API access limitations" for the Splunk Cloud REST API for details.

https://docs.splunk.com/Documentation/SplunkCloud/7.2.4/RESTTUT/RESTandCloud

HTTP Event Collector

Refer to:

https://docs.splunk.com/Documentation/SplunkCloud/7.2.4/Data/UsetheHTTPEventCollector

Define the URL for the HTTP Event Collector

For self-service HTTP Event Collector deployment, use the URL to access the Splunk Cloud Instance. The URL has the following format:

<protocol>://input-<host>:<port>/<endpoint>

where:

- <protocol> is either HTTP or HTTPS
- <host> is the Splunk Cloud URL
- <port> is the HEC port number (8088 on self-service Splunk Cloud instances)
- <endpoint> is the HEC endpoint

For example:

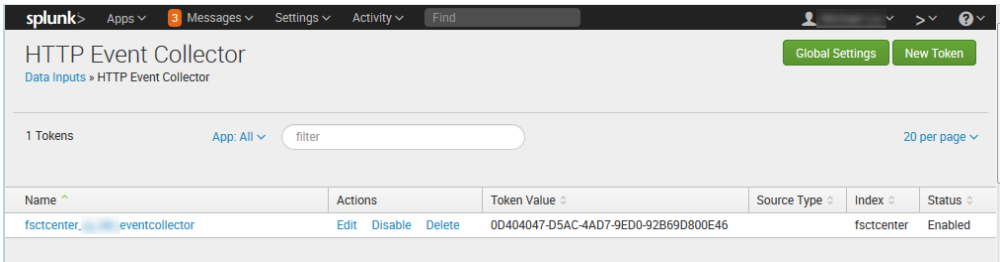
```
https://input-forescout.splunkcloud.com:8088/services/collector
```

Create HTTP Event Collector as a Data Input

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

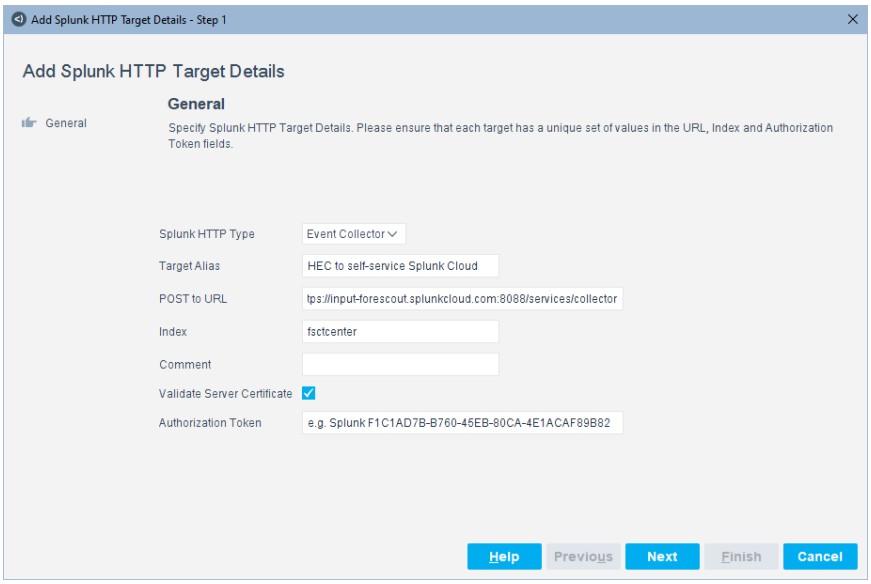
1. Select **Settings**, and then select **Data inputs**.

2. The Data inputs page opens. In the HTTP Event Collector row, select **Add new**.
3. Enter the information into the Add Data section. This will create a token. Save this token.



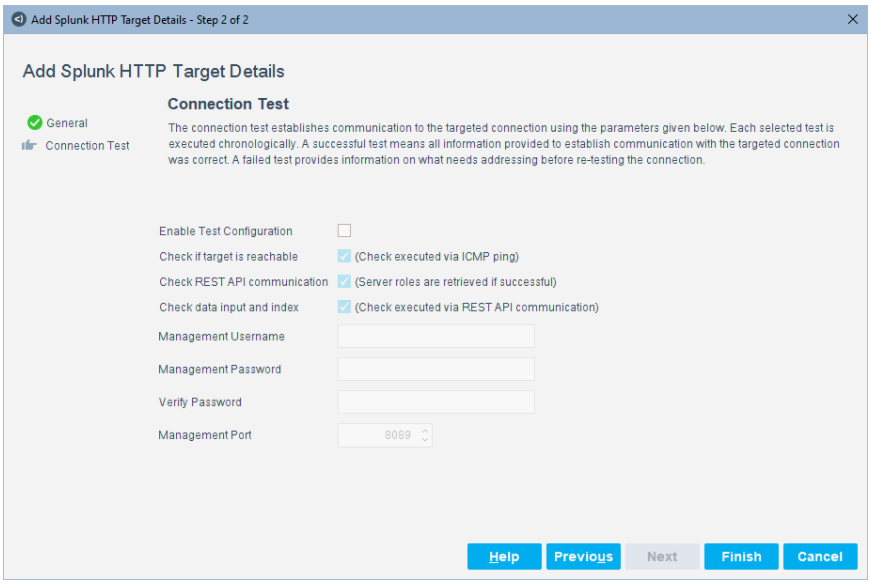
Create Splunk HTTP Target in Forescout eyeExtend for Splunk

1. Go to Forescout eyeExtend for Splunk, select **Options**, select **Splunk** and then select the Splunk HTTP Targets tab.
2. Select **Add**.



3. In the Add Splunk HTTP Target Details – Step 1 pane:
   a. In the POST to URL field, paste the URL of the Instance with the *input-* prefix and 8088 port number.
   b. In the Authorization Token field, paste the token value from the Splunk HTTP Event Collector page.

4. Select **Next**.



5. In the Add Splunk HTTP Target Details – Step 2 pane, disable the **Enable Test Configuration** checkbox. See Test the Connection.
6. Complete the Add Splunk HTTP Target Details. Refer to the "Event Collector section in the *Forescout eyeExtend for Splunk Configuration Guide*.

Test the Connection

Test for HTTP Event Collector (HEC) is not supported. To test the connection from the Forescout platform to the Splunk Cloud:

- In the Add Splunk HTTP Target Details – Step 1 pane, select REST API and create a REST API target. For the REST: Username, enter the credentials of the user who will make the test call. Refer to the "REST API" section in the *Forescout eyeExtend for Splunk Configuration Guide*. The Splunk Cloud URL has the following format:

  <protocol>://<host>:<port>/<endpoint>

  where:

  – <protocol> is either HTTP or HTTPS
  – <host> is the Splunk Cloud URL
  – <port> is the REST API port number (8089 on Splunk Cloud instances)
  – <endpoint> is the REST API endpoint

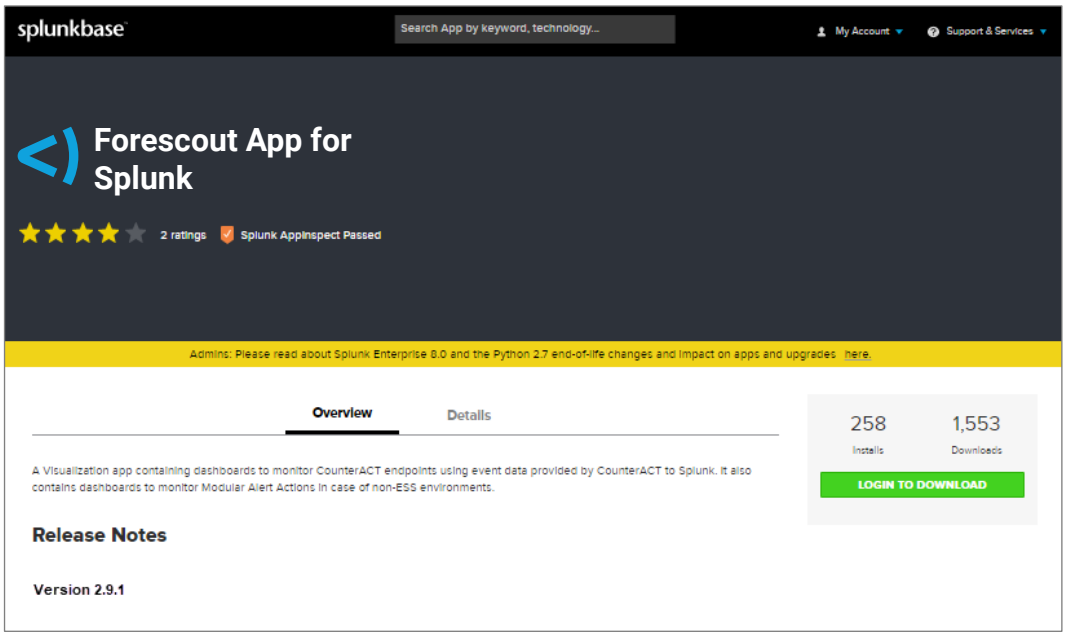
- Due to a REST API limitation on Cloud (see REST API), a user who runs the Test needs to have the edit_tcp capability. To add this capability to the user, refer to:

  https://docs.splunk.com/Documentation/Splunk/7.2.4/Security/Rolesandcapabilities#Add.2C_edit.2C_and_remove_capabilities_from_roles

  – Use *admin* (if you have *admin* access on the Splunk Cloud) who has edit_tcp capability.

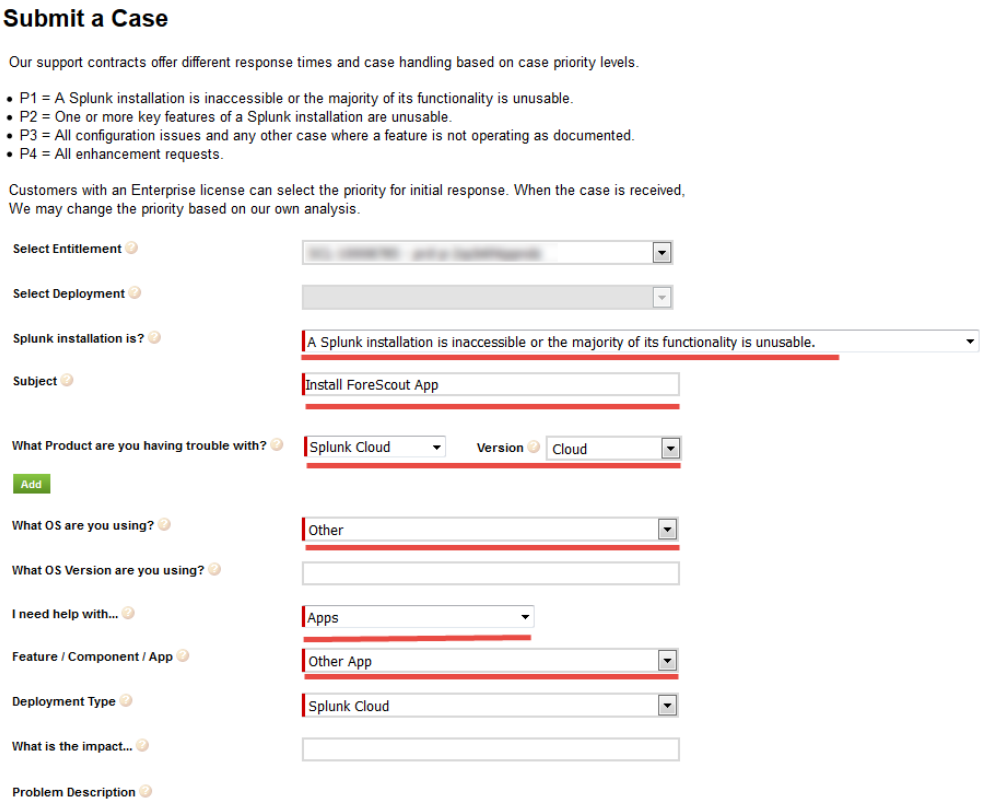
Managed Splunk Cloud

1. On the Splunk App page, select the **Manage Apps** icon in the left pane.
2. The Apps page opens. Select **Browse more apps**.
3. In the search field, enter *Forescout* and run the search.
4. Under the Forescout Apps for Splunk, select the **View on Splunkbase** link.
5. The Forescout Apps for Splunk installation page opens.
6. Select **2.9.1** in the version field and then select **Download**.



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

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



10. Make the selections according to the screen image above.

11. **Submit** the ticket.

REST API

There is a limitation to use REST API on Splunk Cloud deployments. Refer to "REST API access limitations" for the Splunk Cloud REST API for details.

https://docs.splunk.com/Documentation/SplunkCloud/7.2.4/RESTTUT/RESTandCloud

HTTP Event Collector

Refer to:

https://docs.splunk.com/Documentation/SplunkCloud/7.2.4/Data/UsetheHTTPEventCollector

Define the URL for the HTTP Event Collector

For managed cloud HTTP Event Collector deployment, use the URL to access the Splunk Cloud Instance. The URL has the following format:

<protocol>://http-inputs-<host>:<port>/<endpoint>

where:

- <protocol> is either HTTP or HTTPS
- <host> is the Splunk Cloud URL
- <port> is the HEC port number (443 on managed Splunk Cloud instances)
- <endpoint> is the HEC endpoint

For example:

```
https://http-inputs-forescout.splunkcloud.com:443/services/collector
```

Create HTTP Event Collector as a Data Input

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

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

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

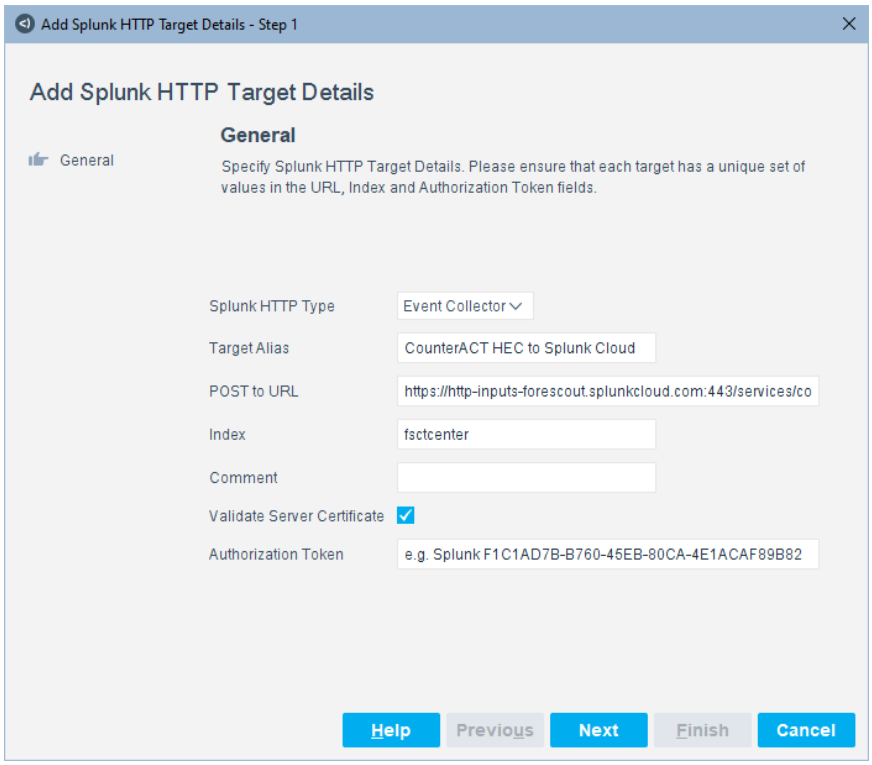
For more information, refer to:

https://docs.splunk.com/Documentation/SplunkCloud/7.2.4/Data/UsetheHTTPEventCollector

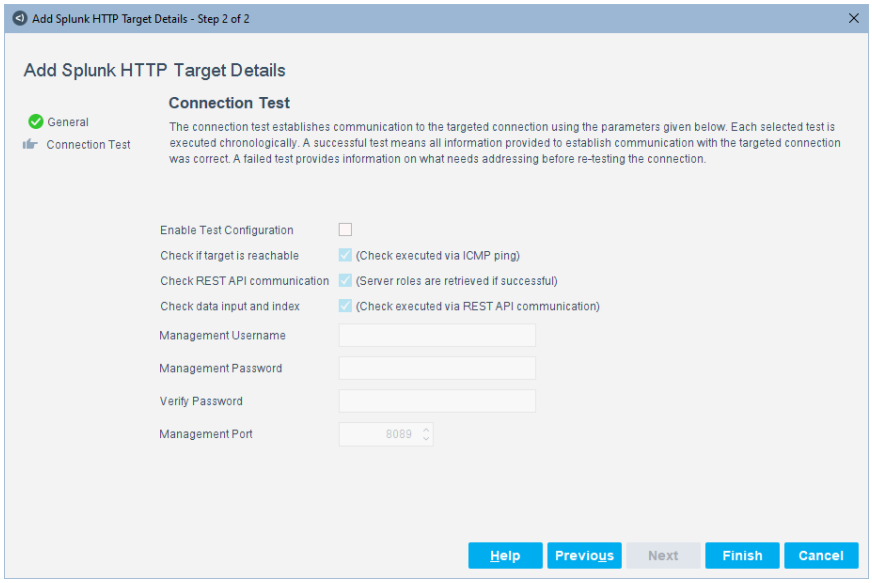
Create Splunk HTTP Target in the Forescout Platform

1. In the Forescout platform, select **Options**, select **Splunk** and then select the Splunk HTTP Targets tab.

2. Select **Add**.



3. In the Add Splunk HTTP Target Details – Step 1 pane:
   c. In the POST to URL field, paste the URL of the Instance with the *http-inputs-* prefix and 443 port number.
   d. In the Authorization Token field, paste the token value from the Splunk HTTP Event Collector page.
4. Select **Next**.



5. In the Add Splunk HTTP Target Details – Step 2 pane, disable the **Enable Test Configuration** checkbox. See Test the Connection.
6. Complete the Add Splunk HTTP Target Details. Refer to the "Event Collector" section in the *Forescout eyeExtend for Splunk Configuration Guide*.

Test the Connection

Test for HTTP Event Collector (HEC) is not supported. To test the connection from the Forescout platform to the Splunk Cloud:

- In the Add Splunk HTTP Target Details – Step 1 pane, select REST API and create a REST API target. For the REST: Username, enter the credentials of the user who will make the test call. Refer to the "REST API" section in the *Forescout eyeExtend for Splunk Configuration Guide*. The Splunk Cloud URL has the following format:

  <protocol>://<host>:<port>/<endpoint>

  where:

  – <protocol> is either HTTP or HTTPS
  – <host> is the Splunk Cloud URL
  – <port> is the REST API port number (8089 on Splunk Cloud instances)
  – <endpoint> is the REST API endpoint

- Due to a REST API limitation on Cloud (see REST API), a user who runs the Test needs to have the edit_tcp capability. To add this capability to the user, refer to:

  https://docs.splunk.com/Documentation/Splunk/7.2.4/Security/Rolesandcapabilities#Add.2C_edit.2C_and_remove_capabilities_from_roles

  – File a ticket with Splunk Cloud Support to add this capability to the user.
  – Use *admin* (if you have *admin* access on the Splunk Cloud) who has edit_tcp capability.

Set up Secure Connection Messaging to the Splunk Cloud

The alerts forwarded by the Forescout Adaptive Response Add-On from the Splunk Cloud to Forescout eyeExtend for Splunk are sent over via HTTPS.

See Appendix D: System Certificate for Web Portal for details. Then open a Splunk Support ticket and request that the Forescout Public Key Certificate is appended to the cacert.pem file at the following location:

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

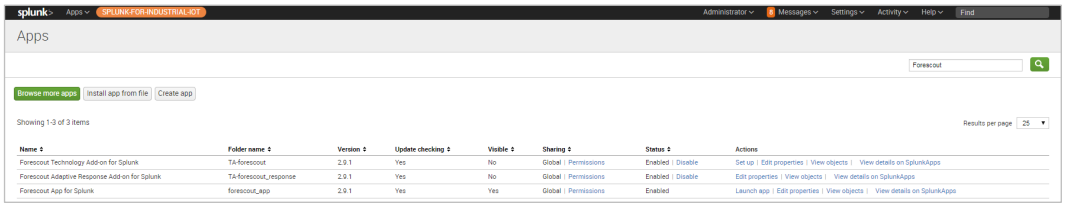
This step is very important. If you do not open a support ticket, the Adaptive Response alerts will not work.

Set up the Forescout Technology Add-on for Splunk Cloud

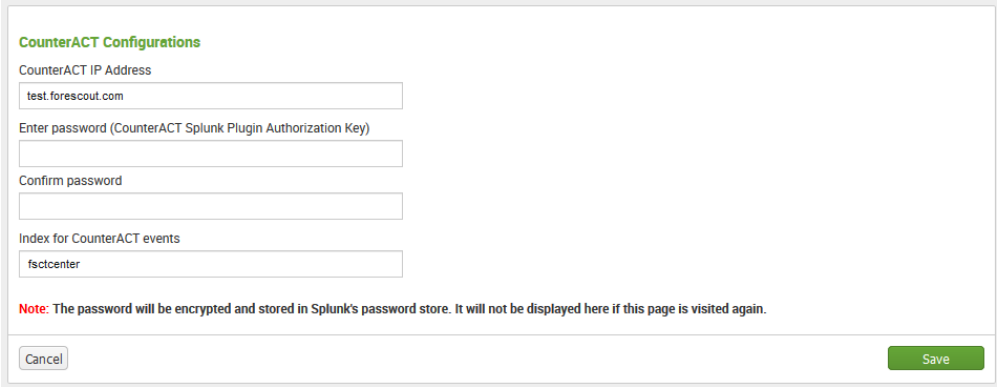
The Forescout Technology Add-on for Splunk supports data communication between the Forescout platform and the Forescout App for Splunk. The best practice is to install it from Splunkbase.

To set up the Technology Add-on for Splunk Cloud:

1. **Login** to the Splunk Cloud Instance.
2. Go to the Splunk Apps page to locate the Forescout Technology Add-on for Splunk.



3. On the Forescout Technology Add-on for Splunk row, under Actions, select **Set up**.



4. In the CounterACT IP Address or Hostname field, enter the FQDN, or IPv4 or IPv6 address of the Enterprise Manager or standalone CounterACT Appliance of your environment.

If you are configuring the Forescout Technology Add-on for Splunk with the FQDN, specify it in all lower case characters.

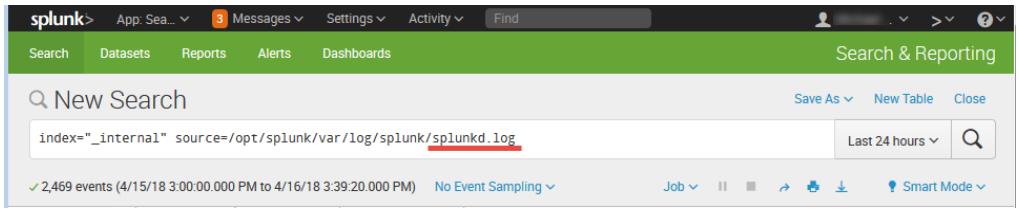
5. In the Enter password field, enter the **Alert Service Authorization Token**. You can get this token from the General Settings pane of the Forescout eyeExtend for Splunk configuration. See Obtain an Authorization Token for details. Confirm the password.
6. Select **Save**.
7. In Splunk Cloud Instance, select **Settings** and then select **Server controls**.
8. Select **Restart Splunk**.

Accessing Logs within Splunk Cloud Instance

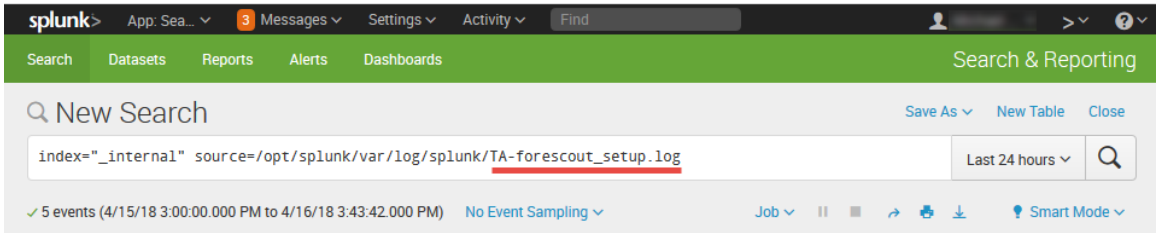
Because CLI is not provided on the Splunk Cloud, you will need to access your logs via the search function.

Below are example searches for:

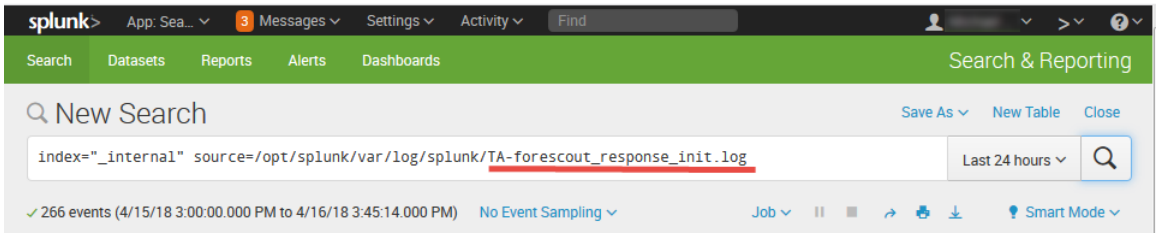
- Splunkd log
- TA-forescout_setup log
- TA-forescout_response_init log



Splunkd log



TA-forescout_setup log



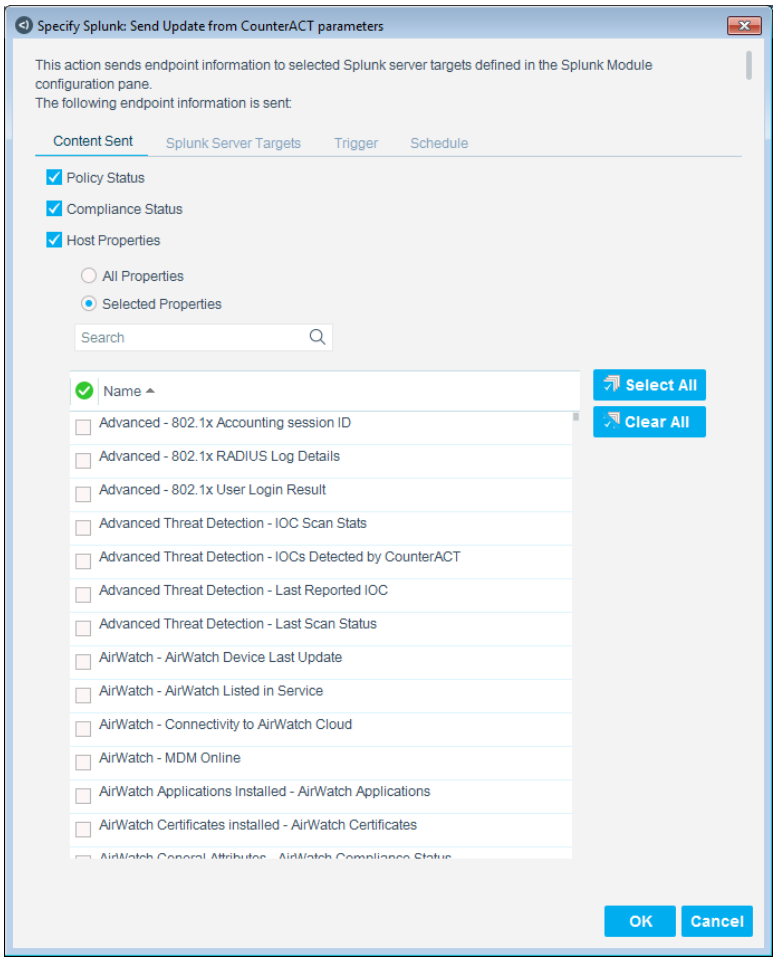
TA-forescout_response_init log

Appendix C: Working with Forescout Platform Data in Splunk

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

About Forescout Platform Data Events

Forescout platform 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, the Forescout platform 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, the Forescout platform sends *a separate event message* for each endpoint containing policy rules configured for that endpoint in the Forescout platform.

- When the **Host Properties** option is selected, the Forescout platform sends *a separate event message* for each endpoint containing host property values for that endpoint information.
- When the **Compliance Status** option is selected, the Forescout platform includes Compliance Status host property in the aforementioned event message.

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

Field	Description
ip	The IP address of the endpoint for which information is reported.
ctupdate	The message, identified as a Forescout platform 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`** .
mac	The MAC address of the endpoint for which information is reported.
ipv6	The IPv6 address of the endpoint for which information is reported.
nbtdomain	The NETBIOS Domain of the endpoint for which information is reported.
dnsdomain	The DNS domain of the endpoint for which information is reported, in case the NETBIOS Domain host property is not available for the endpoint.
nbthost	The NETBIOS hostname of the endpoint for which information is reported.
user	The User of the endpoint for which information is reported.
hostname	The DNS Name of the endpoint for which information is reported.
compliance	The Compliance Status of the endpoint for which information is reported.
host_properties	The Forescout platform host properties of the endpoint for which information is reported.
policies	The Forescout platform policies of the endpoint for which information is reported.

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

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

Refer to the *Forescout eyeExtend for Splunk Configuration Guide* for more details of action configuration options.

Considerations When Working with Forescout Platform Events in Splunk

Consider the following points when you work with Forescout platform 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 the Forescout platform 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 the Forescout platform, 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 Forescout Platform Data to the CIM Model

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

Certificates

Tags: certificate

Splunk Reference:

https://docs.splunk.com/Documentation/CIM/4.12.0/User/Certificates

Data Model Field	Forescout Platform Field Tag
ssl_name	Name
ssl_serial	Serial_Number
ssl_is_valid	Status
ssl_issuer_common_name	CN
ssl_subject_unit	OU

Data Model Field	Forescout Platform Field Tag
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:

https://docs.splunk.com/Documentation/CIM/4.12.0/User/ComputeInventory

Data Model Field	Forescout Platform Field Tag
cpu_cores	Number_Of_Cores
family	Family
cpu_load_percent	Load_Percentage

Compute_Inventory: Network

Tags: network

Splunk Reference:

https://docs.splunk.com/Documentation/CIM/4.12.0/User/ComputeInventory

Data Model Field	Forescout Platform Field Tag
ip	IP_Address
dns	DNS_HostName
mac	MAC_Address

Compute_Inventory: Memory

Tags: memory

Splunk Reference:

https://docs.splunk.com/Documentation/CIM/4.12.0/User/ComputeInventory

Data Model Field	Forescout Platform Field Tag
mem	Capacity

Compute_Inventory: Storage

Tags: storage

Splunk Reference:

https://docs.splunk.com/Documentation/CIM/4.12.0/User/ComputeInventory

Data Model Field	Forescout Platform Field Tag
storage	Size__Megabytes_
storage_free	Free_Space__Megabytes_

Blocked_Malware

Tags: malware,attack

Splunk Reference:

https://docs.splunk.com/Documentation/CIM/4.12.0/User/Malware

Data Model Field	Forescout Platform 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.

Forescout Platform 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

Appendix D: System Certificate for Web Portal

This section addresses the system certificates for the Splunk web portal on the Enterprise Manager.

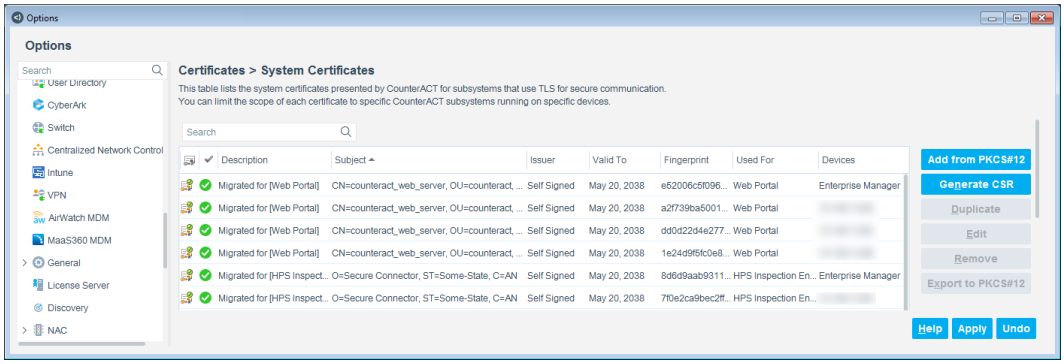
You must install a certificate. For information on how to install the system certificate for the Enterprise Manager, refer to the *Forescout Administration Guide*.

To generate a certificate:

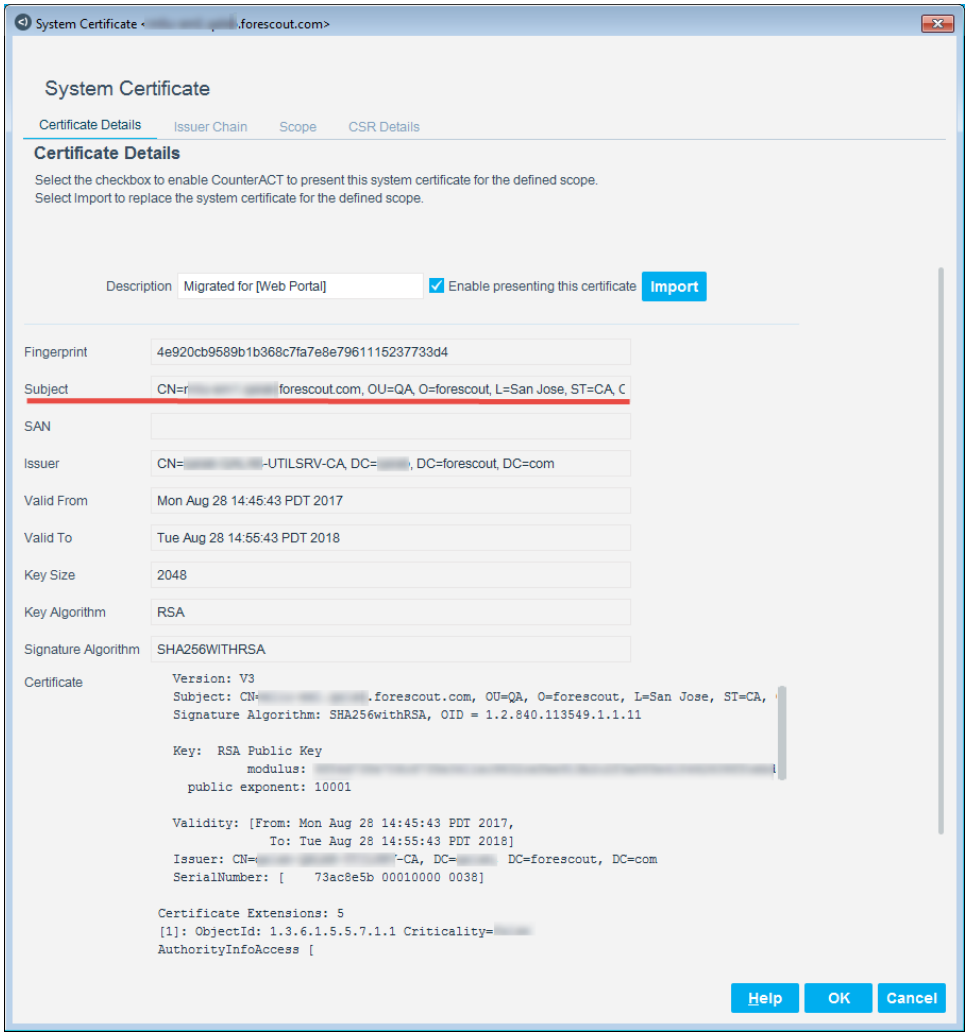
1. Select **Options**, select **Certificates**, and then select **System Certificates**.

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

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



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



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

Appendix E: Default Rate Limiting

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, Forescout eyeExtend for Splunk resets its alerts' data traffic count.
`config.rate_limit.window.max_alerts = 15`	Maximum number of alert messages accepted by the Forescout eyeExtend for Splunk.
`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 Forescout eyeExtend for Splunk from the Forescout App for Splunk. These values can be edited on Forescout eyeExtend for Splunk 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 Forescout eyeExtend for Splunk. 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 Forescout eyeExtend for Splunk 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 Forescout platform operator, warning about this condition. The operator needs to check the alert configuration, correct it, and then restart the module.

Appendix F: Compatibility with CIM Data Models

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

CIM Model: Certificates

Event Type	ct_certificate
Search	source=counterACT sourcetype=fsctcenter* ctupdate=hostinfo hwi_certificate=*
Tags	certificate

Splunk Reference: https://docs.splunk.com/Documentation/CIM/4.12.0/User/Certificates

Fields

Data Model Field	Forescout Platform 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

Event Type	ct_hostinfo_cpu
Search	source=counterACT sourcetype=fsctcenter* ctupdate=hostinfo hwi_processor=*
Tags	cpu

Splunk Reference:
https://docs.splunk.com/Documentation/CIM/4.12.0/User/ComputeInventory

Fields

Data Model Field	Forescout Platform Field
cpu_cores	Number_Of_Cores
family	Family
cpu_load_percent	Load_Percentage

CIM Model: Compute_Inventory: Network

Event Type	ct_hostinfo_network
Search	source=counterACT sourcetype=fsctcenter* ctupdate=hostinfo hwi_network_adapters=*
Tags	network

Splunk Reference:
https://docs.splunk.com/Documentation/CIM/4.12.0/User/ComputeInventory

Fields

Data Model Field	Forescout Platform Field
ip	IP_Address
dns	DNS_HostName
mac	MAC_Address

CIM Model: Compute_Inventory: Memory

Event Type	ct_hostinfo_memory
Search	source=counterACT sourcetype=fsctcenter* ctupdate=hostinfo hwi_physical_memory=*

Tags	memory

Splunk Reference:
https://docs.splunk.com/Documentation/CIM/4.12.0/User/ComputeInventory

Fields

Data Model Field	Mapped Forescout Platform Field
mem	Capacity

CIM Model: Compute_Inventory: Storage

Event Type	ct_hostinfo_storage
Search	source=counterACT sourcetype=fsctcenter* ctupdate=hostinfo hwi_disk=*
Tags	storage

Splunk Reference:
https://docs.splunk.com/Documentation/CIM/4.12.0/User/ComputeInventory

Fields

Data Model Field	Forescout Platform Field
storage	Size__Megabytes_
storage_free	Free_Space__Megabytes_

CIM Model: Blocked_Malware

Event Type	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: https://docs.splunk.com/Documentation/CIM/4.12.0/User/Malware

Fields

Data Model Field	Mapped Forescout Platform Field
file_hash	Threat_File_MD5
file_name	Threat_File_Name
sender	host