



ForeScout

eyeExtend for Splunk

Configuration Guide

Version 2.9.2



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 Technical Documentation page on the Forescout website for additional documentation: <https://www.Forescout.com/company/technical-documentation/>
- 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.

2020-06-26 08:40

Table of Contents

About Splunk Integration.....	6
About Certification Compliance Mode	7
What's New	7
Support for IPv6	7
Use Cases	8
Logging	8
Continuous Posture Tracking	8
Adaptive Response Actions Triggered by Splunk Data Correlation	8
Splunk Bi-directional Use Cases.....	9
Additional Splunk Documentation	10
About Forescout eyeExtend for Splunk.....	10
Forescout App for Splunk	10
Forescout Technology Add-on for Splunk	11
Forescout Adaptive Response Add-on for Splunk.....	11
How It Works	12
Components.....	13
Considerations.....	13
Splunk Instance Credentials.....	14
What to Do	14
Requirements.....	14
Forescout Requirements.....	14
Supported Vendor Requirements	15
Splunk Cloud Requirements	15
Forescout eyeExtend (Extended Module) Licensing Requirements.....	15
Per-Appliance Licensing Mode	16
Flexx Licensing Mode	17
More License Information	18
Install the Module	18
Upgrade to eyeExtend for Splunk 2.9.2	18
Install Forescout eyeExtend for Splunk.....	19
Configure the Module	20
Set Up the Forescout Technology Add-on for Splunk.....	21
Obtain an Authorization Token	22
Secure Connection Messaging to the Splunk Enterprise Server.....	25
Add a Splunk HTTP Target.....	27
Test the Connection.....	33
Modify Splunk Enterprise Server Settings.....	34
Add a Splunk Syslog Target	36
General Settings	39

Edit Splunk Syslog Targets	41
Test the Module.....	42
Understand Test Results.....	43
Create Splunk Policies Using Templates	43
Create a Send Endpoint and Policy Details to Splunk Policy	44
Support for Batch Messaging.....	44
Create the Policy	47
Create a Splunk Stage 1: Add to HTTP Notification Action Group Policy	50
Create the Policy	50
Create a Splunk Stage 2: Execute HTTP Notification Action Policy	52
Create the Policy	52
Action Status Tracking	54
Create Custom Splunk Policies	55
Detect Endpoints – Policy Properties	63
Splunk Alerts	63
Manage Splunk Devices – Policy Actions	64
Splunk: Send Custom Notification Action	65
Splunk: Send Update from CounterACT Action.....	66
Use Forescout eyeExtend for Splunk	70
Run Splunk Audit Actions	71
Send Custom Notification to Splunk Enterprise Server Targets	71
Send Updates from the Forescout Platform	74
Support for Multiple Channels for each Splunk Target	79
Best Practices	79
Forescout-to-Splunk Logging	79
Splunk to Forescout Messaging.....	79
Splunk Actions on the Forescout Platform	80
What Data is Sent to Splunk?.....	80
Appendix A: Default Communication Settings	80
Appendix B: Splunk Cloud Deployments	81
Splunk Cloud vs Splunk Enterprise.....	81
Deploy Splunk Cloud.....	82
Types of Splunk Clouds	82
Indexing Requirements for Splunk Cloud Instance.....	82
Self-Service Splunk Cloud	82
REST API	83
HTTP Event Collector	83
Managed Splunk Cloud.....	85
REST API	87
HTTP Event Collector	88
Set Up Secure Connection Messaging to the Splunk Cloud.....	90
Set Up the Forescout Technology Add-on for Splunk Cloud.....	91
Access Logs within Splunk Cloud Instance.....	92

Appendix C: System Certificate for Web Portal..... 92

Additional Forescout Documentation..... 94

Documentation Downloads94

Documentation Portal95

Forescout Help Tools.....95

About Splunk Integration

Splunk® Enterprise data analytics help organizations:

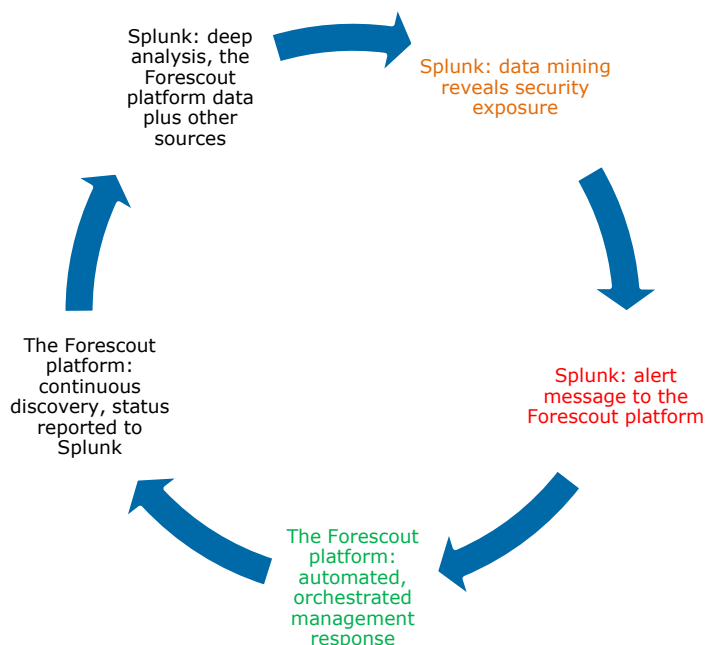
- Leverage the data that their infrastructure and security tools provide
- Understand their security posture
- Pinpoint and investigate anomalies
- Create alerts and reports

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

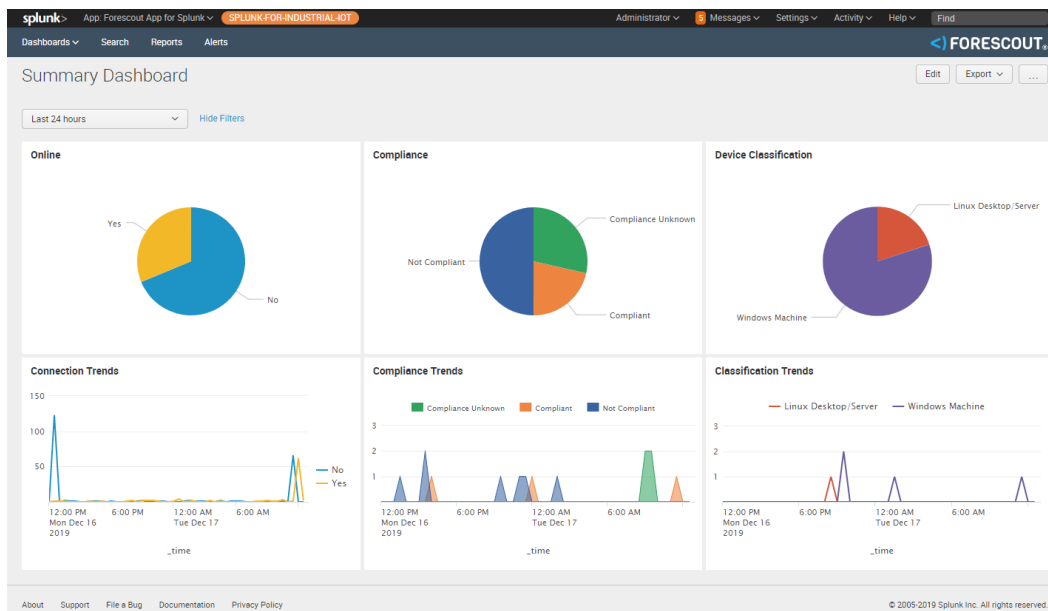
By combining the Forescout platform's dynamic device visibility, access, and security capabilities with Splunk Enterprise's data mining capabilities, security managers can:

- 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.



About Certification Compliance Mode

Forescout eyeExtend for Splunk supports Certification Compliance mode. For information about this mode, refer to the *Forescout Installation Guide*. See [Additional ForeScout Documentation](#) for information on how to access this guide.

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. There are no new feature enhancements in ForeScout eyeExtend for Splunk version 2.9.2.

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 ForeScout platform 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 Forescout eyeExtend for Splunk. Be sure to review the [Best Practices](#).

To understand how this module helps you achieve these goals, see [About Forescout eyeExtend for Splunk](#).

Logging

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

Audit and Event Logs

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

Continuous Posture Tracking

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:

- Device compliance status summaries
- Patterns of network access over time
- Trends in Forescout platform policies
- Significant changes in device processes and applications
- Device system health information including hardware and certificate information
- Experienced Splunk users can customize the searches and dashboards provided with the Forescout App or combine 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.

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

User Behavior Analytics (UBA)

The following minimum Forescout host properties are considered best practice for capturing UBA. They are initially time-stamped upon device connection.

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

Policy-based

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

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

Frequency

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

Splunk Bi-directional Use Cases

Due to bi-directional communication between the Forescout platform and Splunk, the Forescout platform is able to perform actions on endpoints via Splunk correlation. For example, a device tries to SSH too many Linux servers with the "root" account. The event instructs the Forescout platform to block the endpoint(s) or leverage any other action available via the Forescout platform implementation.

Splunk Sizing

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

Additional Splunk Documentation

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

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

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

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

About Forescout eyeExtend for Splunk

Forescout eyeExtend for Splunk integrates the Forescout platform and Splunk, which lets you:

- Use policies and actions provided by Forescout eyeExtend for Splunk to regularly push device properties and associated data to Splunk. For details, see [Create a Send Endpoint and Policy Details to Splunk Policy](#) and [Splunk: Send Update from CounterACT Action](#).
- In the Forescout App for Splunk, view Forescout platform data in a dedicated, customizable Splunk dashboard. Refer to the *Forescout App & Add-ons for Splunk How-to Guide* for details. See [Additional Forescout Documentation](#) for information on how to access this guide.
- Define Forescout platform policies that respond to Splunk alerts. See [Create Splunk Policies Using Templates](#).
- In the Saved Searches bundled with the add-on, configure Splunk to send alerts to the Forescout platform based on custom search queries. Searches can combine data from multiple data sources.
- Forescout eyeExtend for Splunk works with the Forescout Technology Add-on for Splunk and the Forescout Adaptive Response Add-on for Splunk to support communication between the Forescout platform and Splunk. 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 App & Add-ons for Splunk How-to Guide*.

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

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. It also displays the index name to which Forescout eyeExtend for Splunk sends its update messages.
- **Authentication:** The add-on stores the 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.

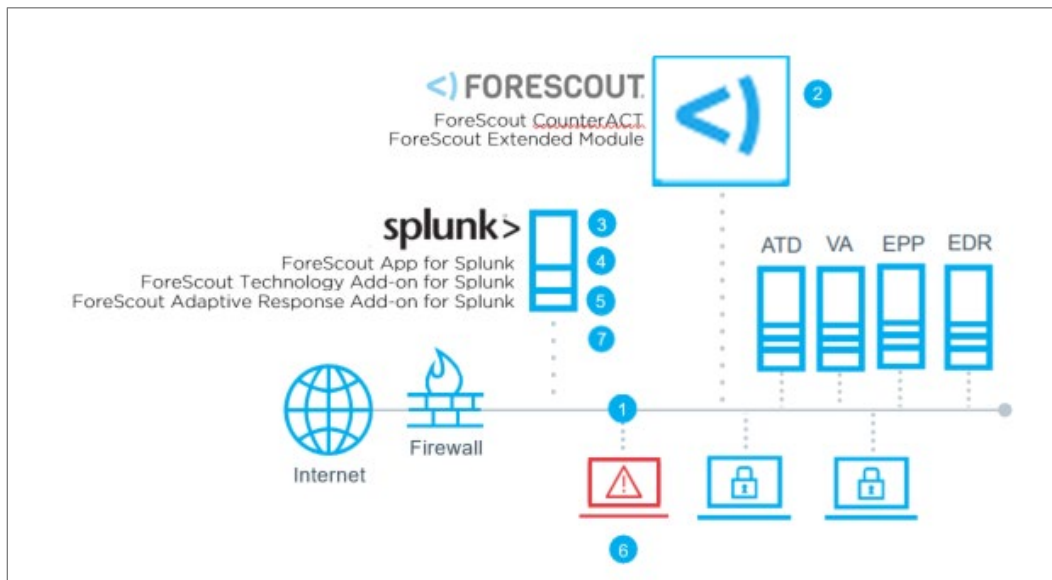
Forescout Adaptive Response Add-on for Splunk

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.

How It Works

This section provides a basic overview of the Splunk and Forescout platform architecture.

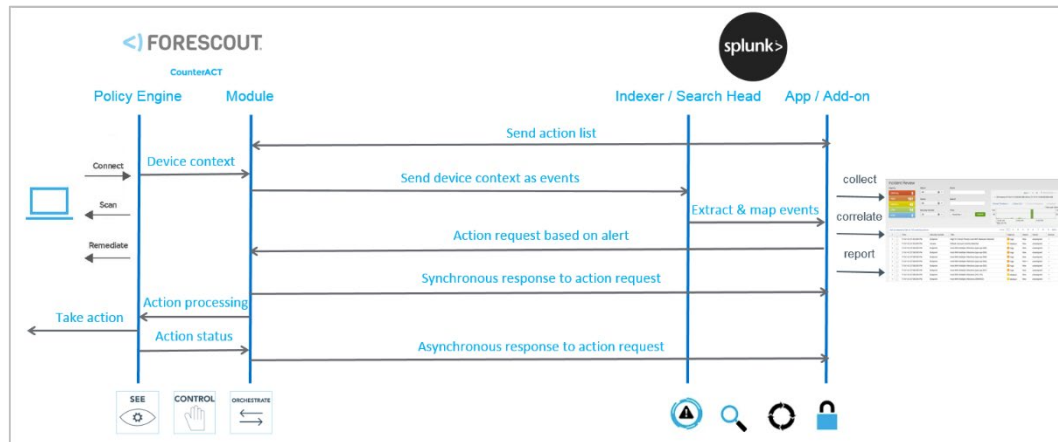


1. The Forescout platform discovers, classifies, and assesses devices as they connect to the network.
2. The Forescout platform sends real-time, pre-correlated device data, including networking context, in a single message packet to Splunk for long-term storage and easier correlation with other data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

Components

Four components are installed to support this integration:

1. Forescout eyeExtend for Splunk is installed on the CounterACT Appliance.
2. The Forescout Technology Add-on for Splunk is installed on the Splunk Enterprise Server.
3. The Forescout Adaptive Response Add-on for Splunk is installed on the Splunk Enterprise Server.
4. The Forescout App for Splunk is installed on the Splunk Enterprise Server.



Results of the integration:

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

Considerations

This section addresses any additional Forescout eyeExtend for Splunk considerations.

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

Splunk Instance Credentials

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

What to Do

To set up the integration:

- See [Requirements](#) to verify that all requirements are met
- [Install the Module](#)
- [Configure the Module](#)
- [Test the Module](#)
- [Create Splunk Policies Using Templates](#)
- (Optional) [Create Custom Splunk Policies](#)

Requirements

Verify that the following requirements are met:

- [Forescout Requirements](#)
- [Supported Vendor Requirements](#)
- [Splunk Cloud Requirements](#)
- [Forescout eyeExtend \(Extended Module\) Licensing Requirements](#)

Forescout Requirements

This module requires the following Forescout releases and other components:

- The Forescout App for Splunk interacts with an Enterprise Manager running version 8.1 or 8.2.
- A module license for Forescout eyeExtend for Splunk. See [Forescout eyeExtend \(Extended Module\) Licensing Requirements](#).
- Verify that the following policies are active:
 - Classification
 - Compliance

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

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

To categorize policies:

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

Supported Vendor Requirements

The Forescout App & Add-ons for Splunk published on Splunkbase and Forescout eyeExtend for Splunk support the following Splunk versions:

- Splunk Enterprise version 7.0 or 7.2
- Splunk Enterprise Security version 5.2
- For information about the vendor models (hardware/software) and versions (product/OS) that are validated for integration with this Forescout component, refer to the [Forescout Compatibility Matrix](#).

Splunk Cloud Requirements

- Splunk Cloud Enterprise version 7.2
- Splunk data integration requires a Splunk Cloud license. Refer to the following:

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

For more information about Splunk Cloud, see [Appendix B: Splunk Cloud Deployments](#).

Forescout eyeExtend (Extended Module) Licensing Requirements

This Forescout eyeExtend module requires a valid license. Licensing requirements differ based on which licensing mode your deployment is operating in:

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

To identify your licensing mode:

- From the Console, select **Help > About Forescout**.




Per-Appliance Licensing Mode

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

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

To continue working with the module after the demo period expires, you must purchase a permanent module license.

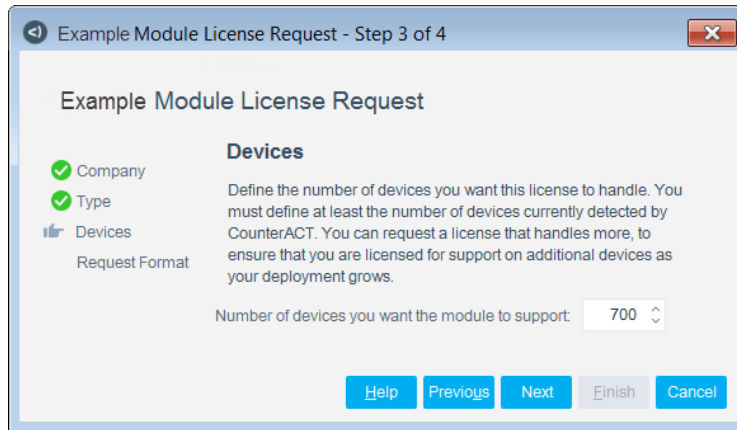
Demo license extension requests and permanent license requests are made from the Console.

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

Requesting a License

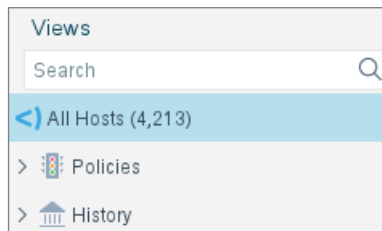
When requesting a demo license extension or permanent license, you are asked to provide the device *capacity* requirements. This is the number of devices that you want this license to handle. You must define at least the number of devices currently detected by the Forescout platform. You can request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

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



To view the number of currently detected devices:

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




Flexx Licensing Mode

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

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

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

Each eyeExtend license has an associated capacity, indicating the number of endpoints the license can handle. The capacity of each eyeExtend license varies by module but does not exceed the capacity of the Forescout eyeSight license.

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

More License Information

For more information on eyeExtend (Extended Module) licenses:

- **Per-Appliance Licensing.** Refer to the *Forescout Administration Guide*.
- **Flexx Licensing.** Refer to the *Flexx Licensing How-to Guide*.

You can also contact your Forescout sales representative for more information.

Install the Module

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

This section describes the steps for setting up your system when integrating with Splunk:

- [Upgrade to eyeExtend for Splunk 2.9.2](#)
- [Install Forescout eyeExtend for Splunk](#)

Upgrade to eyeExtend for Splunk 2.9.2

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 2.9.2 and the module does not operate as expected, you cannot roll back to a previous release.

It is recommended to 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 to Forescout version 8.1 or 8.2. This includes upgrading Forescout eyeExtend for Splunk to version 2.9.2. Refer to the *Forescout Administration Guide* for instructions. See [Additional Forescout Documentation](#) for information on how to access this guide.
- 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 HTTP Targets tab.
- 9. Select each of the channels and then select **Test**.

The upgrade is complete.

Install Forescout eyeExtend for Splunk


This section describes how to download the module from the Forescout Customer Support site and install it in the Console.


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

To install the module:

1. Navigate to one of the following Forescout download portals, depending on the licensing mode your deployment is using:
 - [Product Updates Portal](#) - **Per-Appliance Licensing Mode**
 - [Customer Portal, Downloads Page](#) - **Flexx Licensing Mode**
- To identify your licensing mode, select **Help > About ForeScout** from the Console.
2. Download the module `.fpi` file.
3. Save the file to the machine where the Console is installed.
4. Log into the Console and select **Options** from the **Tools** menu.
5. Select **Modules**. The Modules pane opens.
6. Select **Install**. The Open dialog box opens.
7. Browse to and select the saved module `.fpi` file.
8. Select **Install**. The Installation screen opens.

9. Select **I agree to the License Agreement** to confirm that you have read and agree to the terms of the License Agreement and select **Install**. The installation cannot proceed unless you agree to the license agreement.

 *The installation begins immediately after selecting Install and cannot be interrupted or canceled.*

 *In modules that contain more than one component, the installation proceeds automatically one component at a time.*

10. When the installation completes, select **Close** to close the window. The installed module is displayed in the Modules pane.

 *Some components are not automatically started following installation.*

Configure the Module

After Forescout eyeExtend for Splunk is installed on your targeted CounterACT Appliance, configure the module to ensure that the Forescout platform can communicate with the Splunk instance.

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

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

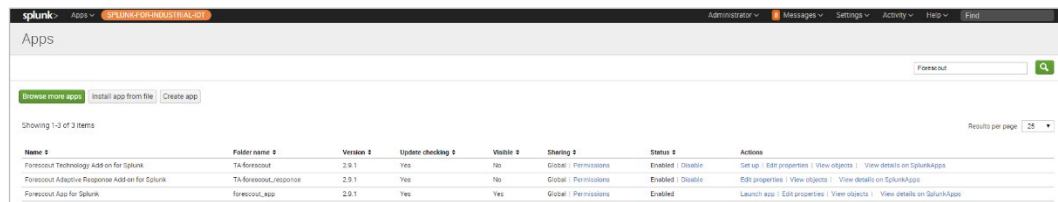
1. The installation of the Forescout App for Splunk and the two Add-ons are required to be installed first. Refer to the *Forescout App & Add-ons for Splunk How-to Guide* for more information.
2. Obtain [Splunk Instance Credentials](#) for configuring the HTTP targets on Forescout eyeExtend for Splunk.
3. [Obtain an Authorization Token](#). Using Splunk Event Collector messages is the recommended protocol. Event Collector is a proprietary Splunk HTTP(S) channel. Follow the procedure described in this section to use Event Collector Messages.
4. [Secure Connection Messaging to the Splunk Enterprise Server](#).
5. (Optional) Add a Splunk target. The following protocols can be used by the Forescout platform to send information to Splunk:
 - **Using HTTPS POST messages to the Splunk REST API:** Define server targets. See [Add a Splunk HTTP Target](#) for details.
 - **Using Syslog messaging:** To use Syslog, define one or more Splunk Enterprise server targets. See [Add a Splunk Syslog Target](#) for details.
6. (Optional) If you are configuring the Forescout Technology Add-on for Splunk, see [Set Up the Forescout Technology Add-on](#) for details.
7. On Forescout eyeExtend for Splunk, [Test the Module](#).

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. Log in to the Splunk Instance.
2. Search the Splunk Apps page to locate the Forescout Technology Add-on for Splunk.



3. Under Actions, select **Set up**.

The screenshot shows the 'CounterACT Configurations' form. It includes fields for 'CounterACT IP Address or Hostname' (with 'forescout.com' entered), 'Enter password (Alert Service Authorization Token)', 'Confirm password', and 'Index for CounterACT events' (with 'factscenter' entered). A note states: 'The password will be encrypted and stored in Splunk's password store. It will not be displayed here if this page is visited again.' There are 'Cancel' and 'Save' buttons at the bottom.

4. 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.

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

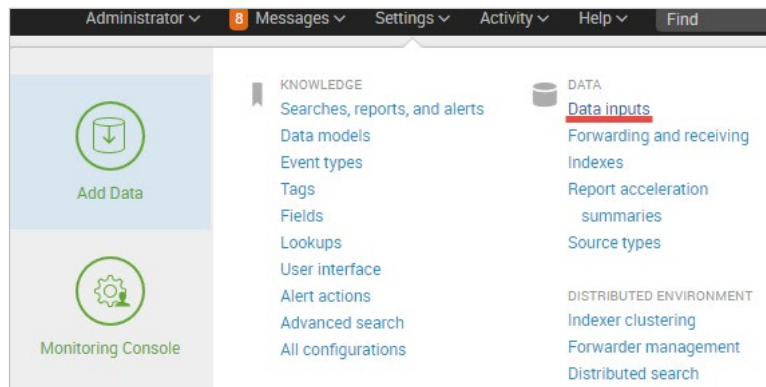
Obtain an Authorization Token

This section describes how to get an Authentication Token. This key is required for creating a Splunk HTTP Target.

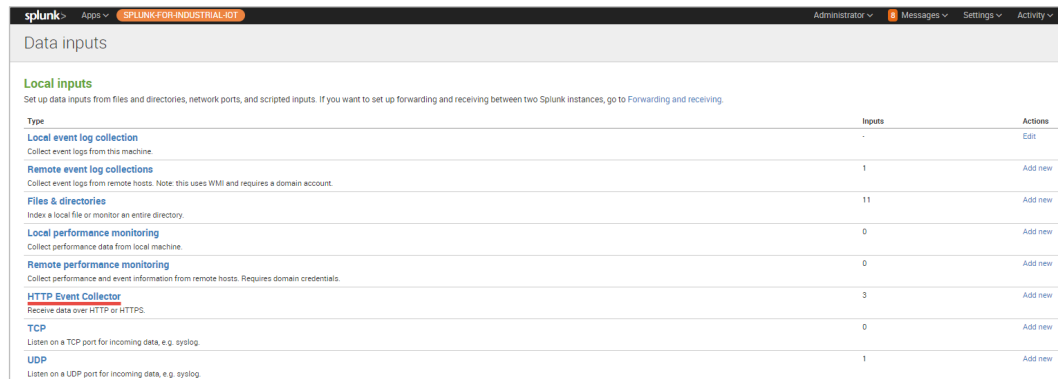
Before you can configure event collectors in Forescout eyeExtend for Splunk, you must first get a token value (key) from the HTTP Event Collector Data Input.

To obtain an authorization token to define an event collector:

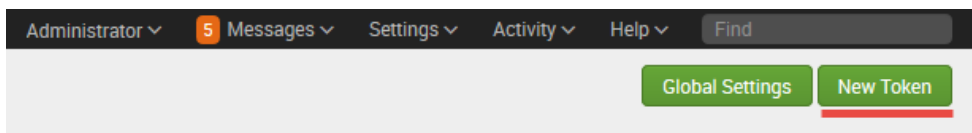
1. In the Forescout App for Splunk, select **Settings** and then select **Data inputs**.



The Data Inputs page opens.



2. Select **HTTP Event Collector**.



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

The screenshot shows the 'Add Data' configuration page in Splunk. The progress bar indicates the 'Select Source' step is complete. On the left, under 'Files & Directories', the 'HTTP Event Collector' is selected. The right panel is titled 'Configure a new token for receiving data over HTTP'. It contains the following fields and options:

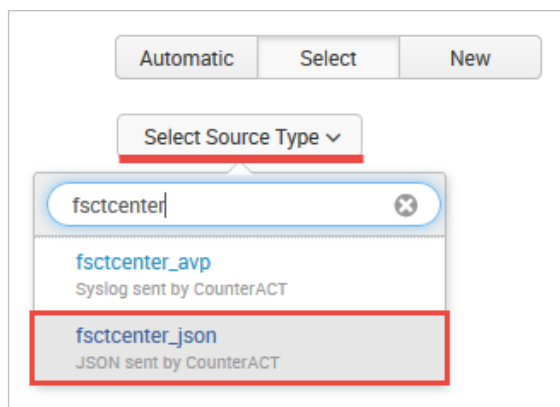
- Name:** A text input field.
- Source name override:** A text input field with 'optional' as a placeholder.
- Description:** A text input field with 'optional' as a placeholder.
- Output Group (optional):** A dropdown menu currently set to 'None'.
- Enable indexer acknowledgement:** An unchecked checkbox.

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

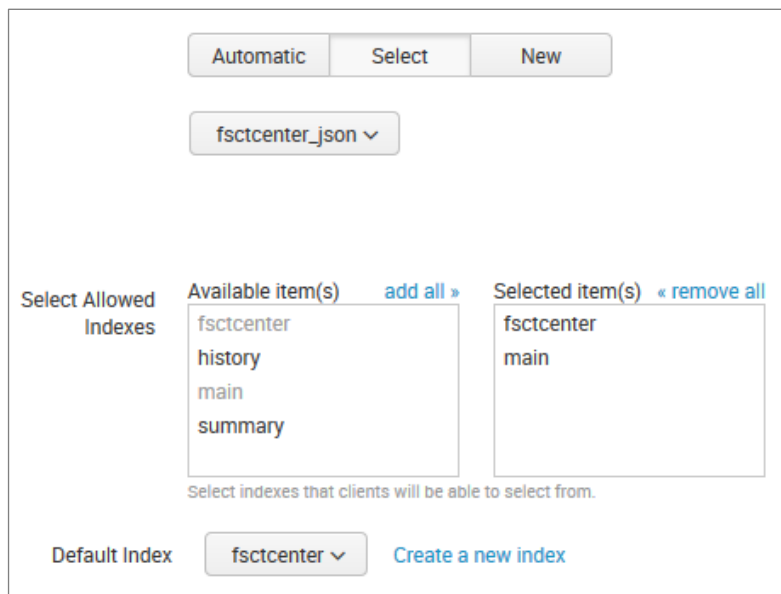
The screenshot shows the 'Add Data' configuration page in Splunk, now at the 'Input Settings' step. The progress bar shows 'Input Settings' is the current step. The page contains the following sections:

- Source type:** A section with a description and three tabs: 'Automatic', 'Select' (which is highlighted with a red underline), and 'New'.
- Index:** A section with a description and a list of available indexes: 'fsctcenter', 'history', 'main', and 'summary'. Below the list is a note: 'Select indexes that clients will be able to select from.'
- Default index:** A dropdown menu currently set to 'Default' and a link to 'Create a new index'.

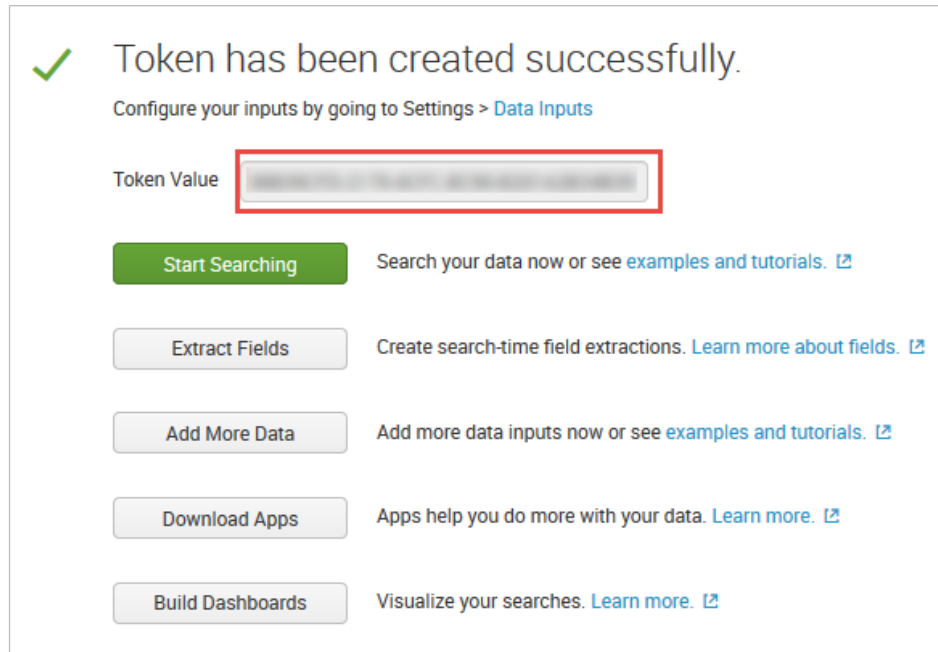
5. In the Source type section, select **Select**.



6. Select **Select Source Type** and enter *fscntcenter* in the search field. Then select **fscntcenter_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 *fscntcenter*.



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 is required in order to [Add a Splunk HTTP Target](#).

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

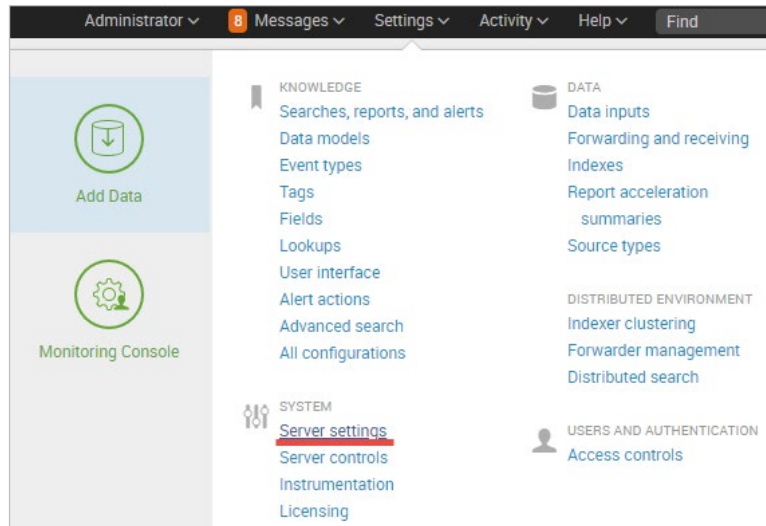
Secure Connection Messaging to the Splunk Enterprise Server

Forescout eyeExtend for Splunk updates messages sent to the Splunk Enterprise server via HTTP Event Collector or HTTP REST. It can also use HTTPS.

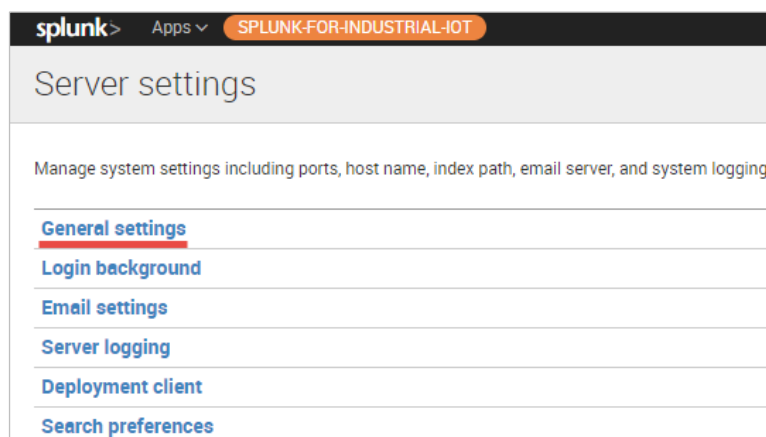
If the Splunk Enterprise server is configured to use SSL (HTTPS) over Splunk Web, by default, Splunk Enterprise generates a self-signed certificate that it uses for HTTPS messaging. Because this certificate is not signed by any certificate authority, the Forescout platform does not validate SSL handshakes based on this certificate.

To select HTTPS:

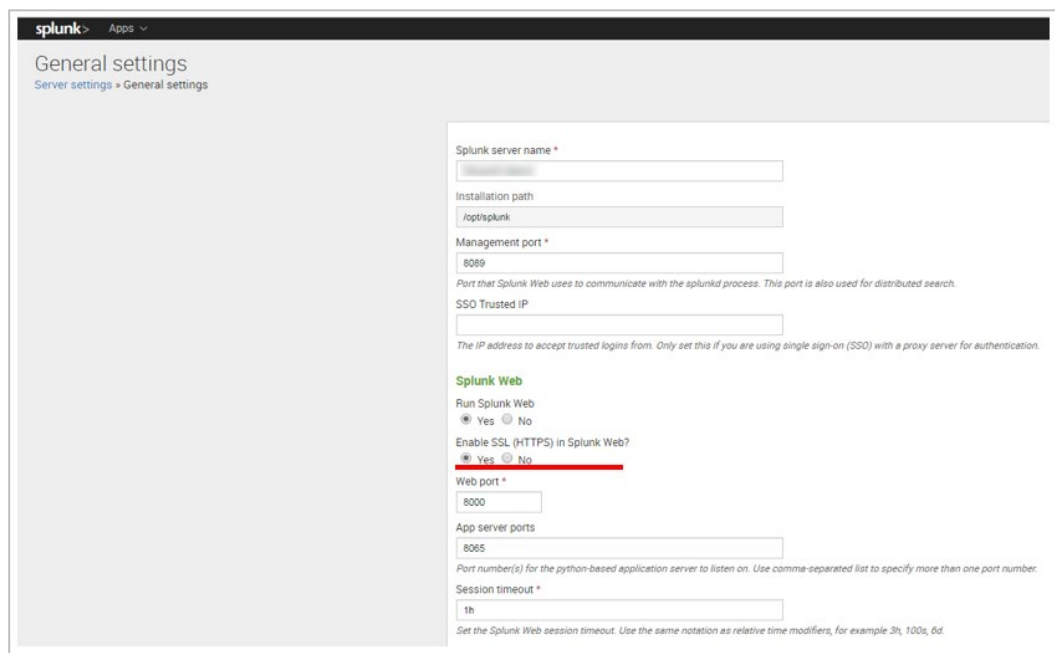
1. Select **Settings** > **Server settings**.



2. Select **General settings**.



3. In the Splunk Web section, review the **Enable SSL (HTTPS) in Splunk Web** setting.



The screenshot shows the 'General settings' page in the Splunk web interface. The 'Splunk Web' section is highlighted with a red border. It contains the following fields and options:

- Splunk server name ***: A text input field.
- Installation path**: A text input field with the default value `/opt/splunk`.
- Management port ***: A text input field with the default value `8089`. Below it is a note: "Port that Splunk Web uses to communicate with the splunkd process. This port is also used for distributed search."
- SSO Trusted IP**: A text input field. Below it is a note: "The IP address to accept trusted logins from. Only set this if you are using single sign-on (SSO) with a proxy server for authentication."
- Splunk Web** section header.
- Run Splunk Web**: Radio buttons for **Yes** (selected) and **No**.
- Enable SSL (HTTPS) in Splunk Web?**: Radio buttons for **Yes** (selected) and **No**. This section is highlighted with a red border.
- Web port ***: A text input field with the default value `8000`.
- App server ports**: A text input field with the default value `8065`. Below it is a note: "Port number(s) for the python-based application server to listen on. Use comma-separated list to specify more than one port number."
- Session timeout ***: A text input field with the default value `1h`. Below it is a note: "Set the Splunk Web session timeout. Use the same notation as relative time modifiers, for example 3h, 100s, 6d."

4. To enable HTTPS, select **Yes**.

5. Select **Save**.

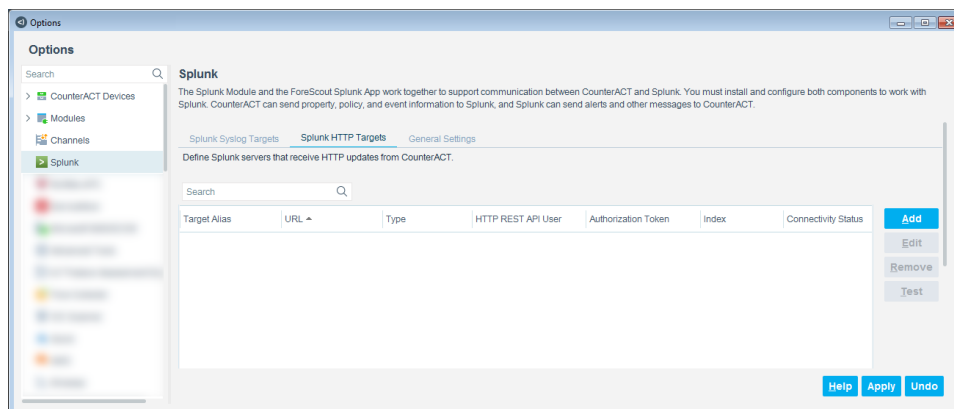
For more information about HTTPS configuration in Splunk, refer to the Splunk knowledge base.

Add a Splunk HTTP Target

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

To configure the module to use HTTP REST messaging:

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



3. Select **Add**.

4. From the Splunk HTTP Type dropdown menu, select and configure the setting for one of the following:
- [Event Collector](#)
 - [REST API](#)

Event Collector

An Event Collector is a Splunk-specific message type used to report event and endpoint data. The default port in Splunk for these messages is 8088.

To configure an event collector:

1. In the Add Splunk HTTP Target Details General pane, select **Event Collector** from the Splunk HTTP Type drop-down menu.
2. Configure the following settings:

Target Alias	Enter an alias to make it easier for you to select destinations when sending updates to the Splunk Enterprise server.
POST to URL	<p>Enter the target URL displayed in the POST message header. In most cases, the URL takes the form of the example shown. Replace <i>my.splunk.com</i> with the FQDN or the IPv4 or IPv6 address of your Splunk Enterprise server. Enclose an IPv6 address in square brackets, for example:</p> <p><code>https://[fd6f: :df7]:8088/services/collector</code></p> <p>If the Splunk Enterprise server does not use the default port, specify the actual port used. See Appendix A: Default Communication Settings.</p>
Index	Enter the index for the Event Collector target or keep the default value of <i>fsctcenter</i> . This is the index on the Splunk Enterprise server to which the update messages are sent. Each index must be uniquely named.
Comment	(Optional) Enter text that indicates the location or other information that identifies the server.
Validate Server Certificate	<p>Select this option to validate the identity of the third-party server before establishing a connection, when the eyeExtend module communicates as a client over SSL/TLS. To validate the server certificate, either of the following certificate(s) must be installed:</p> <ul style="list-style-type: none"> ▪ Self-signed server certificate – the server certificate must be installed on the CounterACT Appliance ▪ Certificate Authority (CA) signed server certificate – the CA certificate chain (root and intermediate CA certificates) must be installed on the CounterACT Appliance <p>Use the Certificates > Trusted Certificates pane to add the server certificate to the Trusted Certificate list. For more information about certificates, refer to the appendix, "Configuring the Certificate Interface" in the <i>Forescout Administration Guide</i>.</p>
Authorization Token	In the Splunk App HTTP Event Collector pane, copy the <i>Token Value</i> and paste it in the Authorization Token field.

3. Select **Next**.

Add Splunk HTTP Target Details - Step 2 of 2

Add Splunk HTTP Target Details

General

Connection Test

Connection Test

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

On managed cloud deployments, uncheck the checkboxes for "Check if target is reachable", "Check REST API communication" and "Check data input and index", which are for on-prem deployments only.

Enable Test Configuration ☒

Check if target is reachable ☒ (Check executed via ICMP ping, on-prem only)

Check REST API communication ☐ (Server roles are retrieved if successful, on-prem only)

Check data input and index ☒ (Check executed via REST API communication, on-prem only)

Management Username

Management Password

Verify Password

Management Port

Help Previous Next Finish Cancel

4. Configure the following settings:

Enable Test Configuration	This option is enabled by default. Disable this option if you need to disable the testing of the Splunk HTTP Target connection.
Check if target is reachable	Checks the Splunk HTTP target connection by executing an ICMP ping. This option is enabled by default. Disable this option if you do not need to check if the target is reachable.
Check REST API communication	<p>Verifies if the Splunk Enterprise server's REST API interface is reachable. If it is reachable, this test retrieves and displays the server roles configured on the Splunk Enterprise server.</p> <p>This option is enabled by default. The Management Username, Management Password, Verify Password, and Management Port fields are also required.</p> <p>Disable this option if you do not need to check REST API communication.</p> <p>If both Check REST API communication and Check data input and index are disabled, the fields for Management Username, Management Password, Verify Password, and Management Port are not required and are disabled.</p>

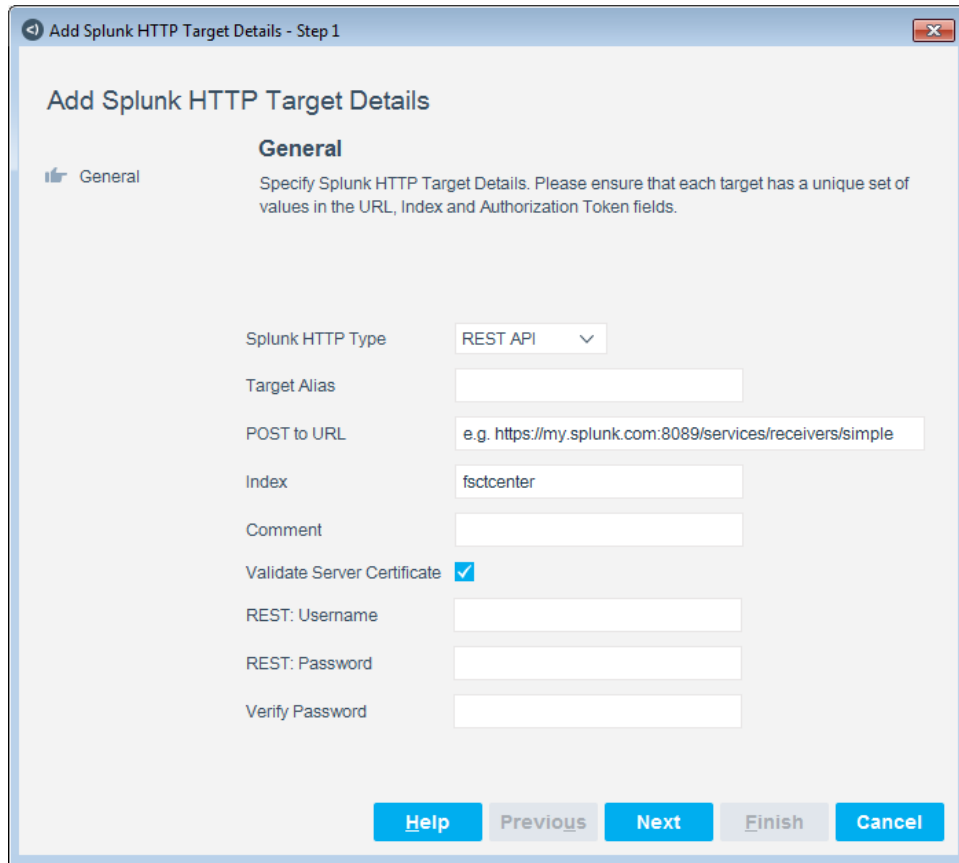
Check data input and index	<p>Verifies if the data input configured in the Splunk HTTP target is enabled.</p> <p>For HTTP Event Collector, it also verifies if the index configured in the target on Forescout eyeExtend for Splunk is also configured in that data inputs settings on the Splunk Enterprise server.</p> <p>This option is enabled by default. The Management Username, Management Password, Verify Password, and Management Port fields are also required.</p> <p>Disable this option if you do not need to check data input and index.</p> <p>If both Check REST API communication and Check data input and index are disabled, the fields for Management Username, Management Password, Verify Password, and Management Port are not required and are disabled.</p>
Management Username	The username the Forescout platform uses to access the API on Splunk. Refer to the <i>Forescout App & Add-ons for Splunk How-to Guide</i> .
Management Password	The password credentials the Forescout platform uses to access the API on Splunk. Refer to the <i>Forescout App & Add-ons for Splunk How-to Guide</i> .
Verify Password	Re-enter the password to verify it.
Management Port	<p>The default port is 8088.</p> <p>See Appendix A: Default Communication Settings.</p>

5. Select **Finish**. The new HTTP Event Collector target is displayed in the Splunk pane.

REST API

To configure a REST API:

1. In the Add Splunk HTTP Target Details General pane, select **REST API** from the Splunk HTTP Type drop-down menu.



2. Configure the following settings:

Target Alias	Enter an alias to make it easier for you to select destinations when sending updates to the Splunk Enterprise server.
POST to URL	Enter the target URL displayed in the POST message header. In most cases the URL takes the form of the example shown. Replace <i>my.splunk.com</i> with the FQDN or the IPv4 or IPv6 address of your Splunk Enterprise server. Enclose an IPv6 address in square brackets. If the Splunk Enterprise server does not use the default port, specify the actual port used. See Appendix A: Default Communication Settings .
Index	Enter the index for the HTTP REST API target or keep the default value of <i>fscntcenter</i> . Each index must be uniquely named.
Comment	(Optional) Enter text that indicates the location or other information that identifies the server.

Validate Server Certificate	<p>Select this option to validate the identity of the third-party server before establishing a connection, when the eyeExtend module communicates as a client over SSL/TLS. To validate the server certificate, either of the following certificate(s) must be installed:</p> <ul style="list-style-type: none"> Self-signed server certificate – the server certificate must be installed on the CounterACT Appliance Certificate Authority (CA) signed server certificate – the CA certificate chain (root and intermediate CA certificates) must be installed on the CounterACT Appliance <p>Use the Certificates > Trusted Certificates pane to add the server certificate to the Trusted Certificate list. For more information about certificates, refer to the appendix, "Configuring the Certificate Interface" in the <i>Forescout Administration Guide</i>.</p>
REST: Username REST: Password	Enter the credentials that the Forescout platform uses to access the API on Splunk. Enter the credentials of the account created in Splunk for the Forescout platform. Refer to the <i>Forescout App & Add-ons for Splunk How-to Guide</i> .
Verify Password	Re-enter the password to verify it.

3. Select **Next**.

Test the Connection

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

Add Splunk HTTP Target Details - Step 2 of 2

Add Splunk HTTP Target Details

Connection Test

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

On managed cloud deployments, uncheck the checkboxes for "Check if target is reachable", "Check REST API communication" and "Check data input and index", which are for on-prem deployments only.

Enable Test Configuration ☒

Check if target is reachable ☒ (Check executed via ICMP ping, on-prem only)

Check REST API communication ☒ (Server roles are retrieved if successful, on-prem only)

Management Username: Corporate

Management Password: [Redacted]

Verify Password: [Redacted]

Management Port: 8089

Buttons: Help, Previous, Next, Finish, Cancel

1. For REST API, the first three options in this pane are editable. The other fields are read-only.


Enable Test Configuration	This option is enabled by default. Disable this option to disable testing of the Splunk HTTP Target connection.
Check if target is reachable	Checks the Splunk HTTP target connection by executing an ICMP ping. This option is enabled by default. Disable this option if you do not need to check if the target is reachable.
Check REST API communication	Verifies if the Splunk Enterprise server's REST API interface is reachable. If it is reachable, this test retrieves and displays the server roles configured on the Splunk Enterprise server. This option is enabled by default. Disable this option if you do not need to check REST API communication.
Management Username	(Read-Only) The username and password credentials that the Forescout platform uses to access the API on Splunk.
Management Password	Refer to the <i>Forescout App & Add-ons for Splunk How-to Guide</i> .
Verify Password	(Read-Only) Applicable to Event Collector only.
Management Port	(Read-Only) The default port is 8089. See Appendix A: Default Communication Settings .

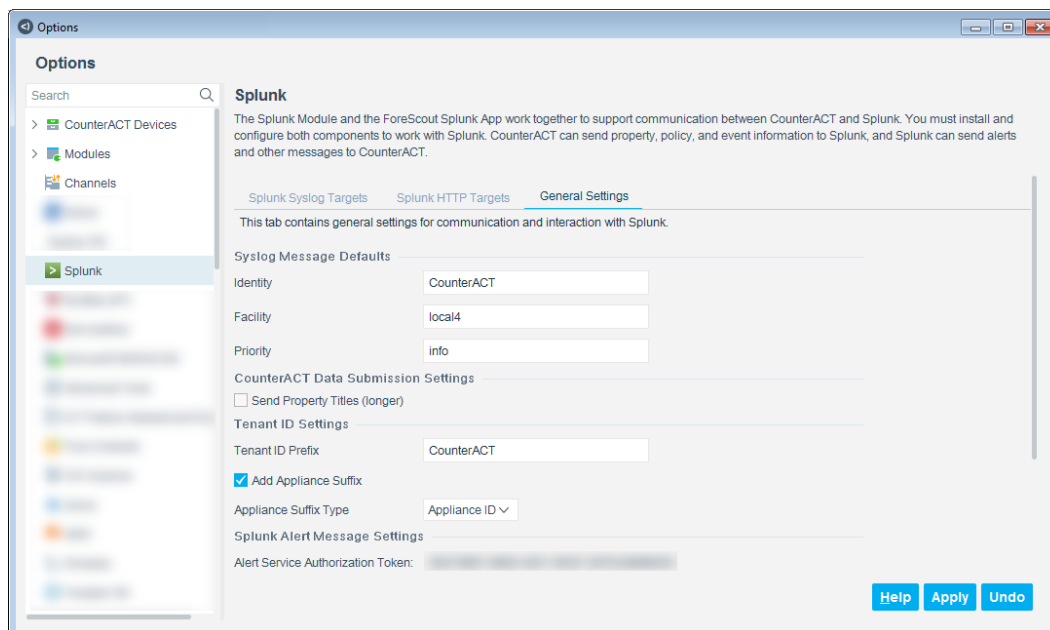
2. Select **Finish**. The server is displayed in the Splunk pane, Splunk HTTP Targets tab.
3. Repeat the steps for additional Event Collector/REST API Splunk HTTP targets.

Modify Splunk Enterprise Server Settings

You can modify the Splunk Enterprise server settings in the Console.

To modify Splunk Enterprise server settings:

1. Select the server, then select **Edit**.
 -  Verify that data inputs defined on the Splunk Enterprise server use the port and other settings you define here. Refer to the *Forescout App & Add-ons for Splunk How-to Guide*.
2. In the Splunk pane, select the General Settings tab.



3. Enter the following options and fields that are relevant when REST/HTTP messaging is used to report data to Splunk:

Syslog Message Defaults	Identity	Free-text field for identifying the Syslog message. This value overrides default message settings of the Syslog Plugin, but only for messages sent to Splunk.
	Facility	The Syslog message facility that is transmitted as part of the message. This value overrides default message settings of the Syslog Plugin, but only for messages sent to Splunk.
	Priority	The Syslog message severity that is transmitted as part of the message Priority field. This value overrides default message settings of the Syslog Plugin, but only for messages sent to Splunk.
CounterACT Data Submission Settings	Send Property Titles	<p>The Forescout platform sends host property information to Splunk as Field:Value pairs in JSON format. By default, the Field: label is the internal property tag of each property. Select this option to send two sets of property value information to Splunk:</p> <p>Using the property tag as the Field: label: va_os : Windows 8.1 64-bit Pro</p> <p>Using the property's full name as the Field: label: Windows Version : Windows 8.1 64-bit Pro</p>


Tenant ID Settings	Tenant ID Prefix	Specify the prefix for the Tenant ID value in update messages. Forescout eyeExtend for Splunk generates a random suffix (on each appliance) and appends it to the Tenant ID prefix value to generate the Tenant ID. The Tenant ID is then sent as part of every update message sent by Forescout eyeExtend for Splunk to the Splunk Enterprise server.
	Add Appliance Suffix	Select this option to enable or disable the Tenant ID suffix generation on each CounterACT Appliance.
	Appliance Suffix Type	This configuration is possible only if the Add Appliance Suffix option is selected. This field lets you control the nature of the Tenant ID suffix generated. Depending on your selection, the Tenant ID suffix corresponding to each CounterACT Appliance can be: <ul style="list-style-type: none"> ▪ GUID or Globally Unique Identifier ▪ Appliance IP address (IPv4 or IPv6 address) ▪ Appliance ID (a Forescout platform-generated node identifier)
Splunk Alert Message Settings	Alert Service Authorization Token	This string is used in the HTTP message header of alert messages sent to the Forescout platform by the Forescout App for Splunk.

4. Select **Apply**.
5. When prompted for confirmation, select **Yes**, and then select **Close**.
6. The best practice is to perform a **Test** after setting up a connection. See [Test the Module](#).

Add a Splunk Syslog Target

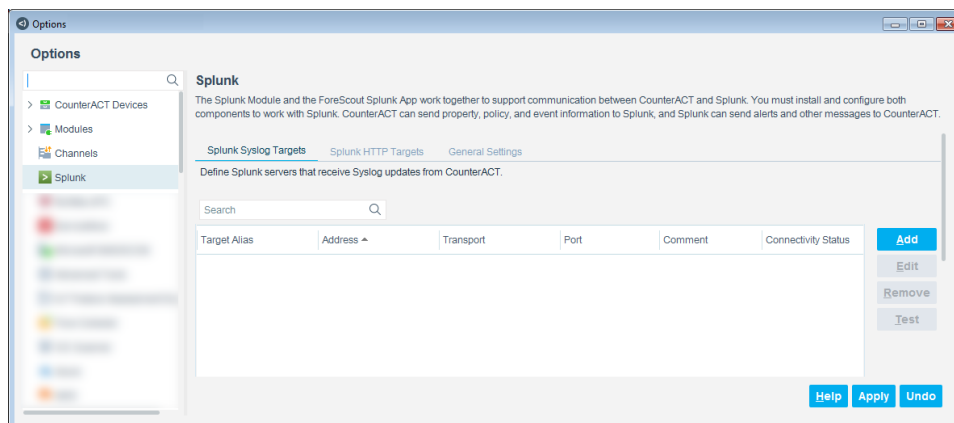
(Optional) Use the following procedure to configure the module to send information to Splunk using Syslog messages instead of Splunk Event Collector messages.

The Syslog message payload is sent in JSON format. The Syslog Maximum Transmission Unit (MTU) is restricted by an RFC standard. If the message payload is larger than the defined Syslog MTU, the message will be truncated. The truncated message is delivered and displayed in the Splunk console, but not in JSON format. The Syslog size depends on the transport layer, refer to <https://tools.ietf.org/html/rfc5426#section-3.2>.

 *Forescout eyeExtend for Splunk does not support secure communication for Syslog Targets.*

To configure Splunk Syslog Targets:

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




3. Select **Add**.

 The screenshot shows the 'Add Splunk Syslog Target Details - Step 1' dialog box. It has a 'General' tab selected. The main area contains the following fields: 'Target Alias' (text input), 'Address' (text input), 'TCP/UDP' (dropdown menu with 'UDP' selected), 'Port' (spin box with '515' selected), and 'Comment' (text input). At the bottom, there are 'Help', 'Previous', 'Next', 'Finish', and 'Cancel' buttons.

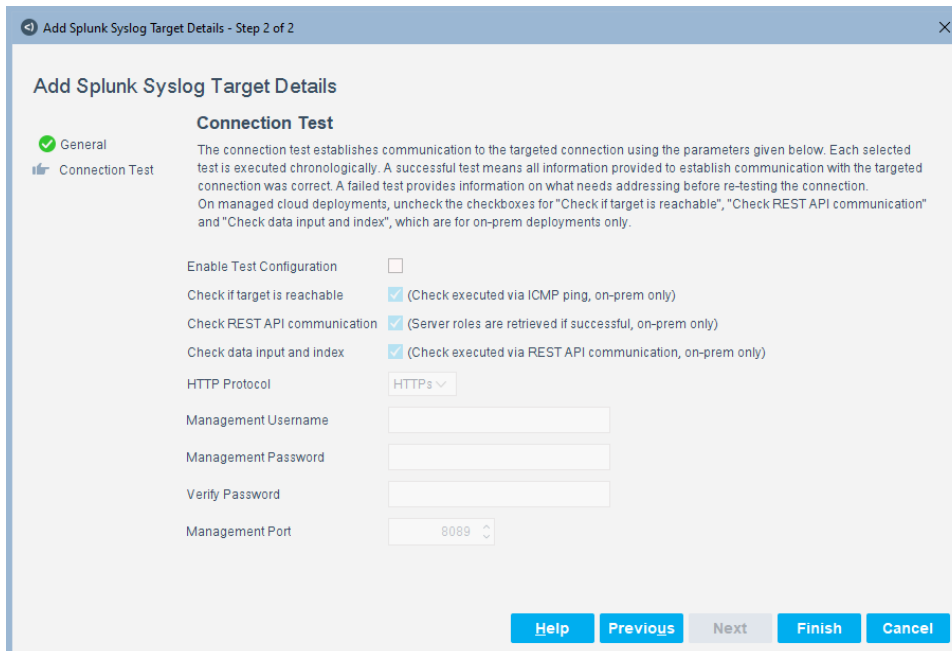
4. Enter the following information:

Target Alias	Enter an alias to make it easier for you to select destinations when sending updates to the Splunk Enterprise server.
Address	Enter the FQDN or IPv4 or IPv6 address of the Splunk Enterprise server.

TCP/UDP	Select the protocol used for Syslog messaging with the server. <ul style="list-style-type: none"> UDP (default): Select if you are concerned with speed of data messaging. TCP: Select if you are concerned with accurate and successful transference of data.
Port	Select the port on the server that is used for Syslog messaging. If the Splunk Enterprise server uses a different port from the default, specify the actual port used. See Appendix A: Default Communication Settings .
Comment	(Optional) Enter text that indicates the location or other information that identifies the server.



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

5. Select **Next** and then disable the checkbox for **Enable Test Configuration**. (**Test** is not recommended for Syslog as the protocol does not send acknowledgments back to the sender.)



Add Splunk Syslog Target Details - Step 2 of 2

Add Splunk Syslog Target Details

General  **Connection Test** 

Connection Test

The connection test establishes communication to the targeted connection using the parameters given below. Each selected test is executed chronologically. A successful test means all information provided to establish communication with the targeted connection was correct. A failed test provides information on what needs addressing before re-testing the connection. On managed cloud deployments, uncheck the checkboxes for "Check if target is reachable", "Check REST API communication" and "Check data input and index", which are for on-prem deployments only.

Enable Test Configuration ☐

Check if target is reachable ☒ (Check executed via ICMP ping, on-prem only)

Check REST API communication ☒ (Server roles are retrieved if successful, on-prem only)

Check data input and index ☒ (Check executed via REST API communication, on-prem only)

HTTP Protocol

Management Username

Management Password

Verify Password

Management Port

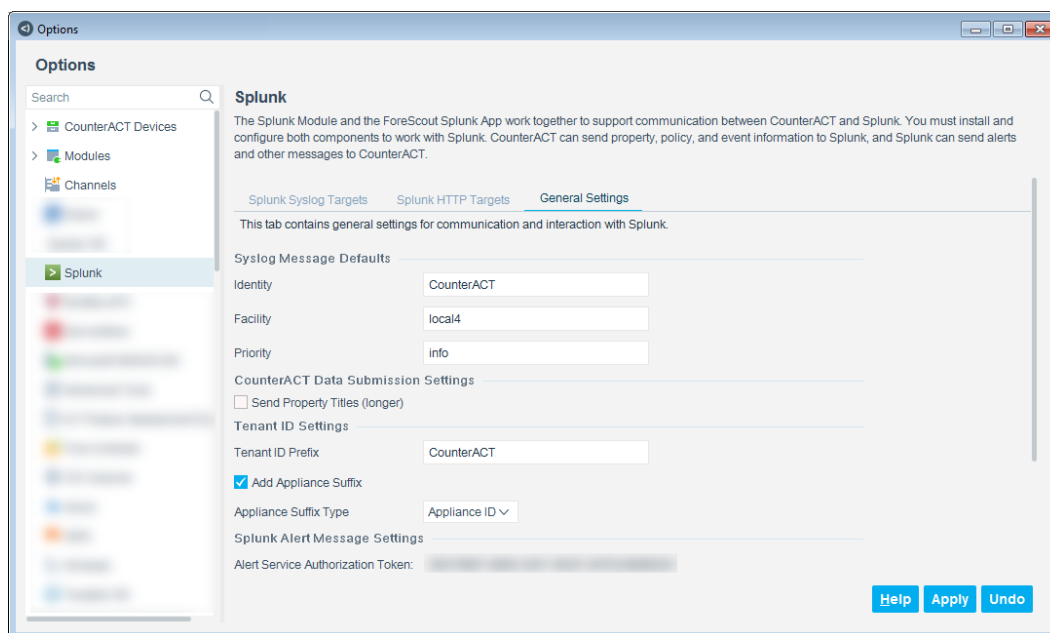
Help Previous Next Finish Cancel

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

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

General Settings

1. In the Splunk pane, select the General Settings tab.



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

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

CounterACT Data Submission Settings	Send Property Titles (longer)	<p>The Forescout platform sends host property information to Splunk as Field:Value pairs in JSON format. By default, the Field: label is the internal property tag of each property. Select this option to send two sets of property value information to Splunk:</p> <p>Using the property tag as the Field: label: va_os : Windows 8.1 64-bit Pro</p> <p>Using the property's full name as the Field: label: Windows Version : Windows 8.1 64-bit Pro</p>
Tenant Settings	Tenant ID Prefix	<p>Specify the prefix for the Tenant ID value in update messages.</p> <p>You can choose to configure the module to generate a suffix to the tenant ID prefix. If suffix generation is selected, the module will generate a suffix (on each Appliance) and append it to the Tenant ID prefix value to generate the Tenant ID. The Tenant ID is then sent as part of every update message sent by Forescout eyeExtend for Splunk to the Splunk Enterprise server. In the configuration wizard, enable or disable the Tenant ID suffix generation and specify the type of suffix value in the Tenant ID.</p>
	Add Appliance Suffix	Select this option to enable or disable the Tenant ID suffix generation on each CounterACT Appliance.
	Appliance Suffix Type	<p>This configuration is possible only if the Add Appliance Suffix option is selected. This field lets you control the nature of the Tenant ID suffix generated. Depending on your selection, the Tenant ID suffix corresponding to each CounterACT Appliance can be:</p> <ul style="list-style-type: none"> ▪ GUID or Globally Unique Identifier ▪ Appliance IP address (IPv4 or IPv6 address) ▪ Appliance ID (a Forescout platform-generated node identifier)
Splunk Alert Message Settings	Alert Service Authorization Token	This string is used in the HTTP message header of alert messages sent to the Forescout platform by the Forescout App for Splunk.

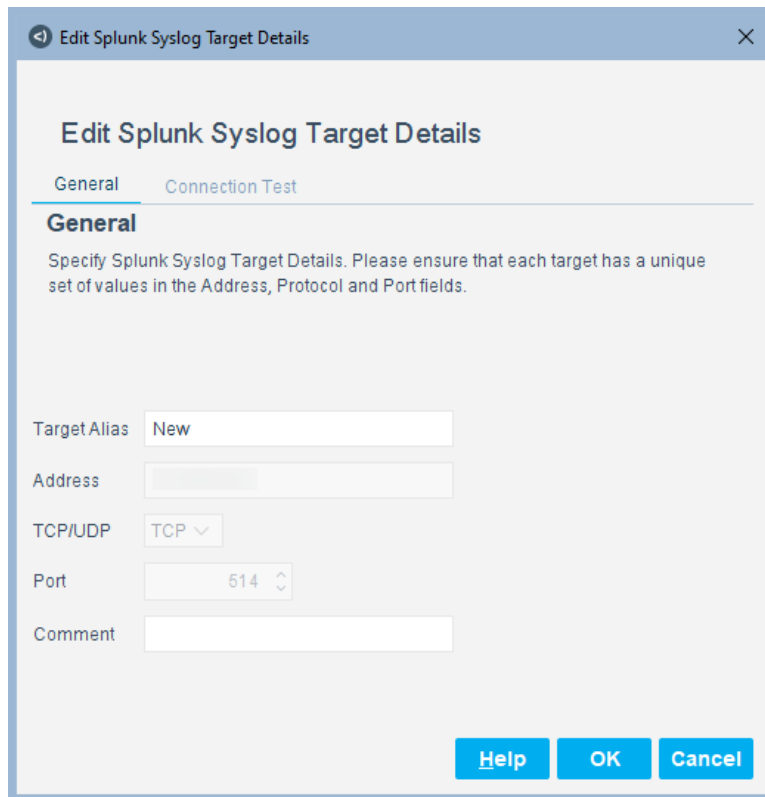
2. In the Splunk pane, select **Apply**.
3. When prompted for confirmation, select **Yes**, and then select **Close**.
4. You are now ready to [Test the Module](#).

Edit Splunk Syslog Targets


Only limited editing can be done on existing Splunk Syslog Targets.

To edit Splunk Syslog Targets:

1. In the Options pane, select **Splunk**.
2. Select **Splunk** in the left pane. The Splunk pane opens to the Splunk Syslog Targets tab.
3. Select an existing syslog target and select **Edit**.



4. Edit the Target Alias and Comment fields, then select **OK**.
5. To change the TCP/UDP protocol or the Port, delete the Syslog Target and reconfigure it.

 *Even if you reconfigure a Syslog Target with the same Target Alias and Address, if a policy was previously configured to send messages to that Syslog Target, it will have to be reconfigured as well.*

Test the Module

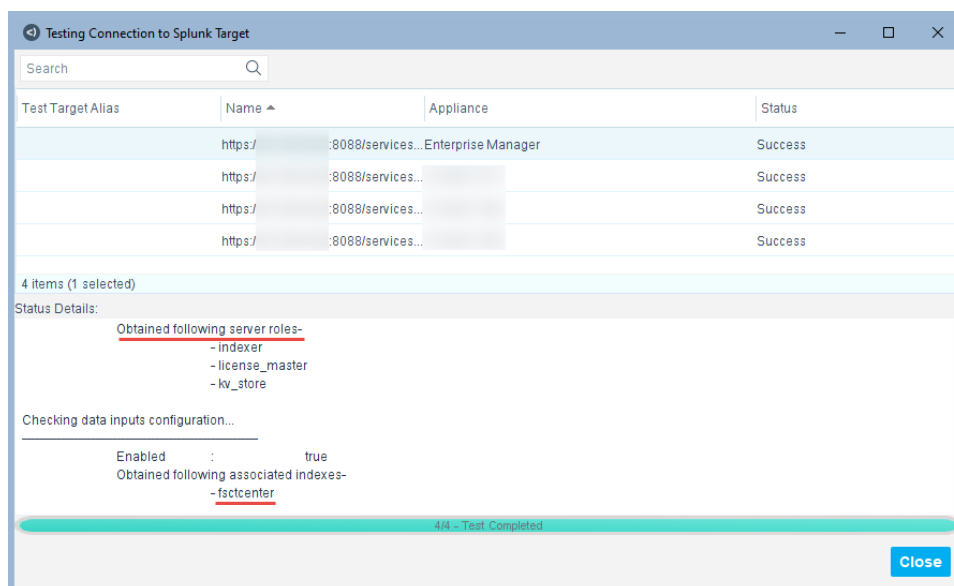
You can run a test to check the network connection to a Splunk Syslog target and/or a Splunk HTTP target (for Splunk Cloud).

After a test is run, details of the test are displayed to guide you in troubleshooting your connection difficulties.

To test the module configuration:

1. In the Options pane, select **Splunk**.
2. Select an item in the Splunk Syslog Targets tab or the Splunk HTTP Targets tab, and then select **Test**.
3. Using the configured settings, the Forescout platform attempts to connect with the Splunk Syslog/HTTP target.

The test results are displayed.



4. Select one of the appliances shown in the test results to view the Status Details listed in the bottom half of the screen. The results display the selections in the Connection Test pane. If **Check REST API communication** is not selected, the Status Details will not display server roles. If **Check data input and index** is not selected, the Status Details will not display the index.








Checking for reachability	Verifies if the Splunk Enterprise server can be reached via ICMP.
Checking for Splunk server roles	Verifies if the Splunk Enterprise server's REST API interface is reachable. If it is reachable, this test retrieves and displays server roles configured on the Splunk Enterprise server.

Checking data inputs configuration	Verifies if the data input configured in the Syslog/HTTP target is enabled. For HTTP Event Collector and Syslog TCP and Syslog UDP targets, it also verifies if the index configured in the target on Forescout eyeExtend for Splunk is also configured in that data inputs settings on the Splunk Enterprise server.
---	--

5. Review the test results. See [Understand Test Results](#).
6. Select **Close**. If necessary, make appropriate changes to the Splunk Enterprise and/or Forescout platform configuration and re-test.

Understand Test Results

The definitions in this section describe the various test states and their icons.

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

Create Splunk Policies Using Templates

This section describes how to use templates to create policies to detect, manage, and remediate endpoints based on the Splunk integration. See the following sections:

- [Create a Send Endpoint and Policy Details to Splunk Policy](#) that sends endpoint and policy information to Splunk.
- [Create a Splunk Stage 1: Add to HTTP Notification Action Group Policy](#) that detects messages that request the HTTP Notification action, and places the matching endpoints in the Splunk HTTP Notification Action Group. Use this as a reference and follow the correct action group based on the action requested from Splunk.
- [Create a Splunk Stage 2: Execute HTTP Notification Action Policy](#) that executes the HTTP Notification action for the endpoints in the HTTP Notification Action Group.



Before applying the templates, it is recommended that you have a basic understanding of Forescout platform policies before working with the templates. Refer to the Policy Management and Policy Templates chapters in the *Forescout Administration Guide*. See [Additional Forescout Documentation](#) for information on how to access this guide.

Create a Send Endpoint and Policy Details to Splunk Policy

This section describes how to use the Send Endpoint and Policy Details to Splunk template to set up a policy to send endpoint properties, classification, and policy details to the Splunk Enterprise server. This information is sent as batched messages. You can view the message sent to the Splunk Enterprise server using Splunk's App: Search & Reporting or the Forescout App for Splunk search capability.

Support for Batch Messaging

The properties of a host are batched together and sent to the Splunk Enterprise server as a single nested JSON message. The batched message encapsulates all device properties for each device, thus improving overall system performance for both Forescout eyeExtend for Splunk and the Splunk Enterprise server.

To view batched messages:

1. Select **Search & Reporting**.

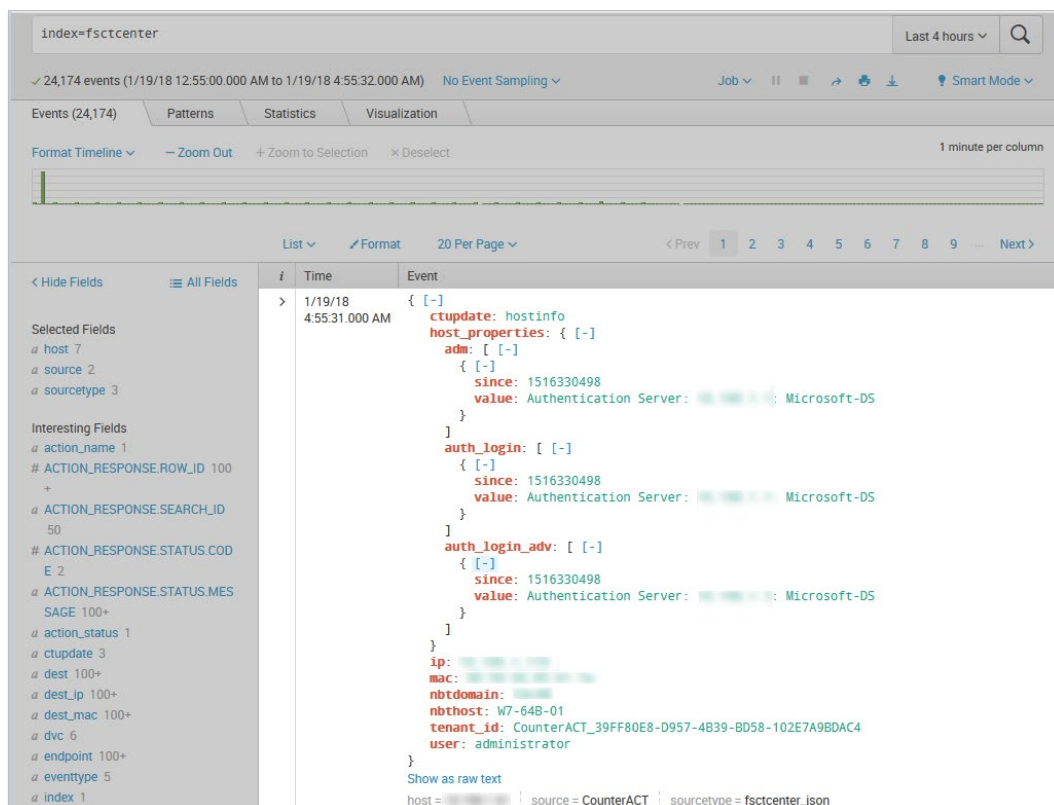


2. In the **New Search** field, enter "index=fsctcenter".

The following example shows search results for "index=fsctcenter", which include several (batched) messages.

i	Time	Event
>	1/19/18 5:00:24.000 AM	<pre>{ [-] ctupdate: hostinfo dnsdomain: [REDACTED].forescout.com host_properties: { [+] } ip: [REDACTED] mac: [REDACTED] tenant_id: CounterACT_39FF80E8-D957-4B39-BD58-102E7A98DAC4 }</pre> <p>Show as raw text</p> <p>host = [REDACTED] source = CounterACT sourcetype = fsctcenter_json</p>
>	1/19/18 5:00:17.000 AM	<pre>{ [-] ctupdate: hostinfo dnsdomain: [REDACTED].forescout.com host_properties: { [+] } ip: [REDACTED] mac: [REDACTED] tenant_id: CounterACT_39FF80E8-D957-4B39-BD58-102E7A98DAC4 }</pre> <p>Show as raw text</p> <p>host = [REDACTED] source = CounterACT sourcetype = fsctcenter_json</p>
>	1/19/18 5:00:15.000 AM	<pre>{ [-] ctupdate: hostinfo host_properties: { [+] }</pre>

3. Select a message to expand the entry and display it in full.

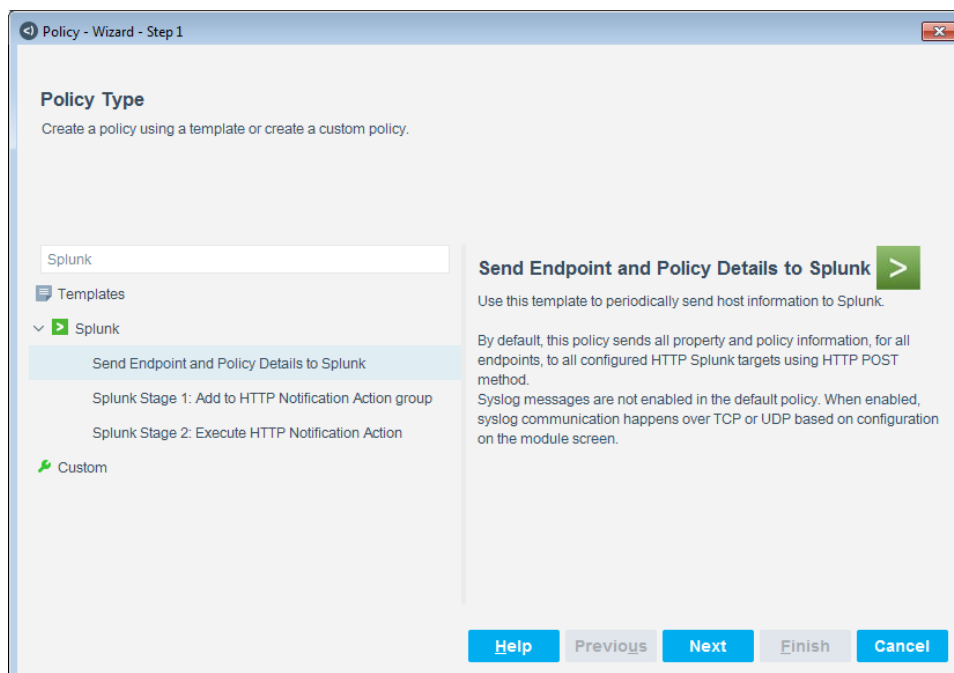


The screenshot shows the Splunk search results for the query `index=fscntcenter`. The search returned 24,174 events. The selected event is displayed in the main pane, showing a JSON object with the following structure:

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

The event is dated 1/19/18 4:55:31.000 AM. The source is `CounterACT` and the sourcetype is `fscntcenter_json`.

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



The screenshot shows the 'Policy - Wizard - Step 1' dialog box. The 'Policy Type' section is active, showing a list of templates. The 'Send Endpoint and Policy Details to Splunk' template is selected. The description for this template is:

Use this template to periodically send host information to Splunk.

By default, this policy sends all property and policy information, for all endpoints, to all configured HTTP Splunk targets using HTTP POST method. Syslog messages are not enabled in the default policy. When enabled, syslog communication happens over TCP or UDP based on configuration on the module screen.

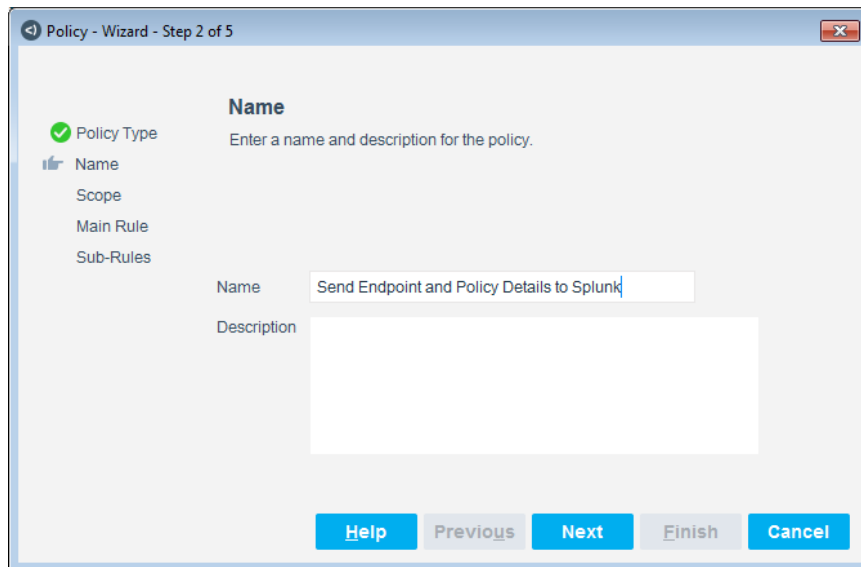
The 'Send Endpoint and Policy Details to Splunk' button is highlighted. The 'Custom' option is also visible. The 'Next' button is enabled.

Create the Policy

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


To create the policy:

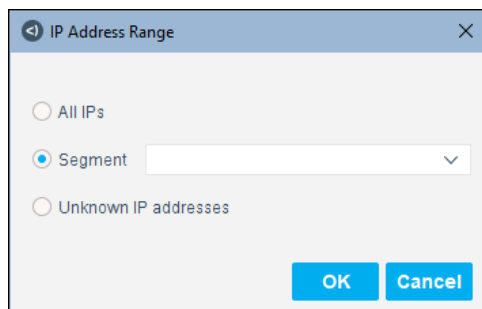
1. Log in to the Console and select **Policy**. The Policy Manager opens.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **Splunk** folder and select **Send Endpoint and Policy Details to Splunk**.
4. Select **Next**.



The screenshot shows a window titled "Policy - Wizard - Step 2 of 5". On the left, a sidebar lists the steps: "Policy Type" (checked with a green icon), "Name" (selected with a blue icon), "Scope", "Main Rule", and "Sub-Rules". The main area is titled "Name" and contains the instruction "Enter a name and description for the policy." Below this, there are two input fields: "Name" and "Description". The "Name" field contains the text "Send Endpoint and Policy Details to Splunk". The "Description" field is empty. At the bottom, there are five buttons: "Help", "Previous", "Next" (highlighted in blue), "Finish", and "Cancel".

5. Enter a name for the policy. Optionally, enter a description.
 - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as `My_Compliance_Policy`.
 - Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
 - Ensure that the name indicates whether the policy criteria must be met or not met.
 - Avoid having another policy with a similar name.

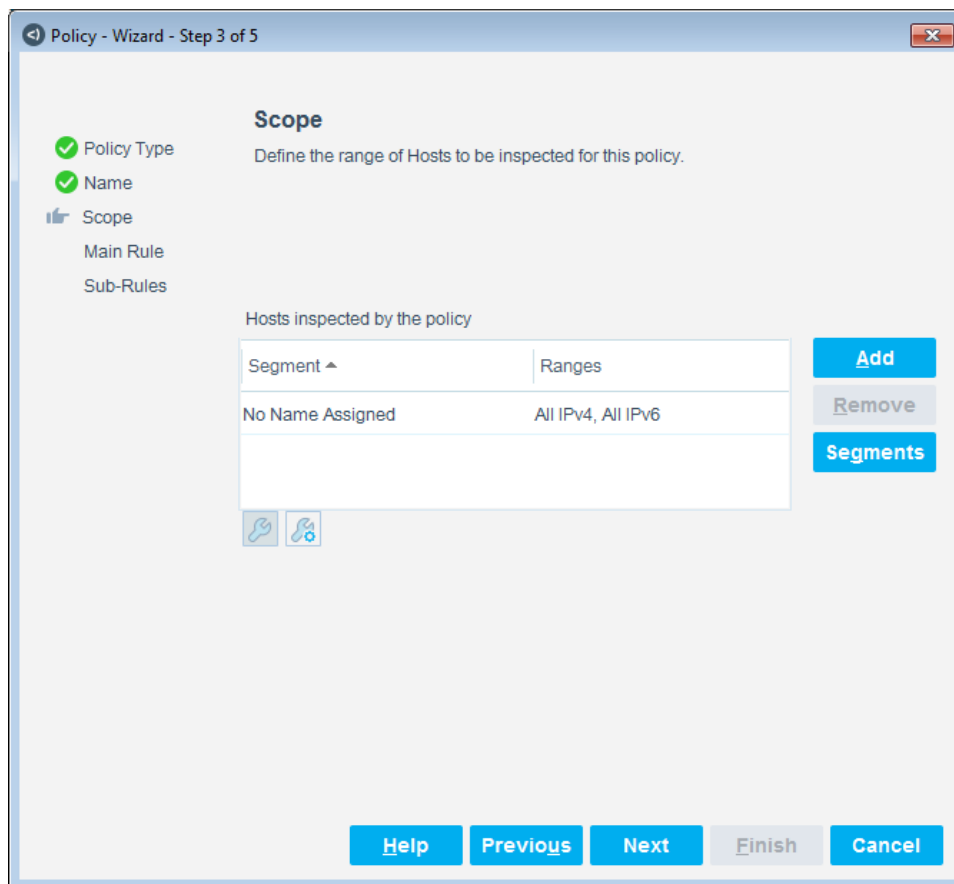
 *Policy names are displayed in the Policy Manager, the Views pane, NAC Reports, and in other features. Precise names make working with policies and reports more efficient.*
6. Select **Next**. Both the IP Address Range dialog box and the Scope pane open.
7. Use the IP Address Range dialog box to define which endpoints are inspected.



The following options are available:

- **All IPs:** Include all IP addresses in the Internal Network.
- **Segment:** Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
- **Unknown IP addresses:** Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

8. Select **OK**. The added range is displayed in the Scope pane.



9. Select **Next**.

Policy rules instruct the Forescout platform how to detect and handle hosts defined in the policy scope. By default, the main rule of this policy applies no conditions. It includes all endpoints detected by the Forescout platform within the specified policy scope.

Policy - Wizard - Step 4 of 5

Main Rule

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

Condition

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

All criteria are True

Criteria

No items to display

Actions

Actions are applied to hosts matching the above condition.

Enable	Action	Details
<input checked="" type="checkbox"/>	Splunk: Send Update from CounterACT	Splunk: Send Update from CounterACT. Schedul...

Buttons: Add, Edit, Remove

Buttons: Help, Previous, Next, Finish, Cancel

The default action, **Splunk: Send Update from CounterACT** sends the following information to Splunk for each detected endpoint:

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

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

10. Select **Finish**.

11. In the Policy Manager, select **Apply**.

Create a Splunk Stage 1: Add to HTTP Notification Action Group Policy

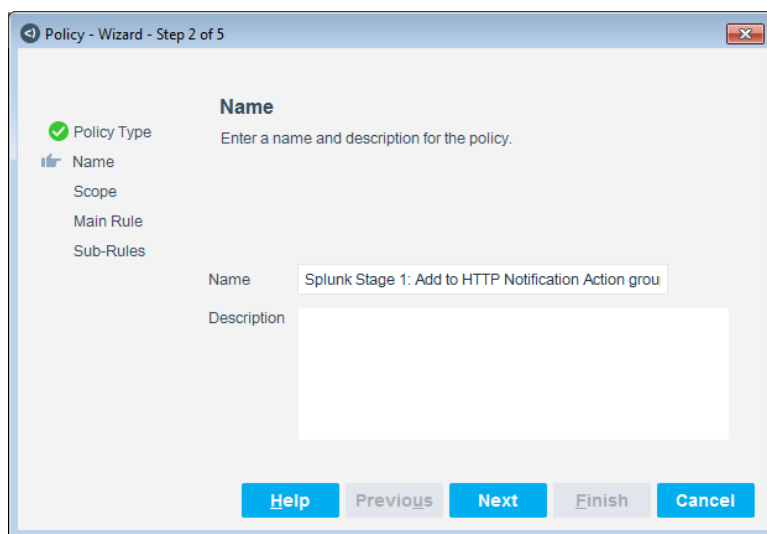
Create policies based on this template to detect messages that request the HTTP Notification action and place them in the Splunk HTTP Notification group. Use this as a reference and follow the correct action group based on the action requested from Splunk.

Create the Policy

This section describes how to create a policy from the Splunk Stage 1: Add to HTTP Notification Action Group policy template.

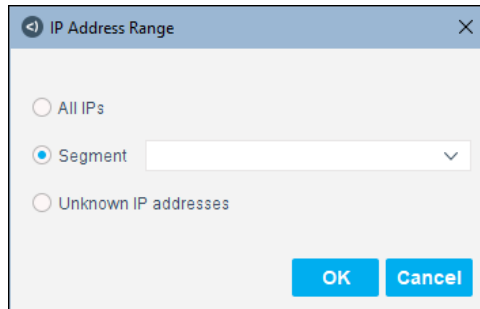
To create the policy:

1. Log in to the Console and select **Policy**. The Policy Manager opens.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **Splunk** folder and select **Splunk Stage 1: Add to HTTP Notification Action group**.
4. Select **Next**.



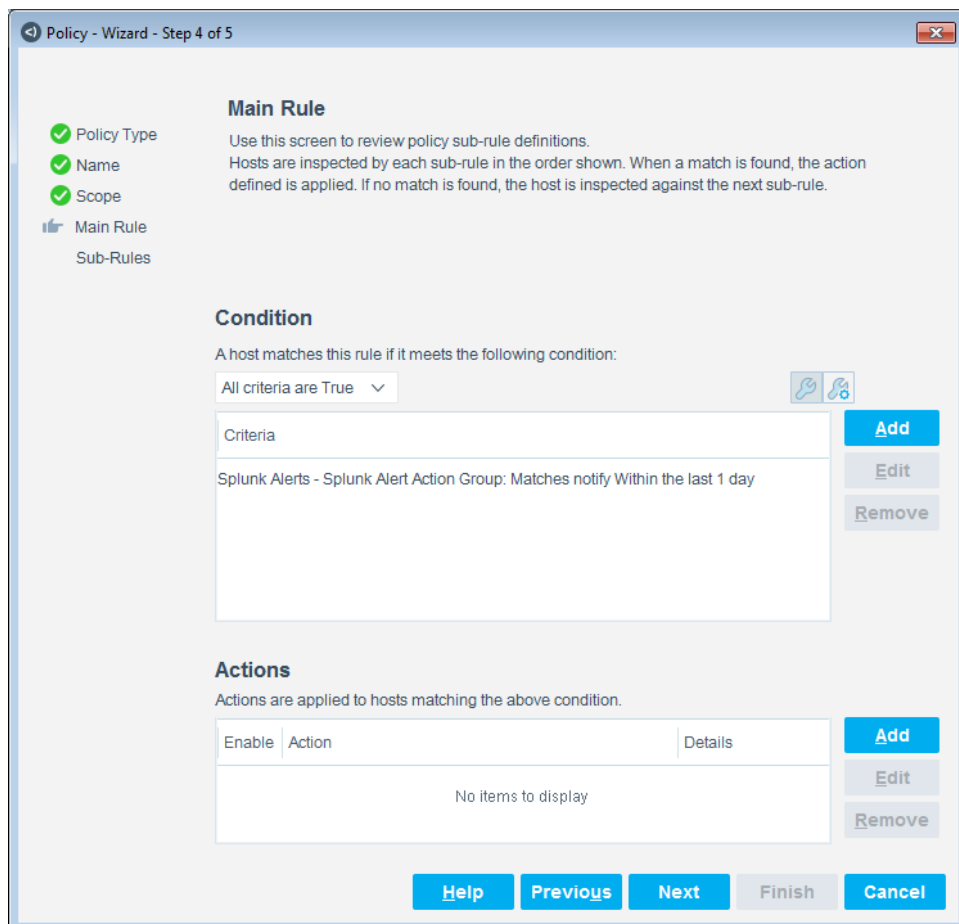
The screenshot shows a 'Policy - Wizard - Step 2 of 5' dialog box. On the left, a sidebar lists the steps: 'Policy Type' (checked with a green checkmark), 'Name', 'Scope', 'Main Rule', and 'Sub-Rules'. The main area is titled 'Name' and contains the instruction 'Enter a name and description for the policy.' Below this, there are two input fields: 'Name' and 'Description'. The 'Name' field contains the text 'Splunk Stage 1: Add to HTTP Notification Action grou'. The 'Description' field is empty. At the bottom of the dialog, there are five buttons: 'Help', 'Previous', 'Next', 'Finish', and 'Cancel'. The 'Next' button is highlighted in blue.

5. Enter a name for the policy. Optionally, enter a description.
6. Select **Next**. Both the IP Address Range dialog box and the Scope pane open.
7. Use the IP Address Range dialog box to define which endpoints are inspected.



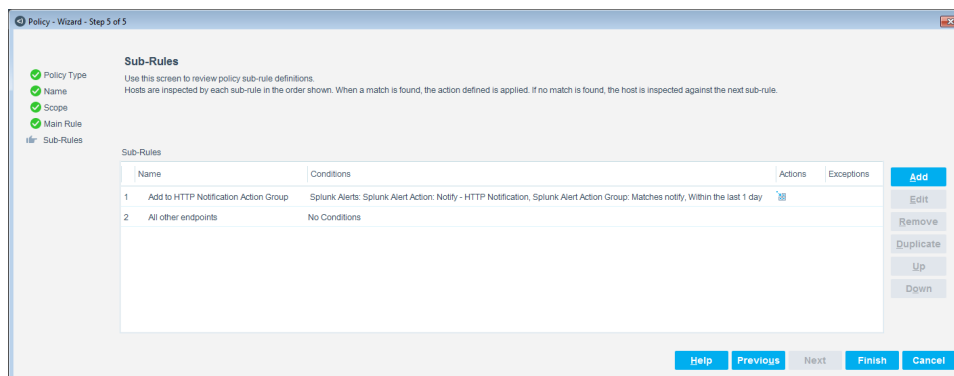
The following options are available:

- **All IPs:** Include all IP addresses in the Internal Network.
 - **Segment:** Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
 - **Unknown IP addresses:** Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.
8. Select **OK**. The added range is displayed in the Scope pane.
 9. Select **Next**.



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

10. Select Next.



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

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

11. Select Finish.

12. In the Policy Manager, select Apply.

Create a Splunk Stage 2: Execute HTTP Notification Action Policy

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

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

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

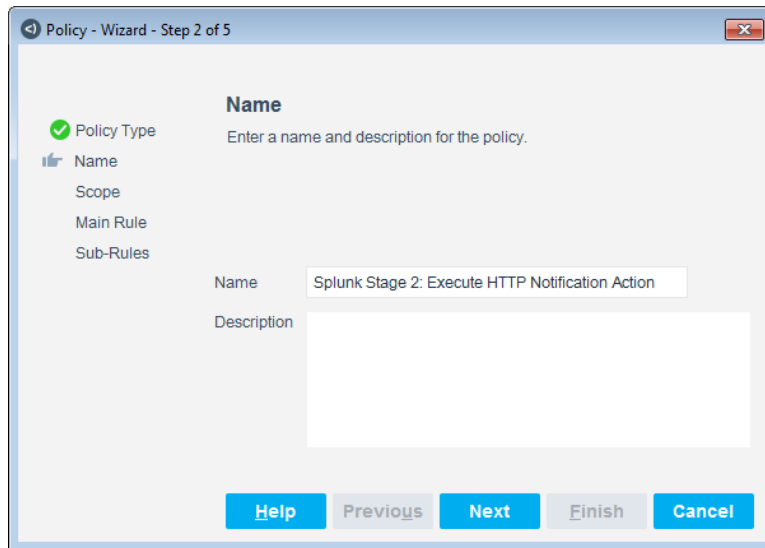
Create the Policy

This section describes how to create a policy from the Splunk Stage 2: Execute HTTP Notification Action policy template.

To create the policy:

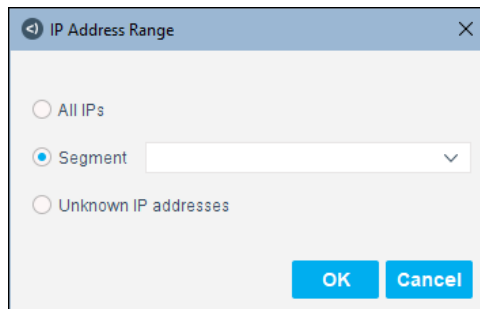
1. Log in to the Console and select **Policy**. The Policy Manager opens.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.

3. Expand the **Splunk** folder and select **Splunk Stage 2: Execute HTTP Notification Action**.
4. Select **Next**.



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

5. Enter a name for the policy. Optionally, enter a description.
6. Select **Next**. Both the IP Address Range dialog box and the Scope pane open.
7. Use the IP Address Range dialog box to define which endpoints are inspected.



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

The following options are available:

- **All IPs**: Include all IP addresses in the Internal Network.
 - **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
 - **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.
8. Select **OK**. The added range is displayed in the Scope pane.
 9. Select **Next**.

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

10.Select **Finish**.

11.In the Policy Manager, select **Apply**.


Action Status Tracking

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 four hours after the alert message is received.

The following action status values, displayed in the Dashboard, are reported by the Forescout platform.

Success	The action completed without failure.
Failure	The action completed with a failure or the action 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	<p>No status can be reported for one of the following reasons:</p> <ul style="list-style-type: none"> ▪ No active policy detects the relevant Splunk Last Alert property or applies the requested action. ▪ The endpoint has been deleted from 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 data purges by the Forescout platform clear action data before reports are generated.
Invalid	<ul style="list-style-type: none"> ▪ The endpoint IP is outside the network scope defined in the Forescout platform. ▪ An unspecified internal error occurred.

 *If Forescout 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.*

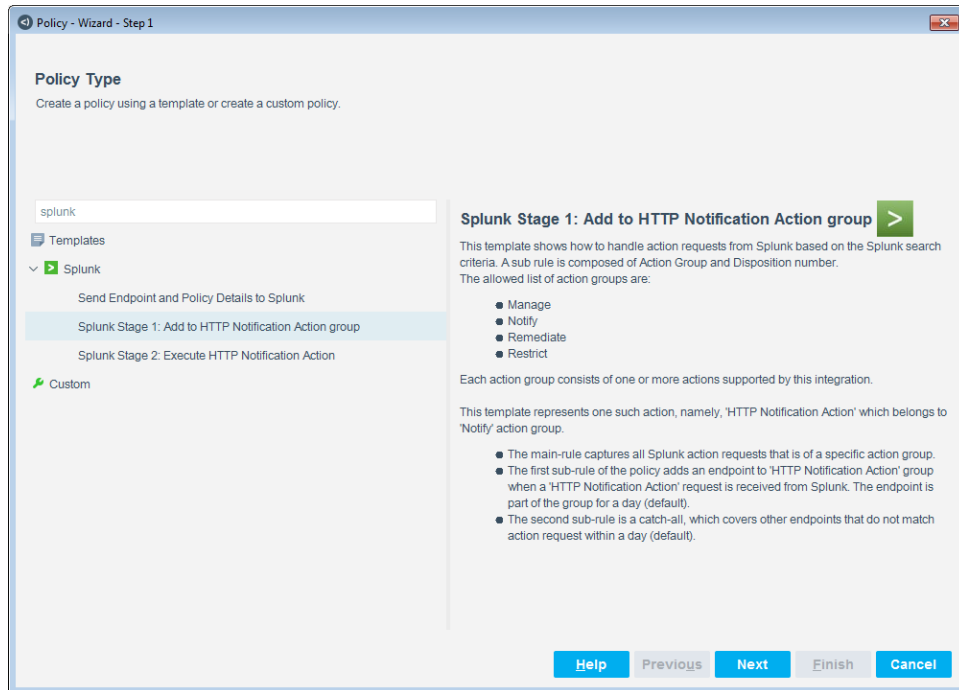
Create Custom Splunk Policies

You may need to create a custom policy to capture Splunk action requests supported by this integration but not covered in the policy templates provided with this module. In addition to the bundled the Forescout platform properties and actions available for detecting and handling endpoints, you can work with properties and actions provided by this module to create custom policies.

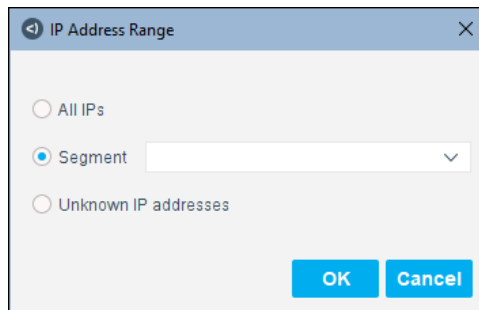
To ensure all conditional properties for responding to an action requests are adequately fulfilled, it is best to create this custom policy out of Stage 1 and Stage 2 policy templates provided with the Forescout platform.

To create a custom Splunk Stage 1 policy:

1. Log in to the Console and select **Policy**. The Policy Manager opens.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **Splunk** folder and select **Splunk Stage 1: Add to HTTP Notification Action Group**.



4. Select **Next**.
5. Enter a custom name for the policy. Optionally, enter a description.
6. Select **Next**. Both the IP Address Range dialog box and the Scope pane open.
7. Use the IP Address Range dialog box to define which endpoints are inspected.



The following options are available:

- **All IPs**: Include all IP addresses in the Internal Network.
 - **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
 - **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.
8. Select **OK**. The added range is displayed in the Scope pane.
 9. Select **Next**.

Policy - Wizard - Step 4 of 5

Progress: Policy Type, Name, Scope, Main Rule (selected), Sub-Rules

Main Rule

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

Condition

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

All criteria are True

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

Buttons: Add, Edit, Remove

Actions

Actions are applied to hosts matching the above condition.

Enable	Action	Details
No items to display		

Buttons: Add, Edit, Remove

Navigation: Help, Previous, Next, Finish, Cancel

10. Select Next.

Policy - Wizard - Step 5 of 5

Progress: Policy Type, Name, Scope, Main Rule, Sub-Rules (selected)

Sub-Rules

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

	Name	Conditions	Actions	Exceptions
1	Add to HTTP Notification Action Group	Splunk Alerts: Splunk Alert Action: Notify - HTTP Notificatio...		
2	All other endpoints	No Conditions		

Buttons: Add, Edit, Remove, Duplicate, Up, Down

Navigation: Help, Previous, Next, Finish, Cancel

11. Select the first Sub-Rule and select Edit.

Policy: 'Splunk Stage 1: Add to HTTP Notification Action group1'-->Sub-Rule: 'Add to ...'

Name

Name Add to HTTP Notification Action Group Edit

Description All endpoints matching Splunk action request is added t...

Condition


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

All criteria are True ⚙️

Criteria	
Splunk Alerts - Splunk Alert Action: Notify - HTTP Notification Splunk Alert ...	Add Edit Remove

Actions

Actions are applied to hosts matching the above condition.

Ena...	Action	Details	
<input checked="" type="checkbox"/>	 Add to Group	Add to Group. ...	Add Edit Remove

Advanced

Recheck match Every 8 hours, All admissions Edit

Exceptions None.

Help OK Cancel

12.In the **Condition** section, add or edit the condition.

Condition

Search

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

☒ **Splunk Alert Action Group**

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

☒ Meets the following criteria

☐ Does not meet the following criteria

Matches

☐ Match case

☒ **Splunk Alert Action**

Actions are grouped by 'Splunk Alert Action Group'. Each action is prefixed with the action group it belongs to. Make sure to fix matching the value entered in 'Splunk Alert Action Group' field. Prefix would be one of 'manage', 'notify', 'remediate' or 'restrict'. If you are using multiple entries, correct status is sent back to Splunk only for actions requested from Splunk.

☒ Meets the following criteria

☐ Does not meet the following criteria

Search

☒ Name

- ☐ Manage - Recheck Host
- ☒ Notify - HTTP Notification
- ☐ Notify - HTTP Redirection to URL
- ☐ Notify - Send Balloon Notification
- ☐ Notify - Send Email
- ☐ Notify - Send Email to User
- ☐ Remediate - Disable Dual Homed
- ☐ Remediate - Kill Cloud Storage
- ☐ Remediate - Kill Instant Messaging
- ☐ Remediate - Kill Peer-to-peer
- ☐ Restrict - Switch Block

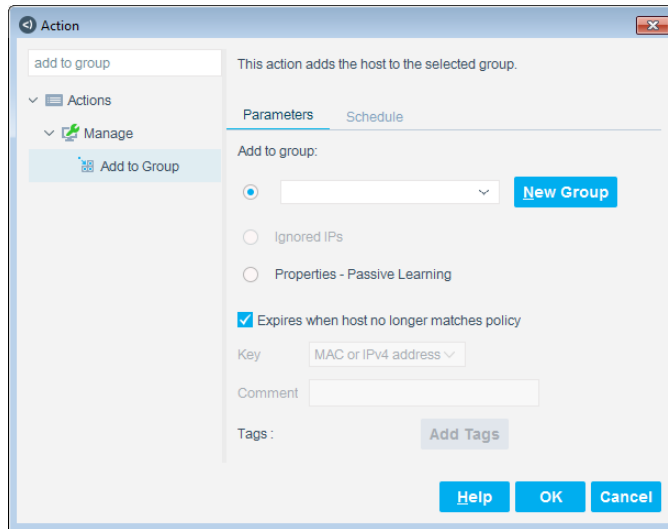
Help OK Cancel

13. Add or edit the Splunk Alert Action.

The Splunk Alert Action Group should be the same as the one specified in the main rule.

14. Select **OK**.

15. In the **Actions** section, add or edit the action.

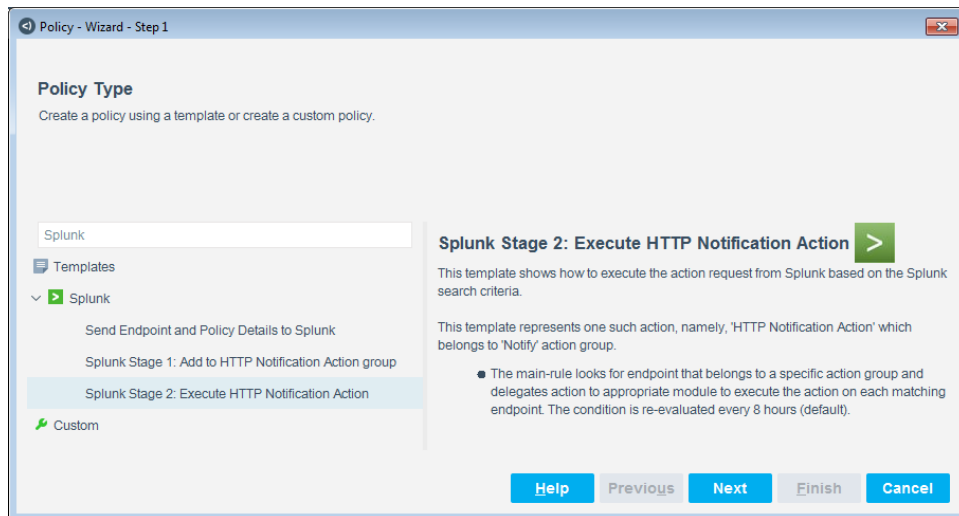


16. Select **OK**.

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

To create a custom Splunk Stage 2 policy:

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

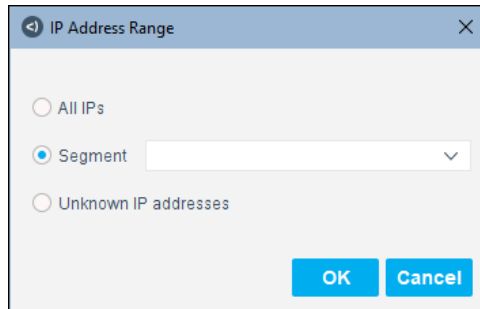


4. Select **Next**.

5. Enter a custom name for the policy. Optionally, enter a description.

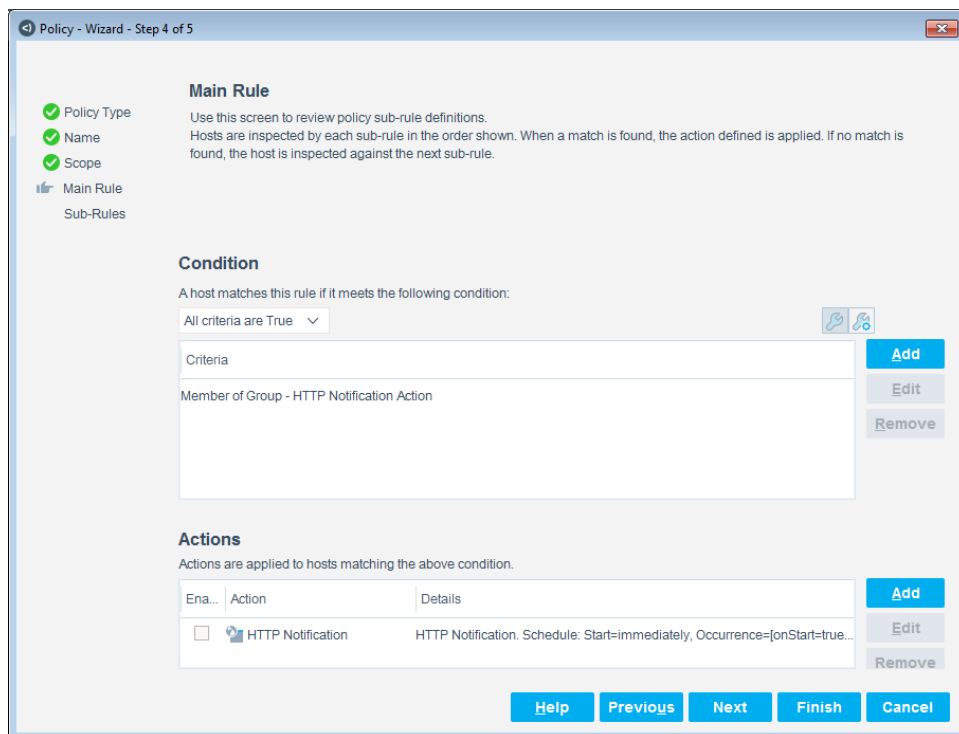
6. Select **Next**. Both the IP Address Range dialog box and the Scope pane open.

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

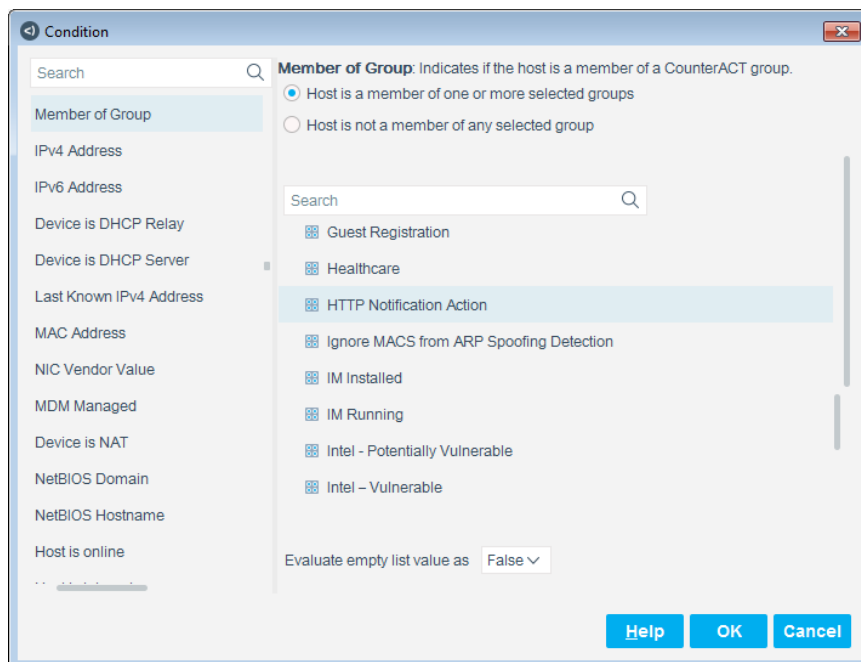


The following options are available:

- **All IPs:** Include all IP addresses in the Internal Network.
 - **Segment:** Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
 - **Unknown IP addresses:** Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.
8. Select **OK**. The added range is displayed in the Scope pane.
 9. Select **Next**.

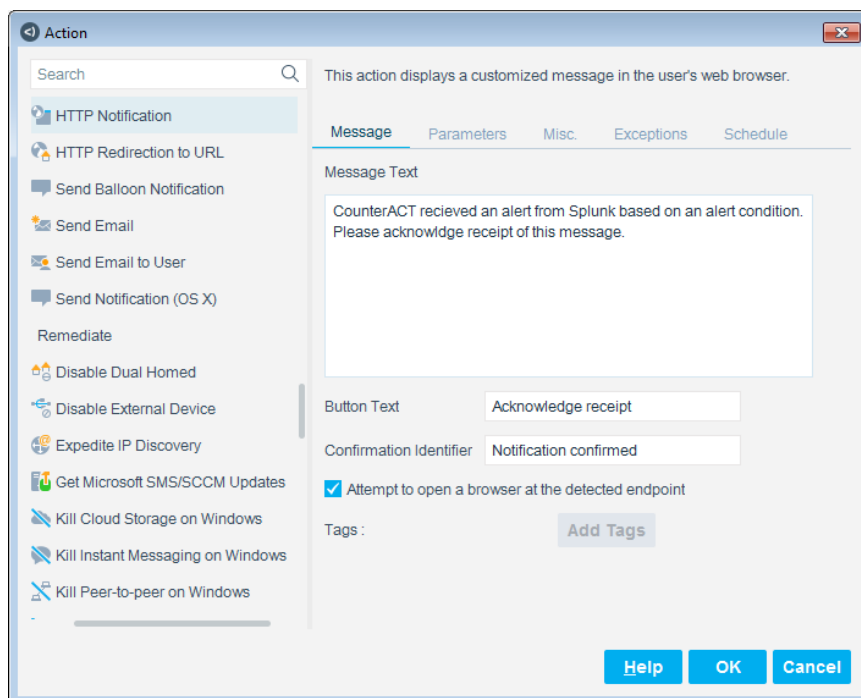


10. In the **Condition** section, select the "Member of" item and select **Edit**.



11. Edit the main rule condition to specify the group from the Stage 1 policy template. Select **OK**.

12. In the **Actions** section, select the action in the main-rule and select **Edit**.



13. Edit the main rule action. Select **OK**.

14. Select **Finish**.

Detect Endpoints – Policy Properties

The endpoints need to be configured as part of the custom policy.

Splunk Alerts

Splunk alert messages are sent to the Forescout platform to request an action to an endpoint. In the Forescout Splunk App, search for and select **Splunk Alerts**. Splunk alerts indicate information for alert messages received from Splunk for an endpoint.

To configure Splunk alerts:

1. The properties for Splunk Alerts are displayed in eyeExtend for Splunk in the custom policy Condition pane.

2. The following Alerts are available:

Splunk Alert Action Group	Select the action group contained in the alert. This maps to an action group in the Forescout platform. Select the Action Group value, which can be one of: manage, notify, remediate, or restrict.
----------------------------------	---

Splunk Alert Action	<p>Select the entry that has the prefix matching the value entered in the Splunk Alert Action Group. The prefix value is one of: manage, notify, remediate, or restrict.</p> <p>Actions are grouped by Splunk Alert Action Group. Each action is prefixed with the action group to which it belongs.</p> <p>If the group meets or does not meet the selected criteria, a request for action (alert) will be sent to the Forescout platform.</p> <p>When selecting multiple entries, the correct status is sent back to Splunk only for actions requested from Splunk.</p> <p>The following sub-properties are available:</p> <ul style="list-style-type: none"> ▪ Manage – Recheck Host ▪ Notify – HTTP Notification ▪ Notify – HTTP Redirection to URL ▪ Notify – Send Balloon Notification ▪ Notify – Send Email ▪ Notify – Send Email to User ▪ Remediate – Disable Dual Homed ▪ Remediate – Kill Cloud Storage ▪ Remediate – Kill Instant Messaging ▪ Remediate – Kill Peer-to-peer ▪ Restrict – Switch Block
Splunk Alert Action Server	<p>Enter the IP address of the Splunk Target defined in the configuration of the Splunk integration. Select the server that triggered the alert action request.</p>
Splunk Alert Action Search Name	<p>Enter the search name that triggered the alert action request.</p> <p>Find the search name in the Splunk server console by going to Settings > Searches, alerts and reports, and typing counteract in the search field. The search name is in the first column.</p>

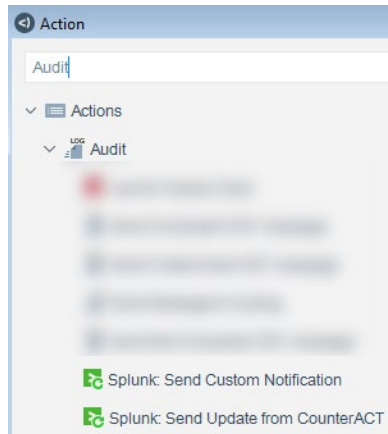
3. Select **OK**.

Manage Splunk Devices – Policy Actions

This section describes the actions that are made available when Forescout eyeExtend for Splunk is installed.

To access Splunk actions:

1. Go to the Actions tree from the Policy Actions dialog box.
2. Expand the Audit folder in the Actions tree.



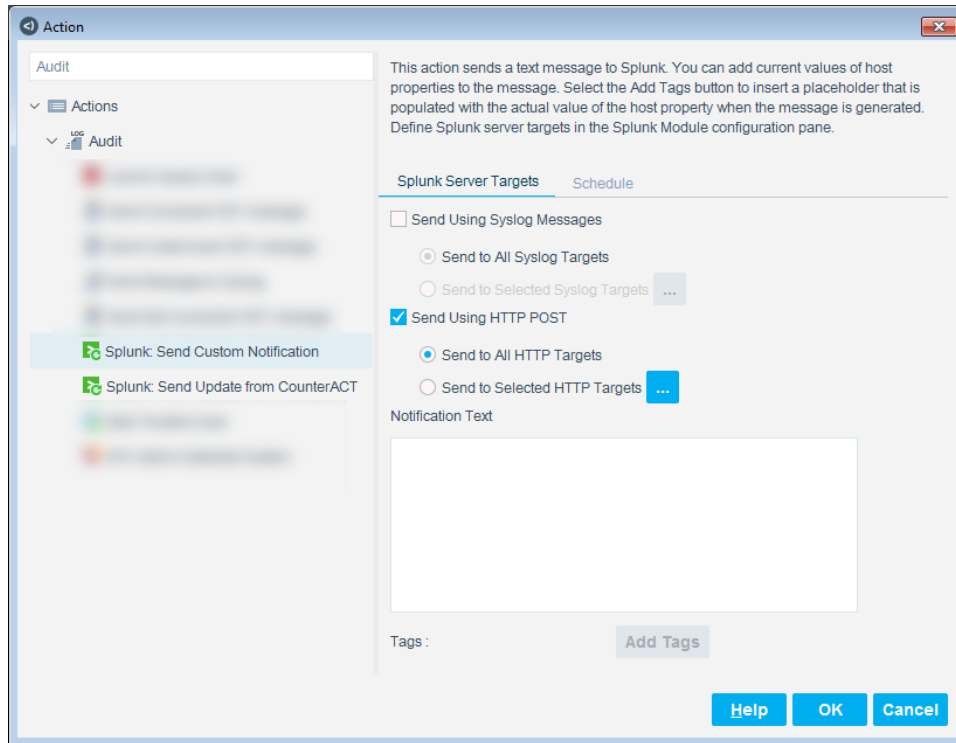
3. The following actions are available:

- [Splunk: Send Custom Notification Action](#)
- [Splunk: Send Update from CounterACT Action](#)

Splunk: Send Custom Notification Action

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

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



To use this action:

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

Splunk: Send Update from CounterACT Action

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

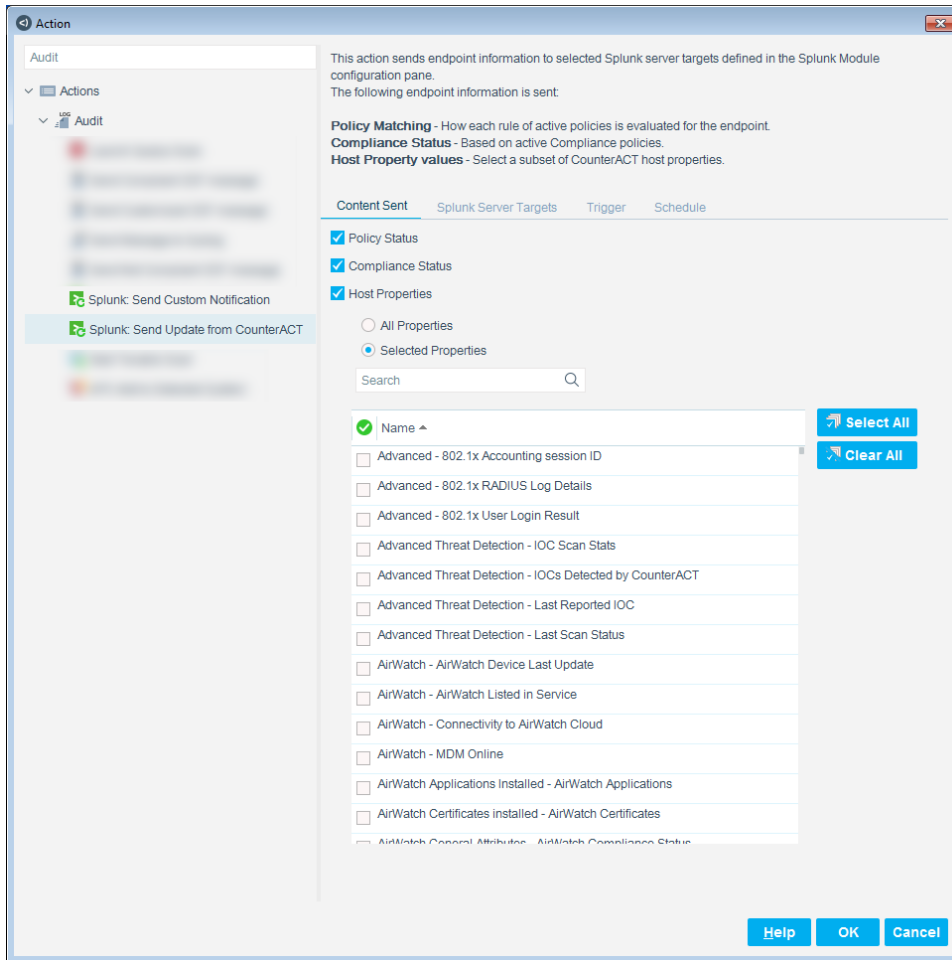
- MAC Address
- IPv4 Address

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

If none of these parameters are available, the fields are removed from the update message. If, for a given device, one or more of these attributes cannot be resolved, then the update messages will contain only the ones that have been successfully resolved.

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

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



Content Sent Tab

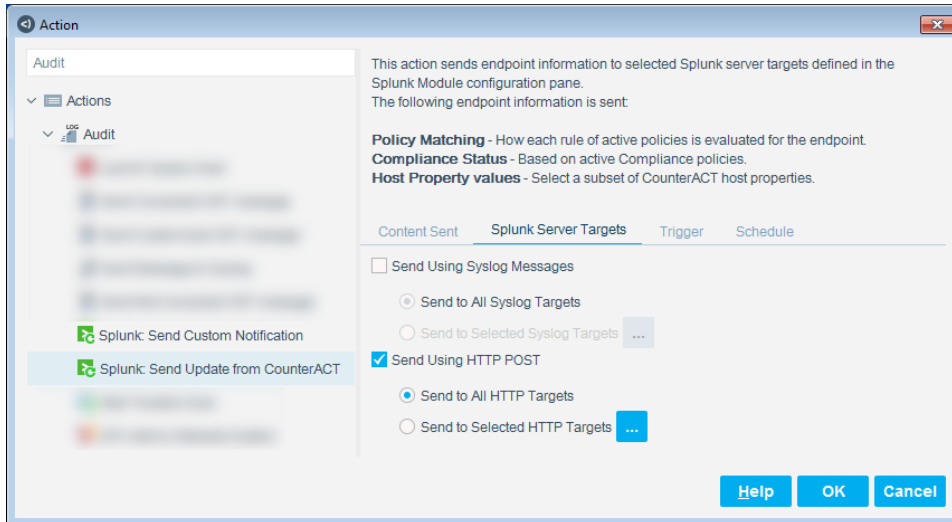
Specify the data that is included in the message sent to Splunk:

- Select the **Policy Status** option to include the most recent results of policy-based evaluation of the endpoint. The Forescout platform reports whether the endpoint matches each rule of all active policies.
- Select the **Compliance Status** option to include the aggregate Compliance status of the endpoint, based on the Compliance properties.
- Select the **Host Properties** option to include host property values for the endpoint. Do one of the following:
 - Select the **All Properties** option to include all host property values.
 - Select the **Selected Properties** option and select properties you want to include. Use the Search field to quickly locate properties.

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

Splunk Server Target Tab

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

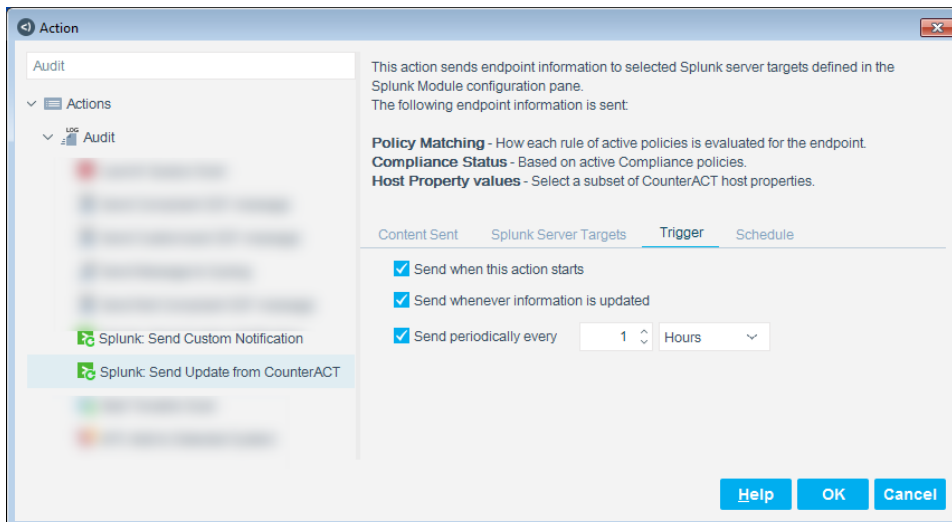


For each message type you selected, do one of the following:

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

Trigger Tab

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

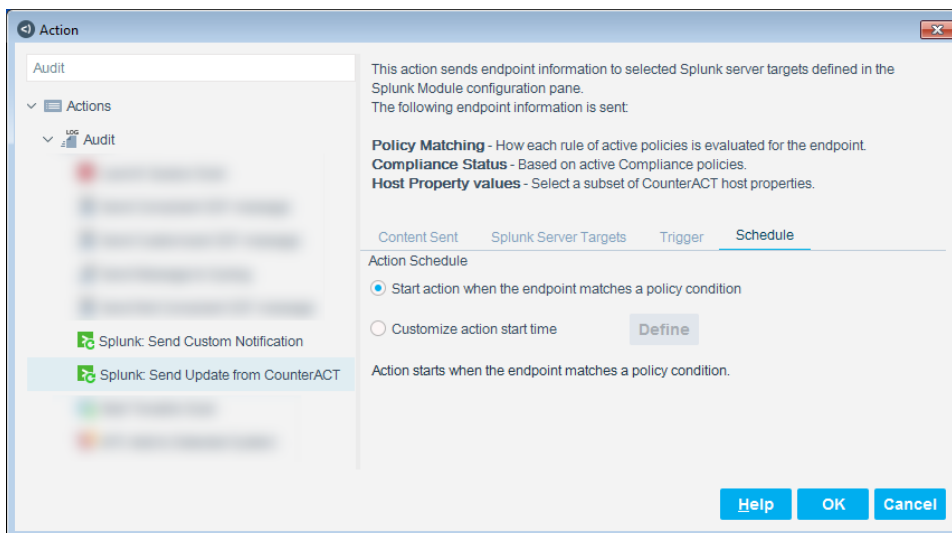


- Select the **Send when this action starts** option to send a message when the endpoint matches the conditions of a policy rule that invokes this action.

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

Schedule Tab

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




Use Forescout eyeExtend for Splunk

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

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

To access the inventory:

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

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

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

To access the Home tab:

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

Refer to *Working in the Console>Working with Forescout Detections* in the *Forescout Administration Guide* or the Console Online Help for information about working with the Asset Inventory. See [Additional Forescout Documentation](#) for information on how to access this guide.

Run Splunk Audit Actions

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

- [Send Custom Notification to Splunk Enterprise Server Targets](#)
- [Send Updates from the Forescout Platform](#)

Send Custom Notification to Splunk Enterprise Server Targets

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

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

To send a customized notification:

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

Specify Splunk: Send Custom Notification parameters

This action sends a text message to Splunk. You can add current values of host properties to the message. Select the Add Tags button to insert a placeholder that is populated with the actual value of the host property when

Splunk Server Targets Schedule

☐ Send Using Syslog Messages

☒ Send to All Syslog Targets

☐ Send to Selected Syslog Targets ...

☒ Send Using HTTP POST

☒ Send to All HTTP Targets

☐ Send to Selected HTTP Targets ...

Notification Text

Tags : Add Tags

OK Cancel

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

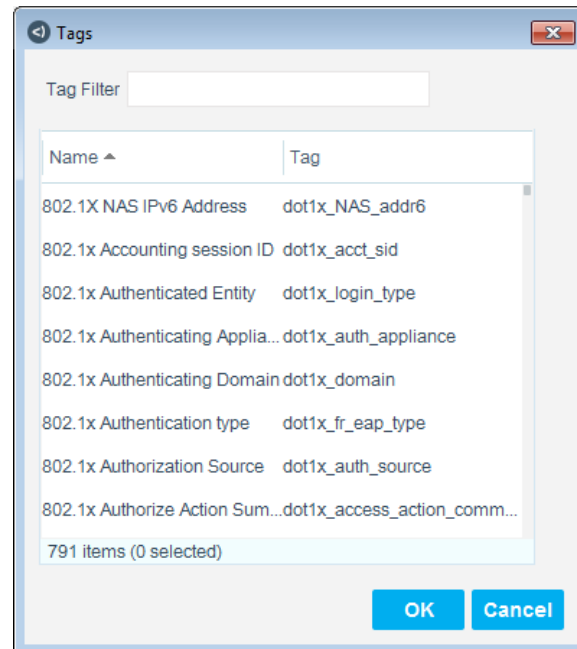
In the Splunk Server Targets tab, enter your configurations.

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

Notification Text

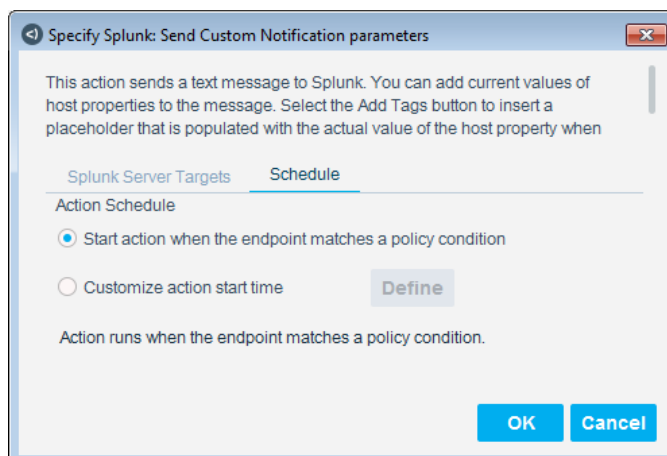
Compose the message text. You can use property tags to include endpoint-specific or user-specific values in this field. Refer to the *Forescout Administration Guide* for details on property tags.

- Select **Add Tags**.



- Hold down the <Ctrl> key and select the tags for the notification text and then select **OK**.
- The Notification Text field populates with the selected tags.

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



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

Action Scheduler

Start

☒ Immediately (on policy match)

☐ Wait for

☐ On ... at

Activity pattern

☒ Constantly

☐ Scheduled

Duration

☒ No end date

☐ End after

☐ End on ... at

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

Send Updates from the Forescout Platform

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

The following endpoint information is sent:

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

To send an update to the Forescout platform:

1. In the Console, Home tab, right-click an **IP address**.
2. Select **Audit** and then select **Splunk: Send Update from CounterACT**.

3. The Specify Splunk: Send Update from CounterACT parameters dialog box opens to the Content Sent tab.

Specify Splunk: Send Update from CounterACT parameters

This action sends endpoint information to selected Splunk server targets defined in the Splunk Module configuration pane.
The following endpoint information is sent:

Content Sent | Splunk Server Targets | Trigger | Schedule

☒ Policy Status
☒ Compliance Status
☒ Host Properties

☐ All Properties
☒ Selected Properties

Search

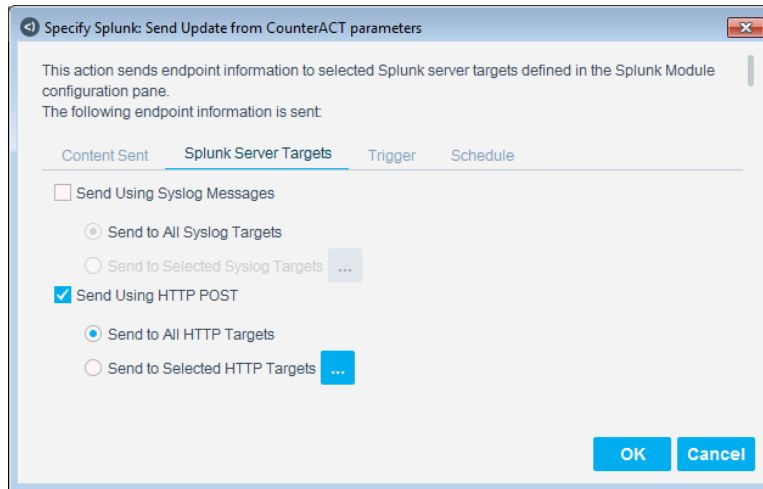
☒ Name ^

- ☐ Advanced - 802.1x Accounting session ID
- ☐ Advanced - 802.1x RADIUS Log Details
- ☐ Advanced - 802.1x User Login Result
- ☐ Advanced Threat Detection - IOC Scan Stats
- ☐ Advanced Threat Detection - IOCs Detected by CounterACT
- ☐ Advanced Threat Detection - Last Reported IOC
- ☐ Advanced Threat Detection - Last Scan Status
- ☐ AirWatch - AirWatch Device Last Update
- ☐ AirWatch - AirWatch Listed in Service
- ☐ AirWatch - Connectivity to AirWatch Cloud
- ☐ AirWatch - MDM Online
- ☐ AirWatch Applications Installed - AirWatch Applications
- ☐ AirWatch Certificates installed - AirWatch Certificates
- ☐ AirWatch Control Attributes - AirWatch Compliance Status

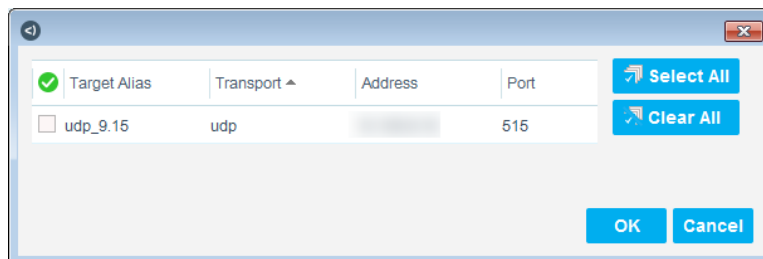
Select All | Clear All

OK | Cancel

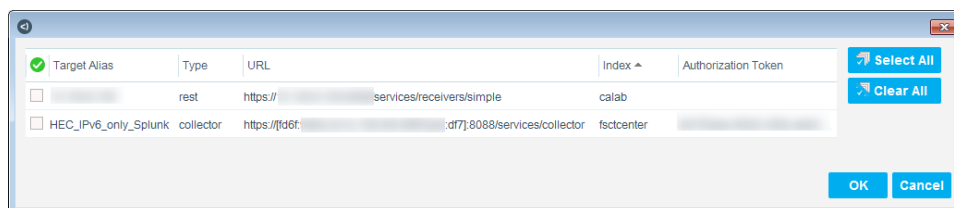
4. You can use the default settings and simply select specific options in the Host Properties Name field or you can **Select All**.
5. Alternately, set your own customized settings.
6. Select the Splunk Server Targets tab.




7. Select **Send Using Syslog Messages** and/or select **Send Using HTTP POST**. If you select **Send Using Syslog Messages**, do one of the following:
- Leave the default setting, **Send to All Syslog Targets**. This option sends the message to all Splunk Enterprise server targets defined in the Forescout platform.
 - Select **Send to Selected Syslog Targets**. This option sends an update message to a subset of Splunk Enterprise server targets defined in the Forescout platform. Then select one or more addresses and select **OK**.



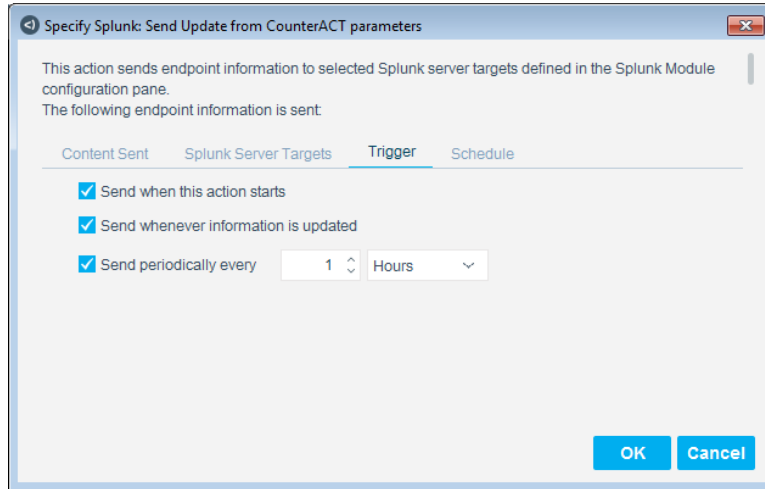
8. If you select **Send Using HTTP POST**, do one of the following:
- Leave the default setting, **Send to all HTTP Targets**.
 - Select **Send to Selected HTTP Targets**. This option sends an update message to a subset of Splunk HTTP targets defined in the Forescout platform. Select one or more URLs and then select **OK**.



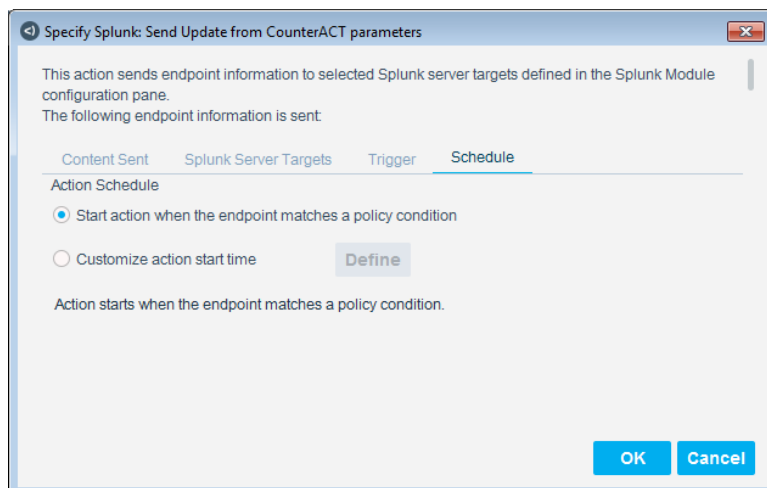
For details on configuring two or more HTTP channels with the same URL, see [Support for Multiple Channels for each Splunk Target](#).

 You can configure two HTTP targets with same URLs as long as either the Index or the Authorization Token fields are different.

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

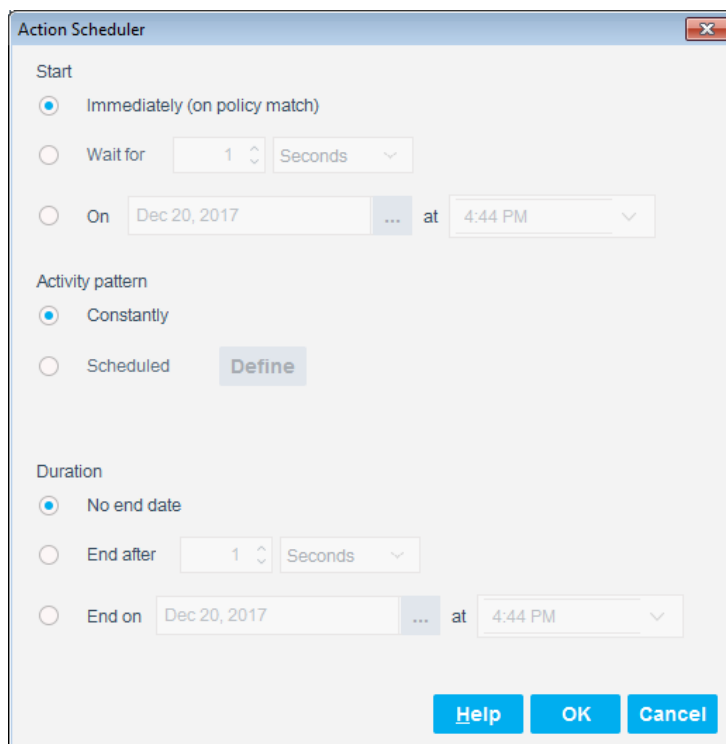


10. Select one or more of the following options:
 - Select **Send when this action starts** to send an update message when the endpoint matches the conditions of a policy rule that invokes this action.
 - Select **Send whenever information is updated** to send an update message when the specified information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



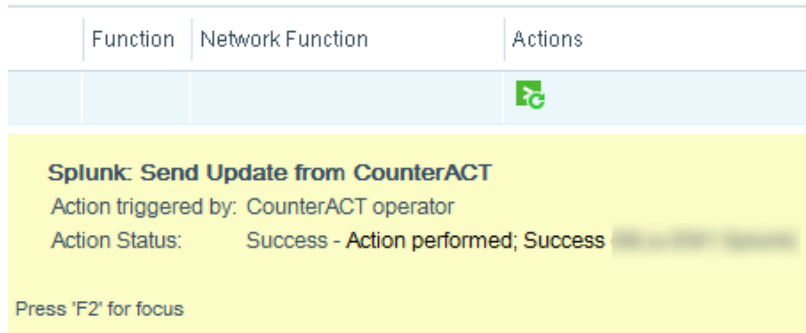
12. Do one of the following:

- Leave the default setting of **Start action when host matches policy condition**. This option sends an update message immediately upon discovering a specific policy criterion.
- Select **Customize action start time** or select **Define** to open the Action Scheduler dialog box.



- a. Use the available options to specify when the action is applied, to delay application of the action, or to specify repeat application of the action.
- b. When finished, select **OK**.

13. In the Specify Splunk: Send Custom Notification parameters dialog box, select **OK**.
14. In the Console, Home tab, hover over the green icon in the Action field of the selected IP address. The Splunk: Send Update from CounterACT information is displayed.



Support for Multiple Channels for each Splunk Target

To configure a new HTTP destination:

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

Best Practices

This section describes the best practices for using Forescout eyeExtend for Splunk.

Forescout-to-Splunk Logging

A best practice for logging to Splunk from the Forescout platform is to use the Event Collector. The Event Collector is a token-based, encrypted HTTP messaging service. See [Obtain an Authorization Token](#).

Splunk to Forescout Messaging

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

Splunk Actions on the Forescout Platform

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

What Data is Sent to Splunk?

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

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

Appendix A: Default Communication Settings

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

Name	Direction	Protocol	Port	To customize
REST	To Splunk	HTTPS	8089	Enter custom port/URL in the POST to URL field when you Configure the Module .
Event Collector	To Splunk	HTTPS	8088	
Syslog	To Splunk	TCP/UDP	515	1. In Splunk: Clone the Data Input and customize port. 2. In the Forescout platform: Customize the Port and TCP/UDP fields when you Configure the Module .
Alert API	To the Forescout platform	HTTP	80	In Splunk: edit the URL of the built-in alerts.

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 <i>Forescout App & Add-ons for Splunk How-to Guide</i> .
<ul style="list-style-type: none"> ▪ Managed Splunk Cloud: The apps must be installed by Splunk Cloud Support. ▪ Self-Service Splunk Cloud: You can install the apps. See Deploy Splunk Cloud .	N/A
TCP and UDP data cannot be sent directly to Splunk Cloud. You must use an on-premises forwarder to send such data. The default port for the forwarder to Splunk Cloud are ports 9997 or 9998. Make sure the port on the firewall is open to Splunk Cloud. Refer to Splunk documentation.	Splunk Enterprise allows direct monitoring of TCP and UDP . See Add a Splunk Syslog Target .
HTTP Event Collector (HEC): For Managed Splunk Cloud deployments, HEC must be enabled by Splunk Support.	HTTP Event Collector (HEC): See Obtain an Authorization Token .

Deploy Splunk Cloud

This section describes 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 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" in the following link for details:

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

Due to the REST API limitation on Cloud, a user who runs a **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](https://docs.splunk.com/Documentation/Splunk/7.2.4/Security/Rolesandcapabilities#Add.2C%20edit.2C%20and%20remove%20capabilities%20from%20roles)

- Use an account with the admin role (if you have *admin* access on the Splunk Cloud) with the `edit_tcp` capability.

You can also refer to KB 10495 as follows:

<https://forescout.force.com/support/s/article/REST-API-test-needs-edit-tcp-capability-to-work-on-managed-cloud>

There is also a limitation on the Splunk Cloud that restricts the maximum REST API inputs to 10K. Some JSON raw data from the Forescout platform to the Splunk Cloud will exceed 10K. Any data inputs above 10K will be truncated and will be in text format and not JSON format. Refer to KB 10498 as follows:

<https://forescout.force.com/support/s/article/Splunk-REST-API-target-only-allows-up-to-10K-payload>

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

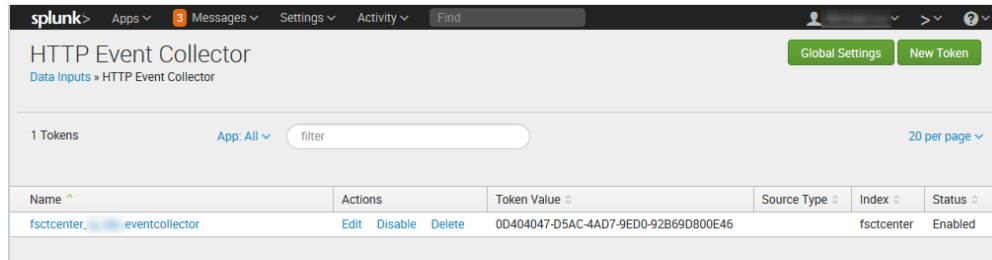
For example:

```
https://input-[redacted].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 the Forescout Platform

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

Add Splunk HTTP Target Details - Step 1

Add Splunk HTTP Target Details

General

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

Splunk HTTP Type: Event Collector

Target Alias: HEC to self-service Splunk Cloud

POST to URL: https://input-

Index: fsstcenter

Comment:

Validate Server Certificate: ☒

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

Buttons: Help Previous Next Finish Cancel

3. In the General 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**.

Add Splunk HTTP Target Details - Step 2 of 2

Add Splunk HTTP Target Details

General
Connection Test

Connection Test

The connection test establishes communication to the targeted connection using the parameters given below. Each selected test is executed chronologically. A successful test means all information provided to establish communication with the targeted connection was correct. A failed test provides information on what needs addressing before re-testing the connection.
On managed cloud deployments, uncheck the checkboxes for "Check if target is reachable", "Check REST API communication" and "Check data input and index", which are for on-prem deployments only.

Enable Test Configuration ☒

Check if target is reachable ☒ (Check executed via ICMP ping, on-prem only)

Check REST API communication ☐ (Server roles are retrieved if successful, on-prem only)

Check data input and index ☐ (Check executed via REST API communication, on-prem only)

Management Username

Management Password

Verify Password

Management Port

Help Previous Next Finish Cancel

5. In the Connection Test pane, disable the checkboxes for **Check REST API communication** and **Check data input and index**.

6. Select **Finish**.

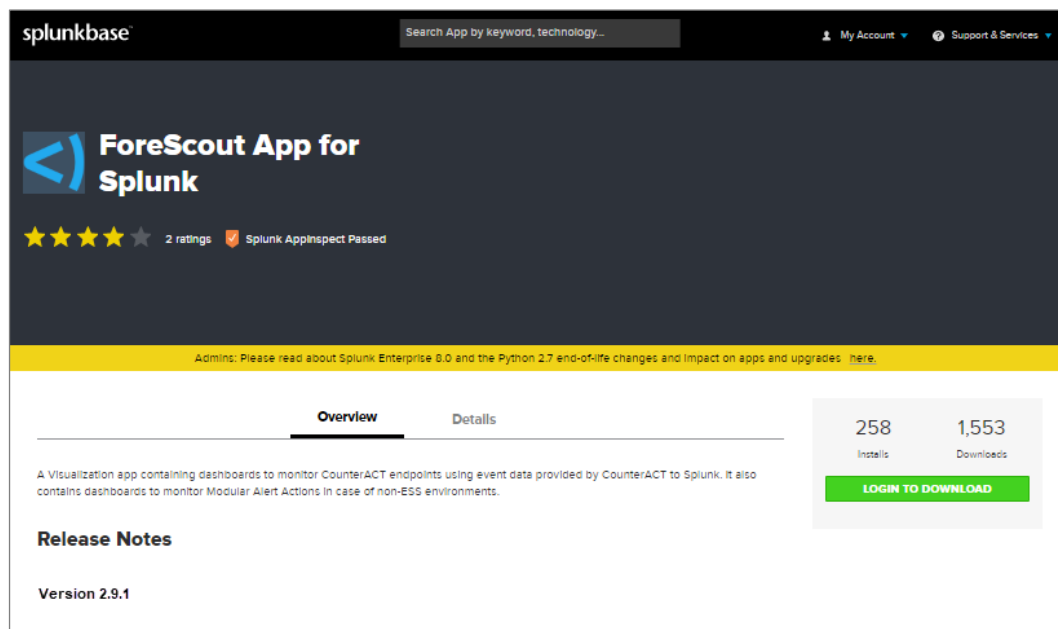
7. **Apply** the changes.

8. To test the connection, select **Test**.

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 App 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.

Submit a Case

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

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

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

Select Entitlement

Select Deployment

Splunk installation is?

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

Subject

Install ForeScout App

What Product are you having trouble with?

Splunk Cloud

Version

Cloud

Add

What OS are you using?

Other

What OS Version are you using?

I need help with...

Apps

Feature / Component / App

Other App

Deployment Type

Splunk Cloud

What is the impact...

Problem Description

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" in the following link for details:

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

Due to the REST API limitation on Cloud, a user who runs a **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 an account with the admin role (if you have *admin* access on the Splunk Cloud) with the edit_tcp capability.

You can also refer to KB 10495 as follows:

<https://forescout.force.com/support/s/article/REST-API-test-needs-edit-tcp-capability-to-work-on-managed-cloud>

There is also a limitation on the Splunk Cloud that restricts the maximum REST API inputs to 10K. Some JSON raw data from the Forescout platform to the Splunk Cloud will exceed 10K. Any data inputs above 10K will be truncated and will be in text format and not JSON format. Refer to KB 10498 as follows:

<https://forescout.force.com/support/s/article/Splunk-REST-API-target-only-allows-up-to-10K-payload>

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**.

Add Splunk HTTP Target Details - Step 1

Add Splunk HTTP Target Details

General

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

Splunk HTTP Type: Event Collector

Target Alias: CounterACT HEC to Splunk Cloud

POST to URL: https://http-inputs-forescout.splunkcloud.com:443/services/co

Index: fscntcenter

Comment:

Validate Server Certificate: ☒

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

Buttons: Help, Previous, Next, Finish, Cancel

3. In the General pane:
 - a. In the POST to URL field, paste the URL of the Instance with the *http-inputs-* prefix and 443 port number.
 - b. In the Authorization Token field, paste the token value from the Splunk HTTP Event Collector page.
4. Select **Next**.

Add Splunk HTTP Target Details - Step 2 of 2

Add Splunk HTTP Target Details

General **Connection Test**

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

On managed cloud deployments, uncheck the checkboxes for "Check if target is reachable", "Check REST API communication" and "Check data input and index", which are for on-prem deployments only.

Enable Test Configuration ☒

Check if target is reachable ☒ (Check executed via ICMP ping, on-prem only)

Check REST API communication ☐ (Server roles are retrieved if successful, on-prem only)

Check data input and index ☐ (Check executed via REST API communication, on-prem only)

Management Username

Management Password

Verify Password

Management Port

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

5. In the Connection Test pane, disable the checkboxes for **Check REST API communication** and **Check data input and index**.
6. Select **Finish**.
7. **Apply** the changes.
8. To test the connection, select **Test**.

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 C: 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
```

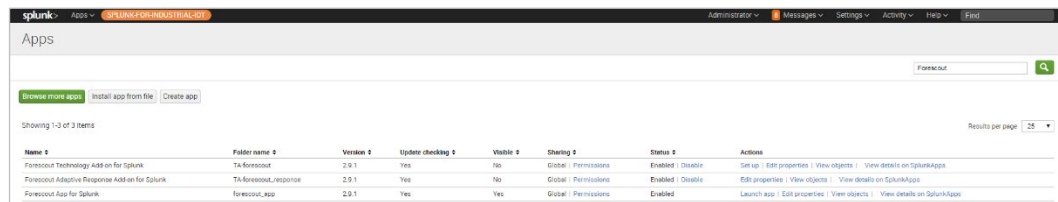
- This step is very important. If you do not open a support ticket, the Adaptive Response alerts will not work.**

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. Log in 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**.

The screenshot shows the 'CounterACT Configurations' form. It has four input fields: 'CounterACT IP Address or Hostname' (with 'forescout.com' entered), 'Enter password (Alert Service Authorization Token)', 'Confirm password', and 'Index for CounterACT events' (with 'fsc:center' entered). A note at the bottom states: 'Note: The password will be encrypted and stored in Splunk's password store. It will not be displayed here if this page is visited again.' There are 'Cancel' and 'Save' buttons at the bottom.

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 lowercase characters.

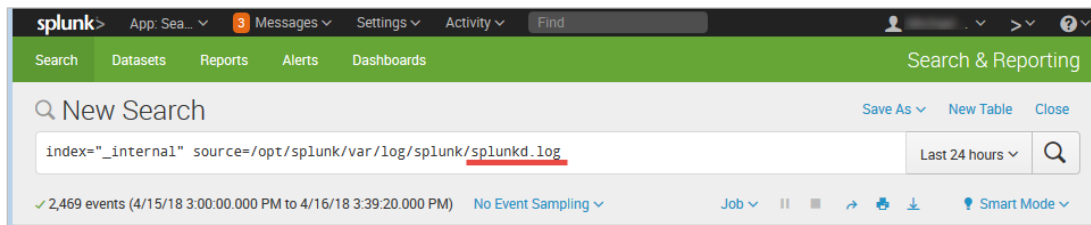
5. In the Enter password field, enter the **Alert Service Authorization Token**. You can get this token from the General Settings pane of the Forescout eyeExtend for Splunk configuration. See [Obtain an Authorization Token](#). Confirm the password.
6. Select **Save**.
7. In Splunk Cloud Instance, select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

Access Logs within Splunk Cloud Instance

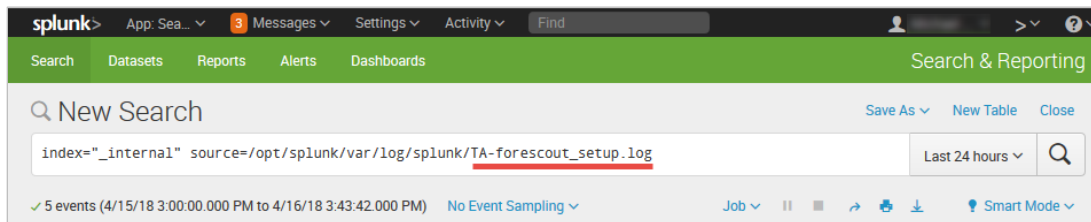
Because CLI is not provided on the Splunk Cloud, you will need to access your logs via the search function.

Below are example searches for:

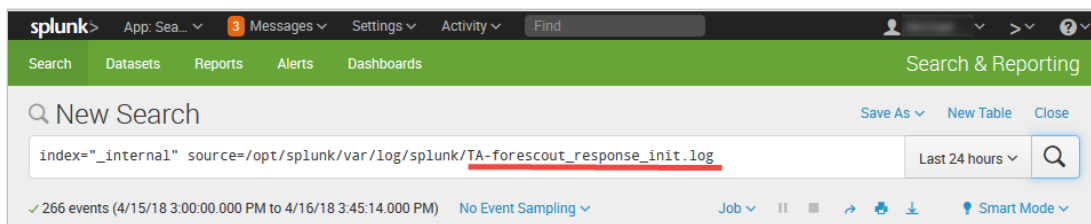
- Splunkd log
- TA-forescout_setup log
- TA-forescout_response_init log



Splunkd log



TA-forescout_setup log



TA-forescout_response_init log

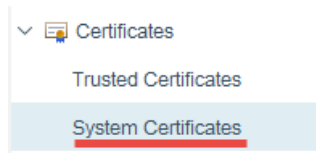
Appendix C: System Certificate for Web Portal

This section addresses the system certificates for the Splunk web portal on the 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*. See [Additional Forescout Documentation](#) for information on how to access this 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 dialog box, 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.

 A screenshot of a dialog box titled 'System Certificate - Step 1 of 6'. The main heading is 'Manage System Certificate'. On the left is a sidebar with options: 'CSR Form' (selected), 'CSR Details', 'Import', 'Issuer Chain', 'Scope', and 'Description'. The main area is titled 'CSR Form' and contains the instruction 'Complete the following Certificate Signing Request (CSR) fields.' Below this are five input fields: 'Subject' (with a sub-label 'Common Name'), 'Organization', 'Organizational Unit', and 'Locality'. At the bottom are buttons for 'Help', 'Previous', 'Next', 'Finish', and 'Cancel'.

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.

 A screenshot of the 'Options' window. The left sidebar shows various system components. The main area is titled 'Certificates > System Certificates' and contains a table of certificates. The table has columns: Description, Subject, Issuer, Valid To, Fingerprint, Used For, and Devices. There are five rows of certificates, all marked as 'Migrated for [Web Portal]' and 'Self Signed'. To the right of the table are buttons: 'Add from PKCS#12', 'Generate CSR', 'Duplicate', 'Edit', 'Remove', 'Export to PKCS#12', 'Help', 'Apply', and 'Undo'.

Description	Subject	Issuer	Valid To	Fingerprint	Used For	Devices
Migrated for [Web Portal]	CN=counteract_web_server, OU=counteract...	Self Signed	May 20, 2038	e52006c5096...	Web Portal	Enterprise Manager
Migrated for [Web Portal]	CN=counteract_web_server, OU=counteract...	Self Signed	May 20, 2038	a27739ba5001...	Web Portal	
Migrated for [Web Portal]	CN=counteract_web_server, OU=counteract...	Self Signed	May 20, 2038	dd5d22d4e277...	Web Portal	
Migrated for [Web Portal]	CN=counteract_web_server, OU=counteract...	Self Signed	May 20, 2038	1e24d9f5f0e8...	Web Portal	
Migrated for [HPS Inspect...]	O=Secure Connector, ST=Some-State, C=AN	Self Signed	May 20, 2038	8d5d9aab9311...	HPS Inspection En...	Enterprise Manager
Migrated for [HPS Inspect...]	O=Secure Connector, ST=Some-State, C=AN	Self Signed	May 20, 2038	7f0e2ca9bec2f...	HPS Inspection En...	

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

System Certificate <[redacted], fore Scout.com>

System Certificate

Certificate Details Issuer Chain Scope CSR Details

Certificate Details

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

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

Fingerprint 4e920cb9589b1b368c7fa7e8e7961115237733d4

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

SAN

Issuer CN=[redacted]-UTILSRV-CA, DC=[redacted], DC=fore Scout, DC=com

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

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

Key Size 2048

Key Algorithm RSA

Signature Algorithm SHA256WITHRSA

Certificate

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

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

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

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

Help OK Cancel

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

Additional Fore Scout Documentation

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

- [Documentation Downloads](#)
- [Documentation Portal](#)
- [Fore Scout Help Tools](#)

Documentation Downloads

Documentation downloads can be accessed from the [Technical Documentation Page](#), and one of two Fore Scout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** – [Product Updates Portal](#)
- **Flexx Licensing Mode** – [Customer Support Portal](#)

📄 *Software downloads are also available from these portals.*

To identify your licensing mode:

- From the Console, select **Help > About Forescout**.

Technical Documentation Page

The Forescout Technical Documentation page provides a link to the searchable, web-based [Documentation Portal](#), as well as links to a wide range of Forescout technical documentation in PDF format.

To access the Technical Documentation page:

- Go to <https://www.Forescout.com/company/technical-documentation/>

Product Updates Portal

The Product Updates Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend modules. The portal also provides additional documentation.

To access the Product Updates Portal:

- Go to <https://updates.forescout.com/support/index.php?url=counteract> and select the version you want to discover.

Customer Support Portal

The Downloads page on the Forescout Customer Support Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend modules. Software and related documentation only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Customer Support Portal:

- Go to <https://Forescout.force.com/support/> and select **Downloads**.

Documentation Portal

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

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/

Forescout Help Tools

You can access individual documents, as well as the [Documentation Portal](#), directly from the Console.

Console Help Buttons

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

Forescout Administration Guide

- Select **Administration Guide** from the **Help** menu.

Plugin Help Files

- After the plugin is installed, select **Tools > Options > Modules**, select the plugin, and then select **Help**.

Content Module, eyeSegment Module, and eyeExtend Module Help Files

- After the component is installed, select **Tools > Options > Modules**, select the component, and then select **Help**.

Documentation Portal

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