Contact Information
Forescout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA
https://www.forescout.com/support/
Toll-Free (US): 1.866.377.8771
Tel (Intl): 1.408.213.3191
Support: 1.708.237.6591

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

Legal Notice
© 2019 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.
# Table of Contents

## About Splunk Integration

- Support for Splunk Enterprise and Splunk Enterprise Security ............................................. 7
- About Certification Compliance Mode ......................................................................................... 7
- What's New ....................................................................................................................................... 7
- Support for Splunk Cloud ................................................................................................................. 7
- Support for Batch Messaging ........................................................................................................... 8
- Support for MAC-only Devices and IPv6 Devices ......................................................................... 8
- New Information Is Appended to Every Message ......................................................................... 8
- Support of Customized Indexes ....................................................................................................... 9
- Support for Multiple Channels for each Splunk Target ................................................................. 9
- New Test Button with In-Depth Results ......................................................................................... 9
- Improved Performance .................................................................................................................... 9

## About Forescout eyeExtend for Splunk

- Forescout App for Splunk ............................................................................................................ 12
- Forescout Technology Add-on for Splunk ..................................................................................... 13
- Forescout Adaptive Response Add-on for Splunk ........................................................................ 13

## How It Works

- Components ................................................................................................................................. 15
- Considerations ............................................................................................................................... 15
- Splunk Instance Credentials ......................................................................................................... 16

## What to Do

- .................................................................................................................................................... 16

## Requirements

- Forescout Requirements ................................................................................................................ 16
- Supported Vendor Requirements .................................................................................................. 17
- Splunk Cloud Requirements .......................................................................................................... 17
- About Support for Dual Stack Environments .............................................................................. 17
- Forescout eyeExtend (Extended Module) Licensing Requirements ........................................... 17
  - Per-Appliance Licensing Mode .................................................................................................... 18
  - Flexx Licensing Mode .................................................................................................................. 19
- More License Information .............................................................................................................. 20

## Install the Module

- Upgrade to Splunk Module Version 2.9 and Forescout Apps for Splunk 2.7 ............................. 20
- Install Forescout eyeExtend for Splunk ......................................................................................... 21

## Configure the Module

- .................................................................................................................................................... 22
Define an Event Collector ................................................................. 23
Secure Connection Messaging to the Splunk Enterprise Server .......... 26
Add a Splunk HTTP Target ............................................................... 27
Test the Connection ........................................................................ 32
Modify Splunk Enterprise Server Settings ..................................... 34
Add a Splunk Syslog Target ............................................................... 35

Test the Module .............................................................................. 40
Understand Test Results ................................................................. 42

Create Splunk Policies Using Templates ........................................ 42
Create a Send Endpoint and Policy Details Policy ....................... 43
Create the Policy ............................................................................ 46
How Devices are Detected and Handled ...................................... 47
Create a Splunk Stage 1 – Add to HTTP Notification Action Group Policy ... 49
Create a Policy .............................................................................. 49
How Devices are Detected and Handled ...................................... 50
Create a Splunk Stage 2 – Execute HTTP Notification Action Policy ... 53
Create a Policy .............................................................................. 54
How Devices are Detected and Handled ...................................... 56

Create Custom Splunk Policies ..................................................... 57
Detect Endpoints – Policy Properties .......................................... 62
Splunk Alerts ................................................................................. 62
Manage Splunk Devices – Policy Actions ..................................... 63
Splunk: Send Custom Notification Action .................................... 64
Splunk: Send Update from Forescout Action .................................. 65

Use Forescout eyeExtend for Splunk ............................................. 67
Run Splunk Audit Actions ............................................................... 68
Send Custom Notification to Splunk Enterprise Server Targets ....... 68
Send Updates from the Forescout Platform .................................. 71
Best Practices ................................................................................. 76
Forescout-to-Splunk Logging .......................................................... 77
Splunk to Forescout Messaging ..................................................... 77
Splunk Actions on the Forescout Platform ................................... 77
What Data is Sent to Splunk? ......................................................... 77

Appendix A: Default Communication Settings ............................ 77

Appendix B – Splunk Cloud Deployments .................................... 78
Splunk Cloud vs Splunk Enterprise .............................................. 78
Deploy Splunk Cloud ...................................................................... 78
Types of Splunk Clouds ................................................................. 79
Indexing Requirements for Splunk Cloud Instance ....................... 79
Self-Service Splunk Cloud .............................................................. 79
REST API ........................................................................................ 80
HTTP Event Collector ................................................................. 80
Managed Splunk Cloud ................................................................. 82
REST API.................................................................84
HTTP Event Collector ......................................................84
Set Up Secure Connection Messaging to the Splunk Cloud ............85
Set Up and Configure the Forescout Technology Add-on for Splunk Cloud........86
Access Logs within Splunk Cloud Instance ................................87

Appendix C: System Certificate for Web Portal........................................................................88

Additional Forescout Documentation.................................................................90
  Documentation Downloads ............................................................................91
  Documentation Portal ....................................................................................91
  Forescout Help Tools.......................................................................................92
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.

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

The result is enhanced threat insight, quicker incident response, automated control, and greater operational efficiency.
Support for Splunk Enterprise and Splunk Enterprise Security

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

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

About Certification Compliance Mode

Forescout eyeExtend for Splunk supports Certification Compliance mode. For information about this mode, refer to the Forescout Installation Guide.

What’s New

This section describes what is new in Forescout eyeExtend for Splunk.

Support for Splunk Cloud

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.

See Appendix B – Splunk Cloud Deployments.

**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.

**Support for MAC-only Devices and IPv6 Devices**

IPv6 addresses can be reported as a host property inside the `hostinfo` message sent Forescout eyeExtend for Splunk. IPv6 addresses are sent as part of the identity header in all messages sent by the module. Additionally, the Forescout platform also reports devices that have only a MAC address.

**New Information Is Appended to Every Message**

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

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

For more information, see Add a Splunk HTTP Target and Add a Splunk Syslog Target.
Support of Customized Indexes

Forescout eyeExtend for Splunk now supports the index of your choice. The default setting is \textit{fsctcenter}, however, you can change it to an index of your own. See \textit{Configure the Module}.

Support for Multiple Channels for each Splunk Target

To configure a new HTTP destination:

- For the Event Collector, the user 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, the user can configure two or more HTTP channels with same URLs as long as there are different \textit{Indexes}.
- For the RESTful API and Event Collector, TCP and UDP can be used as a form of multi-channel for each Splunk target.

This implementation provides greater granularity to the user.

New Test Button with In-Depth Results

To ensure your connection to the Splunk Enterprise server, a Test button has been added to the configuration section of Forescout eyeExtend for Splunk. After a test is run, details of the test are displayed to guide you in troubleshooting your connection difficulties. See \textit{Test the Module}.

Improved Performance

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

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

Use Cases

This section describes use cases supported by Forescout eyeExtend for Splunk. Be sure to review the \textit{Best Practices}.

To understand how this module helps you achieve these goals, see \textit{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-CAAAFBE

User Behavior Analytics (UBA)
The following minimum Forescout host properties are considered best practice for capturing UBA, and 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

Additionally, in order to capture a timestamp, a separate log should be set up for device disconnect.

**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

**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 Bidirectional Use Cases**

Due to bidirectional 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/](https://splunk-sizing.appspot.com/).

**Additional Splunk Documentation**

Refer to online documentation for more information about the Splunk solution: [http://docs.splunk.com/Documentation/Splunk](http://docs.splunk.com/Documentation/Splunk)

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

1. Go to [https://splunkbase.splunk.com/app/3381/](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 Policy and Splunk: Send Update from Forescout Action.


- 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 data in a dedicated, customizable Splunk dashboard. This bidirectional 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 to the user to allow storing information such as 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 credentials entered by the user 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 actions information which are 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**

Perform the following steps to set up the integration:

- Verify that all requirements are met. See [Requirements](#).
- [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:

- 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**

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

**Splunk Cloud Requirements**

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

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

**About Support for Dual Stack Environments**

Forescout version 8.1 detects endpoints and interacts with network devices based on both IPv4 and IPv6 addresses. However, **IPv6 addresses are not yet supported by this module**. The functionality described in this document is based only on IPv4 addresses. IPv6-only endpoints are typically ignored or not detected by the properties, actions, and policies provided by this module.

**Forescout eyeExtend (Extended Module) Licensing Requirements**

This Forescout eyeExtend product 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**.

![About ForeScout Console](image)

**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.

![Example Module License Request - Step 3 of 4](image)

**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.

![View](image)

**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 products. 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 products. 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 products, packaging individual licensed modules are supported. The Open Integration Module is an eyeExtend product 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 to for setting up your system when integrating with Splunk:

- Upgrade to Splunk Module Version 2.9 and Forescout Apps for Splunk 2.7
- Install Forescout eyeExtend for Splunk

Upgrade to Splunk Module Version 2.9 and Forescout Apps for Splunk 2.7

This section describes how to upgrade from Forescout eyeExtend for Splunk 2.5, 2.7, and 2.8 and Forescout Apps for Splunk version 2.5, 2.6 or 2.7.

- Before upgrading, make sure that you have Forescout eyeExtend for Splunk 2.5 installed and the Forescout Apps & Add-ons for Splunk version 2.5 or 2.6 in working condition.
- Before upgrading, make sure that you have Forescout eyeExtend for Splunk 2.7 installed and the Forescout Apps & Add-ons version 2.7 in working condition.

*Rollback is not available for this module. If you upgrade to Forescout eyeExtend for Splunk version 2.9 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:
   a. Forescout Technology Add-on for Splunk
   b. Forescout App for Splunk
   c. Forescout Adaptive Response Add-on for Splunk

2. On Splunkbase, use Browse More Apps to find all three Forescout Splunk Apps v2.7.

3. Select Load an App with the Upgrade App feature to upgrade them in any order.

4. After all the App and Add-ons are upgraded and configured, restart Splunk by selecting Settings/SYSTEM > Server Controls > Restart.

5. In the Console, upgrade to Forescout version 8.1. This includes upgrading Forescout eyeExtend for Splunk. Refer to the Forescout Administration Guide for instructions.

6. In the left pane, select Options and then select Splunk. The Splunk configuration pane opens to the Splunk Syslog Targets tab.

7. Select each of the channels and then select Test.

8. Select the Splunk HTTPS Targets tab.

9. Select each of the channels and then select Test.
   The upgrade is complete.

Install 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 will not proceed if you do not agree to the license agreement.

- The installation will begin immediately after selecting Install, and cannot be interrupted or canceled.

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

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

- Some components are not automatically started following installation.

**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. **Define an Event Collector**. Using Splunk Event Collector messages is the recommended protocol. Event Collector is a proprietary Splunk HTTP(S) channel introduced in Splunk 6.3. Follow the procedure described in this section to use Event Collector Messages.

4. **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. On Forescout eyeExtend for Splunk, Test the Module.

Define an Event Collector

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 define an event collector:

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

The Data Inputs page opens.
2. Select **HTTP Event Collector**.


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

5. In the Source type section, select **Select**.
6. Select **Select Source Type** and enter `fsctcenter` in the search field. Then select `fsctcenter_json` from the drop-down menu.

7. In the Index section of the Input Settings page, select one or more allowed indexes. The default setting is `fsctcenter`.

8. Select **Review**. Check your settings.

9. Select **Submit**. The new token value is created.
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.
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 HTTPS Targets tab.
3. Select **Add**.

![Add Splunk HTTP Target Details](image)

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 8089.

**To configure an event collector:**

1. In the Add Splunk HTTP Target details 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**
Enter the target URL displayed in the POST message header. In most cases, the URL takes the form of the example shown. Replace `my.splunk.com` with the Fully Qualified Domain Name (FQDN) or the IPv4 address of your Splunk Enterprise server. If the Splunk Enterprise server does not use the default port, specify the actual port used.
See [Appendix A: Default Communication Settings](#).

**dIndex**
Enter the index on the Splunk Enterprise server, where the update messages are sent to.

**Comment**
Enter optional text that indicates the location or other information to identify the server.

**Validate Server Certificate**
Select this option to validate the identity of the third-party server before establishing a connection, when the eyeExtend product communicates as a client over SSL/TLS. To validate the server certificate, either of the following certificate(s) must be installed:
- 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

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 [Forescout Administration Guide](#).

**Authorization Token**
In the Splunk App HTTP Event Collector pane, copy the `Token Value` and paste it in the **Authorization Token** field.

3. Select **Next**.
4. Configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Test Configuration</td>
<td>This option is enabled by default. Clear this checkbox if you need to disable the testing of the Splunk Syslog Target connection.</td>
</tr>
<tr>
<td>Check if target is reachable</td>
<td>Checks the Splunk Syslog target connection by executing an ICMP ping. This check is enabled by default. Clear this checkbox if you do not need to find out if the target is reachable.</td>
</tr>
<tr>
<td>Check REST API communication</td>
<td>Performs a check to verify whether 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 check is enabled by default.</td>
</tr>
<tr>
<td>Check data input and index</td>
<td>Performs a check to verify whether the data input configured in the Syslog/HTTP target is enabled. 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. This check is enabled by default.</td>
</tr>
<tr>
<td>Management Username</td>
<td></td>
</tr>
</tbody>
</table>
Management Password | The username and password credentials the Forescout platform uses to access the API on Splunk. Refer to the Forescout App & Add-ons for Splunk How-to Guide.
--- | ---
Verify Password | Re-enter the password.
Management Port | The default port is 8089. See Appendix A: Default Communication Settings.

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

**REST API**

**To configure an event collector:**

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

   The settings are refreshed according to your selection.

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 | The target URL displayed in the POST message header. In most cases the URL takes the form of the example shown. Replace my.splunk.com with the IP address of your Splunk Enterprise server. If the Splunk Enterprise server uses a different port from the default (8089), specify the actual port used. See Appendix A: Default Communication Settings.

Index | Enter the index for the HTTP REST API target or keep the default value of fsctcenter.

Comment | (Optional) Enter text that indicates the location or other information that identifies the server.

REST: Username | 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 Forescout App & Add-ons for Splunk How-to Guide.

REST: Password | 

Verify Password | Re-enter the password.

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

<table>
<thead>
<tr>
<th><strong>Enable Test Configuration</strong></th>
<th>This option is enabled by default. Clear this checkbox if disable testing of the Splunk HTTP Target connection.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Check if target is reachable</strong></td>
<td>Checks the Splunk HTTP target connection by executing an ICMP ping. This check is enabled by default. Clear this checkbox if you do not want to find out if the target is reachable.</td>
</tr>
<tr>
<td><strong>Check REST API communication</strong></td>
<td>Performs a check to verify whether 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 check is enabled by default.</td>
</tr>
<tr>
<td><strong>Management Username</strong></td>
<td>(Read-Only) The username and password credentials that the Forescout platform uses to access the API on Splunk.</td>
</tr>
<tr>
<td><strong>Management Password</strong></td>
<td>Refer to the Forescout App &amp; Add-ons for Splunk How-to Guide.</td>
</tr>
<tr>
<td><strong>Verify Password</strong></td>
<td>(Read-Only) Applicable to Event Collector only.</td>
</tr>
<tr>
<td><strong>Management Port</strong></td>
<td>(Read-Only) The default port is 8089. See Appendix A: Default Communication Settings.</td>
</tr>
</tbody>
</table>

5. Select **Finish**. The server is displayed in the Splunk pane, Splunk HTTP Targets tab.
6. Repeat for additional Event Collector/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.

   - ![CounterACT Options](image)

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

<table>
<thead>
<tr>
<th>Syslog Message Defaults</th>
<th>Identity</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Facility</td>
<td>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.</td>
</tr>
</tbody>
</table>
### 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
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:
- Using the property tag as the **Field: label**: `va_os : Windows 8.1 64-bit Pro`
- Using the property’s full name as the **Field: label**: `Windows Version : Windows 8.1 64-bit Pro`

### Tenant ID Prefix
Specify the prefix for the Tenant ID value in update messages. 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.

### 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. In the Splunk pane, 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.

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

> 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. In the Options dialog box, select **Splunk** in the left pane. The Splunk pane opens to the Splunk Syslog Targets tab.

3. Select **Add**.

4. Enter the following information:

<p>| Target Alias | Enter an alias to make it easier for you to select destinations when sending updates to the Splunk Enterprise server. |</p>
<table>
<thead>
<tr>
<th><strong>Address</strong></th>
<th>The hostname or IP address of the Splunk Enterprise server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UDP/TCP</strong></td>
<td>The protocol used for Syslog messaging with the server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>UDP</strong> (default) – select if you are concerned with speed of data messaging.</td>
</tr>
<tr>
<td></td>
<td>• <strong>TCP</strong> – select if you are concerned with accurate and successful transference of data.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Comment</strong></td>
<td>Optional text that indicates the location or other information that identifies the server.</td>
</tr>
</tbody>
</table>

Note: 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**.
6. Configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Test Configuration</td>
<td>Enabled by default, you can disable the testing of the Splunk Syslog Target connection. When this option is not selected, all fields in the Connection Test pane are disabled.</td>
</tr>
<tr>
<td>Check if target is reachable</td>
<td>Checks the Splunk Syslog target connection by executing an ICMP ping. Clear this checkbox if you do not want to find out if the target is reachable. This check is enabled by default.</td>
</tr>
<tr>
<td>Check REST API communication</td>
<td>Performs a check to verify if the Splunk Enterprise server’s REST API interface is reachable. If it is reachable, this test retrieves and displays the server roles configured on the Splunk Enterprise server. This check is enabled by default.</td>
</tr>
<tr>
<td>Check data input and index</td>
<td>Performs a check to verify if the data input configured in the Syslog/HTTP target is enabled. This check is enabled by default. Enabled. This check also displays the indexes configured in that data inputs settings on the Splunk Enterprise server.</td>
</tr>
<tr>
<td>HTTP Protocol</td>
<td>• HTTP – Uses a Splunk-specific message to report event and endpoint data.</td>
</tr>
<tr>
<td></td>
<td>• HTTPS – Uses an encrypted Splunk-specific message to report event and endpoint data</td>
</tr>
<tr>
<td>Management Username</td>
<td>The username and password 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 Forescout App &amp; Add-ons for Splunk How-to Guide.</td>
</tr>
<tr>
<td>Management Password</td>
<td></td>
</tr>
<tr>
<td>Verify Password</td>
<td>Verify the password.</td>
</tr>
<tr>
<td>Management Port</td>
<td>The default port is 8089. If the Splunk Enterprise server uses a different port, specify the actual port used. See Appendix A: Default Communication Settings.</td>
</tr>
</tbody>
</table>

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

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

8. In the Splunk pane, select the General Settings tab.
The CounterACT Data Submission Settings and Splunk Alert Message Settings sections are relevant when using Event Collector messaging to report data to Splunk:

<table>
<thead>
<tr>
<th>Syslog Message defaults</th>
<th>Identity</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Facility</td>
<td>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 <em>Forescout Core Extensions Module: Syslog Plugin Configuration Guide</em>.</td>
</tr>
<tr>
<td></td>
<td>Priority</td>
<td>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 <em>Forescout Core Extensions Module: Syslog Plugin Configuration Guide</em>.</td>
</tr>
</tbody>
</table>
### CounterACT Data Submission Settings

<table>
<thead>
<tr>
<th>CounterACT Data Submission Settings</th>
<th>Send Property Titles (longer)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The Forescout platform sends host property information to Splunk as Field:Value pairs in JASON format. By default, the Field: label is the internal property tag of each property. Select this option to send two sets of property value information to Splunk: Using the property tag as the Field: label: va_os : Windows 8.1 64-bit Pro Using the property’s full name as the Field: label: Windows Version : Windows 8.1 64-bit Pro</td>
</tr>
</tbody>
</table>

### Tenant Settings

<table>
<thead>
<tr>
<th>Tenant Settings</th>
<th>Tenant ID Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Specify the prefix for the Tenant ID value in update messages. You can choose to configure the module to generate a suffix to the aforementioned tenant ID prefix. If the suffix generation is selected, the module will generate a suffix (on each appliance) and append it to the Tenant ID prefix value to generate the Tenant ID. The Tenant ID is then sent as part of every update message sent by Forescout eyeExtend for Splunk to the Splunk Enterprise server. In the configuration wizard, enable/disable the Tenant ID suffix generation and specify the type of suffix value in the Tenant ID.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Add Appliance Suffix</th>
<th>Add Appliance Suffix Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable/Disable</td>
<td>This configuration is possible only if the Add Appliance Suffix option is selected. This field lets the user control the nature of the Tenant ID suffix generated. Depending on user selection, the Tenant ID suffix corresponding to each CounterACT Appliance can be: ▪ GUID ▪ Appliance IP address ▪ Appliance ID (a Forescout-platform-generated Node identifier)</td>
</tr>
</tbody>
</table>

### Splunk Alert Message Settings

<table>
<thead>
<tr>
<th>Splunk Alert Message Settings</th>
<th>Alert Service Authorization Token</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This string is used in the HTTP message header of alert messages sent to the Forescout platform by the Forescout App for Splunk.</td>
</tr>
</tbody>
</table>

9. In the Splunk pane, select **Apply**.

10. When prompted for confirmation, select **Yes**, and then select **Close**.

11. You are now ready to **Test the Module**.

---

**Test the Module**

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

<table>
<thead>
<tr>
<th>Checking for reachability</th>
<th>This check verifies whether the Splunk Enterprise server can be reached via ICMP.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checking for Splunk server roles</td>
<td>This check verifies whether 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.</td>
</tr>
<tr>
<td>Checking data inputs configuration</td>
<td>This check verifies whether 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.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>State / Icon</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>🌟</td>
<td>New Splunk target or no test has been attempted yet on this Splunk target.</td>
</tr>
<tr>
<td>🗨</td>
<td>Test failed on the Splunk target.</td>
</tr>
<tr>
<td>🕵️</td>
<td>Connectivity status expired.</td>
</tr>
<tr>
<td>🔄</td>
<td>Test message successfully sent from Forescout eyeExtend for Splunk to the Splunk Enterprise server.</td>
</tr>
<tr>
<td>←</td>
<td>Splunk test alert was received after a test message was sent successfully.</td>
</tr>
<tr>
<td>⚠️</td>
<td>Splunk test alert was received, but no test message sent for this target.</td>
</tr>
<tr>
<td>⚠️</td>
<td>Test message could not be sent on some appliances.</td>
</tr>
</tbody>
</table>

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. Refer to the following sections:

- [Create a Send Endpoint and Policy Details 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 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 a Splunk Stage 2 – Execute HTTP Notification Action Policy](#) that executes the HTTP Notification action for 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 Forescout Templates and Policy Management chapters in the *Forescout Administration Guide*.

**Create a Send Endpoint and Policy Details Policy**

This section describes how to use the Send Endpoint and Policy Details 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 and you can view the message sent to the Splunk Enterprise server using Splunk’s Search and Reporting app or the Forescout App for Splunk search capability.
The following example shows search results for "index=fsctcenter", which include several (batched) messages.

Select a message to expand the entry and display it in full.
A single message contains multiple host properties or policies for a particular endpoint.
Create the Policy

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

To create the policy:

1. Log in to the Console and select Policy.
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.

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

   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 Scope pane and the IP Address Range dialog box 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 pane opens. See [How Devices are Detected and Handled](#) for details of default policy logic.

10. Select **Next**. The Sub-rules pane opens. See [How Devices are Detected and Handled](#) for details of default policy logic.

11. Select **Finish**. The policy is created.

**How Devices are Detected and Handled**

This section describes the main rule and sub-rules of the policy created by the template. Policy rules instruct the Forescout platform how to detect and handled hosts defined in the policy scope.
Endpoints that match the Main Rule are included in policy sub-rule inspection. When endpoints do not match the Main Rule, policy evaluation ends. Sub-rules are not evaluated for these endpoints.

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

**Main Rule**

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

The Splunk: Send Update from Forescout Action can send the following information to Splunk for each detected endpoint:

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

For details about specifying the information that is sent to Splunk and for other action options, see Splunk: Send Update from Forescout Action.

Sub-Rules

There are no sub-rules in this policy.

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 a Policy

This section describes how to create a policy from the Splunk Stage 1 – Add to HTTP Notification Action Group policy template. See How Devices are Detected and Handled for details of default policy logic.

To create a policy:

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

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

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 Scope pane and the IP Address Range dialog box 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. See How Devices are Detected and Handled for details of default policy logic.
10. Select Finish. The policy is created.

**How Devices are Detected and Handled**

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

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

**Main Rule**

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

![Policy Wizard - Step 4 of 5](image)

**Sub-Rules**

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

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

**To define the action:**

1. Select **Splunk Alerts** in the Sub-rules, Condition dialog box.
2. Select **Edit**.
3. Select **Splunk Alert Action Group** and then select **Meets the following criteria**.

4. Use the drop-down menus to specify the criteria for meeting the Action Group alert.

5. Select **Splunk Alert Action** and then select **Meets the following criteria**.
6. Select **Notify – HTTP Notification** and then select **OK**.

### 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 a Policy

This section describes how to create a policy from the Execute HTTP Notification Action policy template. See How Devices are Detected and Handled for details of default policy logic.

To create the policy:

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

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

   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 Scope pane and the IP Address Range dialog box 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**. See **How Devices are Detected and Handled** for details of default policy logic.

10. Select **Finish**. The policy is created.

**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.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The action completed without failure.</td>
</tr>
<tr>
<td>Failure</td>
<td>The action completed with a failure, or timed out.</td>
</tr>
<tr>
<td>Pending</td>
<td>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.</td>
</tr>
<tr>
<td>Init</td>
<td>The action is in Initializing state, and not yet complete.</td>
</tr>
</tbody>
</table>

**No Status**

No status can be reported for one of the following reasons:

- No active policy detects the relevant Splunk Last Alert property, or applies the requested action.
- The endpoint has been deleted from the Forescout platform.
- Even though the IP address of the endpoint is within the Forescout platform’s network scope, the endpoint has not been detected by the Forescout platform.
- Scheduled data purges by the Forescout platform clear action data before reports are generated.
Invalid

- The endpoint IP is outside the network scope defined in the Forescout platform.
- An unspecified internal error occurred.

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.

How Devices are Detected and Handled

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

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

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

Main Rule

The main rule looks for an endpoint that is part of a specific group and when it finds a match, applies a defined action. The conditions defined in the Criteria section are re-checked every 8 hours (default.)
Sub-Rules
There are no sub-rules in this policy.

Create Custom Splunk Policies

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

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

To create a custom Splunk Stage 1 policy:

1. Log in to the Console and select Policy. The Policy Manager opens.
2. Select **Add** to create a policy.

3. Select **Splunk Stage 1: Add to HTTP Notification Action Group** template.

4. Select **Next**.

5. In the **Name pane**, change the name of the policy to a custom name and then select **Next**.

6. In the **Scope pane**, set an appropriate scope and then select **Next**.
7. Edit the main rule to specify the desired Splunk Alert Action Group. Select Next. The Sub-Rules pane opens.

8. In the Condition section, edit the first Sub-Rule and give it a custom name.

9. In the Actions section, add or edit the Splunk Alert Action. The Splunk Alert Action Group should be the same as the one specified in the main rule.

10. Select OK.
11. In the Splunk Alert Action section, select the **Splunk Alert Action** to be associated with the custom policy. Select **OK**.

12. The second sub-rule does not need to be edited. Select **Finish**.
To create a custom Splunk Stage 2 policy:
1. Log in to the Console and select Policy. The Policy Manager opens.
2. Select Add to create a policy. The Policy Wizard opens.
4. Select Next.
5. In the Name pane, change the name of the policy to a custom name and then select Next.
6. In the Scope pane, set an appropriate scope and then select Next.
7. In the **Condition** section, select the “Member of” item and edit the main rule condition to specify the group from the Stage 1 policy template.

8. In the **Actions** section, add or edit the action in the main-rule to the action for the custom policy.

9. Select **OK**.

10. 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.

There are three aspects of each Splunk alert check: Splunk Alert Action Group, Splunk Alert Action, and Splunk Alert Action Server.

**To configure Splunk alerts:**

1. In the Forescout Splunk App, search for and select **Splunk Alerts**. In the Condition pane, the configurations for Splunk Alerts are displayed.

2. The **Splunk Alert Action Group** field maps to an action group in the Forescout platform. In the Condition pane, select the Action Group values.
3. The **Splunk Alert Action** field maps the action(s) the selected group. If the group meets or does not meet the selected criteria, a request for action (alert) will be sent to the Forescout platform.

4. The **Splunk Alert Action Server** – Enter the IP address of the server that triggers the alert action request.

5. 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 Forescout 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: add this action to policies that apply or remove the **Switch Block** action to track port blocking in Splunk.

![Action](image)

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.
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 Forescout Action**

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

This action submits endpoint data to Splunk. This action is the primary method used for transmitting data from 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 [Send Endpoint and Policy Details to Splunk](#) policy template provided with the module.

**Content Sent Tab**

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

- Select the **Policy Status** option to include the most recent results of policy-based evaluation of the endpoint. 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 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 on the Console > Working with Inventory Detections* in the *Forescout Administration Guide* or the Console Online Help for information about working with the Asset Inventory.

**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.
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 | Send to All Syslog Targets – Select this option to send a notification to all Splunk Syslog targets. These are all targets that display in the Splunk Syslog Targets tab of the Splunk configuration pane.  
|                           | Send to Selected Syslog Targets – Select this option and then select More. A dialog box opens. Select the target(s) and then select OK. |
| Send Using HTTP POST      | Send to All HTTP Targets (default) – Select this option to send a notification to all Splunk HTTP targets. These are all targets that display in the Splunk HTTP Targets tab of the Splunk configuration pane.  
|                           | Send to Selected HTTP Targets – Select this option and then select More. A dialog box opens. Select the target(s) and then select OK. |
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.

- 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](image)

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 dialog box](image)

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. Then select **Send Using Syslog Messages** and/or select **Send Using HTTP POST**.
7. 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 Send Update from CounterACT information is displayed.

---

### 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 Define an Event Collector.

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 allow the Splunk Administrator to take manual actions. Automatic actions are based on Splunk-driven use case, while manual actions can be taken on any host-based on non-automated use cases. Actions on 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 Updates from CounterACT action. This action by default sends all Policy Statuses, Compliance Statuses and Host Properties to Splunk.

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

Appendix A: Default Communication Settings
The following table lists default settings for the communication between Splunk and the Forescout platform.

<table>
<thead>
<tr>
<th>Name</th>
<th>Direction</th>
<th>Protocol</th>
<th>Port</th>
<th>To customize</th>
</tr>
</thead>
<tbody>
<tr>
<td>REST</td>
<td>To Splunk</td>
<td>HTTPS</td>
<td>8089</td>
<td>Enter custom port/URL in the POST to URL field when you Configure the Module.</td>
</tr>
<tr>
<td>Event Collector</td>
<td>To Splunk</td>
<td>HTTPS</td>
<td>8088</td>
<td></td>
</tr>
<tr>
<td>Syslog</td>
<td>To Splunk</td>
<td>TCP/UDP</td>
<td>515</td>
<td>1. In Splunk: Clone the Data Input, and customize port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2. In the Forescout platform: Customize the Port and TCP/UDP fields when you</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Configure the Module.</td>
</tr>
</tbody>
</table>
### Appendix B – Splunk Cloud Deployments

This section describes information relating to Splunk Cloud.

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

### Splunk Cloud vs Splunk Enterprise

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

<table>
<thead>
<tr>
<th>Splunk Cloud</th>
<th>Splunk Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security</strong> – The security of the cloud deployment is managed and controlled by the Splunk Cloud team. There are more layers of security with Splunk Cloud.</td>
<td><strong>Security</strong> – Access and security of your Splunk deployment is locally managed and maintained by each customer.</td>
</tr>
<tr>
<td><strong>CLI access</strong> – 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.</td>
<td><strong>CLI access</strong> – refer to the Forescout App &amp; Add-ons for Splunk How-to Guide</td>
</tr>
<tr>
<td>- <strong>Managed Splunk Cloud</strong> – the apps must be installed by Splunk Cloud Support.</td>
<td>N/A</td>
</tr>
<tr>
<td>- <strong>Self-Service Splunk Cloud</strong> – you can install the apps</td>
<td></td>
</tr>
<tr>
<td>See <a href="#">Deploy Splunk Cloud</a></td>
<td></td>
</tr>
<tr>
<td><strong>TCP and UDP data</strong> 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.</td>
<td>Splunk Enterprise allows direct monitoring of <strong>TCP and UDP</strong>. See <a href="#">Add a Splunk Syslog Target</a>.</td>
</tr>
<tr>
<td><strong>HTTP Event Collector (HEC)</strong> – For Managed Splunk Cloud deployments, HEC must be enabled by Splunk Support</td>
<td><strong>HTTP Event Collector (HEC)</strong> – see <a href="#">Define an Event Collector</a>.</td>
</tr>
</tbody>
</table>

### 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:

<table>
<thead>
<tr>
<th><strong>Self-service Splunk Cloud</strong></th>
<th><a href="https://prd-*%5C.cloud%5C.splunk%5C.com">https://prd-*\.cloud\.splunk\.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>This is purchased directly from the Splunk website. For installation, see <a href="https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/User/TypesofSplunkClouddeployment">Self-Service Splunk Cloud</a>.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Managed Splunk Cloud</strong></th>
<th>https://*.splunkcloud.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed Splunk Cloud means you need to work with Splunk Sales to obtain your Splunk Cloud deployment. For installation, see <a href="https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/User/TypesofSplunkClouddeployment">Managed Splunk Cloud</a>.</td>
<td></td>
</tr>
</tbody>
</table>

For more information, refer to: [https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/User/TypesofSplunkClouddeployment](https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/User/TypesofSplunkClouddeployment)

**Indexing Requirements for Splunk Cloud Instance**

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

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

![New Index](image)

For more information, refer to: [https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/User/Datapolicies](https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/User/Datapolicies)

**Self-Service Splunk Cloud**

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

**REST API**

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

- You cannot use SAML authentication with REST API.

1. You will need to get the deployment name and credentials from Splunk Cloud Support.

2. Open the port 8089 **on the firewall** from the CounterACT Appliance to Splunk Cloud.

3. To access REST API, use this URL:
   
   https://input-<deployment-name>.cloud.splunk.com:8089

**HTTP Event Collector**

**Define the URL for the HTTP Event Collector**

**Self-service HTTP Event Collector**

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

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

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

**HEC API Access**

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

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

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

XXXXXXX = the unique ID for the Splunk Cloud Instance.

**Create HTTP Event Collector as a Data Input**

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

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

2. The Data inputs page 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**.
3. In the POST to URL field, paste the URL of the Instance with the *input-* prefix.
4. In the Authorization Token field, paste the token value from the Splunk HTTP Event Collector page.

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

1. On the Splunk App page, select the **Manage Apps** icon in the left pane.
2. The Apps page opens. Select **Browse more apps**.
3. In the search field, enter *Forescout* and run the search.
4. Under the Forescout Apps for Splunk, select the **View on Splunkbase** link.
5. The Forescout Apps for Splunk installation page opens.
6. Select **2.7.0_2** 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 **Customer Portal**.
9. Open a Splunk support ticket requesting installation of the app on your Splunk Cloud deployment.

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

11. Submit the ticket.
**REST API**

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

- *You cannot use SAML authentication with REST API.*

To access REST API, use this URL:

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

**HTTP Event Collector**

**Define the URL for the HTTP Event Collector**

*Self-service HTTP Event Collector*

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


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

**HEC API Access**

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

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

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

XXXXXX = the unique ID for the Splunk Cloud Instance.

**Create HTTP Event Collector as a Data Input**

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

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

Splunk Support will provide you with the Authorization Token required for sending HTTP events to Splunk Cloud.
For more information, refer to the following: [https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/User/AdddatausingHTTPeventcollector](https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/User/AdddatausingHTTPeventcollector)

**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.

**To enable HTTPS communication:**

1. **Open port 443 on the firewall** from the Splunk Cloud to the Enterprise Manager or the stand-alone CounterACT Appliance.
2. In the Forescout platform, use the ‘fstool cert’ utility to create a Certificate Signing Request (CSR) as follows:
   a. Use ‘fstool cert gen’ to generate the certificate request.
   b. Answer the questions required for certificate generating. Below is an example.

   > To create the server-side certificate, test.forescout.com was used as the FQDN in the DNS name of the Enterprise Manager field. The FQDN used by the Forescout platform needs to be recognized by Splunk Cloud.
C. A file containing the request is created in `/tmp/ca_request.csr`.

3. Get the CSR signed by a trusted Certificate Authority (for example, VeriSign).

4. Once the certificates are installed on the CounterACT Appliance using `fstool cert import` CLI and confirmed by `fstool cert test` CLI.

5. Open a Splunk Support ticket and request that the Forescout Public Key Certificate is appended to the cacert.pem file at the following location:

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

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

### Set Up and Configure the Forescout Technology Add-on for Splunk Cloud

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

1. Log in to the Splunk Cloud Instance.
2. Go to the Splunk/Apps page and within the Forescout Technology Add-on for Splunk row, select Set up.

3. In the CounterACT IP Address or Hostname field, enter the **FQDN** of the Enterprise Manager or standalone CounterACT Appliance of your environment.

   _If you are configuring Forescout Technology Add-on for Splunk with the Forescout platform's Fully Qualified Domain Name (FQDN), then it must be specified in all lower case characters._

4. In the Enter password field, enter the **Alert Service Authorization Token**. You can get this token from the General Settings pane of the Splunk configuration.

5. Select **Save**.

6. In Splunk Instance, select **Settings** and then select **Server controls**.

7. 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
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.

**To generate a certificate:**

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

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

![System Certificate - Step 1 of 8](image)

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.

![Certificate Management](image)

5. Once imported, you can view the certificate by selecting the web portal Enterprise Manager and then selecting **Edit**.
6. The FQDN of the Enterprise Manager selected is displayed in the *Subject* field and the *Certificate* field is populated.

**Additional Forescout Documentation**

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

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

Documentation downloads can be accessed from the Forescout Resources Page, or one of two Forescout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** – Product Updates Portal
- **Flexx Licensing Mode** – Customer Portal

Software downloads are also available from these portals.

To identify your licensing mode:
- From the Console, select Help > About Forescout.

Forescout Resources Page

The Forescout Resources Page provides links to the full range of technical documentation.

To access the Forescout Resources Page:

Product Updates Portal

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

The Downloads page on the Forescout Customer Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Forescout Customer 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.

If your deployment is using Flexx Licensing Mode, you may not have received credentials to access this portal.
To access the Documentation Portal:
- Go to https://updates.forescout.com/support/files/counteract/docs_portal/ and use your customer support credentials to log in.

Forescout Help Tools
Access information 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.

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

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

Online Documentation
- Select Online Documentation from the Help menu to access either the Forescout Resources Page (Flexx licensing) or the Documentation Portal (Per-Appliance licensing).