eyeExtend for Splunk 2.9.1

Release Notes

January 2020

Version Information

Forescout eyeExtend for Splunk® version 2.9.1.

This section describes requirements for this version.

Forescout Requirements

- Forescout version 8.1.
- A module license for Forescout eyeExtend for Splunk. See Forescout eyeExtend (Extended Module) Licensing Requirements for details.
- 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 integration of the Forescout platform with Splunk, you must also install the ***Forescout App for Splunk*** in the applicable Splunk instance(s). See How to Install.

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 Hardware Inventory Plugin (v 1.0.2.2, delivered with the Endpoint Module version 1.1.0).
   - For integration of the Forescout platform with Splunk, you must also install the ***Forescout App for Splunk*** in the applicable Splunk instance(s). See 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. See the *Forescout App & Add-ons for Splunk How-to Guide.*

Supported Vendor Requirements

- Splunk Enterprise version 7.0 or 7.2
- Splunk Enterprise Security version 5.2

- For information about the vendor models (hardware/software) and versions (product/OS) that are validated for integration with this Forescout component, refer to the Forescout Compatibility Matrix.

Splunk Cloud Requirements

- Splunk Cloud Enterprise version 7.2
- Splunk data integration requires a Splunk Cloud license. Refer to:
- https://docs.splunk.com/Documentation/SplunkCloud/7.2.4/User/Datapolicies

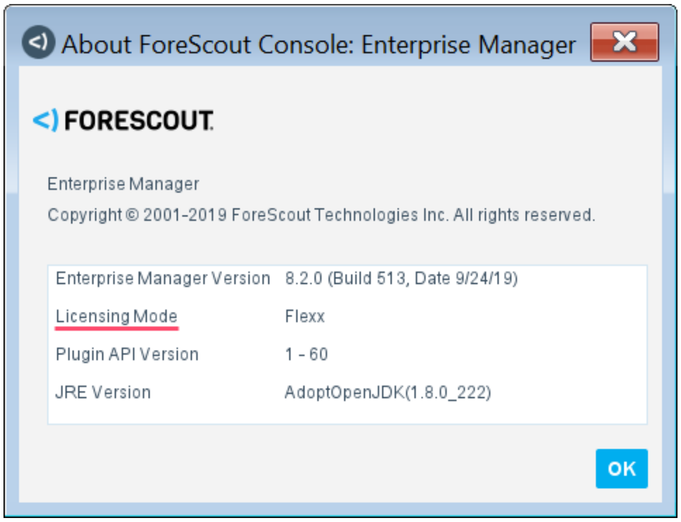
Forescout eyeExtend (Extended Module) Licensing Requirements

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: Enterprise Manager

FORESCOUT

Enterprise Manager

Copyright © 2001-2019 ForeScout Technologies Inc. All rights reserved.

Enterprise Manager Version	8.2.0 (Build 513, Date 9/24/19)
Licensing Mode	Flexx
Plugin API Version	1 - 60
JRE Version	AdoptOpenJDK(1.8.0_222)

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.

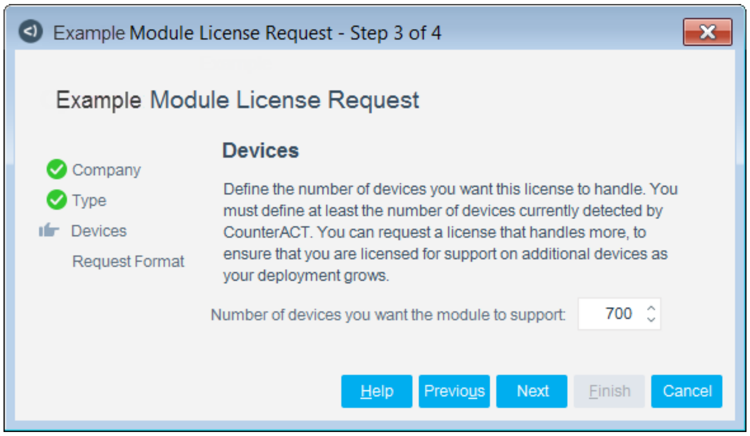
Demo license extension requests and permanent license requests are made from the Console.

> *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

Example Module License Request

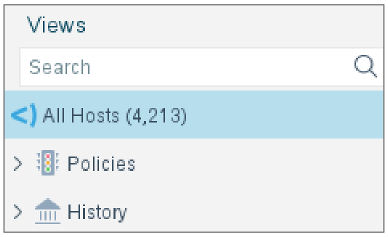
Devices

Define the number of devices you want this license to handle. You must define at least the number of devices currently detected by CounterACT. You can request a license that handles more, to ensure that you are licensed for support on additional devices as your deployment grows.

Number of devices you want the module to support: 700

To view the number of currently detected devices:

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



Flexx Licensing Mode

When you set up your Forescout deployment, you must activate a license file containing valid licenses for each feature you want to work with in your deployment, including eyeExtend 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. T*he 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.

App & Add-ons Version Information

Forescout Apps & Add-ons for Splunk, version 2.9.1

App & Add-ons Requirements

This section describes requirements for this version.

Splunk Requirements

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

- Create an account on the Splunk server with an admin role
- Splunk Enterprise version 7.0 or 7.2
- Splunk Enterprise Security version 5.2

- Splunk Processing Capacity: Refer to https://docs.splunk.com/Documentation/Splunk/7.2.4/Capacity/Referencehardware
- Splunk System Configuration: Refer to https://docs.splunk.com/Documentation/Splunk/7.2.4/Deploy/Deploymentcharacteristics
- Splunk User Permissions: Refer to https://docs.splunk.com/Documentation/Splunk/7.2.4/Admin/Aboutusersandroles

To integrate the Forescout platform with Splunk that ***does not*** run Splunk Enterprise Security (for more information, refer to the Splunk deployment guides at

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

Splunk Cloud Requirements

- Splunk Cloud Enterprise version 7.2
- Splunk data integration requires a Splunk Cloud license. Refer to:
- https://docs.splunk.com/Documentation/SplunkCloud/7.2.4/User/Datapolicies

External Requirements

This section describes system requirements, including:

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

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

Supported Forescout Versions

Customers who are working with the following Forescout version can install the module:

- Forescout version 8.1

External Systems Connections

This section covers the Forescout-related installation and configuration.

Install the Forescout Platform

The Forescout platform must be installed and configured in order to get data into Splunk. Contact your Forescout team for more details or reach out to:

support@forescout.com

Install Forescout eyeExtend for Splunk

Forescout eyeExtend for Splunk must be installed and configured in order to get data into Splunk. Contact your Forescout team for more details or reach out to:

support@forescout.com

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

- ***Establish Connection to Splunk***- this establishes a connection between your CounterACT® Appliance and a Splunk Instance.
- ***Test your Configuration*** - test your connection between your CounterACT Appliance and a Splunk Instance.

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

For Further Assistance

For further assistance with Forescout eyeExtend for Splunk, contact Professional Services.

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

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

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

Communication	Recommended	Alternative
Retrieve Action Info The Forescout App for Splunk polls the Forescout action_info API to retrieve a list of available actions.	REST API Default port: 443	REST API on HTTP

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

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

About This Release

This section describes updates and important information related to the component delivered in this version. This release also includes enhancements and fixes provided in previous versions. See Previous Releases.

See also:

- Feature Enhancements
- Fixed Issues
- Known Issues
- How to Install

Feature Enhancements

This section describes the new features and/or feature enhancements for this release.

IPv6 Support

This release supports IPv6 as follows:

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

- In Forescout Apps, IPv6 addresses are supported in the Forescout platform configuration of the Forescout Technology Add-on for Splunk (TA-forescout) for a standalone CounterACT Appliance or an Enterprise Manager.
- In events sent from eyeExtend for Splunk to the Splunk server, endpoints can contain IPv6 addresses or IPv6-only addresses, with or without MAC addresses.
- Adaptive Response action alerts apply to endpoints with IPv6 addresses or IPv6-only addresses, with or without MAC addresses.

Fixed Issues

This section describes the fixed issues for this version of Forescout eyeExtend for Splunk.

Defect #	Description
SPA-171	In the App for Splunk, when a user selected a policy from the drop-down menu in the Policy dashboard, the dashboard did not update to show only the results for the selected policy and the Policy dashboard ignored endpoints that did not contain an IPv4 address. Now, on selecting a policy in the policy picker, the dashboard updates to show only data for that policy and the Policy dashboard shows data for endpoints that do not have an IPv4 address.

Known Issues

This section describes the known issues for this version of Forescout eyeExtend for Splunk.

Defect #	Description
SPL-523	When the Splunk server certificate is revoked, a **Test** fails due to certificate revocation, but the policy still succeeds. The workaround is to perform a **Test** after setting up a connection.
SPA-194	To use the **Test** feature on REST API device configuration for Splunk Cloud, the *edit_tcp* capability has to be granted to the Splunk user. Refer to the sections "Self-Service Splunk Cloud" or "Managed Splunk Cloud" in the *Forescout eyeExtend for Splunk Configuration Guide* or the *Forescout App & Add-on for Splunk How-to Guide*. Refer also to KB 10495 as follows: https://forescout.force.com/support/s/article/REST-API-test-needs-edit-tcp-capability-to-work-on-managed-cloud

Defect #	Description
SPA-195	To use the **Test** feature on HTTP Event Collector (HEC) device configuration for Splunk Cloud, disable the checkboxes for **Check REST API communication** and **Check data input and index** in the Connection Test pane. Refer to the sections "Self-Service Splunk Cloud" or "Managed Splunk Cloud" in the *Forescout eyeExtend for Splunk Configuration Guide* or the *Forescout App & Add-on for Splunk How-to Guide*. Refer also to KB 10494 as follows: https://forescout.force.com/support/s/article/The-Check-REST-API-communication-inside-TEST-feature-won-t-work
SPA-196	Only partial JSON payload (up to 10K) was received on Splunk Cloud server if the JSON input size was greater than 10K. Refer to the sections "Self-Service Splunk Cloud" or "Managed Splunk Cloud" in the *Forescout eyeExtend for Splunk Configuration Guide* or the *Forescout App & Add-on for Splunk How-to Guide*. Refer also to KB 10498 as follows: https://forescout.force.com/support/s/article/Splunk-REST-API-target-only-allows-up-to-10K-payload
SPA-202	The Forescout Adaptive Response Add-on for Splunk (TA-forescout_response) on the Splunk Cloud does not send out RESTful API calls for the Forescout alert list because the file, inputs.conf, is removed by Splunk Cloud automation. Follow the procedure for "Post-Installation Check for Adaptive Response Add-on in Splunk Cloud Deployment" in the *Forescout App & Add-on for Splunk How-to Guide*. Refer also to KB 10499 as follows: https://forescout.force.com/support/s/article/input-conf-file-is-removed-from-the-TA-forescout-response-app-by-managed-cloud-automation
SPA-206	The Forescout logo color is not displayed consistently on the three Forescout apps posted on Splunkbase due to an undefined background color.
SPA-210	The Response Dashboard does not capture and display alert and action counts on the Splunk Cloud. Refer to the section "Response Dashboard" in the *Forescout App & Add-on for Splunk How-to Guide*. Refer also to KB 10500 as follows: https://forescout.force.com/support/s/article/Response-Dashboard-on-Splunk-server-is-not-showing-alerts-related-counts-correctly

How to Install

To install the module:

1. Navigate to one of the following Forescout download portals, depending on the licensing mode your deployment is using:
   - Product Updates Portal - ***Per-Appliance Licensing Mode***
   - Customer Portal, Downloads Page - ***Flexx Licensing Mode***

To identify your licensing mode, select **Help > About ForeScout** from the Console.

2. Download the module `.fpi` file.
3. Save the file to the machine where the Console is installed.
4. Log into the Console and select **Options** from the **Tools** menu.
5. Select **Modules**. The Modules pane opens.
6. Select **Install**. The Open dialog box opens.
7. Browse to and select the saved module `.fpi` file.
8. Select **Install**. The Installation screen opens.
9. Select **I agree to the License Agreement** to confirm that you have read and agree to the terms of the License Agreement and select **Install**. The installation cannot proceed unless you agree to the license agreement.

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

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

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

    🗎 *Some components are not automatically started following installation.*

More Release Information

This section provides additional release information.

Rollback Support

Rollback is not available for this module. This means that if you upgrade to this module version and the module does not operate as expected, you cannot roll it back to a previous release.

Previous Releases

Installing this release also installs fixes and enhancements provided in the releases listed in this section. To view Release Notes of previous version releases, see:

https://www.forescout.com/company/resources/eyeextend-for-splunk-2-9-release-notes/

https://www.forescout.com/company/resources/extended-module-for-splunk-release-notes-2-8-0/

Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

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

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

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

Legal Notice

2020-01-27 11:35