ForeScout Extended Module for Splunk® version 2.8

Release Notes

June 2018

Module Version Information

ForeScout Extended Module for Splunk® Module 2.8.

This section describes requirements for this version.

Module Requirements

- ForeScout CounterACT® version 8.0
- A module license for the Splunk Module. See ForeScout Extended Module License Requirements for details.
- This module is a component of the ForeScout Extended Module for Splunk and requires a module license.
- 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 CounterACT-Splunk integration, 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 1.0).
   - For CounterACT-Splunk integration, 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 the ForeScout Extended Module for Splunk (Splunk Module) and requires a module license. See the *ForeScout App & Add-ons for Splunk How-to Guide.*

ForeScout Extended Module for Splunk® version 2.8

Release Notes

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 https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/User/Datapolicies

ForeScout Extended Module License Requirements

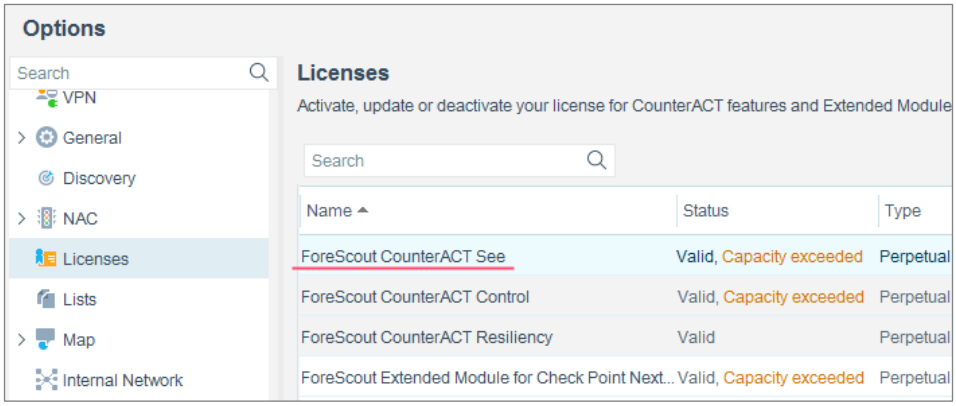
This ForeScout Extended Module requires a valid license. Licensing requirements differ based on which licensing mode your deployment is operating in:

- Per-Appliance Licensing Mode
- Centralized Licensing Mode

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Per-Appliance Licensing Mode

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

When the demo period expires, you will be required to purchase a permanent module license. *In order to continue working with the module, you must purchase the license*.

Demo license extension requests and permanent license requests are made from the CounterACT 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 CounterACT 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 CounterACT. 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 CounterACT, Console Modules pane.

To view the number of currently detected devices:

1. Select the **Home** tab.

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

Centralized Licensing Mode

When you set up your CounterACT deployment, you must activate a license file containing valid licenses for each feature you want to work with in your deployment, including Extended Modules. After the initial license file has been activated, you can update the file to add additional Extended Module licenses or change endpoint capacity for existing Extended Modules. For more information on obtaining Extended Module licenses, contact your ForeScout 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 Extended Module license has an associated capacity, indicating the number of endpoints the license can handle. The capacity of each Extended Module license varies by module, but does not exceed the capacity of the *See* license.

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

More License Information

Refer to the *CounterACT Administration Guide* for information on Extended Module licenses. You can also contact your ForeScout representative or license@forescout.com for more information.

About This Release

This version contains important Fixed Issues and Feature Enhancements.

Installing this release also installs fixes and enhancements provided in previous releases. See Previous Releases for more information. See How to Install for installation details.

Feature Enhancements

This release provides the following feature enhancements:

Splunk Cloud Deploymenta

ForeScout supports integration with Splunk Cloud™. Splunk Cloud provides the benefits of Splunk Enterprise and if purchased Splunk 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.

Full information about Splunk Cloud is listed in the *ForeScout Extended Module for Splunk Configuration Guide. [Tracked as SPL-502]*

App & Add-ons Version Information

ForeScout Apps & Add-ons for Splunk, version 2.7.0

Click for information about the ForeScout Extended Module for Splunk (Splunk Module), version 2.8.

App & Add-ons Requirements

This section describes requirements for this version.

Splunk Requirements

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

- Create an account on Splunkbase.
- Splunk Enterprise version 6.4, 6.5, 6.6, or 7.0.

- Splunk Enterprise Security version 4.5 or 4.7.
- Splunk Processing Capacity - See Splunk Enterprise Capacity Planning Manual version 6.6.
- Splunk System Configuration - See Splunk Enterprise Distributed Deployment Manual, version 6.6.
- Splunk User Permissions - See About Users and User Roles version 6.6.

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

https://docs.splunk.com/Documentation/Splunk/6.6.3/Installation/SystemRequirements

Splunk Cloud Requirements

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

  https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/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 CounterACT® Versions

Customers who are working with the following CounterACT version can install the module ForeScout CounterACT® version 8.0.

External Systems Connections

This section covers the CounterACT-related installation and configuration.

Install CounterACT

ForeScout CounterACT is required to 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 Extended Module for Splunk

The ForeScout Extended Module for Splunk is required to 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 Extended Module 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 the ForeScout Extended Module for Splunk, refer to the *ForeScout Extended Module for Splunk Configuration Guide*.

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

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

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

Communication	Recommended	Alternative
Retrieve Action Info The ForeScout App for Splunk polls CounterACT's action_info API to retrieve a list of available actions.	REST API Default port: 443	REST API on HTTP
Ongoing Data Reporting CounterACT sends endpoint data to Splunk. This is the protocol used by the Splunk Module in CounterACT to implement the **Splunk: Send Update from CounterACT** action.	Event Collector Default port: 8088	Syslog (port 515/TCP/UDP) RESTful API HTTPS (8089)
Splunk Action Request ▪ Splunk sends alerts to CounterACT'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 CounterACT 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 version contains important Fixed Issues and Feature Enhancements.

Installing this release also installs fixes and enhancements provided in previous releases. See Previous Releases for more information. See How to Install for installation details.

Feature Enhancements

This release provides the following feature enhancements:

Splunk Cloud Deployment

ForeScout supports integration with Splunk Cloud™. Splunk Cloud provides the benefits of Splunk Enterprise and if purchased Splunk 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.

Full information about Splunk Cloud is listed in the *ForeScout Extended Module for Splunk Configuration Guide. [Tracked as SPL-502]*

Fixed Issues

There are no fixed issues for this release.

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 - ***Centralized Licensing Mode***

   To find out which licensing mode your deployment is working with, see Identifying Your Licensing Mode in the Console.
2. Download the module **`.fpi`** file.

3. Save the file to the machine where the CounterACT Console is installed.
4. Log into the CounterACT 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.

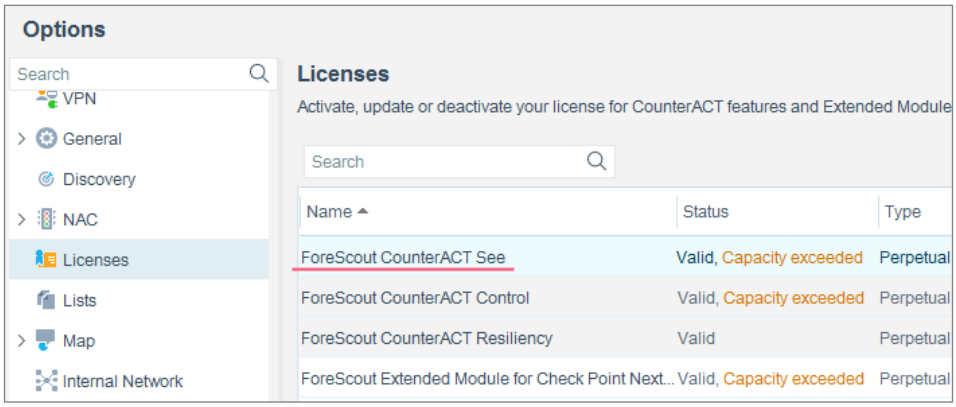
10. When the installation completes, select **Close** to close the window. The installed module is displayed in the Modules pane.

    Some components are not automatically started following installation.

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Contact your ForeScout representative if you have any questions about identifying your licensing mode.

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://updates.forescout.com/support/files/plugins/splunk/2.7.0/2.7.0-27000050/RN.pdf

https://updates.forescout.com/support/files/plugins/splunk/2.5.0.2012/2.5.0.2012-25002012/RN.pdf

https://updates.forescout.com/support/files/plugins/splunk/2.5.0/2.5.0-25000037/RN.pdf

https://updates.forescout.com/support/files/plugins/splunk/2.0.0/2.0.0-20000067/RN.pdf

http://updates.forescout.com/support/files/plugins/splunk/1.2.0/1.2.0-1203/RN.pdf

https://updates.forescout.com/support/files/plugins/splunk/1.0.1/1.0.1-15/RN.pdf

Legal Notice

2018-06-22 17:11