

March 2019

Version Information

Forescout eyeExtend for CrowdStrike® version 1.2.

Forescout Requirements

- Forescout version 8.1.
- A module license for Forescout eyeExtend for CrowdStrike. See [Forescout eyeExtend \(Extended Module\) Licensing Requirements](#).
- Core Extensions Module version 1.1, with the IOC Scanner Plugin running.

CrowdStrike Requirements

The module requires the following CrowdStrike Falcon components:

- A valid UUID, API Key, password and connectivity to CrowdStrike Streaming API Version 4.9 or later
 - A valid username, password and connectivity to CrowdStrike Query API Version 3.3 or later
-  *The Query API requires a special set of username and password credentials that can only be created by support@crowdstrike.com. This is not to be confused with the credentials that you use for the Falcon CrowdStrike user interface.*

Network Requirements

When your environment routes Internet communications through a proxy server, you will need to configure the connection parameters for the proxy server that handles communication between this CrowdStrike Cloud Platform and its connecting CounterACT® device.

To have a good performance, each connecting CounterACT device should handle no more than 40,000 devices on the network. Create multiple connecting appliance clusters if you have more devices on the network.

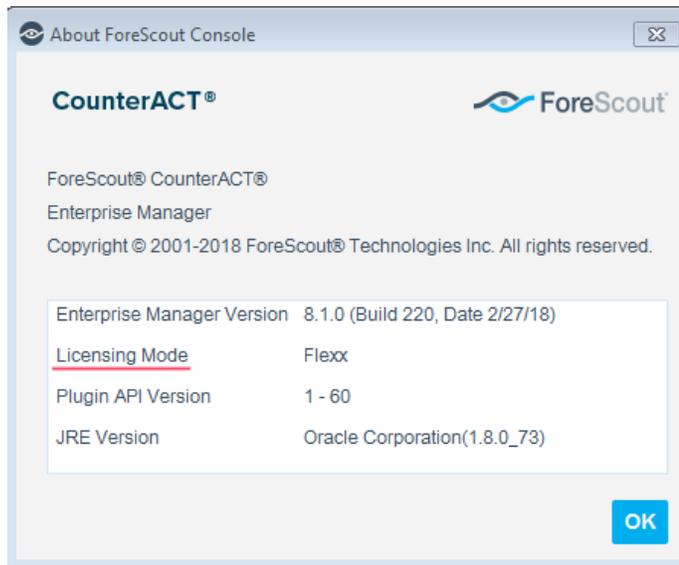
Forescout eyeExtend (Extended Module) Licensing Requirements

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**.



Per-Appliance Licensing Mode

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

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

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

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

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

Requesting a License

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

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



To view the number of currently detected devices:

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



Flexx Licensing Mode

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

About This Release

This release:

- Supports the ability to enable and disable server certificate validation.
- Supports Certification Compliance mode. For information about this mode, refer to the *ForeScout Installation Guide*.
- Changes the way the CrowdStrike host ID is retrieved and endpoints are classified in the default CrowdStrike Agent Hygiene policy. In previous releases, the IP address or MAC address was used to retrieve the CrowdStrike host ID. Endpoints were classified in the default policy based on the CrowdStrike host ID. In this release, IP address, MAC address, and hostname are used to retrieve the CrowdStrike host ID from the Falcon cloud and classify the endpoints in the default policy.

This version contains important [Fixed Issues](#). 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.

Fixed Issues

There are no fixed issues for this release.

Known Limitation

Detection event volume/velocity varies widely depending on the size of the customer environment. It's typically pretty low volume though, as a ballpark, even a 100K endpoint environment isn't likely to have more than 200 detections per 24 hours. Large deviations from this norm are likely indicators of a misconfiguration or an attack (such as a DDOS).

In these rare instances, CrowdStrike implements throttling to prevent threats or attacks that would DDOS the CrowdStrike cloud or downstream enterprise security software such as a SIEM. A good indication CrowdStrike has started to throttle event

detection would be if the ForeScout platform receives an event hours or days after a detection. The following are examples of when CrowdStrike would throttle detection events (example but not limited to):

- If CrowdStrike identifies the same pattern/detection on the same host and process, it will only trigger a detection once (not over and over)
- The same pattern/detection and host (without the same process) will only trigger, at most, once every 5 minutes.
- Maximum of 1,000 detections per day on a single endpoint (clear indication that the host should be investigated)

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 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.*

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/crowdstrike/1.1.0/1.1.0-1100003/RN.pdf>

<https://updates.forescout.com/support/files/plugins/crowdstrike/1.0.0/1.0.0-10000109/RN.pdf>

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.

2019-03-13 09:52