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

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

Legal Notice
© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at https://www.Forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners.
# Table of Contents

**About the FireEye EX Integration** ................................................................. 4  
Advanced Threat Detection with the IOC Scanner Plugin .............................. 4
Use Cases ................................................................................................... 5
Additional FireEye EX Documentation .......................................................... 5

**About This Module** .................................................................................... 5  
How It Works ............................................................................................... 6
What to Do .................................................................................................. 6

**Requirements** .............................................................................................. 7  
Forescout Requirements ................................................................................ 7

**Forescout eyeExtend (Extended Module) Licensing Requirements** .......... 7  
Per-Appliance Licensing Mode .................................................................... 8
Flexx Licensing Mode .................................................................................... 9
More License Information ............................................................................. 9
FireEye EX Requirements ............................................................................. 9
About Support for Dual Stack Environments ................................................. 10

**Define Rsyslog Targets in FireEye EX** ......................................................... 10

**Install the Module** ..................................................................................... 10

**Configure the Module** ............................................................................... 11

**Configure the Forescout Syslog Plugin** ....................................................... 13

**Create Custom FireEye EX Policies** .......................................................... 14

**Additional Forescout Documentation** ......................................................... 15  
Documentation Downloads ........................................................................... 15
Documentation Portal ..................................................................................... 16
Forescout Help Tools ..................................................................................... 16
About the FireEye EX Integration

Cyber criminals often use email spear phishing attacks, as well as malicious file attachments and URLs in emails, to launch advanced cyber-attacks. These email attacks routinely bypass conventional signature-based defenses such as antivirus and spam filters. The FireEye® Email Security (EX) series protects against these email attacks on your corporate email accounts.

This integration combines the email threat detection mechanisms of FireEye EX with the network visibility and compliance enforcement capabilities of the Forescout platform to multiply the benefits of working with an Advanced Threat Detection (ATD) product. Integration with the Forescout platform helps corporate security teams identify, analyze and block advanced email-based cyber-attacks from both corporate and non-corporate email accounts.

Advanced Threat Detection with the IOC Scanner Plugin

Forescout eyeExtend for FireEye EX works with the IOC Scanner Plugin, the Forescout platform’s action center for Advanced Threat Detection (ATD) and response. The IOC Scanner Plugin provides:

- A centralized repository of all threats and their IOCs (indicators of compromise) reported to the Forescout platform by third-party ATD solutions, or added manually.
- Mechanisms that scan all Windows endpoints for threat and IOC information reported to the Forescout platform, evaluate the likelihood of compromise, and apply appropriate actions to endpoints.

Threat detection and response is implemented in the following stages:

- FireEye EX instances in your environment report threats to this plugin as they are detected in emails.
- All threats reported by this module are automatically submitted to the IOC Scanner Plugin, which parses the threat to yield indicators of compromise (IOCs) - measurable events or state properties that can be used as a "fingerprint" to identify the threat. The IOC Scanner Plugin uses these IOCs to mount further scan/analyze/remediate stages of the Forescout platform's ATD response, as follows:

  - **ATD Stage 2 (IOC Scanner Plugin): Real-time hunt for endpoints of interest based on threats and IOCs:** The IOC Scanner Plugin detects endpoints with IOCs associated with recently reported threats.

  - **ATD Stage 3 (IOC Scanner Plugin): Evaluation and remediation:** The IOC Scanner Plugin evaluates the profile of IOCs on endpoints of interest to determine the likelihood that an endpoint is compromised, and applies appropriate blocking/remediation actions.

For more information about IOC-based threat detection and remediation, refer to the *Forescout Core Extensions Module: IOC Scanner Plugin Configuration Guide*. 
Use Cases
This section describes important use cases supported by this module. To understand how this module helps you achieve these goals, see About This Module.

- Identify threats delivered through emails, attachments and embedded URLs that may not have been delivered through corporate emails monitored by FireEye EX. For example, a file on an attached drive or an email attachment delivered to a personal email account. Once identified, you can use Forescout platform polices to perform actions on potentially infected endpoints that immediately:
  - Contain infected endpoints, for example limit or block network access. This prevents lateral movement of the infection to other endpoints.
  - Remediate infected endpoints, for example by killing suspicious processes.
  - Notify stakeholders by, for example, sending an email to corporate security teams with details about which threats were detected on which endpoints.

For more detailed information about this use case, refer to the section about use cases in the Forescout Core Extensions Module: IOC Scanner Plugin Configuration Guide.

Additional FireEye EX Documentation
Refer to FireEye EX online documentation for more information about the FireEye EX solution:

- EX Series Threat Management Guide
- EX Series System Administration Guide


About This Module
This module, together with the IOC Scanner Plugin, lets you integrate the Forescout platform with FireEye EX so that you can view new threats of suspicious emails, attachments and embedded URLs reported by FireEye EX and automatically added to the IOC repository. Refer to the Forescout Core Extensions Module: IOC Scanner Plugin Configuration Guide for more information.
To use the module, you should have a solid understanding of FireEye EX concepts, functionality and terminology, and understand how Forescout platform policies and other basic features work.

**How It Works**

FireEye EX detects spear phishing attacks as well as malicious file attachments and URLs in emails that are used to launch advanced cyber-attacks. When a threat is detected, the FireEye EX server sends a notification (rsyslog format) of the threat details to a pre-defined receiving CounterACT® device. The notification includes:

- timestamp of the event
- threat name, file name, severity and hash
- IOC details identified throughout the lifecycle of the threat on different operating systems (according to how FireEye EX is configured in your environment), such as:
  - Process Names
    - If the reported malicious process indication is an .exe file, the filename is stored in the IOC repository as both a Process IOC and a File Exists IOC. If the malicious process indication is a loaded .dll file, the filename is stored as a File Exists IOC only. The Forescout platform detects .dll or .exe Portable Executable file types only.
  - File Names
  - Registry Keys and Values
  - Service Names
  - Mutex Names
  - DNS Queries
  - Command and Control (CnC) URLs

The Forescout platform adds the data to its IOC repository, where it can be used to trigger policy actions.

Refer to the *Forescout Core Extensions Module: IOC Scanner Plugin Configuration Guide* for details.

**What to Do**

You must perform the following to work with this module:

1. **Install the IOC Scanner Plugin**
2. **Verify that you have met system requirements.** See *Requirements*.
3. **Define Rsyslog Targets in FireEye EX**
4. **Install the Module.**
5. **Configure the Module.**
6. **Configure the Forescout Syslog Plugin**
7. **Create Custom FireEye EX Policies** (optional).
Requirements

This section describes system requirements, including:

- **Forescout Requirements**
- **Forescout eyeExtend (Extended Module) Licensing Requirements**
- **FireEye EX Requirements**

### Forescout Requirements

This module requires the following Forescout releases and other components:

- Forescout version 8.0, 8.1, or 8.2
- Core Extensions Module version 1.0, 1.1, or 1.2 with the following components running:
  - Syslog Plugin version
  - IOC Scanner Plugin version

### 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.

FireEye EX Requirements

This module requires the following FireEye EX components:

- FireEye Email Security (EX) Series version 7.6
- Admin or Operator access to the EX Series appliance is required.
- 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.
About Support for Dual Stack Environments

The Forescout platform 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.

Define Rsyslog Targets in FireEye EX

FireEye EX sends threat detections to the Forescout platform as rsyslog notification messages. To enable the Forescout platform to receive these notifications, you must define one or more CounterACT devices as rsyslog targets, and define the format of the notification message sent by FireEye EX.

- The EX Series appliance must have an established connection to the Internet.
- You must have Admin or Operator access to the EX Series appliance.
- Specify each Counteract connecting device by its IP address.
  - At least one target must be enabled to work with the module.
- Notifications to targets should use the following settings:

<table>
<thead>
<tr>
<th>Format</th>
<th>JSON Extended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delivery</td>
<td>Per Event</td>
</tr>
<tr>
<td>Notifications</td>
<td>All Events</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP</td>
</tr>
</tbody>
</table>

Install the Module

This section describes how to install the module. Before you install this module, first install the IOC Scanner Plugin.

*Before you install this module, the Forescout IOC Scanner Plugin and the Forescout Syslog Plugin must already be running.*

To install the module:

1. Navigate to one of the following Forescout download portals, depending on the licensing mode your deployment is using:
   - **Product Updates Portal** - **Per-Appliance Licensing Mode**
   - **Customer Portal, Downloads Page** - **Flexx Licensing Mode**
   To identify your licensing mode, select Help > About ForeScout from the Console.

2. Download the module `.fpi` file.

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

   - The installation begins immediately after selecting Install and cannot be interrupted or canceled.
   - In modules that contain more than one component, the installation proceeds automatically one component at a time.

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

   - Some components are not automatically started following installation.

**Configure the Module**

Configure the module to ensure that the Forescout platform can communicate with the FireEye EX service.

**To configure the module:**

1. In the Console, select **Options** from the **Tools** menu. The Options pane opens.
2. Select the **Modules** folder.
3. In the left pane, select **FireEye EX**, and select **Configure**.
4. Select Add to define a FireEye EX server to communicate with the Forescout platform.

![Add FireEye EX Server](image)

5. Enter the following information:
   - **IP Address.** The IP address of the FireEye EX server that sends rsyslog notifications to the Forescout platform. See Define Rsyslog Targets in FireEye EX for details.
   - **Description.** A textual description of the FireEye EX server.

6. Select OK. An entry for the FireEye EX server is added to the list in the FireEye EX pane.

7. In the FireEye EX pane, select **Apply.** An Enterprise Manager Console opens.

8. Select **Yes** to save the module configuration.

The table in the FireEye EX pane has two additional display-only columns. These columns shown information on threats reported by FireEye EX appliances:

- **Last Threat Report Time.** Indicates the latest date/time when the Forescout platform received a threat alert from this FireEye EX appliance.
Receiving CounterACT Appliance. The IP address of the connecting CounterACT device that received the last threat notification from this FireEye EX appliance. This is one of the CounterACT devices defined as rsyslog targets at the FireEye EX appliance. See Define Rsyslog Targets in FireEye EX.

Configure the Forescout Syslog Plugin

Configure the Forescout Syslog Plugin to enable the receiving CounterACT device to connect to the FireEye EX server and receive notifications.

Refer to the Forescout Core Extensions Module: Syslog Plugin Configuration Guide for more information about the Syslog Plugin configuration.

To configure the Syslog Plugin:

1. In the Console, select Options from the Tools menu. The Options pane opens.

2. Select the Modules folder.

3. In the Modules pane, select Syslog, and select Configure.

4. Select the CounterACT device(s) defined as an rsyslog server in the Define Rsyslog Targets in FireEye EX section, and select OK. The Module Configuration window opens.

5. Select the Receive From tab.
6. If necessary, set the TCP Port to 514.

7. Select OK to save the configuration.

Create Custom FireEye EX Policies

Forescout platform policies are powerful tools used for automated endpoint access control and management.

**Policies and Rules, Conditions and Actions**

Forescout platform policies contain a series of rules. Each rule includes:

- Conditions based on host property values. The Forescout platform detects endpoints with property values that match the conditions of the rule. Several conditions based on different properties can be combined using Boolean logic.

- Actions can be applied to endpoints that match the conditions of the rule.

In addition to the bundled Forescout platform properties and actions available for detecting and handling endpoints, you can use the *Scan and RemEDIATE Known IOCS* action and *Advanced Threat Detection* properties to create custom policies that:

- Scan potentially compromised Windows endpoints for IOCs reported by Forescout eyeExtend for FireEye EX.

- RemEDIATE infected endpoints.

These items are available when you install the IOC Scanner Plugin.
To create a custom policy:

1. In the Console, select **Policy**. The Policy Manager opens.
2. Select **Add** to create a policy or select **Help** for more information about working with policies.

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 Technical Documentation Page, and 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 Support Portal](#)

Software downloads are also available from these portals.

To identify your licensing mode:

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

Forescout Technical Documentation Page

The Forescout Technical Documentation Page provides access to a searchable, web-based Documentation Portal as well as PDF links to the full range of technical documentation.

To access the Technical Documentation Page:

- Go to [https://www.Forescout.com/company/technical-documentation/](https://www.Forescout.com/company/technical-documentation/)

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:

Customer Support Portal

The Downloads page on the Forescout Customer Support 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 Customer Support Portal:

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

Documentation Portal

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

To access the Documentation Portal:

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

Forescout Help Tools

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 Administration Guide from the Help menu.

Plugin Help Files

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

Documentation Portal

- Select Documentation Portal from the Help menu to access the Documentation Portal.