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 NX Integration** ................................................................. 4
  Use Cases ........................................................................................................... 4
  Additional FireEye NX Documentation .............................................................. 4

**About This Module** ....................................................................................... 5
  About Support for Dual Stack Environments ................................................... 6
  How It Works ..................................................................................................... 6
  What to Do ......................................................................................................... 7

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

**Forescout eyeExtend (Extended Module) Licensing Requirements** ................. 8
  Per-Appliance Licensing Mode ........................................................................ 8
  Flexx Licensing Mode .................................................................................... 9
  More License Information ............................................................................... 10
  FireEye NX Requirements ............................................................................... 10

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

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

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

**Configure FireEye NX** .................................................................................. 14

**Run the FireEye NX Policy Template** ............................................................ 16
  FireEye NX Threat Detection Policy Template ................................................. 16
  Run the Template ............................................................................................ 16

**Create Custom FireEye NX Policies** ............................................................... 20
  FireEye NX – Policy Properties ........................................................................ 21
  FireEye NX Threat Detections .......................................................................... 21

**Display Asset Inventory Data** ......................................................................... 22

**Best Practices for Working with FireEye NX Event Notifications** ................. 23
  Malware Callback ............................................................................................ 23
  Web Infection and Malware Object .................................................................... 24
  Domain Match and Infection Match .................................................................. 24

**Additional Forescout Documentation** ........................................................... 25
  Documentation Downloads ............................................................................... 25
  Documentation Portal ....................................................................................... 26
  Forescout Help Tools ....................................................................................... 26
About the FireEye NX Integration

The Forescout platform integrates with FireEye® NX to help corporate security teams simplify the process of identifying, analyzing and blocking advanced cyber-attacks that threaten network security. This integration combines the threat detection mechanisms of FireEye NX 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. Forescout eyeExtend for FireEye NX enables the Forescout platform and FireEye NX to work together to quickly detect advanced threats and indicators of compromise (IOCs), contain infected endpoints, and disrupt the cyber kill chain preventing further lateral threat propagation and data exfiltration. The core of the FireEye NX platform is a virtual execution engine, complemented by dynamic threat intelligence that enables the security team to prevent, detect, analyze and respond to today's advanced attacks.

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.

- Receive alerts from FireEye NX of threats detected and immediately perform restrictive actions on the endpoints on which they were detected.
- Scan all Windows endpoints for IOCs reported to the Forescout platform by FireEye NX in order to identify potential threats and perform actions on potentially infected endpoints. For example, use Forescout platform policies to run policy actions 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 NX Documentation

Refer to FireEye NX online documentation for more information about the FireEye NX solution:

- NX Series Threat Management Guide
- NX Series System Administration Guide

About This Module

This module, together with the IOC Scanner Module, lets you integrate the Forescout platform with FireEye NX series so that you can:

- Use the FireEye NX Threat Detection Policy Template to create policies that immediately run actions, such as restrictive actions, on endpoints on which FireEye NX detected a Critical or High severity threat.

- Create Custom FireEye NX Policies that use FireEye NX – Policy Properties alongside bundled Forescout platform properties and actions to deal with issues not covered in the FireEye NX Threat Detection policy template.

- View new threats reported by FireEye NX and automatically added to the IOC repository. The repository is a viewable table of all threats received from Forescout eyeExtend for FireEye NX, and is available in the IOC Scanner Plugin. Refer to the Forescout Core Extensions Module: IOC Scanner Plugin Configuration Guide for more information.

- Use the Scan and RemEDIATE Known IOCs action to scan potentially compromised Windows endpoints for the same indicators of compromise (IOCs) reported by Forescout eyeExtend for FireEye NX to the IOC repository. For example, you can use the action to:
  - Scan all, or a subset of, Windows endpoints for IOCs used during a threat infection phase.
  - Trigger a threat remediation action to kill initiated processes.

This action is provided by the IOC Scanner Plugin. Refer to the Forescout Core Extensions Module: IOC Scanner Plugin Configuration Guide for more information.
Create policies that detect and remediate all Windows endpoints on which the Forescout platform detected specific IOCs reported by Forescout eyeExtend for FireEye NX. The Forescout platform provides Advanced Threat Detection properties and policy templates to help you work with the IOCs in the IOC repository. Refer to the Forescout Core Extensions Module: IOC Scanner Plugin Configuration Guide for more information.

Use Asset Inventory tools to display all threats reported by FireEye NX and the endpoints for which FireEye NX reported them. For example, identify multiple endpoints detected with the same threat and analyze any shared endpoint characteristics that may be useful for determining how to handle the endpoints.

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.

To use the module, you should have a solid understanding of FireEye NX concepts, functionality and terminology, and understand how Forescout platform policies and other basic features work.

How It Works

When a threat is detected, the FireEye NX server sends an alert with the threat details to a pre-defined receiving CounterACT® device. The alert includes:

- source/destination IP address
- 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 NX 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, and resolves the data as Forescout platform properties associated with the endpoint on which the threat was discovered, as well as properties on other Windows endpoints. These properties can be used to trigger policy actions.

The IOC repository includes all the IOCs identified by Advanced Threat Detection systems throughout a threat's lifecycle. The Forescout platform can use this information to detect the same threat on other endpoints. For example, the Forescout platform can scan endpoints not monitored by FireEye NX, detect IOCs used during a threat infection phase, and trigger a threat remediation action.

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. Verify that you have met system requirements. See Requirements.
2. Install the Module.
3. Configure the Module.
4. Configure the Forescout Syslog.
5. Configure FireEye NX.
6. Run the FireEye NX Policy Template (optional).
7. Create Custom FireEye NX Policies (optional).

Requirements

This section describes system requirements, including:

- Forescout Requirements
- Forescout eyeExtend (Extended Module) Licensing Requirements
- FireEye NX Requirements

Forescout Requirements

The module requires the following Forescout releases and other components:

- Forescout version 8.0, 8.1, or 8.2
- A module license for Forescout eyeExtend for FireEye NX
- Core Extensions Module version 1.0, 1.1, or 1.2 with the following components:
  - Syslog Plugin
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 NX Requirements**

The module requires the following FireEye NX components:

- FireEye Network Security (NX) Series
- Admin or Operator access to the NX Series appliance
- 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.

**Install the Module**

This section describes how to install the module. Before you install this module, first install the IOC Scanner Plugin, delivered with the Core Extensions Module.

**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 NX 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 Modules pane, select FireEye NX, and select Configure.
4. Select **Add** to define a FireEye NX server to communicate with the Forescout platform.

   *FireEye EX series servers need to be configured separately in Forescout eyeExtend for FireEye NX.*

5. Enter the following information:
   - **IP Address.** The IP address of the FireEye NX server configured to send rsyslog notifications to the Forescout platform. See [Configure FireEye NX](#) for details.
   - **Description.** A textual description of the FireEye NX server.

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

   There are two additional display-only fields in the FireEye NX pane:
   - **Last Threat Report Time.** Indicates the latest date and time when the Forescout platform received a threat notification from the listed FireEye NX server.
   - **Receiving CounterACT Device.** The IP address of the CounterACT device that received the latest threat notification from the listed FireEye NX server. Receiving CounterACT devices must be defined to FireEye as rsyslog servers. See [Configure FireEye NX](#) for details.

7. In the FireEye NX pane, select **Apply**.

8. Select **Yes** to save the module configuration.
Configure the Forescout Syslog Plugin

Configure the Forescout Syslog Plugin to enable the receiving CounterACT device to connect to the FireEye NX 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 then select Configure.
4. Select the CounterACT device you defined as a Syslog server in the Configure FireEye NX section, and then select OK. The Syslog Plugin Configuration window opens.
5. Select the Receive From tab.
6. In the 1st Syslog Source section, set the Source Type field to **NTSyslog security log**, and enter the IP address of the FireEye NX server.

7. Set the TCP Port to **514**.

8. Select **OK** to save the configuration.

## Configure FireEye NX

For each FireEye NX server, designate which CounterACT device will receive the FireEye NX rsyslog notifications. In the FireEye Web UI, define the receiving CounterACT device as an rsyslog server that can receive FireEye rsyslog notifications, and configure the notification settings. Refer to the *NX Series Threat Management Guide* for more information about configuring event notifications.

* If your FireEye NX environment was configured for an earlier version of Forescout eyeExtend for FireEye NX, ensure that the settings match those described in this section.

### To define a receiving CounterACT device as an rsyslog server:

1. In the FireEye NX Web UI, select the Settings tab.

2. On the side bar, select **Notifications**.

3. Select the **rsyslog** column heading. The **Rsyslog Server Listing** options are displayed at the bottom.
4. In the **Name** field, enter a name for the new rsyslog server, and select **Add Rsyslog Server**. The server is added.

5. Select the **Enabled** option for the new rsyslog server. You can select the **Enable All** option to enable all listed servers to receive rsyslog notifications.

6. In the **IP Address** field of the new rsyslog server, enter the IP address of the receiving CounterACT device.

7. In the **Delivery** dropdown list, select the delivery frequency.

8. In the **Notification** dropdown list, select the event type or **All Events** to send rsyslog notifications to the Forescout platform when the specified events are detected.

9. In the **Format** dropdown list, select **JSON Extended**.

10. In the **Send as** dropdown list, select the severity classification for the rsyslog notification.

11. Leave the **Account** field blank. This field will be deprecated.

12. In the **Protocol** dropdown list, select **TCP**.

13. Select **Update** to save the new rsyslog server definition.
Run the FireEye NX Policy Template

This module provides the following policy template, which you can use to manage and restrict threats in a FireEye NX environment.

- FireEye NX Threat Detection Policy Template

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 of the Forescout Administration Guide.

FireEye NX Threat Detection Policy Template

Use this policy to identify the severity of each discovered threat reported by FireEye NX.

In addition, an optional action can be used to send a message to the Syslog server for threats of all severity levels and an optional restrictive action can be used to block the endpoint if the threat is Critical or High (indicating that the threat has a high probability of infection on the endpoint). These actions are disabled by default.

Run the Template

This section describes how to create a policy from the policy template.

To run the template:

1. Log in to the Console and select Policy.
2. Select Add from the Policy Manager. The Policy Wizard opens.
3. Expand the FireEye NX folder and select ATD Stage 1: FireEye NX Threat Detection.
4. Select **Next**.

**Name the Policy**

The Name pane lets you define a unique policy name and useful policy description. 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.

5. Define a unique name for the policy you are creating based on this template, and enter a description.
Naming Tips

- 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.

6. Select **Next**. Both the Scope pane and the IP Address Range dialog box open.

**Define Which Hosts Will Be Inspected - Policy Scope**

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**.

### Main Rule

The main rule of this policy identifies threats detected by FireEye NX scans.

10. Select **Next** to add sub-rules to the policy, or select **Finish** to create the policy.

### Sub-Rules

Hosts that match the Main Rule are included in the policy inspection. *Hosts that do not match this rule are not inspected for this policy.*

Sub-rules let you automatically follow up with hosts after initial detection and handling. Creating sub-rules lets you streamline separate detection and actions into one automated sequence.
Sub-rules are performed in order until a match is found. The sub-rule of this policy detects the severity of each threat. An optional action can be used to send a message to the Syslog server for threats of all severity levels and an optional restrictive action can be used to block the endpoint if the threat is Critical or High (indicating that the threat has a high probability of infection on the endpoint). These actions are disabled by default.

11. Select Finish to create the policy.

12. In the Console, select Apply to save the policy.

Create Custom FireEye NX Policies

Forescout platform policies are powerful tools used for automated endpoint access control and management. You may need to create a custom policy to deal with issues not covered in the FireEye NX policy template.

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 work with FireEye NX related properties to create the custom policies. These items are available when you install the module.
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 NX.
- 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.

**FireEye NX – Policy Properties**

This section describes the property that is available when you install Forescout eyeExtend for FireEye NX.

- **FireEye NX Threat Detections**

**FireEye NX Threat Detections**

Use the *FireEye NX Threat Detections* property in Forescout platform policies to detect threats reported by FireEye NX. For example, create a policy that detects if FireEye NX has detected a Critical severity threat, and trigger remediation when an endpoint meets this condition.

**To access FireEye NX properties:**

1. Go to the Properties tree from the Policy Conditions dialog box.
2. Expand the FireEye NX folder in the Properties tree, and select **FireEye NX Threat Detections**. The following information is available:
   - Threat Severity
– FireEye Event Type. See Best Practices for Working with FireEye NX Event Notifications for more information.
– Threat Name
– Threat File Name
– Threat File Hash
– Threat Hash Type
– Syslog Message (rsyslog notification)

Display Asset Inventory Data

Use the Asset Inventory to view a real-time display of threats detected by FireEye NX.

The Asset Inventory lets you:

- Broaden your view of the organizational network from device-specific to activity-specific.
- View endpoints that have been detected with specific threats. For example, identify multiple endpoints detected with the same threat and analyze any shared endpoint characteristics that may be useful for determining how to handle the endpoints.
- Incorporate inventory detections into policies.

To access the Asset Inventory:

1. Select the Asset Inventory icon from the Console toolbar.
2. Go to FireEye NX Threat Detections.

The following information, based on the FireEye NX Threat Detections property, is available:

– FireEye Event Type
– Threat Name
– Threat File Name
– Threat File Hash
– Threat Hash Type
– Threat Severity
– Last Update

Refer to Working in the Console>Working with Inventory Detections in the Forescout Administration Guide or the Console Online Help for information about working with the Asset Inventory.
Best Practices for Working with FireEye NX Event Notifications

Event notifications inform you when specific events occur, alerting you of potential threats so that you can protect the security of your network.

This section describes best practices that help you:

- Analyze the threat severity of FireEye NX event notifications received by the Forescout platform.
- Decide how to respond to these notifications using Forescout platform policies.

There are five event notification categories, listed according to the typical threat severity associated with the event:

- **Malware Callback**
  - Critical Severity
- **Web Infection and Malware Object**
  - High Severity
- **Domain Match and Infection Match**
  - Low and Medium Severity

These notifications are detected by the Forescout platform as FireEye Event Type criteria via the FireEye NX Threat Detections property.

The FireEye NX Threat Detection Policy Template provided by the module searches for Malware Callback event types since these have the highest probability of infection. You can create custom FireEye NX policies that search for other event types. See Create Custom FireEye NX Policies.

Malware Callback

A malware callback notification on an endpoint indicates that there is an established connection between the infected endpoint and a command and control (CnC) server. This event is typically categorized by the Forescout platform with a threat severity of Critical.

If you identify one or more malware callback notification on an endpoint that also received a web infection notification (see Web Infection and Malware Object), there is a very high probability that the endpoint is infected.

At this point, FireEye recommends immediately patching or otherwise remediating the infected system, as well as preventing the CnC server from communicating with all endpoints in your network.

**Respond Using Forescout Platform Policies**

- Create a policy to automatically trigger restrictive actions (Switch Block, Assign to VLAN or Virtual Firewall) on the potentially infected endpoint.
• If you have other Forescout modules installed in your environment, various orchestration actions may be available to trigger vulnerability scanning or patch management.

• In addition, the IOC Scanner Plugin lets you monitor communications to the CnC server across all endpoints in your network. Refer to the Forescout Core Extensions Module: IOC Scanner Plugin Configuration Guide for more information.

Web Infection and Malware Object

A web infection notification on an endpoint indicates that a web browser initiated an outbound connection to a website that was ultimately determined to be malicious. These attacks usually penetrate the firewall and other perimeter security devices.

A malware object notification indicates the presence of a file attachment with a malicious executable payload. Both of these events are typically categorized as High severity threats.

FireEye recommends confirming the infection by scanning the endpoint to verify that the IOC found matches that of the endpoint. Viewing the IOC details associated with a web infection or malware object event shows registry changes, file system changes, and processes that have been started as a result of the infection. If suspicious changes in the FireEye analysis match changes on the actual endpoint, then the infection can be confirmed.

Respond Using Forescout Platform Policies

• Create a custom policy that scans the potentially infected endpoint (Scan and RemEDIATE Known IOCs action) when such a notification is received (IOCs Detected by CounterACT condition). Refer to the Forescout Core Extensions Module: IOC Scanner Plugin Configuration Guide for more information.

• In addition, you can create a policy to automatically trigger restrictive actions (Switch Block, Assign to VLAN or Virtual Firewall) on the potentially infected endpoint when such a notification is received.

Domain Match and Infection Match

A domain match notification indicates that the website domain has been identified as the source of malicious behavior. An infection match notification refers to the process of identifying a URL pointing to the initial web infection. Both of these events are typically categorized as Low or Medium severity threats.

Respond Using Forescout Platform Policies

• When these types of notifications are received on their own, they likely do not represent an infection. It is recommended to avoid running policies that automatically trigger restrictive actions.

• When these types of notifications are received alongside other, higher risk notifications listed above, follow the best practices listed for each notification type.
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/

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 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.