

# ForeScout<sup>®</sup> Extended Module for FireEye<sup>®</sup> NX

# **Configuration Guide**

Version 2.1



### **Table of Contents**

About the FireEye NX Integration	3
Use Cases	. 3
Additional FireEye NX Documentation	. 3
About This Module	4
About Support for Dual Stack Environments	.5
How It Works	.5
What to Do	.6
Requirements	6
CounterACT Software Requirements	.6
ForeScout Extended Module License Requirements	7
Per-Appliance Licensing Mode	.7
Centralized Licensing Mode	.8
More License Information	.9
FireEye NX Requirements	.9
Install the Module	9
Configure the Module 1	1
Configure the CounterACT Syslog Module 1	2
Configure FireEye NX 1	4
Run the FireEye NX Policy Template1	5
FireEye NX Threat Detection Policy Template1	5
Run the Template1	5
Create Custom FireEye NX Policies 1	9
FireEye NX – Policy Properties2	20
FireEye NX Threat Detections2	20
Display Asset Inventory Data 2	21
Best Practices for Working with FireEye NX Event Notifications	22
Malware Callback	22
Web Infection and Malware Object2	23
Domain Match and Infection Match2	23
Additional CounterACT Documentation 2	24
Documentation Downloads2	24
Documentation Portal	24
CounterACI Help Iools2	25

### About the FireEye NX Integration

ForeScout CounterACT<sup>®</sup> integrates with the FireEye NX Module to help 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 CounterACT to multiply the benefits of working with an Advanced Threat Detection (ATD) product.

The FireEye NX Module enables ForeScout CounterACT 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 allows 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 <u>About This Module</u>.

- 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 CounterACT by FireEye NX in order to identify potential threats and perform actions on potentially infected endpoints. For example, use CounterACT 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 *CounterACT 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

https://www.fireeye.com/products/nx-network-security-products.html

### **About This Module**

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

- Use the <u>FireEye NX Threat Detection Policy Template</u> to create policies that immediately run actions, such as restrictive actions, on endpoints on which FireEye NX detected a Critical or High severity threat.
- <u>Create Custom FireEye NX Policies</u> that use <u>FireEye NX Policy Properties</u> alongside bundled CounterACT 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 the FireEye NX Module, and is available in the IOC Scanner Module. Refer to the CounterACT IOC Scanner Plugin Configuration Guide for more information.

IOC Repository	Threat Exceptio	ns							
vlanage the centraliz	ed IOC repository	r of threats that were	reported to Counte	rACT by Advanced	Threat Detection (ATD)	systems or th	at were added manu	ally.	
Search		Q							
Date Reported	Reported By	Threat Name	File Name	File Size (bytes)	File Hash	Hash Type	Threat Severity 👻	Operating System	Add
/2/17 11:01:20 AM	FireEye NX	Trojan Kelhos	newbos2.exe	767,488	e4d009c290d0051ca.	MD6	High	100	<u>E</u> dit
/2/17 11:05:11 AM	FireEye NX	Trojan Kelhos	newbos2.exe	767,488	#400002900005ca.	MD6	High	181	<u>R</u> emov
/2/17 11:07:00 AM	FireEye NX	Malaware.archive	newbos2.exe.zip	1	e40000c2900%%*ca.	MD6	High	181	10 <u>C</u> s
/2/17 11:08:00 AM	FireEye NX	Virus Parite.MVX	nc—15-49.exe	176,128	e40008(29000010a.	MD6	High	181	
/2/17 11:09:24 AM	FireEye NX	Virus Parite.MVX	nc—15-49.exe	176,128	e40909(2910001ca.	MD6	High	181	
/2/17 12:27:14 PM	FireEye NX	Test.Backdoor	bad.txt	1	aths	-None-	Critical	181	
6 items (0 selected)									

- Use the Scan and Remediate Known IOCs action to scan potentially compromised Windows endpoints for the same indicators of compromise (IOCs) reported by the FireEye NX Module 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 Module. Refer to the *CounterACT IOC Scanner Plugin Configuration Guide* for more information.

 Create policies that detect and remediate all Windows endpoints on which CounterACT detected specific IOCs reported by the FireEye NX Module. CounterACT provides Advanced Threat Detection properties and policy templates to help you work with the IOCs in the IOC repository. Refer to the *CounterACT IOC Scanner Plugin Configuration Guide* for more information.

 Use CounterACT 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

CounterACT version 8.0 detects endpoints and interacts with network devices based on both IPv4 and IPv6 addresses. However, **IPv6 addresses are not yet supported by this component.** 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 component.

To use the module, you should have a solid understanding of FireEye NX concepts, functionality and terminology, and understand how CounterACT 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. CounterACT 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

CounterACT adds the data to its IOC repository, and resolves the data as CounterACT 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. CounterACT can use this information to detect the same threat on other endpoints. For example, CounterACT 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 CounterACT 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. <u>Configure the Module</u>.
- 4. <u>Configure the CounterACT Syslog Module</u>.
- 5. <u>Configure FireEye NX</u>.
- 6. <u>Run the FireEye NX Policy Template</u> (optional).
- 7. <u>Create Custom FireEye NX Policies</u> (optional).

### Requirements

This section describes system requirements, including:

- <u>CounterACT Software Requirements</u>
- ForeScout Extended Module License Requirements
- <u>FireEye NX Requirements</u>

CounterACT continuously supports newly released FireEye NX versions. Refer to the Release Notes for the most updated list:

https://updates.forescout.com/support/files/plugins/fireeye/2.0.0/2.0.0-20000062/RN.pdf

### **CounterACT Software Requirements**

The module requires the following CounterACT releases and other CounterACT components:

- CounterACT version 8.0
- A module license for the FireEye NX Module
- An active Maintenance Contract for the licensed module is required
- Core Extensions Module version 1,0 or above with the following components:
  - Syslog Plugin
  - IOC Scanner Plugin

– DNS Query Extension Plugin

# 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:

- <u>Per-Appliance Licensing Mode</u>
- <u>Centralized Licensing Mode</u>

#### 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.

Options			
Search VPN Search Search VPN Search Sear	Q	Licenses Activate, update or deactivate your license for CounterACT features and Exter Search Q	nded Module
> III NAC		Name A Status	Туре
E Licenses		ForeScout CounterACT See Valid, Capacity exceeded	Perpetual
🖆 Lists		ForeScout CounterACT Control Valid, Capacity exceeded	Perpetual
> 🐺 Map		ForeScout CounterACT Resiliency Valid	Perpetual
X Internal Network		ForeScout Extended Module for Check Point Next Valid, Capacity exceeded	Perpetual

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.

<ul> <li>Example Module License Request - Step 3 of 4</li> <li>Example Module License Request</li> </ul>									
Company Type Devices Request Format	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.

View	/S	
Sear	ch	Q
⊘ All I	Hosts (181)	
> 📳 F	Policies	
> 🏦 F	History	

### **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 <u>ForeScout Customer Portal</u>. 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. The 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 <u>license@forescout.com</u> for more information.

### **FireEye NX Requirements**

The module requires the following FireEye NX components:

- FireEye Network Security (NX) Series version 7.5.3 through 8.1
- Admin or Operator access to the NX Series appliance

### 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
  - <u>Customer Portal, Downloads Page</u> Centralized Licensing Mode

To find out which licensing mode your deployment is working with, see <u>Identifying Your Licensing Mode in the Console</u>.

- 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.

Options					
Search	Q	Licenses			
The second secon		Activate, update or deactivate your lice	nse for Coun	terACT features and Extend	led Module
> 📀 General			0		
Ø Discovery		Search	Q		
> 📳 NAC		Name 🔺		Status	Туре
🔚 Licenses		ForeScout CounterACT See		Valid, Capacity exceeded	Perpetual
Lists		ForeScout CounterACT Control		Valid, Capacity exceeded	Perpetual
> 🥊 Map		ForeScout CounterACT Resiliency		Valid	Perpetual
K Internal Network		ForeScout Extended Module for Check	k Point Next	Valid, Capacity exceeded	Perpetual

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

### **Configure the Module**

Configure the module to ensure that CounterACT can communicate with the FireEye NX service.

#### To configure the module:

- 1. In the CounterACT Console, select **Options** from the **Tools** menu. The Options dialog box opens.
- 2. Navigate to and select the Modules folder.
- **3.** In the **Modules** pane, select **FireEye NX**, and select **Configure**. The FireEye NX pane opens.

CounterACT Options		
Options		
Search Q	FireEye NX	
> 😁 CounterACT Devices	- Define FireEye NX servers that share detected threat information with CounterACT. The reported threats and their IOCs are added to the C	ounterACT IOC
> 🜉 Plugins	repository.	
😫 Channels		
👌 FireEye NX	Search Q	
💫 FireEye HX	FireEye NX Se A Description Last Threat Repor Receiving CounterACT Device	Add
😳 Bromium		⊑dit
흤 Cloud Networking		Remove
O ServiceNow		
🕞 Tanium		
SCAP		
hicrosoft SMS/SCCM		
Advanced Tools Plugin	No items to display	
🐨 IOC Scanner		
🖁 Symantec Endpoint Protecti	Ap	ply Undo

- **4.** Select **Add** to define a FireEye NX server to communicate with CounterACT. The Add FireEye NX Server dialog box opens.
  - FireEye EX series servers need to be configured separately in the CounterACT FireEye EX Module.

📀 Add FireEye	NX Server		<b>—</b>
IP Address			
Description			
		ОК	Cancel

- **5.** Enter the following information:
  - *IP Address*. The IP address of the FireEye NX server configured to send rsyslog notifications to CounterACT. See <u>Configure FireEye NX</u> 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 CounterACT 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 <u>Configure FireEye NX</u> for details.
- **7.** In the FireEye NX pane, select **Apply**. A CounterACT Enterprise Manager Console dialog box opens.



8. Select Yes to save the module configuration.

# **Configure the CounterACT Syslog Module**

Configure the CounterACT Syslog Module to enable the receiving CounterACT device to connect to the FireEye NX server and receive notifications.

See the *CounterACT Syslog Plugin Configuration Guide* for more information about the Syslog Module configuration.

#### To configure the Syslog Module:

- 1. In the CounterACT Console, select **Options** from the **Tools** menu. The Options dialog box opens.
- 2. Navigate to and select the Modules folder.
- **3.** In the **Modules** pane, select **Syslog**, and select **Configure**. The Select Appliances dialog box opens.

Options				
Search Q	Modules			
<ul> <li>CounterACT Devices</li> <li>IP Assignment and Failover</li> <li>Failover Status</li> </ul>	Modules extend CounterACT's capabili more. Some modules, such as Base Modules New and updated Base Modules, Exter	ties by enabling i , contain plugins ided Modules an	ntegration with other tools, allowing deeper inspection, ad that provide added functionality. d Content Modules are available from the product downloo	ditional enforcement actions a ads portal.
🖌 🜉 Modules	U DNS Enforce	Base	Select Appliances	Rollb
Flow Analyzer	DNS Query Extension	Base		Konp
📑 Channels	Device Classification Engine	Base		<u>S</u> ta
	External Classifier	Base	Appliances	Sto
	Flow Analyzer	Base	✓ △ ■ All Segments	Applia
	DIOC Scanner	Base		Config
Auvanceu compliance	IoT Posture Assessment Eng	inBase		Tes
ServiceNow	NBT Scanner	Base		
Microsoft SMS/SCCM	0 NetFlow	Base	Enterprise Manager	Hei
😳 Advanced Tools Plugin	Benorts	Base		Abo
🔡 IoT Posture Assessment En	Cuclos	Paca		
💚 IOC Scanner	- Jysing	Lase		
💿 IBM BigFix	Technical Support	Base		
AWS	🕐 Web GUI	Base	OK Cancel	

- Select the CounterACT device you defined as a Syslog server in the <u>Configure</u> <u>FireEye NX</u> section, and then select **OK**. The Syslog Plugin Configuration window opens.
- 5. Select the *Receive from* tab.

📀 Syslog@ P	lugin Configuration
	Send Events To Syslog Triggers Default Action Configuration Receive From
	1st Syslog Source
	Source Type   <select type=""> //</select>
	IP Address
	2nd Syslog Source
	Source Type   <select type=""> //</select>
	IP Address
	3rd Syslog Source
	Source Type   <select type=""> //</select>
	IP Address
	Ports for Incoming Syslog Messages
	UDP Port 514 🗘
	TCP Port 514 🗘
	Use TLS
	OK Cancel
	OK Cancel

- 6. In the 1rst 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 the CounterACT FireEye Module, 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.

FireEye										
ashboard 🛕 Alerts 🗉 Summaries 😋 Filters 🖨 Settings 🖬 Reports 🕜 About										
Date and Time	Notifica	tion Sottings	Coloct a pr	atocol tura	n holow to r	dienlav an	d odit ite na	ramotore		
User Accounts	Nounca	uon setungs, e	select a pit	nocor typ	e Delow 10 (	nopiay and	reun no pai			
Email			Protocol	email	http	rsyslog	snmp	Rsyslog Settings		
DTI Network	Event 1	ype	Global	✓	$\checkmark$	$\checkmark$		Default format: JSON Extended		
CMS Network			_		-	_		Default delivery: 1 Min per source		
Inline Operational Modes	Domain Match			$\checkmark$	$\checkmark$			Apply Settings		
Inline Policy Exceptions	Tafaatia	- Matab								
Inline Whitelists	Infectio	n Match			•					
Notifications	Malware	e Callback	$\checkmark$	~	$\checkmark$	$\checkmark$	$\checkmark$			
Network										
YARA Rules	Malware	e Object	$\checkmark$	✓	$\checkmark$	$\checkmark$	$\checkmark$			
Guest Images										
Certificates/Keys	Web Inf	ection		•	~	•				
Appliance Backup & Restore	Rsyslog	Server Listing	Add Rsy	slog Serve	er: Name:		Ad	dd Rsyslog Server		
Appliance Licenses	Remove	Name	Enabled	IF	Address		Delivery	Notification Format Send as		
Login Banner		CounterACT_EN	· 🗸	1	0.11.5.11		1 Min per so	ource 🗸 All Events 🔽 JSON Extended 🗸 Default		
				7 [	Account	Pr T	otocol CP 🔽			

- 4. In the Name box, enter a name for the new rsyslog server, and select Add Rsyslog Server. The server is added.
- Select the Enabled checkbox for the new rsyslog server. You can select the Enable All checkbox to enable all listed servers to receive rsyslog notifications.
- 6. In the **IP Address** box 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 CounterACT 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** box blank. This option 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.

- <u>FireEye NX Threat Detection Policy Template</u>
- It is recommended that you have a basic understanding of CounterACT policies before working with the templates. See the CounterACT Templates and Policy Management chapters of the CounterACT 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 CounterACT Console and select the Policy tab.
- 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**. The FireEye NX Threat Detection pane opens.



4. Select Next. The Name pane opens.

#### Name the Policy

The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

**1.** Define a unique name for the policy you are creating based on this template, and enter a description.

📀 Policy - Wizard - Step	o 2 of 5					×
✓ Policy Type I Name Scope Main Rule	<b>Name</b> Enter a nar	ne and desc	ription for th	e policy.		
Sub-Rules	Name Description	ATD Stage	1: FireEye	NX Threat Det	ection	
	<u>H</u> el	p Pre	evio <u>u</u> s	Next	<u>F</u> inish	Cancel

#### 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.
- 2. Select Next. The Scope pane and IP Address Range dialog box opens.

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

**3.** Use The IP Address Range dialog box to define which endpoints are inspected.

IP Address Range		×
<ul> <li>Segment</li> </ul>		~
O Unknown IP addresses		
	ОК	Cancel

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 page.
- Unknown IP addresses: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

Not applicable for this policy template.

- Filter the range by including only certain CounterACT groups and/or by excluding certain endpoints or users or groups when using this policy.
- 4. Select **OK**. The added range appears in the Scope pane.
- 5. Select Next. The Main Rule pane opens.

#### Main Rule

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

	Main Rule		
<ul> <li>Policy Type</li> <li>Name</li> <li>Scope</li> <li>Main Rule</li> <li>Sub-Rules</li> </ul>	Use this screen to review policy sub-rule definitions. Hosts are inspected by each sub-rule in the order shown. \ defined is applied. If no match is found, the host is inspecte	When a match is found, the d against the next sub-rule	action 9.
	Condition		
	A host matches this rule if it meets the following condition:		
	All criteria are True 🗸 🗸		80
	Criteria		Add
	FireEye NX Threat Detections - Threat Name: Any Value Wit	hin the last 1 week	Edit
			<u>R</u> emove
	Actions Actions are applied to hosts matching the above condition.		
	Enable Action	Details	Add
			<u>E</u> dit
	No items to display		Bomoula

6. 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 allow you to 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.

Sub-Rules					
Use this screen to review policy sub-rule definitions. Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.					
auc	Name	Conditions	Actio	Add	
1	FireEye NX Threat Detections - Critical	FireEye NX Threat Det.		<u>E</u> dit	
2	FireEye NX Threat Detections - High	FireEye NX Threat Det.		<u>R</u> emove	
3	FireEye NX Threat Detections - Medium	FireEye NX Threat Det.	. <u>1</u> 00	<u>D</u> uplicate	
4	FireEye NX Threat Detections - Low	FireEye NX Threat Det.	. jug	Up	
				D <u>o</u> wn	
	<u>H</u> elp Pre	evio <u>u</u> s Next	Finish	Cancel	

- 7. Select Finish to create the policy.
- 8. On the CounterACT Console, select **Apply** to save the policy.

# **Create Custom FireEye NX Policies**

CounterACT 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

CounterACT policies contain a series of rules. Each rule includes:

- Conditions based on host property values. CounterACT 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 CounterACT 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 CounterACT 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 the FireEye NX Module.
- Remediate infected endpoints.

These items are available when you install the IOC Scanner Module.

#### To create a custom policy:

- 1. In the CounterACT Console, select the **Policy** tab. 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 the FireEye NX Module.

<u>FireEye NX Threat Detections</u>

### **FireEye NX Threat Detections**

Use the *FireEye NX Threat Detections* property in CounterACT 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.

📀 Condition		×
Search	FireEye NX Threat Detections: Indicates threats detected by FireEye NX scans.	
> 🐟 External Devices > 📸 FireEye HX ~ 🌛 FireEye NX	Threat Severity     Select values to match the threat severity.     Meets the following criteria     Does not meet the following criteria	
FireEye NX Threat Detection	18	
> 🚣 Guest Registration	Search Q	
> 🕋 Hardware	📀 Name 🔺	Select All
> <u> </u> IBM QRadar	Critical	<u>C</u> lear All
> 👌 Linux	High	
> 🗯 Macintosh	Medium	
> 🔲 MAR	Low	
> 🖾 McAfee ePO		
	Help	OK Cancel

#### To access FireEye NX properties:

**1.** Navigate 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 <u>Best Practices for Working with FireEye NX Event</u> <u>Notifications</u> for more information.
  - Threat Name
  - Threat File Name
  - Threat File Hash
  - Threat Hash Type
  - Syslog Message (rsyslog notification)

# **Display Asset Inventory Data**

Use the CounterACT 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. Navigate 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 *CounterACT Administration Guide* or the Console Online Help for information about working with the CounterACT 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 CounterACT.
- Decide how to respond to these notifications using CounterACT 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
- <u>Domain Match and Infection Match</u>
  - Low and Medium Severity

These notifications are detected by CounterACT as *FireEye Event Type* criteria via the <u>FireEye NX Threat Detections</u> property.

The <u>FireEye NX Threat Detection Policy Template</u> 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 <u>Create Custom FireEye NX Policies</u>.

### 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 CounterACT 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 <u>Web Infection and Malware Object</u>), 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 CounterACT 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 Module allows you to monitor communications to the CnC server across all endpoints in your network. Refer to the *CounterACT 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 CounterACT 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 CounterACT 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 CounterACT 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 CounterACT Documentation**

For information about other CounterACT features and modules, refer to the following resources:

- <u>Documentation Downloads</u>
- <u>Documentation Portal</u>
- <u>CounterACT Help Tools</u>

### **Documentation Downloads**

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- Per-Appliance Licensing Mode Product Updates Portal
- Centralized Licensing Mode Customer Portal
- Software downloads are also available from these portals.

To learn which licensing mode your deployment is using, see <u>Identifying Your</u> <u>Licensing Mode in the Console</u>.

#### Product Updates Portal

The Product Updates Portal provides links to CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. The portal also provides a variety of additional documentation.

#### To access the Product Updates Portal:

- 1. Go to <a href="https://updates.forescout.com/support/index.php?url=counteract">https://updates.forescout.com/support/index.php?url=counteract</a>.
- 2. Select the CounterACT version you want to discover.

#### **Customer Portal**

The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, 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. The Documentation page on the portal provides a variety of additional documentation.

#### To access documentation on the ForeScout Customer Portal:

- 1. Go to <a href="https://forescout.force.com/support/">https://forescout.force.com/support/</a>.
- 2. Select Downloads or Documentation.

### **Documentation Portal**

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

If your deployment is using Centralized Licensing Mode, you may not have credentials to access this portal.

#### To access the Documentation Portal:

- 1. Go to <u>www.forescout.com/docportal</u>.
- 2. Use your customer support credentials to log in.
- **3.** Select the CounterACT version you want to discover.

### **CounterACT Help Tools**

Access information directly from the CounterACT Console.

#### **Console Help Buttons**

Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with.

#### **CounterACT Administration Guide**

Select CounterACT Help from the Help menu.

#### **Plugin Help Files**

- 1. After the plugin is installed, select **Options** from the **Tools** menu and then select **Modules**.
- 2. Select the plugin and then select Help.

#### **Documentation Portal**

Select Documentation Portal from the Help menu.

#### 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.

Options					
Search	Q	Licenses Activate, update or deactivate your license for CounterACT features and Extended Module			
> 😧 General © Discovery		Search	Q		
> 🔢 NAC		Name 🔺		Status	Туре
🔚 Licenses		ForeScout CounterACT See		Valid, Capacity exceeded	Perpetual
🚹 Lists		ForeScout CounterACT Control		Valid, Capacity exceeded	Perpetual
> 🖶 Map		ForeScout CounterACT Resiliency		Valid	Perpetual
➢ Internal Network		ForeScout Extended Module for Check	c Point Next	Valid, Capacity exceeded	Perpetual

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

### Legal Notice

© 2018 ForeScout Technologies, Inc. All rights reserved. ForeScout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <u>https://www.forescout.com/company/legal/intellectual-property-patents-trademarks</u>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2018-04-10 09:21