FORESCOUT

Forescout

eyeExtend for Check Point Next Generation Firewall

Configuration Guide

Version 1.3

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

2020-02-25 15:14

Table of Contents

About the Check Point Next Generation Firewall Integration

The Forescout eyeExtend for Check Point® Next Generation Firewall (NGFW) integration significantly magnifies firewall power by leveraging network visibility, inspection, and enforcement capabilities provided by the Forescout platform.

The integration lets security teams:

- Enforce user-based and role-based access in real-time.
- Reduce dependency on the switch as the central access control tool.

To use the module, you should have a solid understanding of Check Point Next Generation Firewall concepts, functionality, and terminology, and understand how Forescout platform policies and other basic features work.

Use Cases

This section describes important use cases supported by Forescout eyeExtend for Check Point NGFW. To understand how this module helps you achieve these goals, see About This Module.

Segment Endpoints to Predefined Roles

Use the Forescout platform's powerful endpoint classification engine to segment endpoints to predefined roles.

Leverage Forescout as a Provider of User-ID for Endpoints

Receive real-time identity information by mapping detected IP addresses to user IDs to support granular filtering of users associated with those IP addresses. The Forescout platform-based IP-to-User-ID capabilities provide vital support in Check Point Role-Based Administration.

About This Module

Forescout eyeExtend for Check Point Next Generation Firewall lets you:

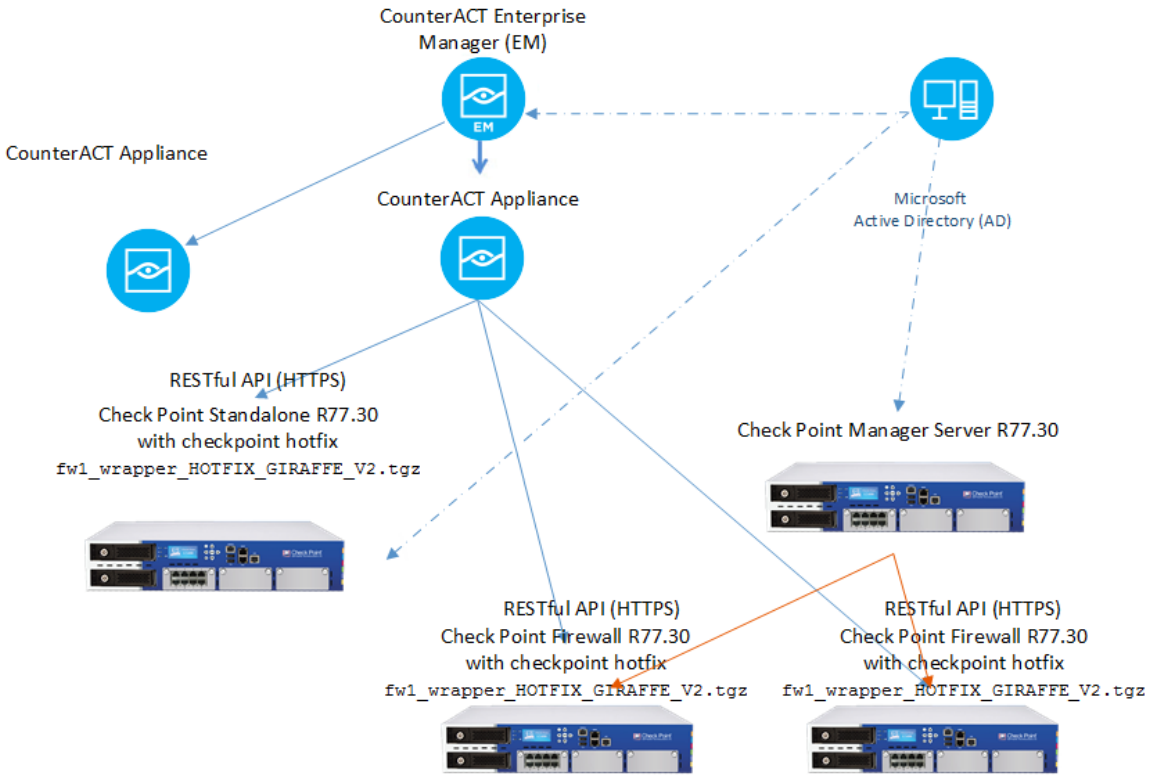
- ***Leverage the Forescout platform as a mission-critical real-time information source***
- ***Map endpoint IP addresses discovered by the Forescout platform to firewall User-IDs***. For example, the module can map the IP address of a user authenticating to a captive portal through a proxy. See Map IP to User-ID.
- ***Register endpoint IP to identity awareness access roles***

About Certification Compliance Mode

Forescout eyeExtend for eyeExtend for Check Point Next Generation Firewall supports Certification Compliance mode. For information about this mode, refer to the *Forescout Installation Guide*. See Additional Forescout Documentation for information on how to access this guide.

How It Works

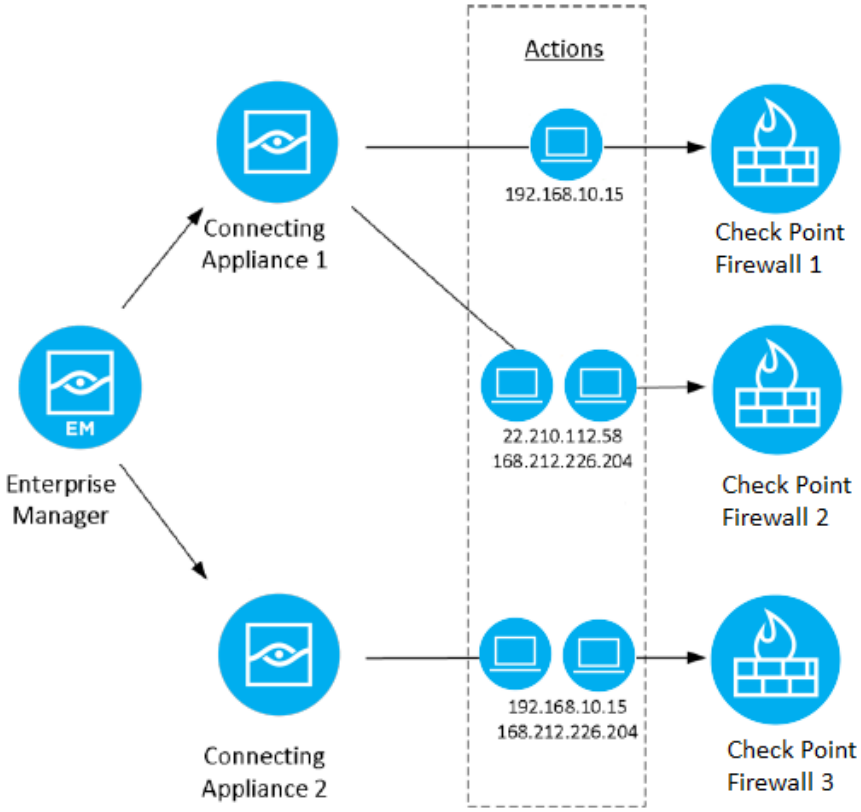
This section describes how the module communicates with Check Point firewalls.



Firewall Management

The module communicates with Check Point firewalls, supplying endpoint IP address information discovered by the Forescout platform using the Map IP to User-ID and Register to Access Role actions.

Each firewall is assigned to a connecting CounterACT® device with which it communicates. Multiple firewalls can be assigned to a single CounterACT device. The connecting CounterACT device then sends the action-related information to the relevant firewall.



What to Do

Perform the following steps to work with this module:

- Verify that requirements are met. See Requirements.
- Download and install the hotfix. See Install the Hotfix.
- Download and install the module. See Install the Module.
- Configure settings in Check Point Next Generation Firewall SmartDashboard. See Check Point Next Generation Firewall Setup.
- Configure the Map IP to User-ID and Register to Access Role actions. See Check Point Next Generation Firewall Policy Actions.

Requirements

This section describes system requirements, including:

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

- Check Point Next Generation Firewall Requirements

Forescout Requirements

The module requires the following Forescout releases and other components:

- Forescout version 8.2.
- A module license for Forescout eyeExtend for Check Point NGFW. See Forescout eyeExtend (Extended Module) Licensing Requirements.

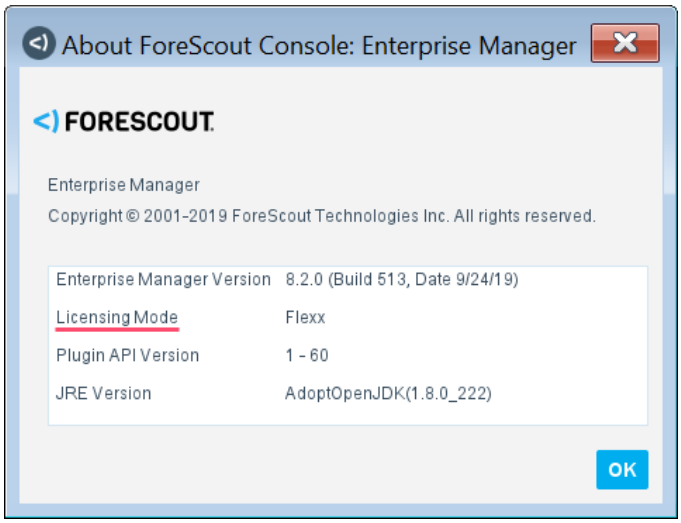
Forescout eyeExtend (Extended Module) Licensing Requirements

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.

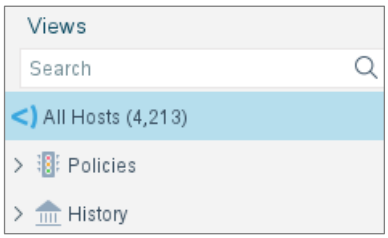
Requesting a License

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. T*he 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.

Check Point Next Generation Firewall Requirements

- Forescout eyeExtend for Check Point Next Generation Firewall supports Check Point Gateway in versions R77.20, R77.30 and R80.10.
- 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.

Deployment Modes

The module requires Check Point Firewall to be deployed in one of the following modes:

Check Point Gateway in version R80.10

- Installing the hotfix is not required. See Install the Module.

Check Point Gateway in version R77.20 or R77.30

- Identity Awareness (IDA) API requires you to Install the Hotfix.
  - R77.20: fw1 wrapper_HOTFIX_GOLLUM_HF_BASE_295.tgz
  - R77.30: fw1_wrapper_HOTFIX_GIRAFFE_V2.tgz
- Enable IDA on Check Point Gateway

Check Point Gateway in Cluster Mode

- Physical gateway
  - Check Point appliance
  - Open server
- Virtual appliance

Requirements Independent of the Management Platform

- Standalone management server (SmartCenter)
- Multi-Domain (Provider-1 with CMAs)

Install the Hotfix

Depending on the Check Point Firewall deployment mode, you may need to install the hotfix before you install the module.

Installing the hotfix is not required if you are using Check Point Gateway version R80.10.

To install the hotfix:

1. Obtain the hotfix installation file from Check Point:

   R77.20: fw1_wrapper_HOTFIX_GOLLUM_HF_BASE_295.tgz

   R77.30: fw1_wrapper_HOTFIX_GIRAFFE_V2.tgz
2. Upload the file to Check Point firewall directory: **/tmp/**
3. In Check Point expert mode, run the command:

   R77.20: tar xvzf fw1_wrapper_HOTFIX_GOLLUM_HF_BASE_295.tgz

   R77.30: tar xvzf fw1_wrapper_HOTFIX_GIRAFFE_V2.tgz
4. Install the hotfix using the command:

   R77.20: ./fw1_wrapper_HOTFIX_GOLLUM_HF_BASE_295_<build_number>

   R77.30: ./fw1_wrapper_HOTFIX_GIRAFFE_V2_<build_number>
5. Reboot Check Point gateway.

Enable IDA on Check Point Gateway

If your Check Point Gateway version is R80.10, see Install the Module.

By default, the IDA API is disabled; however, it can be configured using a hidden command line menu as follows:

1. Open an SSH connection to the gateway.
2. To change to expert mode, enter the command:

   `expert`
3. Enter the expert password.
4. To enable IDA API, run the command:

   `pdp api enable`

Additional commands include:

- To disable usage of the IDA API, use **`pdp api disable`**
- To show the current status of the IDA API, use **`pdp api status`**

Install the Module

This section describes how to install the module. Before you install this module, verify that the requirements have been met. See Requirements.

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.

Check Point Next Generation Firewall Setup

This section describes the configuration required on the Check Point SmartDashboard to:

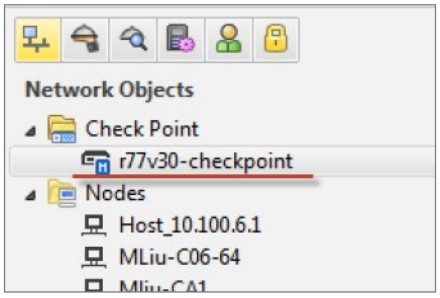
- Create an Access Role
- Set Up a Pre-shared Secret

Create an Access Role

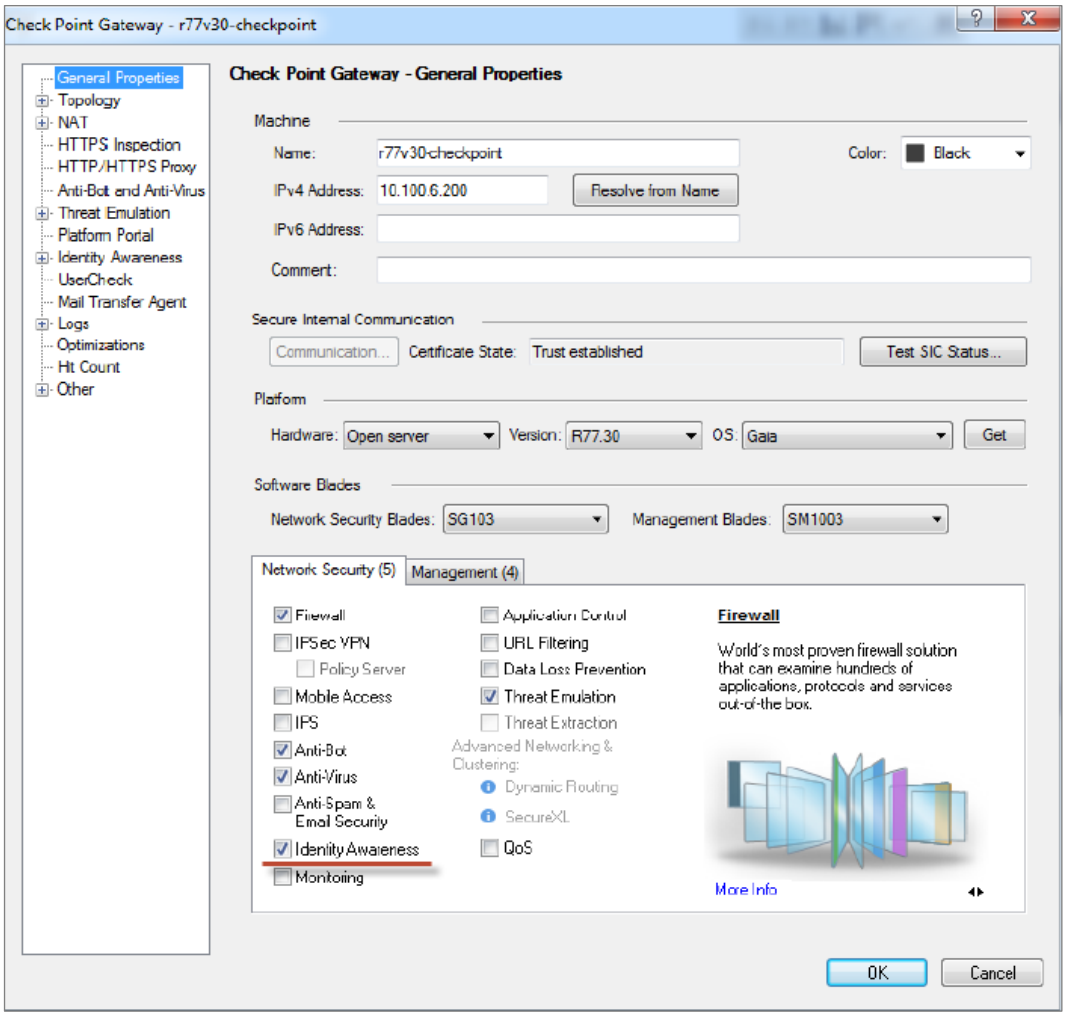
Use the Check Point SmartDashboard to access the Check Point Management Server and create an access role.

To create an access role:

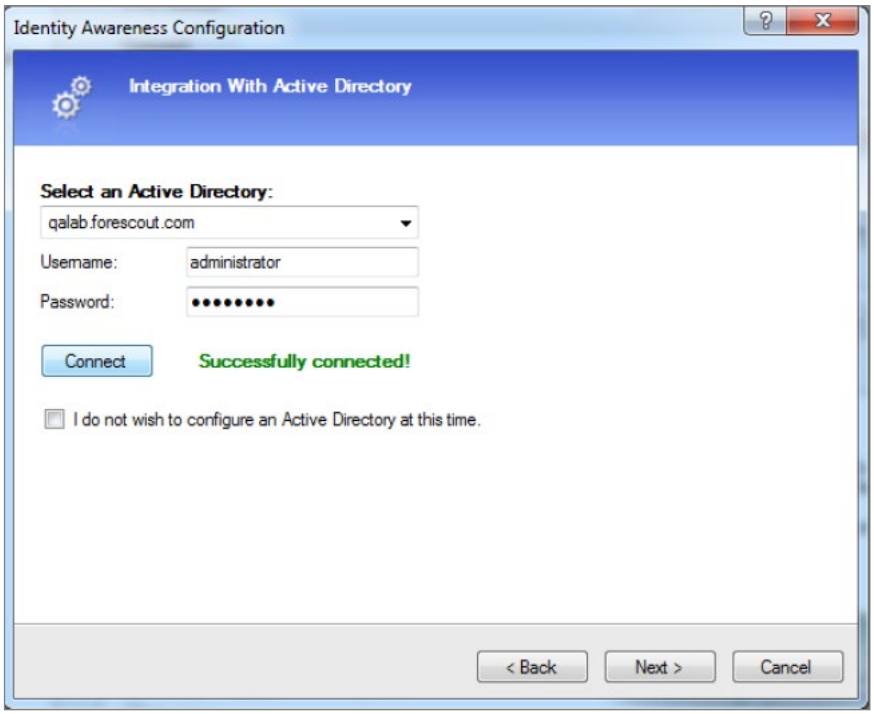
1. In the **Network Objects** pane, select the Check Point server to be configured.



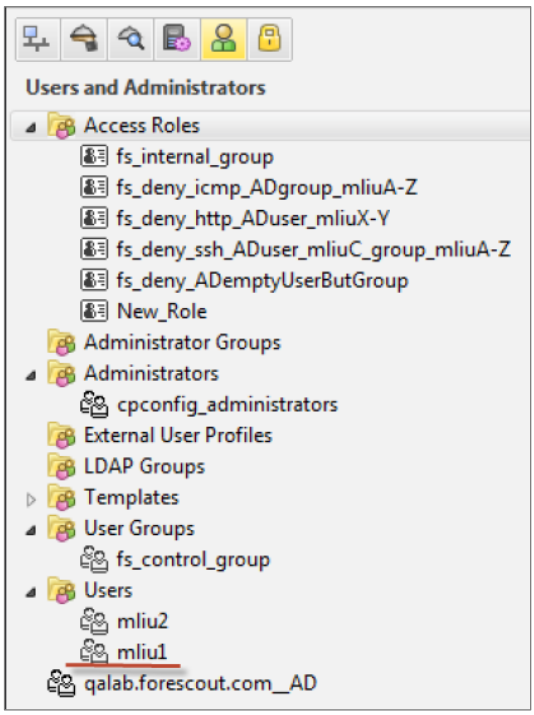
2. Select **General Properties**.



3. Select **Identity Awareness** and select **OK**.



4. In the Identity Awareness Configuration dialog box, configure Microsoft Active Directory as Browser Based Authentication.
   a. Select an Active Directory, for example, qalab.forescout.com.
   b. Enter the login credentials.
   c. Select **Connect** to make initial contact with the Active Directory.



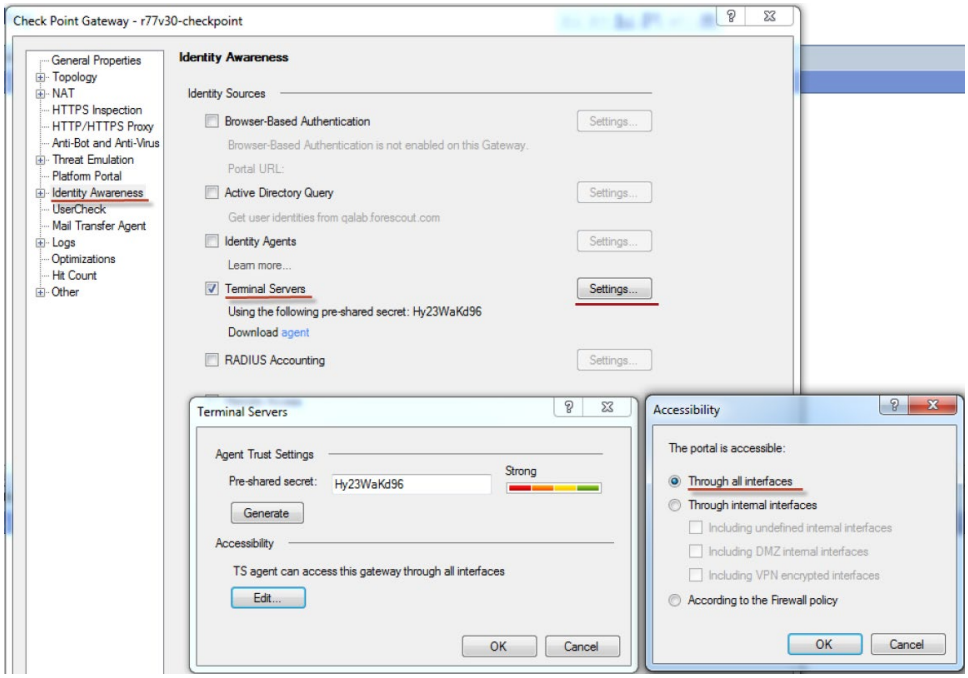
5. In the User and Administrators pane, create an access role based on Microsoft Active Directory data.
6. Select **Install policy** to enable the Identity Awareness feature. The policy is installed on the r77.30 Check Point gateway.

Set Up a Pre-shared Secret

Use the Check Point SmartDashboard to access the Check Point Management Server and set up a pre-shared secret.

To set up a pre-shared secret:

1. In the **General Properties** pane, select **Identity Awareness**.
2. Select the **Terminal Servers** checkbox and select **Settings**.
3. From the **Accessibility** menu, select **Through all interfaces**.



For more information, refer to *Configuring Identity Awareness* in the Check Point *Identity Awareness Administration Guide* for R77 or R80 available at: https://sc1.checkpoint.com/documents/R77/CP_R77_IdentityAwareness_WebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_IdentityAwareness_WebAdminGuide/62050

or

https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_IdentityAwareness_AdminGuide/html_frameset.htm?topic=documents/R80.10/WebAdminGuides/EN/CP_R80.10_IdentityAwareness_AdminGuide/62050

Configure the Module

After Forescout eyeExtend for Check Point NGFW is installed, configure the module to ensure that the Forescout platform can communicate with the Check Point service.

Before configuring the module, review the How It Works section.

Define each firewall server and its login credentials. See Configure Individual Firewalls. Once configured, CounterACT devices synchronize with and provide information to these servers.

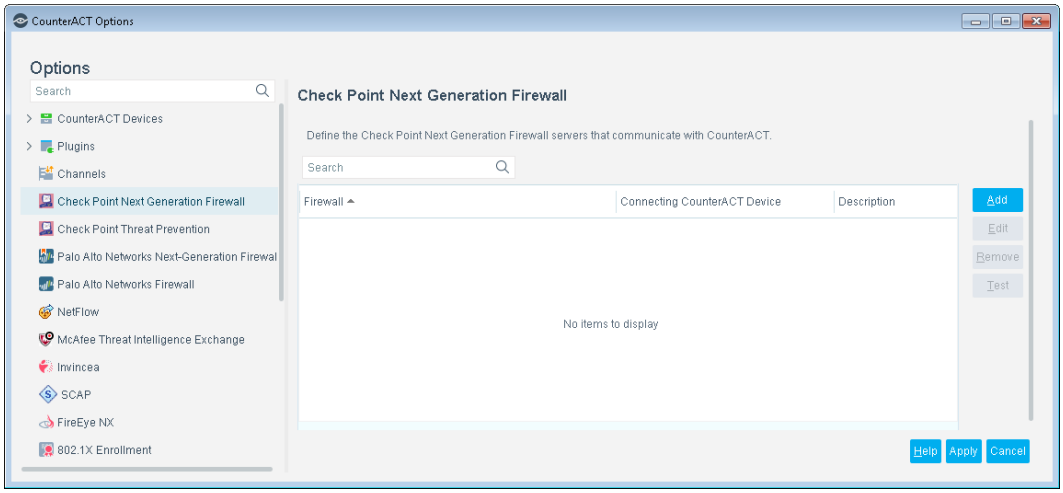
When restarting the module, you need to start and stop the module on all CounterACT devices at the same time. *Do not restart the module on individual CounterACT devices.*

Configure Individual Firewalls

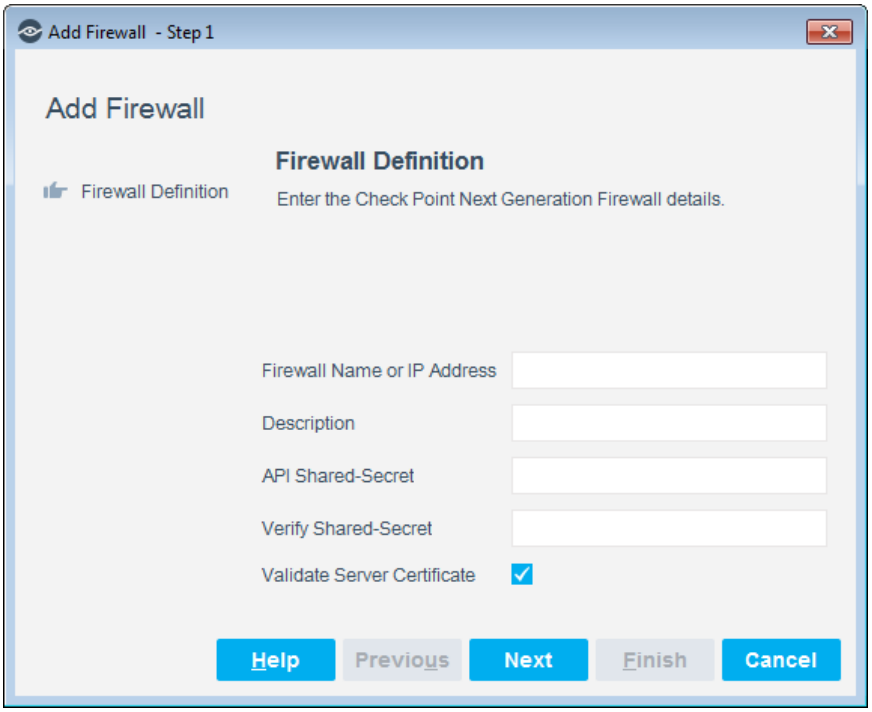
Configure individual firewall options to determine when API calls are sent from the module to the firewall.

To configure the firewall:

1. Select **Options** from the **Tools** menu and then select the **Modules** folder.
2. In the **Modules** pane, select the Check Point Next Generation Firewall Module and select **Configure**.
3. In the Check Point Next Generation Firewall pane, select **Add**.



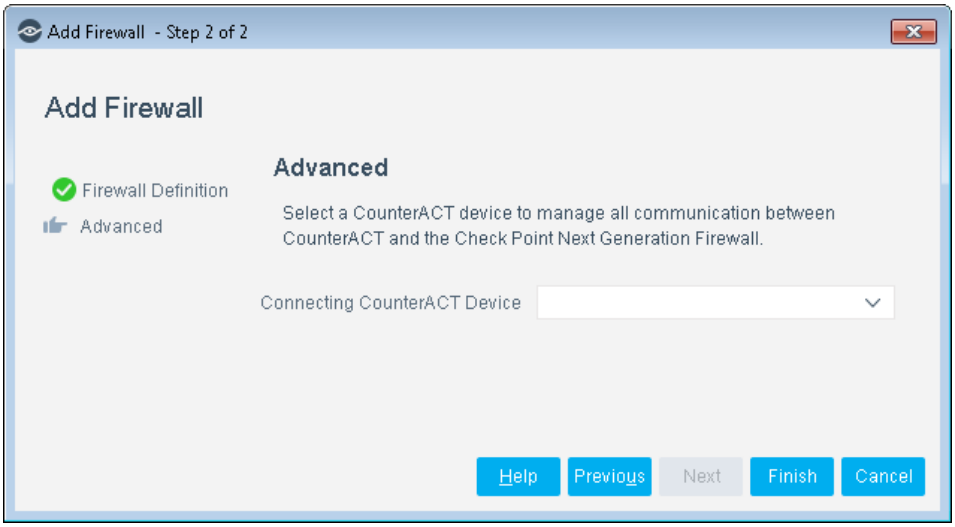
The Firewall Definition pane opens.



4. Configure the following connection parameters:

Firewall Name or IP Address	Enter the firewall name, the Fully Qualified Domain Name (FQDN), or the IPv4 address.
Description	(Optional) Enter a description to include in the list of firewalls.
API Shared-Secret	Enter the pre-shared secret defined in the Check Point SmartDashboard.
Verify Shared-Secret	Re-enter the API shared-secret key to verify it.
Validate Server Certificate	Select this option to validate the identity of the third-party server before establishing a connection, when the eyeExtend product communicates as a client over SSL/TLS. To validate the server certificate, either of the following certificate(s) must be installed: ▪ Self-signed server certificate – the server certificate must be installed on the CounterACT Appliance ▪ Certificate Authority (CA) signed server certificate – the CA certificate chain (root and intermediate CA certificates) must be installed on the CounterACT Appliance Use the Certificates > Trusted Certificates pane to add the server certificate to the Trusted Certificate list. For more information about certificates, refer to the appendix, "Configuring the Certificate Interface" in the *Forescout Administration Guide*.

5. Select **Next**.



6. Select a CounterACT device to manage all communication between the Forescout platform and the firewall.

Connecting CounterACT Device	Select the name or IP address of the CounterACT device to communicate with the firewall server. See Check Point Next Generation Firewall Setup for details.

7. Select **Finish**.

The best practice is to perform a test after setting up a connection. See Test the Module Configuration.

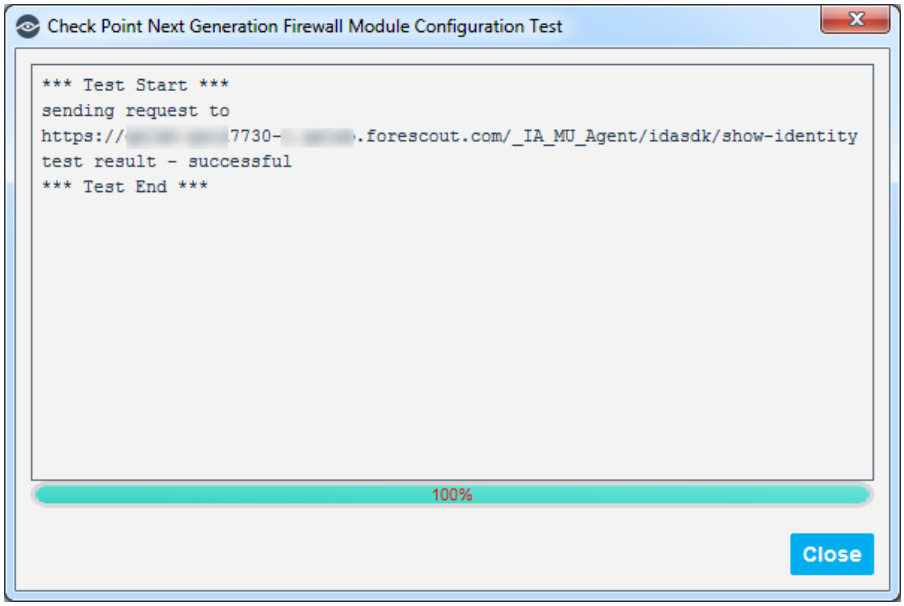
Test the Module Configuration

This section describes how to perform a configuration test. The test checks connectivity between the Check Point r77.30 gateway IP address and the connecting CounterACT device.

To run a test:

1. In the Check Point Next Generation Firewall pane, select the Check Point Firewall Server you want to test, and select **Test**.

   The test results are displayed in the Check Point Next Generation Firewall Module Configuration Test dialog box.



2. Select **Close**.

Create Custom Policies for Check Point Next Generation Firewall

Use Forescout platform policies to:

- Enhance firewall intelligence with dynamic, real-time information on endpoint compliance, functionality, OS, location, risk status, and more. This information is learned by Forescout platform policies and delivered to the firewall to deal with rapid network changes.
- Leverage the Forescout platform as a mission-critical real-time information source.

Custom policy tools provide you with an extensive range of options for detecting and handling endpoints. Specifically, use the policy to instruct the Forescout platform to apply a policy action to endpoints that match (or do not match) property values defined in policy conditions.

Actions

Policy actions let you instruct the Forescout platform how to control detected devices. For example, assign a detected device to an isolated VLAN, or send the device user or IT team an email.

In addition to the bundled Forescout actions available for detecting and handling endpoints, you can work with Forescout platform actions to create custom policies. These items are available when you install the module.

To create a custom policy:

1. Log in to the Console and select **Policy**.
2. Create or edit a policy.

Check Point Next Generation Firewall Policy Actions

This section describes the actions that are made available when Forescout eyeExtend for Check Point NGFW is installed.

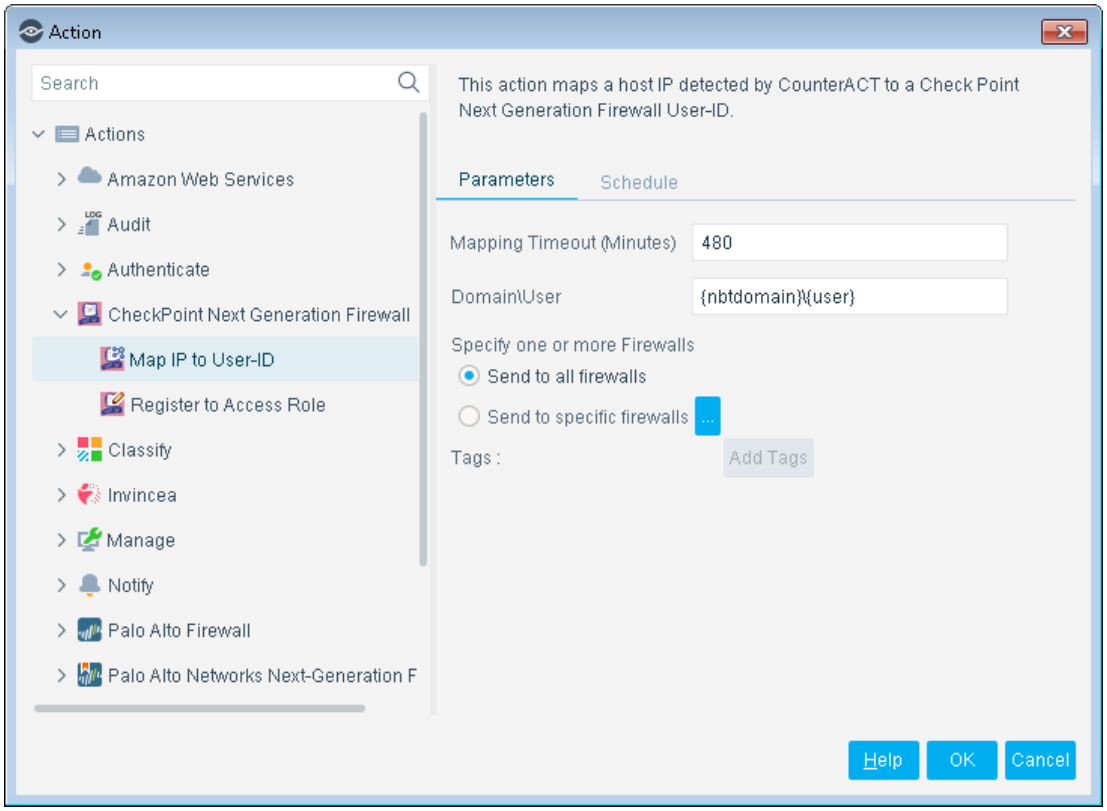
To access the actions:

- In the Policy Actions dialog box, expand the Check Point Next Generation Firewall folder in the Actions tree. The following actions are available:
  - Map IP to User-ID
  - Register to Access Role

Map IP to User-ID

This action lets you map an endpoint IP address detected by the Forescout platform to a Check Point Next Generation Firewall User-ID. The Forescout platform detects a fully qualified domain name (FQDN) to map an endpoint IP address.

Check Point Next Generation Firewall employs a User Identification (User-ID) feature to configure and enforce firewall policies based on users. User-ID identifies the user on the network and the IP addresses of the computers the user is logged into. In certain situations, however, firewalls cannot easily map between an IP address and a user identity. The module leverages the advanced endpoint detection capabilities of the Forescout platform to identify and convey user information to firewalls.

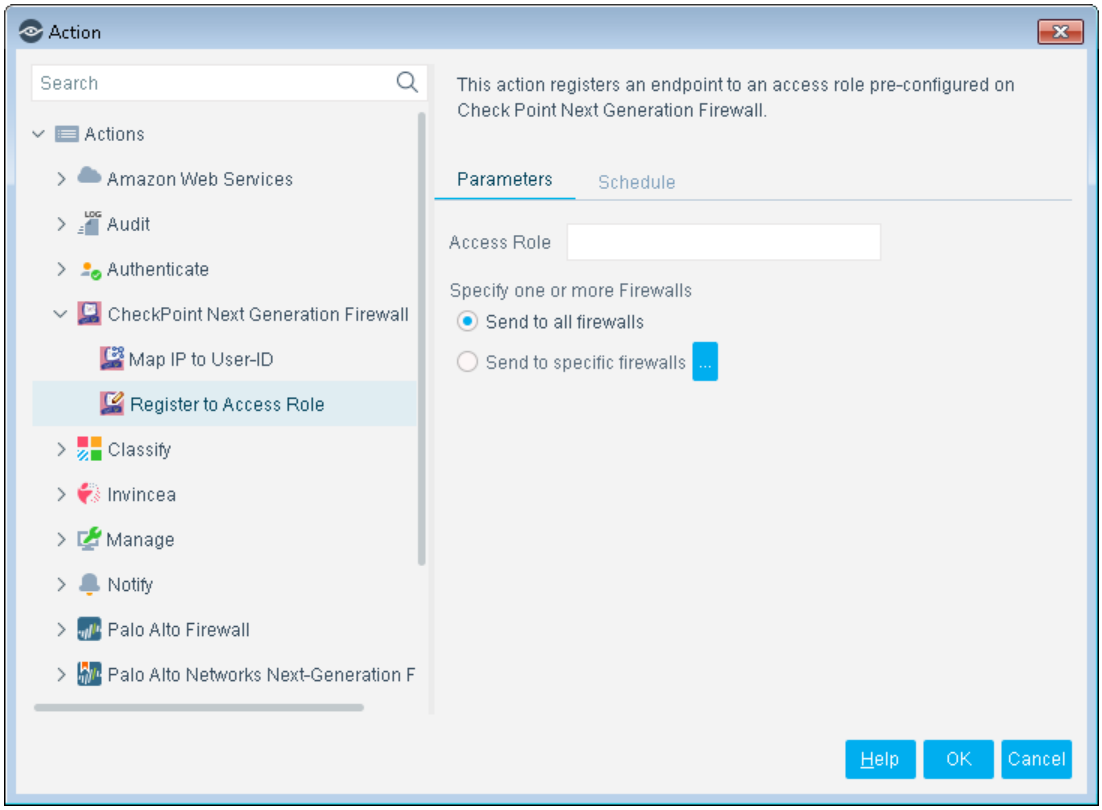


The following parameters are available:

Mapping Timeout (Minutes)	The number of minutes that the action persists in the firewall.
Domain\User	By default, this parameter consists of property tags *{nbtdomain}\{user}* representing the NetBIOS domain and the Windows user name. For non-Windows users, use the Tags feature to replace *{user}* with the appropriate property tag: ▪ *{linux_logged_users}* for Linux ▪ *{mac_logged_users}* for Mac
Specify one or more Firewalls	The target firewall(s) to which the action is applied. See Configure the Module.
Tags	The property tags added to the **Domain\User** field. Note: Click inside the **Domain\User** field to enable this feature.

Register to Access Role

This action registers the endpoint IP address to the predefined access role.



The following parameters are available for selection:

Access Role	One or more access roles defined in the Check Point SmartDashboard. The list must be comma-separated and without spaces.
Specify one or more Firewalls	The target firewall(s) that the action is applied to. See Configure the Module.

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.