ForeScout® Extended Module for Check Point® Next Generation Firewall

Configuration Guide

Version 1.1

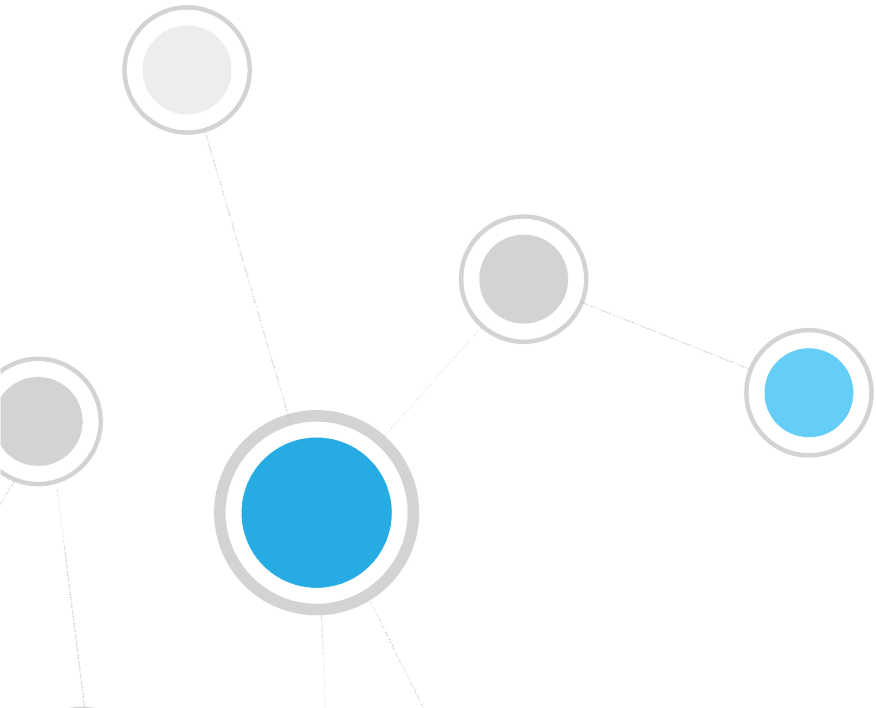


Table of Contents

About the Check Point Next Generation Firewall Integration

The ForeScout® Extended Module for Check Point Next Generation Firewall (NGFW) integration significantly magnifies firewall power by leveraging network visibility, inspection and enforcement capabilities provided by CounterACT.

The integration allows security teams to:

- 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 CounterACT policies and other basic features work.

Use Cases

- Segment Endpoints to Predefined Roles
- Leverage CounterACT as Another Provider of User-ID for Endpoints

Segment Endpoints to Predefined Roles

Use CounterACT's powerful endpoint classification engine to segment endpoints to predefined roles.

Leverage CounterACT as Another Provider of User-ID for Endpoints

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

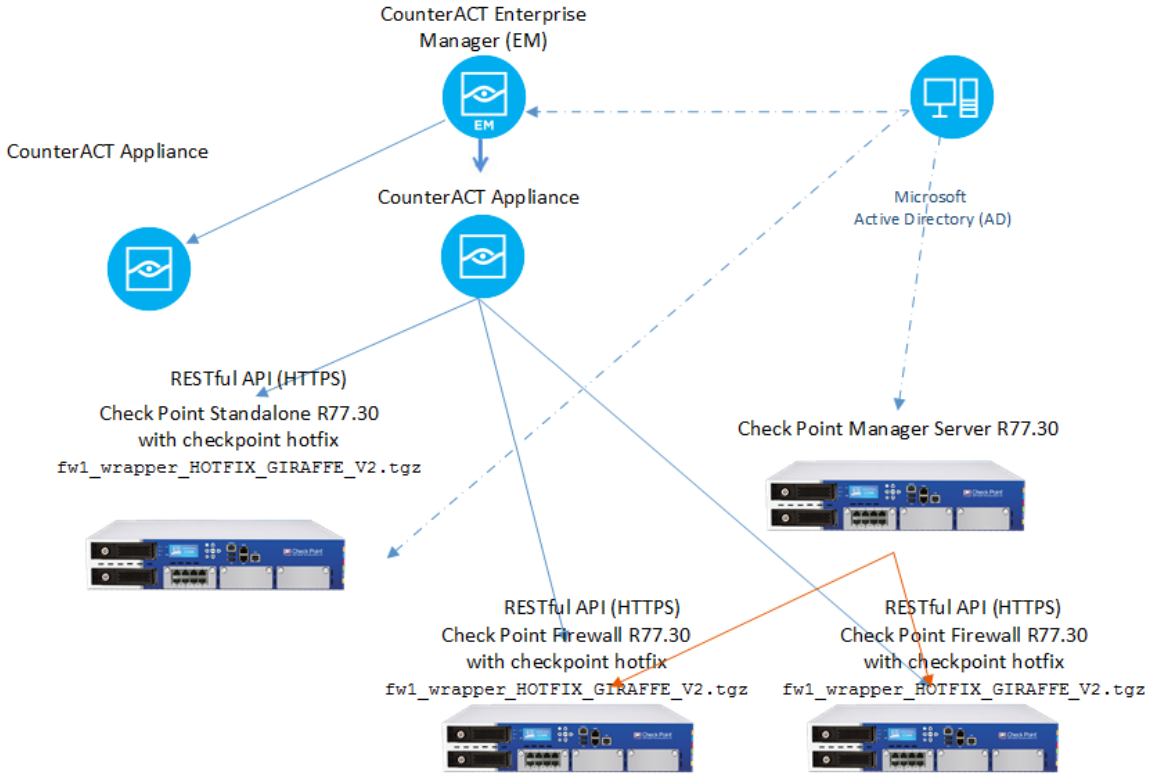
About the Extended Module for Check Point Next Generation Firewall

This module lets you integrate CounterACT with Check Point Next Generation Firewall so that you can:

- ***Leverage CounterACT as a Mission-critical Real-time Information Source***
  - ***Map endpoint IP addresses discovered by CounterACT 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***

How It Works

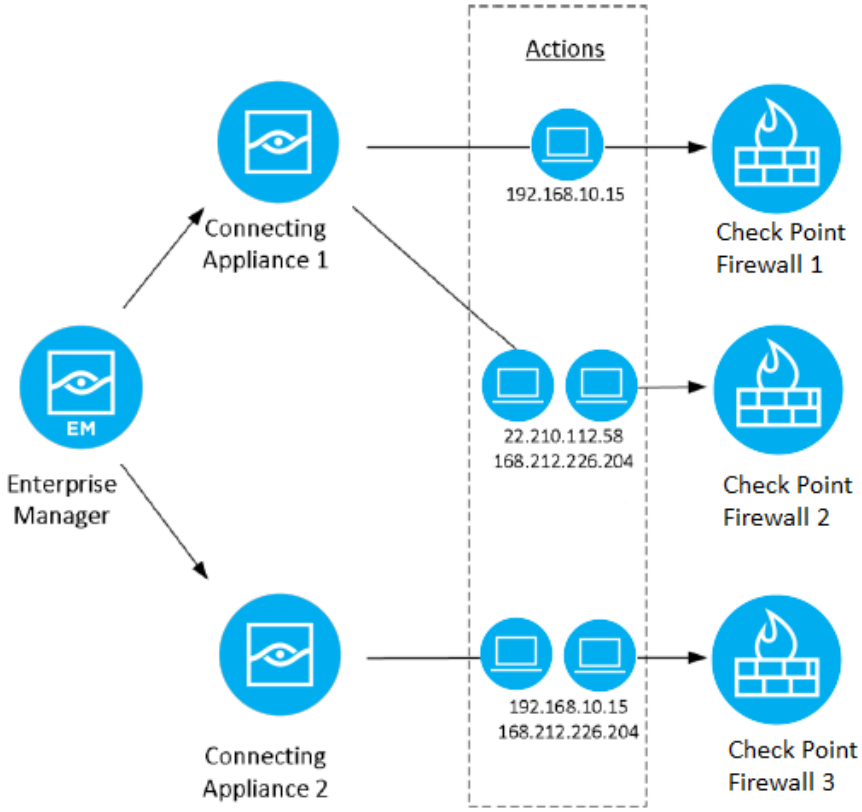
This section describes how the module communicates with Check Point firewalls.



Firewall Management

The module communicates with Check Point firewalls, supplying endpoint IP address information discovered by CounterACT using the CounterACT *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

You must perform the following 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:

- CounterACT Software Requirements
- ForeScout Extended Module Licensing Requirements
- Check Point Next Generation Firewall Requirements

CounterACT Software Requirements

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

- CounterACT version 8.0
- An active Maintenance Contract for the module.

ForeScout Extended Module Licensing Requirements

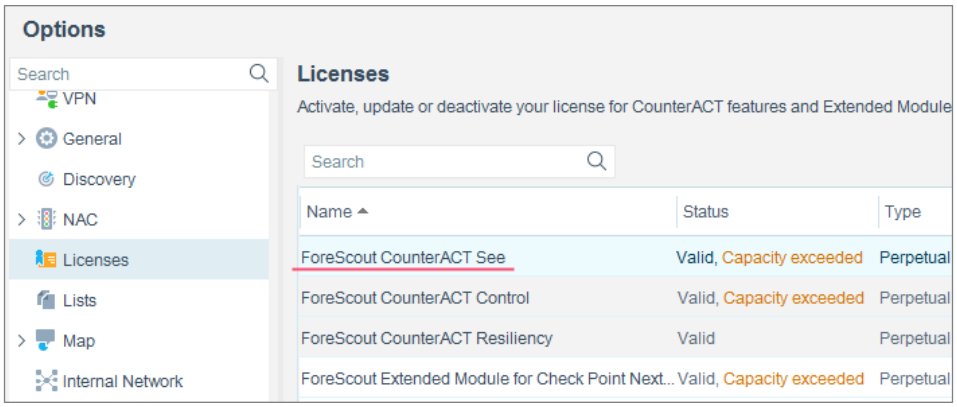
This ForeScout Extended Module requires a valid license. Licensing requirements differ based on which licensing mode your deployment is operating in:

- Per-Appliance Licensing Mode
- Centralized Licensing Mode

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.



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.

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.

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 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 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. T*he 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 license@forescout.com for more information.

Check Point Next Generation Firewall Requirements

The Extended Module for Check Point Next Generation Firewall now supports Check Point Gateway in versions R77.20, R77.30 and R80.10.

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 in the *ForeScout Extended Module for Check Point Next Generation Firewall Configuration Guide*.

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

1. IDA API requires you to Install the Hotfix.
   a. R77.20: fw1 wrapper_HOTFIX_GOLLUM_HF_BASE_295.tgz
   b. R77.30: fw1_wrapper_HOTFIX_GIRAFFE_V2.tgz
2. Enable IDA on Check Point Gateway

Check Point Gateway in Cluster Mode

3. Physical gateway
   c. Check Point appliance
   d. Open server
4. Virtual appliance

Requirements Independent to the Management Platform

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

Install the Hotfix

Installing the hotfix is not required if you are using Check Point Gateway version R80.10. See Install the Module in the *ForeScout Extended Module for Check Point Next Generation Firewall Configuration Guide*.

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 in the *ForeScout Extended Module for Check Point Next Generation Firewall Configuration Guide*.

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

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 - ***Centralized Licensing Mode***

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

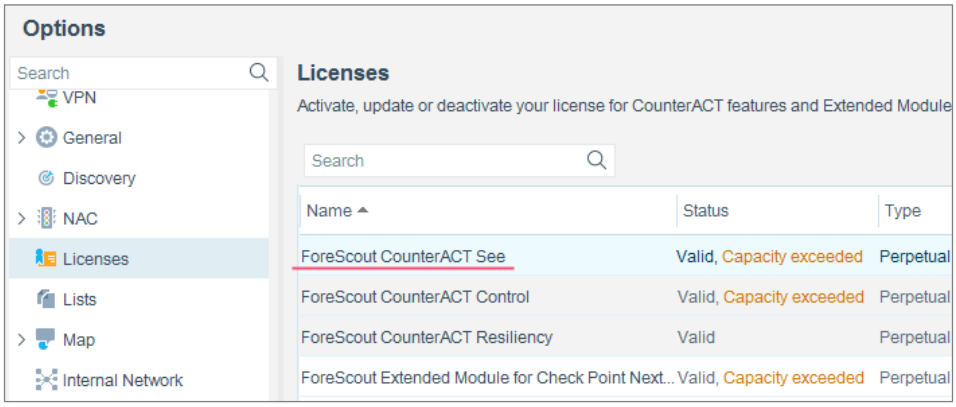
10. When the installation completes, select **Close** to close the window. The installed module is displayed in the Modules pane.

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.



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

Check Point Next Generation Firewall Setup

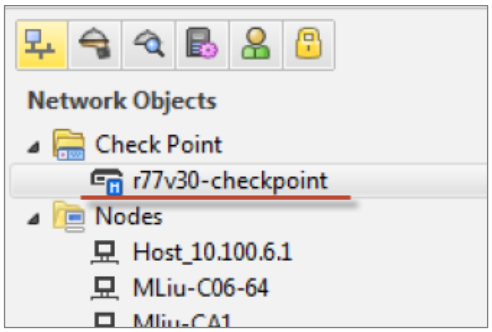
This section describes the configuration required on the Check Point SmartDashboard to:

- Create an Access Role in the Check Point SmartDashboard
- Set Up a Pre-shared Secret in the Check Point SmartDashboard

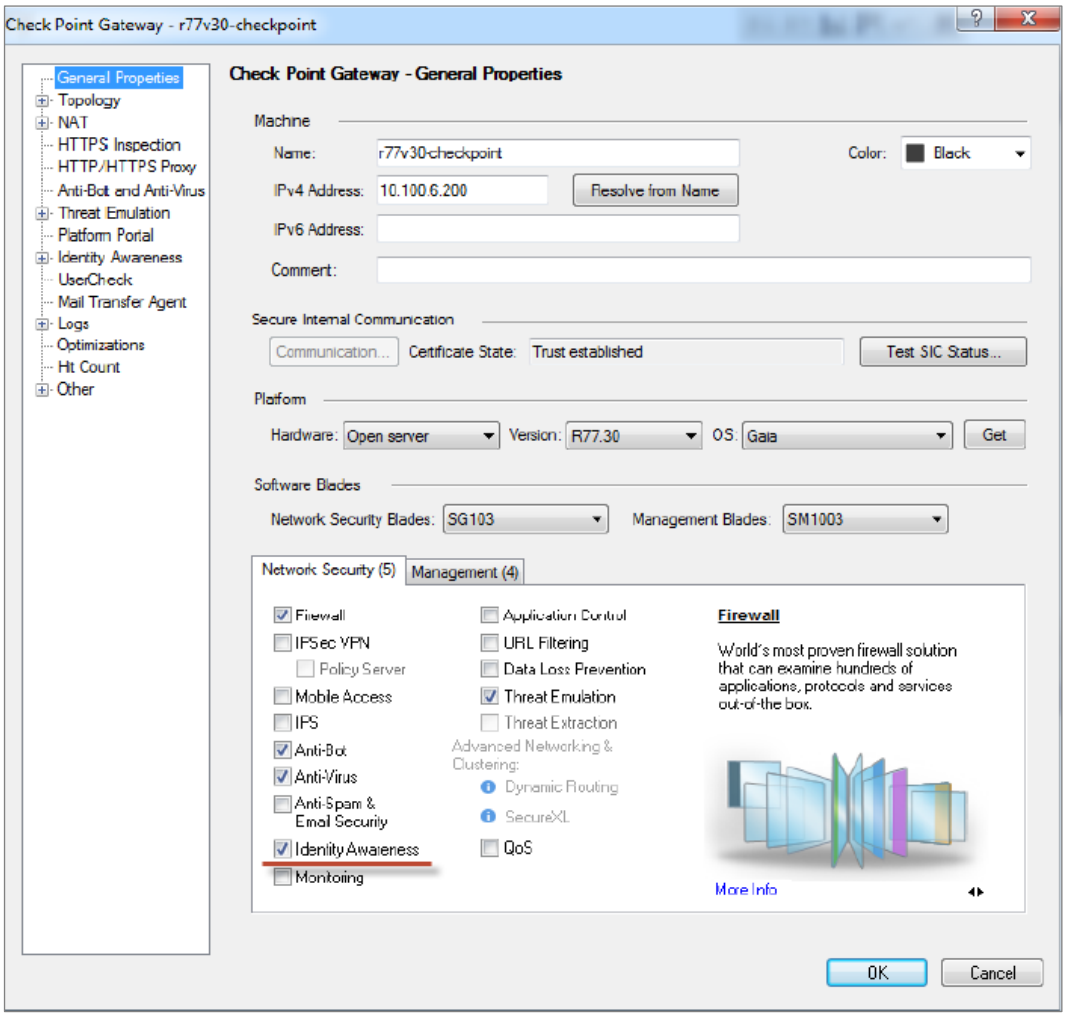
Create an Access Role in the Check Point SmartDashboard

Use the Check Point SmartDashboard to access the Check Point Management Server.

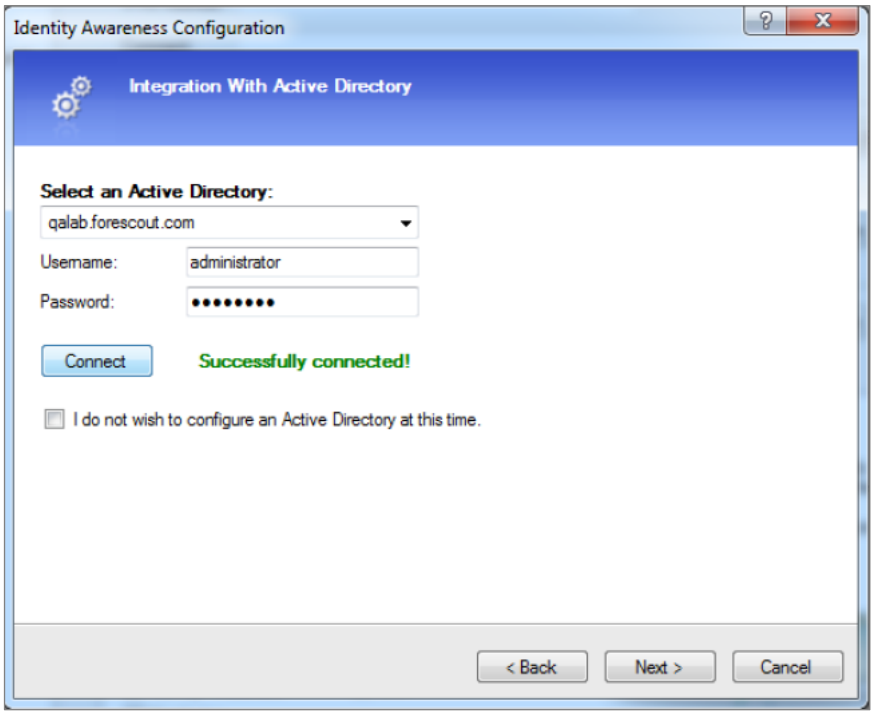
1. In the **Network Objects** pane, select the Check Point server to be configured.



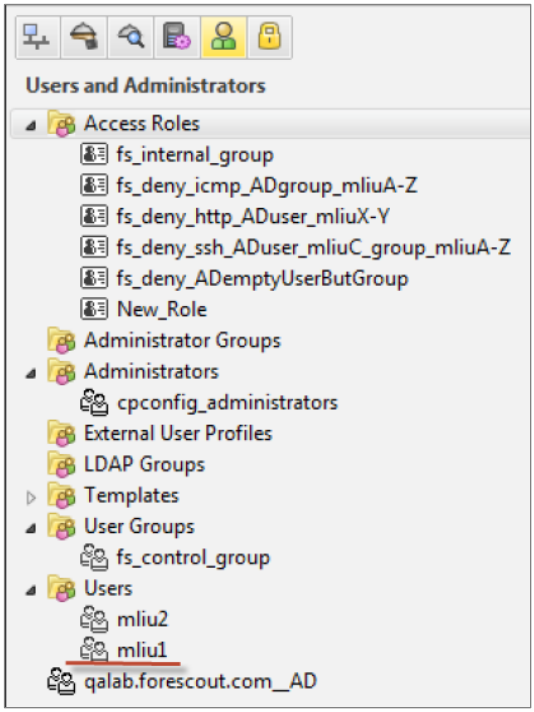
2. Go to **General Properties** and select the **Identity Awareness** checkbox.



3. Configure Microsoft Active Directory as Browser Based Authentication.
   a. Select an Active Directory: qalab.forescout.com.
   b. Enter login credentials.
   c. Select **Connect** to make initial contact with the Active Directory.



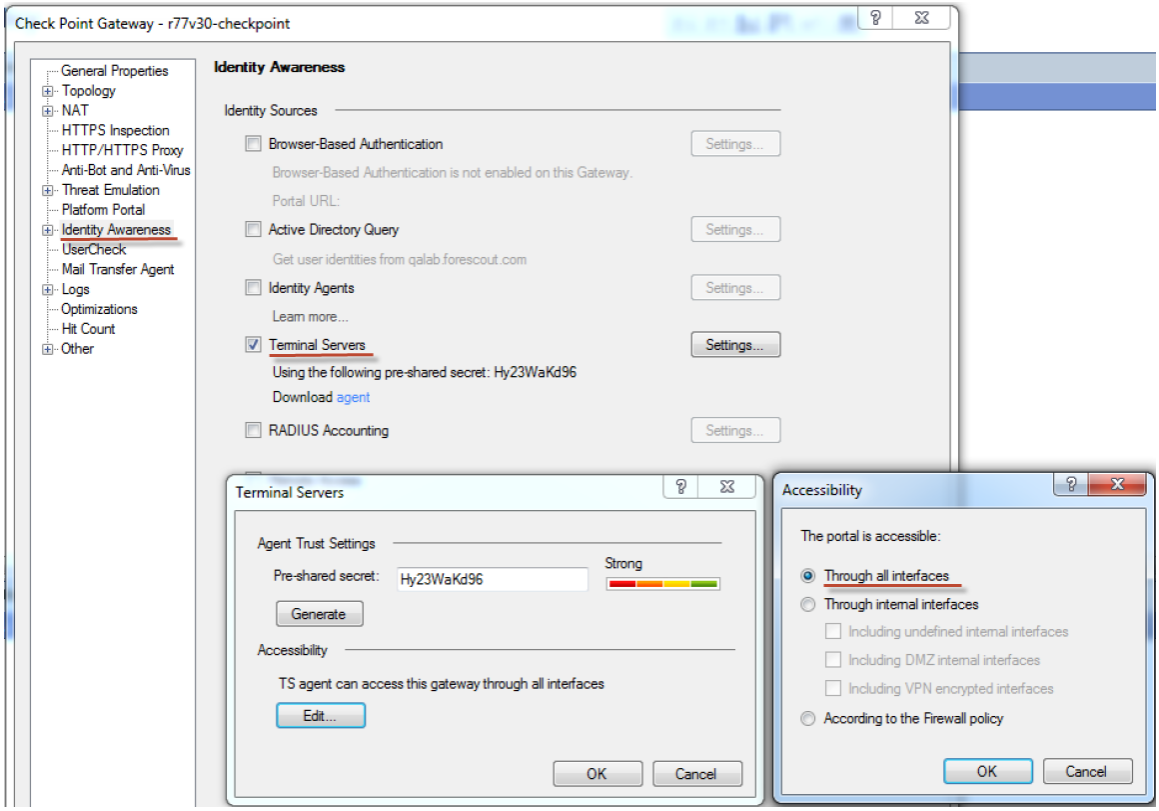
4. In the **User and Administrators** pane, create an access role based on Microsoft Active Directory data.



5. 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 in the Check Point SmartDashboard

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



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

Configure the Module

Configure the module for CounterACT to 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.

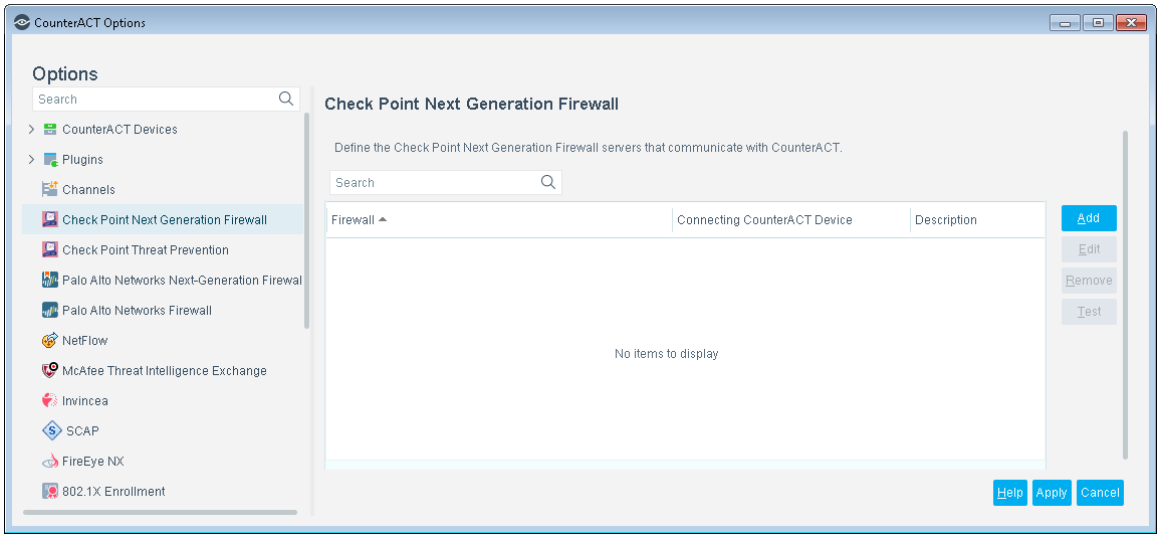
When restarting the module, you need to start and stop the module on all CounterACT devices at the same time. Do not restart the module on individual CounterACT devices.

Configure Individual Firewalls

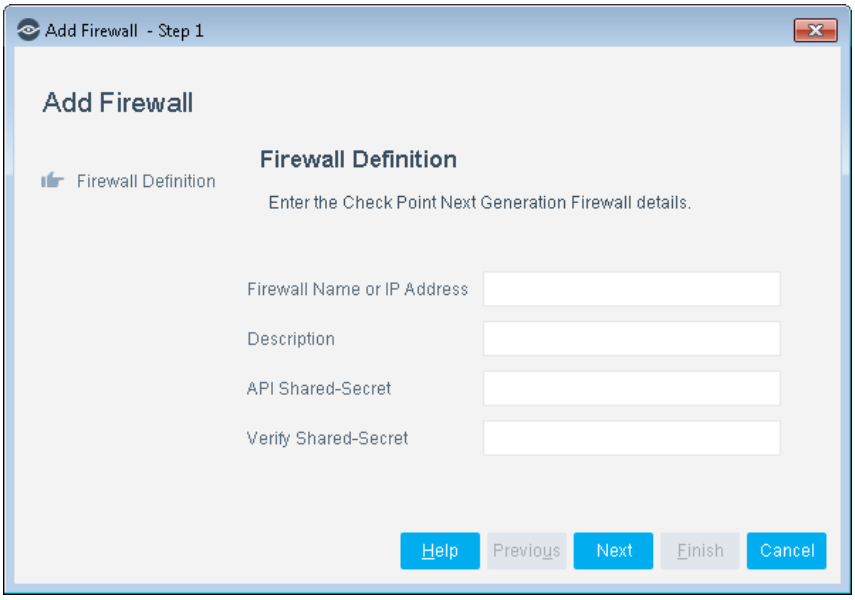
Configure individual firewall options to determine when API calls are sent from the module to the firewall.

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**.



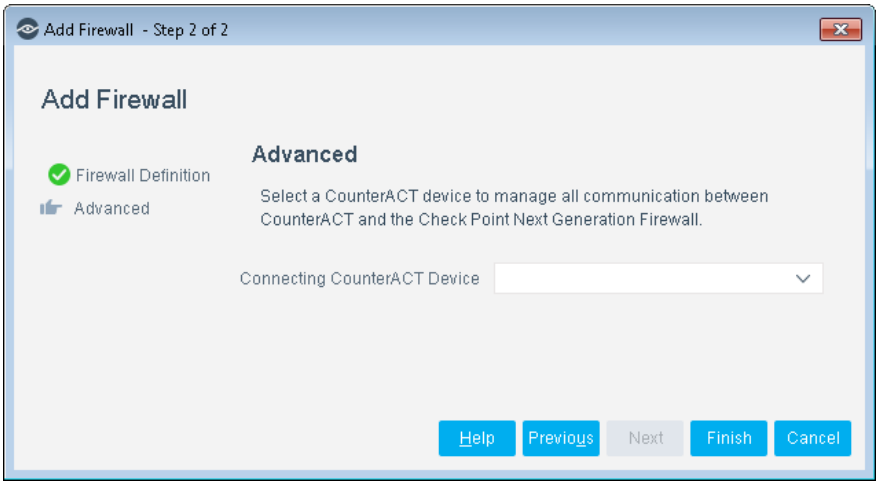
3. In the Check Point Next Generation Firewall pane, select **Add**. The Add Firewall dialog box opens.



4. In the **Firewall Definition** pane, configure the following connection parameters:

Firewall Name or IP Address	IP address or resolvable DNS name
Description	Description to be displayed in the CounterACT list of firewalls (Optional)
API Shared-Secret	Pre-shared secret defined in the Check Point SmartDashboard
Verify Shared-Secret	Reenter API shared-secret key

5. Select **Next**. The Advanced pane opens.



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

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

7. Select **Finish**.

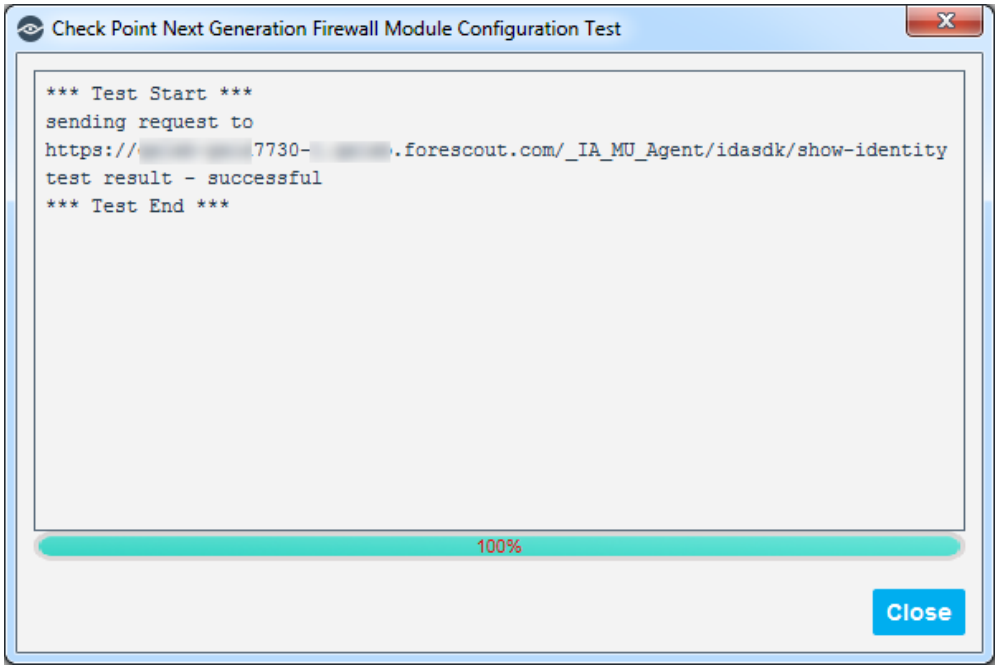
Test the Module Configuration

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 Check Point Next Generation Firewall Module Configuration Test dialog box displays the test results.



2. Select **Close**.

Create Custom Policies for Check Point Next Generation Firewall

Use CounterACT 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 CounterACT policies and delivered to the firewall to deal with rapid network changes.
- Leverage CounterACT 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 CounterACT to apply a policy action to endpoints that match (or do not match) property values defined in policy conditions.

Actions

The CounterACT policy actions let you instruct CounterACT 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 CounterACT actions available for detecting and handling endpoints, you can work with Check Point Next Generation Firewall module related actions to create custom policies. These items are available when you install the module.

For more information about working with policies, select **Help** from the policy wizard.

To create a custom policy:

1. Log in to the CounterACT Console.
2. Select the **Policy** icon from the Console toolbar.
3. Create or edit a policy.

Check Point Next Generation Firewall Policy Actions

This section describes the actions that are made available when the Check Point Next Generation Firewall module is installed.

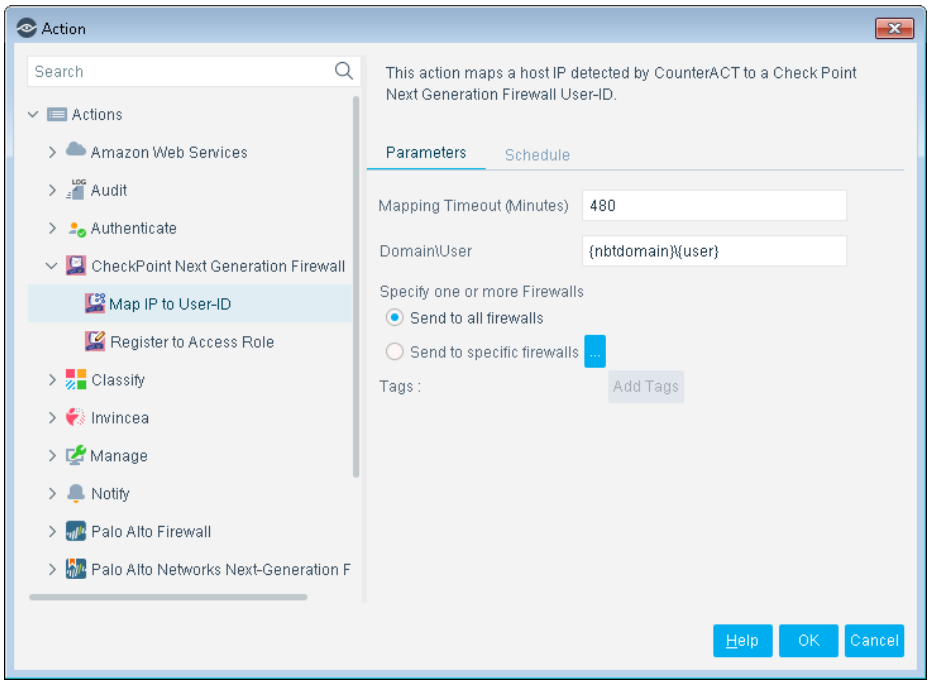
To access Check Point Next Generation Firewall Module actions:

1. Navigate to the Actions tree from the Policy Actions dialog box.
2. 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 CounterACT to a Check Point Next Generation Firewall User-ID. CounterACT 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 CounterACT advanced endpoint detection capabilities to identify and contribute user information to firewalls.

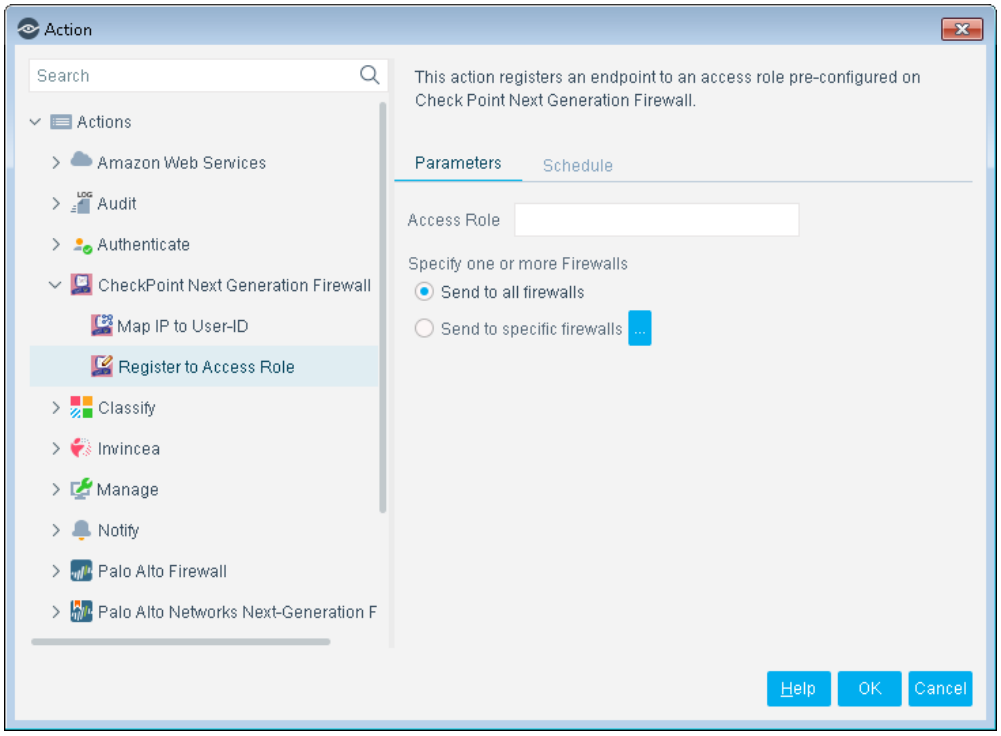


The following parameters are available:

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 CounterACT property tag: ▪ *{linux_logged_users}* for Linux ▪ *{mac_logged_users}* for Mac
Specify one or more Firewalls	The target firewall(s) that the action is applied to. See Configure the Module.
Tags	CounterACT 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 CounterACT Documentation

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

- Documentation Downloads
- Documentation Portal
- CounterACT Help Tools

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 Identifying Your Licensing Mode in the Console.

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 https://updates.forescout.com/support/index.php?url=counteract.
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 https://forescout.force.com/support/.
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 www.forescout.com/docportal.
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**.

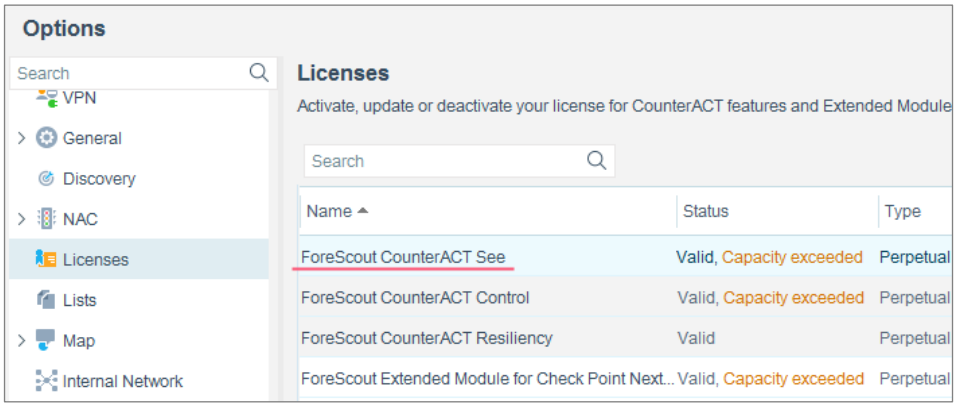
Documentation Portal

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.



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 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.

2018-04-10 09:21