# Table of Contents

**About the Check Point Next Generation Firewall Integration** ...................... 4  
Use Cases ........................................................................................................ 4  
Segment Endpoints to Predefined Roles .......................................................... 4  
Leverage CounterACT as Another Provider of User-ID for Endpoints ............. 4  

**About the Extended Module for Check Point Next Generation Firewall** ... 4  
How It Works .................................................................................................. 5  
Firewall Management ...................................................................................... 5  
What to Do .................................................................................................... 6  

**Requirements** .......................................................................................... 6  
CounterACT Software Requirements ............................................................... 7  
ForeScout Module License Requirements ......................................................... 7  
Requesting a License ..................................................................................... 7  
More License Information ............................................................................. 8  
Check Point Next Generation Firewall Requirements ..................................... 8  
Check Point Gateway in version R80.10 ....................................................... 8  
Check Point Gateway in version R77.20 or R77.30 ........................................ 8  
Check Point Gateway in Cluster Mode ........................................................... 8  
Requirements independent to the management platform ............................... 9  

**Install the Hotfix** ...................................................................................... 9  

**Enable IDA on Check Point Gateway** ...................................................... 9  

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

**Check Point Next Generation Firewall Setup** ......................................... 10  
Create an Access Role in the Check Point SmartDashboard ............................. 10  
Set Up a Pre-shared Secret in the Check Point SmartDashboard ...................... 12  
Configure the Identity Web API ...................................................................... 13  
Create a New Host ....................................................................................... 14  

**Configure the Module** .......................................................................... 15  
Configure Individual Firewalls ....................................................................... 16  

**Test the Module Configuration** ............................................................... 17  

**Create Custom Policies for Check Point Next Generation Firewall** ........ 18  
Actions ....................................................................................................... 18  
Check Point Next Generation Firewall Policy Actions .................................... 19  
Map IP to User-ID ........................................................................................ 19  
Register to Access Role .............................................................................. 20  

**Additional CounterACT Documentation** ................................................. 21
Documentation Portal ......................................................................................... 21
Customer Support Portal ...................................................................................... 22
CounterACT Console Online Help Tools ................................................................. 22
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

Real-time Identity Information

Receive real-time mapping of CounterACT detected IPs to user IDs to support granular filtering of users rather than IP addresses. CounterACT-based IP to User-ID capabilities provide vital support in environments where Active Directory is not available or limited.

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 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 Module License Requirements
- Check Point Next Generation Firewall Requirements
CounterACT Software Requirements

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

- CounterACT version 7.0.0
- Service Pack 2.3.1 or above. It is recommended to install the latest service pack to take advantage of the most current CounterACT updates.

ForeScout Module License Requirements

This ForeScout Module requires a module license. The installation package for the module is in the form of a CounterACT plugin. When installing the plugin 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.

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.

More License Information
See the CounterACT Console User Manual for information on requesting a permanent license or a demo license extension. 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. Go to Install the Module.

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
1. Physical gateway
   a. Check Point appliance
   b. Open server
2. 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. Go to Install the Module.

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, go to 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

The installation package for the module is in the form of a CounterACT plugin.

To install the plugin:

1. Navigate to the Customer Support, ForeScout Modules page and download the plugin .fpi file.
2. Save the file to the machine where the CounterACT Console is installed.
3. Log into the CounterACT Console and select Options from the Tools menu.
5. Select Install. The Open dialog box opens.
6. Browse to and select the saved plugin .fpi file.
7. Select Install.
8. If you have not yet purchased a permanent module license, a message appears indicating that the plugin will be installed with a demo module license. Select Yes and then select Install.
9. An installation or upgrade information dialog box and an End User License Agreement will open. Accept the agreement to proceed with the installation.
10. When the installation completes, select Close. The plugin is displayed in the Plugins pane. The Module Status column indicates the status of your license. See ForeScout Module License Requirements or the CounterACT Console User Manual for details on requesting a permanent license or a demo license extension.
11. Select the plugin and select Start. The Select Appliances dialog box opens.
12. Select the CounterACT devices on which to start the plugin.
13. Select OK. The plugin runs on the selected devices.

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
- Configure the Identity Web API

Create an Access Role in the Check Point SmartDashboard

Use the Check Point SmartDashboard to access the Check Point Management Server.
1. In the Objects pane, select Network Objects, select the Gateways and Servers, and then select the Check Point gateway or 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, for example: lab.forescout.com.
   b. Enter login credentials.
   c. Select **Connect** to make initial contact with the Active Directory.
4. You will need to create an access role based on Microsoft Active Directory data. In the Objects pane, select **New**, select **More**, select **User**, and then select **Access Roles**.

5. In the New dialog box, select **Access Role**. Configure the required fields based on the Microsoft Active Directory data displayed. Select **OK**.

6. In the Check Point SmartDashboard, select **Install Policy** to publish and install the changes.

**Set Up a Pre-shared Secret in the Check Point SmartDashboard**

1. In the **General Properties** pane, select **Identity Awareness**. The Identity Sources pane displays.

2. Select the **Terminal Servers** checkbox and then select **Settings...**

4. Select Through internal interfaces, and then select the required interfaces. Verify that the access settings configuration allows access from CounterACT appliances.

5. Select OK and then select OK. This returns you to the Identity Sources pane.

6. In the Check Point SmartDashboard, select Install Policy to publish and install the changes.

If you are using Check Point Gateway version R80.10, in addition to the above steps, you will also need to configure the Identity Web API. If you are not using R80.10, go to Configure the Module.

**Configure the Identity Web API**

1. In the Gateway Cluster Properties dialog box, select Identity Web API and then select Settings...

2. The Identity Web API Settings dialog box opens. Select Edit.

3. The Accessibility dialog box opens. Select Through internal interfaces and then select the required interfaces.
4. Verify that the access settings configuration allows access from CounterACT appliances.

5. Select **OK**. This returns you to the Identity Web API Settings dialog box.

6. In Authorized Clients, you will need to add the CounterACT device that is configured as the connecting appliance for this gateway. If the CounterACT device is not in the option list, you will need to create a new host for it. If there is no need to create a new host, go to **Configure the Module**.

7. In the Check Point SmartDashboard, select **Install Policy** to publish and install the changes.

**Create a New Host**

1. Return to the Check Point Management Server page of the Check Point SmartDashboard.
2. In the Objects pane, select **New**, and then select **Host**.

![Image of the Objects pane with New selected]

3. The New Host dialog box opens. Enter the **Object Name** and **Machine IP address**.

![Image of the New Host dialog box]

4. Select **OK**.

5. In the Check Point SmartDashboard, select **Install Policy** to publish and install the changes.


**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 **Plugins** folder.
2. In the **Plugins** pane, select the Check Point Next Generation Firewall Plugin 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:

<table>
<thead>
<tr>
<th>Firewall Name or IP Address</th>
<th>IP address or resolvable DNS name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Description to be displayed in the CounterACT list of firewalls (Optional).</td>
</tr>
</tbody>
</table>
| API Shared-Secret           | - If the Check Point Gateway is in version R77.20 or R77.30, enter the pre-shared secret generated in Terminal Servers Settings.  
- If the Check Point Gateway is in version R80.10, enter the client secret generated for the corresponding authorized client in Identity Web API Settings. |
| Verify Shared-Secret        | Re-enter 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 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**.
2. The Check Point Next Generation Firewall Plugin Configuration Test dialog box displays the test results.

   ![Check Point Next Generation Firewall Plugin Configuration Test](image)

3. When finished viewing the results, 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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mapping Timeout (Minutes)</td>
<td>The number of minutes that the action persists in the firewall.</td>
</tr>
<tr>
<td>Domain\User</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>-  {\linux_logged_users} for Linux</td>
</tr>
<tr>
<td></td>
<td>-  {\mac_logged_users} for Mac</td>
</tr>
<tr>
<td>Register to Access Role</td>
<td>This action registers the endpoint IP address to the predefined access role.</td>
</tr>
</tbody>
</table>

**Register to Access Role**

This action registers the endpoint IP address to the predefined access role.
The following parameters are available for selection:

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Role</strong></td>
<td>One or more access roles defined in the Check Point SmartDashboard. The list must be comma-separated and without spaces.</td>
</tr>
<tr>
<td><strong>Specify one or more Firewalls</strong></td>
<td>The target firewall(s) that the action is applied to. See Configure the Module.</td>
</tr>
</tbody>
</table>

**Additional CounterACT Documentation**

For more detailed information about the CounterACT features described here or additional CounterACT features and modules, refer to the following resources:

- [Documentation Portal](#)
- [Customer Support Portal](#)
- [CounterACT Console Online Help Tools](#)

**Documentation Portal**

The ForeScout Documentation Portal is a Web-based library containing information about CounterACT tools, features, functionality and integrations.
To access the Documentation Portal:
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

Customer Support Portal
The Customer Support Portal provides links to CounterACT version releases, service packs, plugins and modules as well as related documentation. The portal also provides a variety of How-to Guides, Installation Guides and more. To access the Customer Support Portal, go to:

To access the Customer Support Portal:
2. Select the CounterACT version you want to discover.

CounterACT Console Online 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.

Console User Manual
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 Plugins.
2. Select the plugin and then select Help.

Documentation Portal
Select Documentation Portal from the Help menu.
Legal Notice

Copyright © ForeScout Technologies, Inc. 2000-2017. All rights reserved. The copyright and proprietary rights in this document belong to ForeScout Technologies, Inc. ("ForeScout"). It is strictly forbidden to copy, duplicate, sell, lend or otherwise use this document in any way, shape or form without the prior written consent of ForeScout. All other trademarks used in this document are the property of their respective owners.

These products are based on software developed by ForeScout. The products described in this document may be protected by one or more of the following U.S. patents: #6,363,489, #8,254,286, #8,590,004, #8,639,800 and #9,027,079 and may be protected by other U.S. patents and foreign patents.

Redistribution and use in source and binary forms are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials and other materials related to such distribution and use acknowledge that the software was developed by ForeScout.

Unless there is another valid written agreement executed by you and ForeScout that governs the ForeScout products and services:

- If you have purchased any ForeScout products or services, your use of such products or services is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you have purchased any ForeScout support service ("ActiveCare"), your use of ActiveCare is subject to your acceptance of the terms set forth at http://www.forescout.com/activecare-maintenance-and-support-policy/;
- If you are evaluating ForeScout’s products, your evaluation is subject to your acceptance of the applicable terms set forth below:
  - If you have requested a General Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/evaluation-license/.
  - If you have requested a Beta Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/beta-test-agreement/.
  - If you have purchased any ForeScout Not For Resale licenses, such license is subject to your acceptance of the terms set forth at http://www.forescout.com/nfr-license/.

Send comments and questions about this document to: documentation@forescout.com

2017-10-30 13:19