



ForeScout CounterACT[®]

Cisco PIX/ASA Firewall Integration Module Configuration Guide

Version 2.1

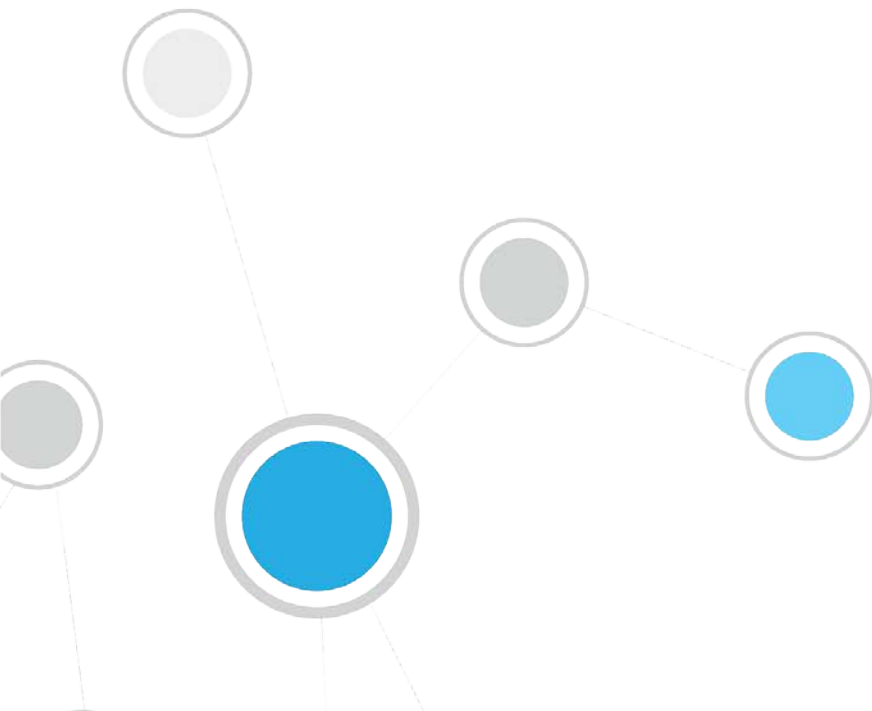


Table of Contents

About the Cisco PIX/ASA Firewall Integration Module	3
Requirements	3
Configuring the Firewall	3
Install and Configure the Module	4
Verify That the Module Is Running	6
Apply Firewall Access Lists to a Host.....	6
Naming CounterACT Object Groups	7
Sample Firewall Commands	7
Cisco PIX/ASA Access-list Action	8
Additional CounterACT Documentation	9
Documentation Downloads	9
Documentation Portal	9
CounterACT Help Tools.....	10

About the Cisco PIX/ASA Firewall Integration Module

The ForeScout CounterACT Cisco PIX/ASA Firewall Integration Module forwards host blocking requests to an external Cisco PIX or ASA firewall.

Blocking is implemented using access lists that reference a set of object groups. CounterACT maintains the object groups, adding and removing hosts from the group as needed.


Requirements

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

- CounterACT version 8.0.
- A firewall user account unique to CounterACT. See [Configuring the Firewall](#) for privileges and access requirements for this user.
- An active Maintenance Contract for CounterACT devices is required.

Configuring the Firewall

Enter the following commands at each firewall while in configuration mode.

 *Record these values, and use them to configure CounterACT communication with the firewall as described in [Install and Configure the Module](#).*

1. Enable SSH Access from a CounterACT Device:

Refer to Cisco documentation for general instructions on how to enable SSH access to the firewall. You will probably need to issue the following sequence of commands:

```
ca gen rsa key 1024
ca save all
aaa authentication ssh console LOCAL
write mem
```

To enable SSH access from a CounterACT device, select INSIDE or OUTSIDE depending on the interface to which the CounterACT device connects.

2. Define a user name (the default is `forescout`), password and restrictive privilege level (`priv_level`) (the default is 4) for the CounterACT device user:
`username <user_name> password <user_password> privilege <priv_level>`
3. Define the privilege level permissions:

```
enable password <priv_password> level <priv_level>
privilege configure level <priv_level> mode enable command configure
privilege configure level <priv_level> command object-group
privilege show level <priv_level> command object-group
privilege configure level <priv_level> command network-object
privilege configure level <priv_level> command port-object
privilege configure level <priv_level> command pdm
```

Install and Configure the Module

This section describes how to install and configure the Cisco PIX/ASA Firewall Integration Module.

To install the module:

1. Navigate to one of the following ForeScout 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 wizard opens.
9. Select **I agree to the License Agreement**, and select **Install**. The installation will not proceed if you do not agree to the license agreement.
 - 📖 *Make sure you have selected the correct module to install. 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 wizard. The installed module is displayed in the Modules pane.

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
- General
- Discovery
- NAC
- Licenses**
- Lists
- Map
- Internal Network

Licenses

Activate, update or deactivate your license for CounterACT features and Extended Module

Search

Name	Status	Type
ForeScout CounterACT See	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Control	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Resiliency	Valid	Perpetual
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.

To configure:

1. Select **Cisco PIX/ASA Firewall Integration** and then select **Configure**.

The Select Appliances dialog box opens.

2. Select the required CounterACT devices and then select **OK**.

The Cisco PIX/ASA Firewall Integration Module Configuration dialog box opens.

Cisco PIX/ASA Firewall integration@Enterprise Manager Plugin Configuration

Firewall name

Firewall Address

User: forescout

User Password

Retype User Password

Privilege Level: 0

Privilege Level Password

Retype Privilege Level Password

Network Group Name Prefix: FS_GROUP_

SSH Port: 22

SSH version: 1

Maximum group size: 0

Show net group members on test

Using clear local-host command.

OK Cancel

The following table summarizes Cisco PIX/ASA Firewall Integration configuration options:

Field Name	Description
Firewall name	The name of the PIX or ASA firewall
Firewall Address	The IP address of the PIX or ASA firewall
User	The CounterACT device SSH user name
User Password	The CounterACT device SSH user password
Privilege Level	The CounterACT device user privilege level
Privilege Level Password	The password to obtain the privilege level
Network Group Name Prefix	A label that identifies network object groups used by CounterACT. This prefix is combined with a numerical value to specify an object group. Together, the prefix and suffix define a set of object groups. See Apply Firewall Access Lists to a Host for more information.
SSH Port	The port number for secure shell communication.
SSH version	The version of SSH used to access the PIX or ASA firewall
Maximum group size	The maximum size of a network object group
Show net group members on test	Specifies whether to list the members of the network object group when you test the module
Using clear local-host command.	Specifies whether to run the clear local-host command at the firewall after a host is added to or removed from a network group. This command clears all existing connections and NAT sessions associated with the endpoint on its local network segment.

3. (Optional) Repeat Steps [0](#) and [2](#) to configure communication between remaining CounterACT devices and additional PIX/ASA firewalls.

Verify That the Module Is Running

After configuring the module, verify that it is running.

To verify:

1. Select **Tools > Options** and then select **Modules**.
2. Navigate to the module and select **Start** if the module is not running.

Apply Firewall Access Lists to a Host

This module provides an action that adds a host to a network object group defined on PIX/ASA firewalls. These object groups are referenced by access list commands.

To add a host to an access list:

1. Define a network object group for use by CounterACT on the firewall.
2. Define an access-list statement that refers to the CounterACT network object group.
Access list restrictions apply to all endpoints in the network object group.
3. Create a policy that uses the [Cisco PIX/ASA Access-list Action](#) to assign hosts to the CounterACT network object group.
 - Hosts that satisfy policy conditions are added to the object group on the target firewall(s). Access list restrictions apply to these hosts.
 - When hosts no longer satisfy policy conditions, they are removed from the object group. Access list restrictions no longer apply to these hosts.

Naming CounterACT Object Groups

Use this naming convention when you define network object groups for use by CounterACT.

The name of the network object groups used by CounterACT is constructed using the values of two string variables as follows:

`<Network_Group_Name><Netgroup_suffix>`

- The **Network Group Name** is a value you specified when you configured the firewall in the module. The default value for this string is `FS_GROUP_`.
- A numerical **Netgroup suffix** you specify in the *Cisco PIX/ASA Access-list* action.

This creates a series of object group names. For example, the default **Network Group Name** string `FS_GROUP_` can be combined with various **Netgroup suffix** values to yield the following series of object groups:

`FS_GROUP_0` `FS_GROUP_1` `FS_GROUP_2` ...

The **Netgroup suffix** value is policy-specific: you define the value when you use the *Cisco PIX/ASA Access-list* action in a CounterACT policy. This means that each policy can use its own object group. At the firewall, you can apply different access list restrictions to each object group.

For example, you can configure the firewall to block internal network access for all members of `FS_GROUP_0`, and to block access to the finance server for all members of `FS_GROUP_1`. Different policies add hosts to each group.

Sample Firewall Commands

The following sample commands define a network object group that uses the CounterACT naming convention:

```
object-group network FS_GROUP_3
network-object host 0.0.0.1
```

- 📄 You cannot define an empty group. A dummy host 0.0.0.1 is added to the group.

The following sample code applies access list restrictions to the CounterACT network object group defined in the previous command:

```
access-list 101 deny ip object-group FS_GROUP_3 any
access-group 101 in interface outside
```

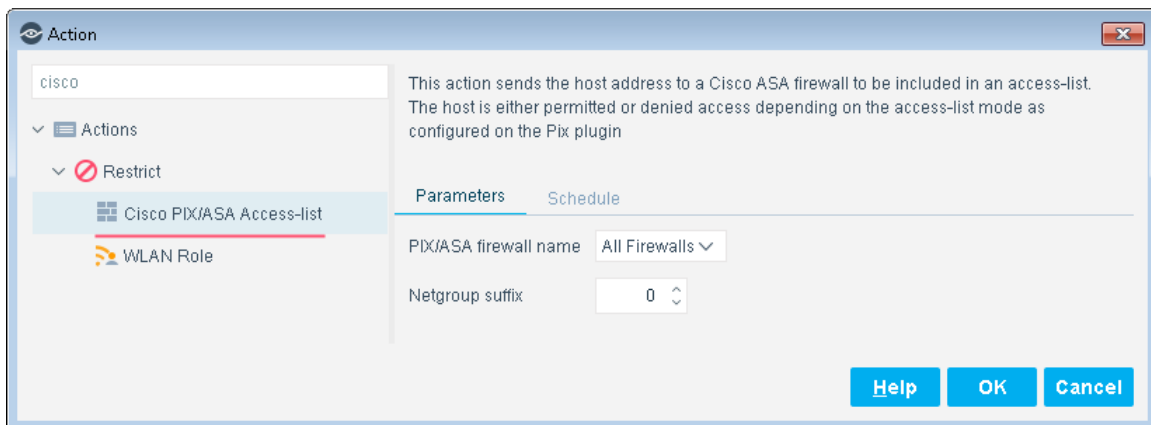
The access-list restrictions apply to the hosts in the FS_GROUP_3 network object group.

Remember to:

- Define all target firewalls in the module configuration pane.
- Copy these object group and access-list definitions to all the firewalls on which you want to implement the action.

Cisco PIX/ASA Access-list Action

This action adds hosts that satisfy the conditions of a policy to a network object group on PIX/ASA firewalls. This object group is referenced by a predefined access list.



The following options are available for this action:

- **PIX/ASA firewall name** – specifies the firewall on which the host is added to the network object group. Select **All Firewalls** to can add the host on all firewalls defined in CounterACT.
- **Netgroup suffix** – a numerical suffix that specifies the target network object group. This suffix is combined with the Network Group Name label configured for the module.

Select the **Schedule** tab to apply standard action scheduling options to this action.

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**.

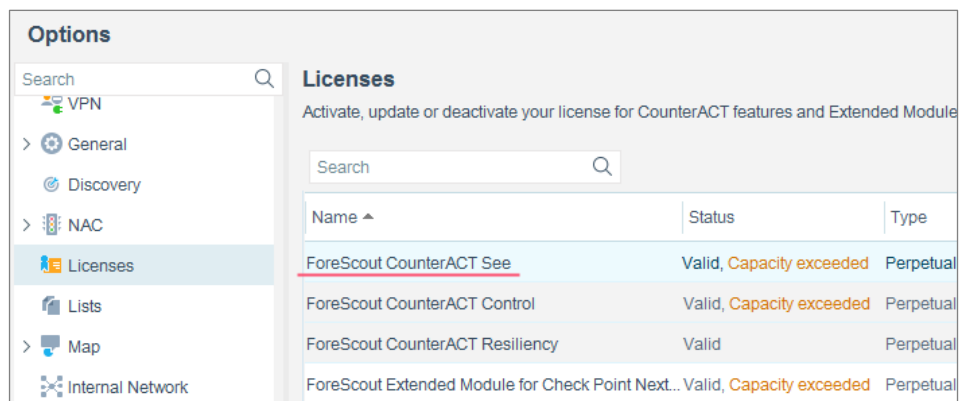
Documentation Portal

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.



Name	Status	Type
ForeScout CounterACT See	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Control	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Resiliency	Valid	Perpetual
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.

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