



CounterACT[®] VPN Concentrator Plugin

Configuration Guide

Version 4.0.7 and Above

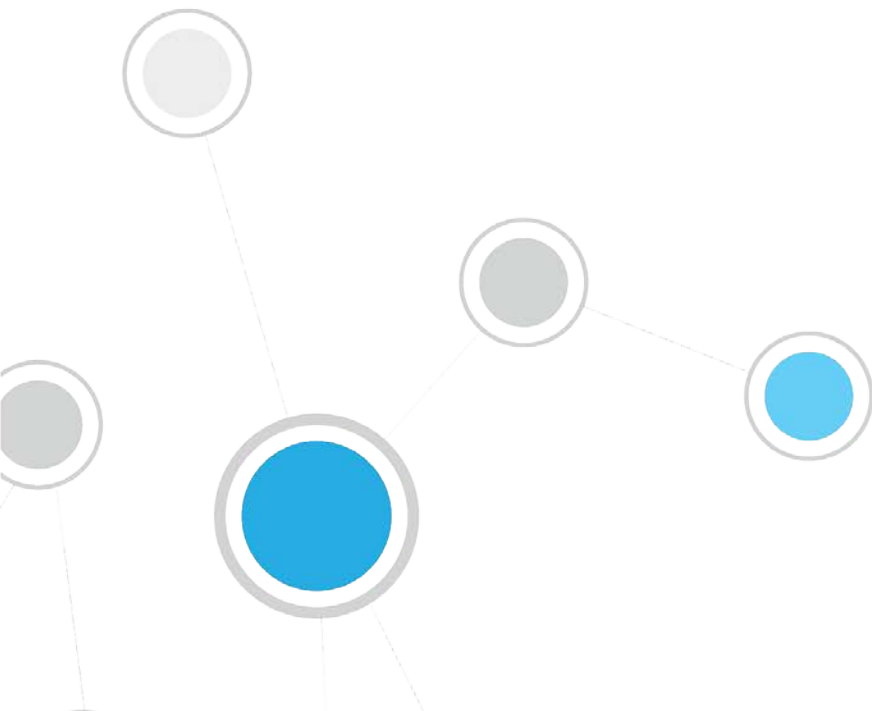


Table of Contents

About the VPN Concentrator Plugin.....	3
Supported VPN Devices.....	3
Supported Authentication Methods	3
Installation.....	3
What to Do After Installation	4
Setup Procedures	5
RADIUS Server Setup	5
Active Directory Setup	5
Additional Setup.....	5
Configuring CounterACT to Work with the VPN Device.....	8
Define Global Plugin Timeouts.....	16
Testing the Configuration	17
CounterACT Policies for VPN Management	18
VPN Host Properties.....	18
The VPN Block Action.....	19
Additional CounterACT Documentation	21
Documentation Portal	21
Customer Support Portal	22
CounterACT Console Online Help Tools.....	22

About the VPN Concentrator Plugin

The VPN Concentrator Plugin is used to track VPN users, disconnect them from the VPN and prevent them from reconnecting. Blocking is carried out by communicating with multiple VPN devices and an authentication server. The authentication server can be either a RADIUS server or an Active Directory server.

Supported VPN Devices

The VPN Concentrator plugin supports the following server packages:

- Cisco VPN 3000 software version 4.1.5 or higher
- Cisco VPN ASA 5500 Series Adaptive Security Appliance
- Juniper 5.5R1 (build 11711) or higher
- Nortel V07_00.062 or higher

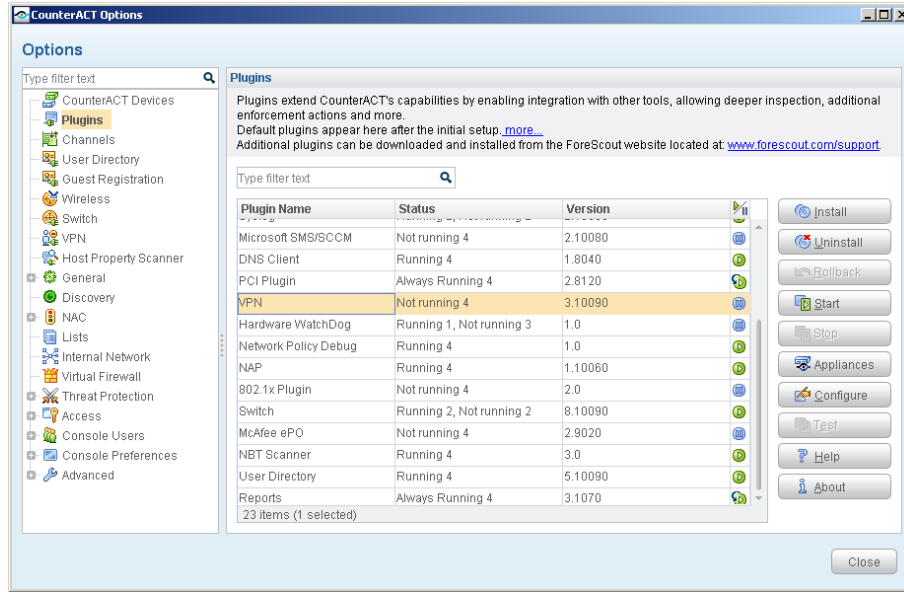
Supported Authentication Methods

- RADIUS
- Active Directory

Installation

To install the plugin:

1. Navigate to the [Customer Support, Base Plugins](#) 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.
4. Select **Plugins**. The Plugins pane opens.
5. Select **Install**. The Open dialog box opens.
6. Browse to and select the saved plugin `.fpi` file.
7. Select **Install**.
8. An installation or upgrade information dialog box and a license agreement dialog box will open. Accept the license agreement to proceed with the installation.
9. Once the installation is complete, select **Close**. The plugin is listed in the Plugins pane.

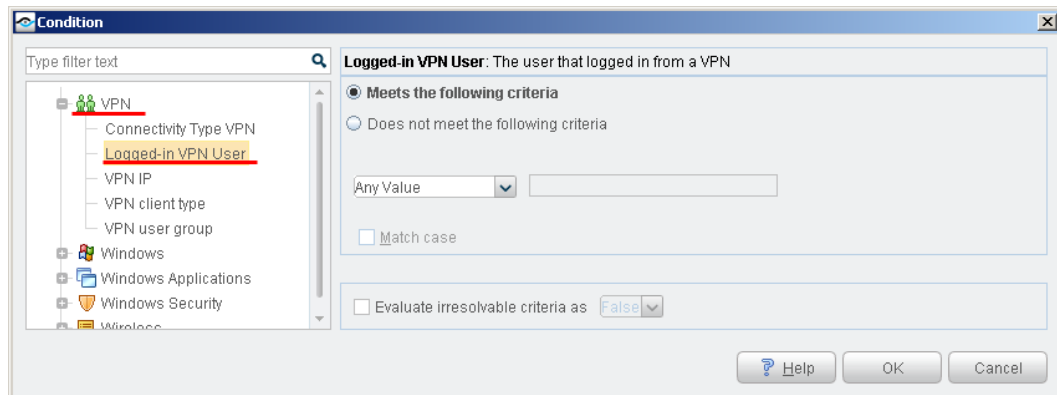


What to Do After Installation

After installing the plugin:

1. Review the set-up instructions described in this document. See [Setup Procedures](#).
2. Configure the plugin. See [Configuring CounterACT to Work with the VPN Device](#)
3. Perform the test (**Test** button). [Testing the Configuration](#).
4. At the Console, define the required policy to carry out VPN blocking. You can utilize the following properties when investigating hosts:
 - VPN Connectivity Type
 - Logged in VPN user
 - VPN IP
 - VPN User Group

Refer to the online Help for more information about working with policies.



Setup Procedures

This section describes the following setup procedures.

- [RADIUS Server Setup](#)
- [Active Directory Setup](#)
- [Additional Setup](#)

RADIUS Server Setup

When RADIUS is used, blocking is performed by configuring the Appliance to act as a proxy between the concentrator and the actual RADIUS server. To do this, you must configure the concentrator to use the Appliance as the RADIUS server, and configure the RADIUS server to accept the Appliance as a RADIUS client.

Access to the user is then blocked by rejecting authentication requests. This effectively stops admission to the network. Since the block is associated with the user, only that user will be blocked. When trying to reconnect, the plugin will be able to identify the authentication attempt and reject it.

After you have defined the configured parameters, you should configure the VPN concentrator to use the Appliance as its first authentication RADIUS server and configure the original RADIUS server as the second on the list.

Additionally, you should configure the RADIUS server to allow requests from the appliance. This requires assigning a server secret at the VPN and the original RADIUS server that are identical, and using this server secret for connection between the appliance and secondary RADIUS Server.

You must also allow access from the appliance to the original RADIUS server.

After configuration, all further authentication requests will go through the appliance, allowing the blocking to occur.

Active Directory Setup

When Active Directory is used, blocking is performed by disabling the blocked user on the Active Directory server. To do this, you must configure the appliance to use an administrative privileged account.

Other than the plugin configuration parameters described above, no other set-up is required for working with Active Directory.

Additional Setup

Enabling the Plugin

To enable the VPN Plugin, disconnect active VPN sessions and set the `readonly` entry in the `snmp_community` section to `2`, as shown in the following example:


```
[snmp_community 1]
name=0x3C.0xB6.0xCD.0xC4.0x27.0x5A.0x8A.0xCD
readonly=2
```

Cisco VPN3k

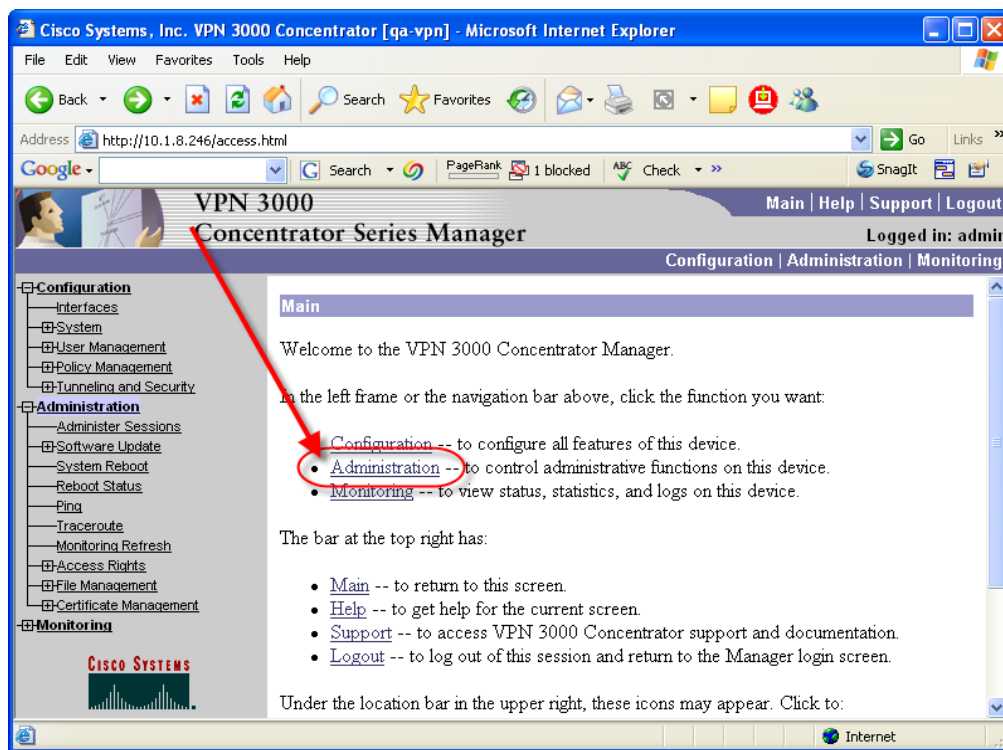
The VPN Plugin should use only SNMPv1 to handle Cisco VPN3k.

Configure Read/Write permissions

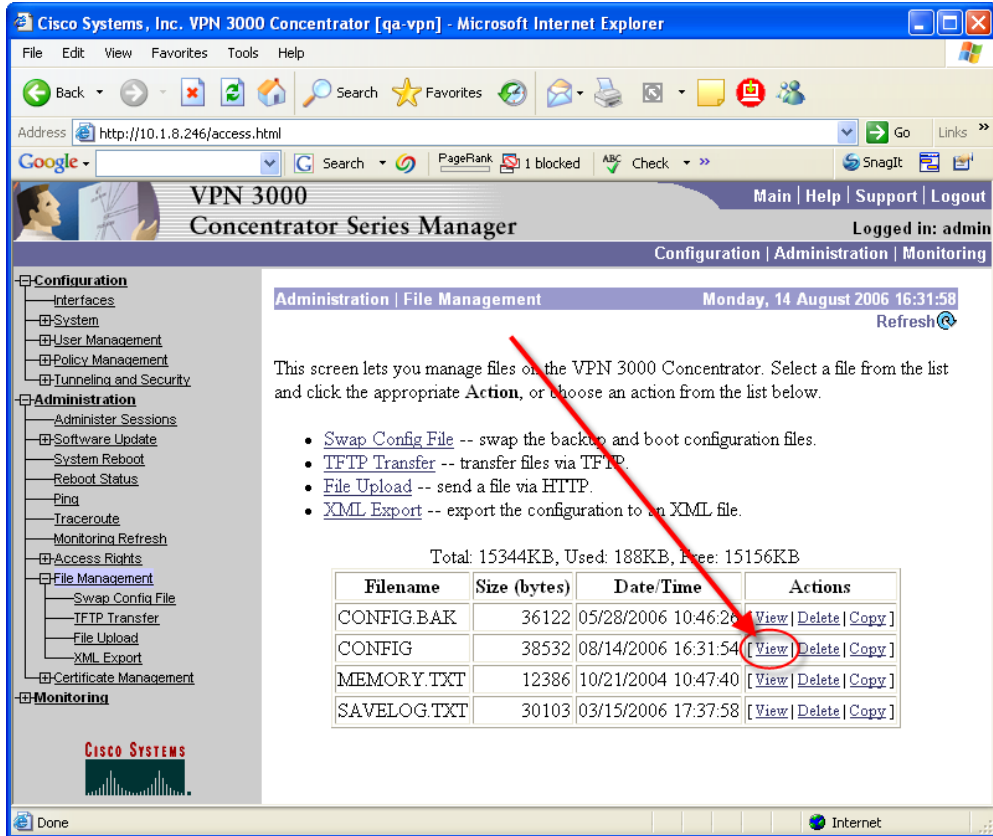
You should modify the VPN concentrator SNMP community to support both read and write. This is done by editing the VPN CONFIG file.

 *If you use FTP to edit and distribute the VPN configuration file, the VPN may require a restart to implement configuration changes.*

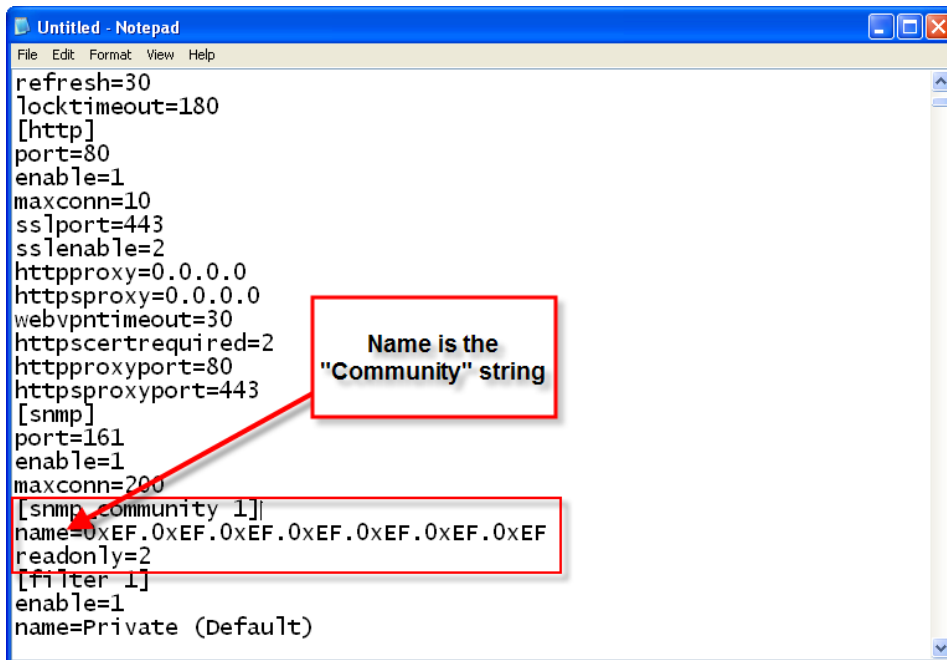
1. Log in to VPN concentrator.
2. Select **Administration > File Management**.



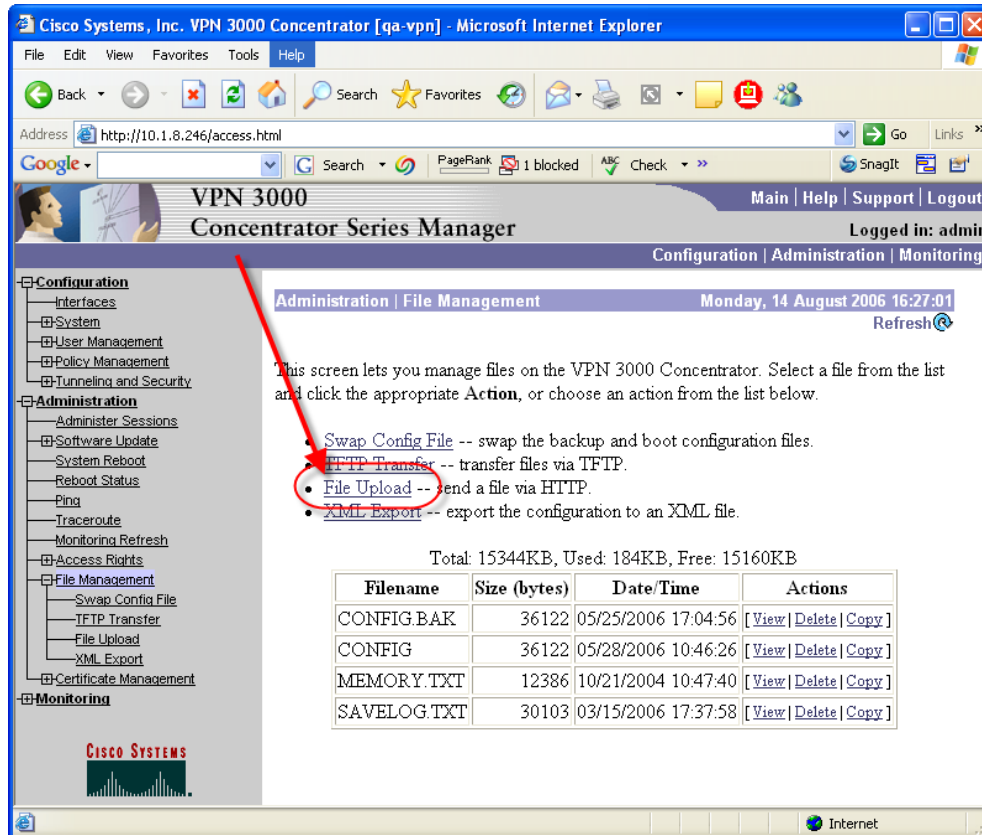
3. View the CONFIG file.



4. Save the file to your local directory as `vpn_config.txt`. It is very important that you save the file with a `txt` extension; otherwise, the VPN concentrator will not start.



5. Edit the file `vpn_config.txt`: To enable each community string for read-write, enter the number 2 for read-only entry.
6. Upload the edited file to the VPN concentrator: Select **Administration > File Management > File Upload**.



7. The File on the VPN Concentrator should be CONFIG; the local file should be your `vpn_config.txt`.
8. Reboot the VPN concentrator: Select **Administration > System Reboot** and choose the Reboot without saving the active configuration option.

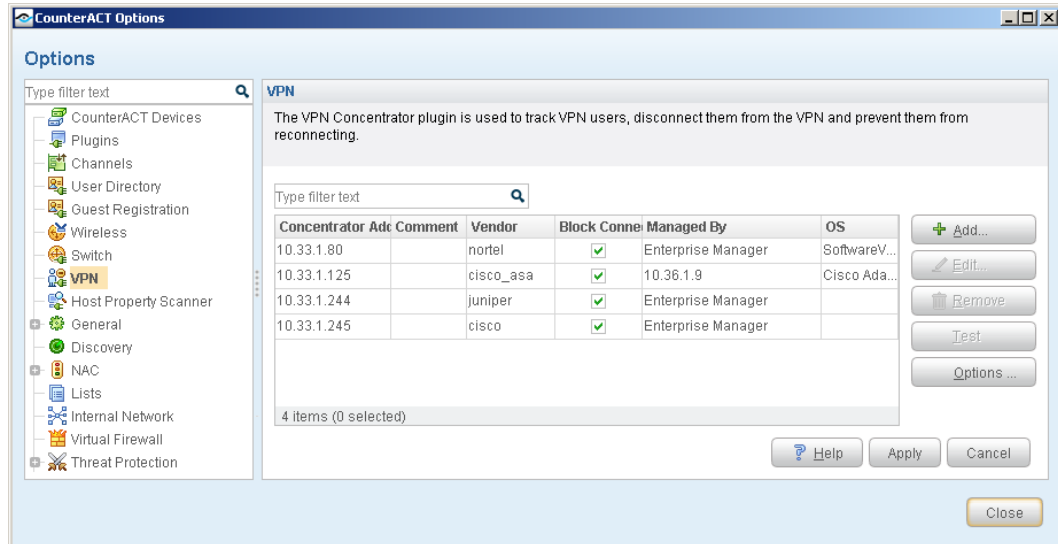
Configuring CounterACT to Work with the VPN Device

This section describes how to configure VPN devices to communicate with CounterACT.

- 📄 You may not have the required user Scope permissions to configure VPN devices or work with the IP addresses assigned to them. If this happens you will receive an error message when attempting to configure the device. Contact your CounterACT Administrator if required.

To define general parameters:

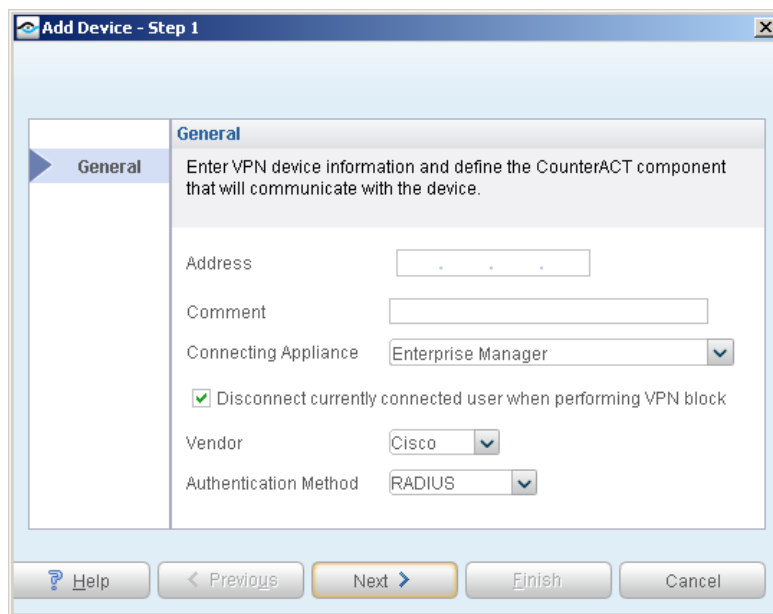
1. Select **Options** from the **Tools** menu and then select **Plugins**.
2. Select **VPN** from the Plugins folder.



3. Select **Add**. The General page of the Add Device wizard opens.

General Page

4. Enter VPN device information and define the CounterACT component that will communicate with the device. This information must be synchronized with the VPN itself.



Field Name	Description
------------	-------------

Field Name	Description
Address	Enter the IP address of the VPN device.
Comment	Enter comments about the device.
Connecting Appliance	<p>Select the name of the CounterACT component that will communicate with this VPN device.</p> <p>Certain Appliances or certain IP assignments made to a particular Appliance may be out of your user <i>Scope</i>. When this happens, you may only view the Appliance configuration and not change it. Appliances that contain Hosts IP assignment out of your <i>Scope</i> will appear with an empty red circle or red circle with a line through it.</p> <p>An empty red circle indicates that you don't have access to any IP addresses managed by the Appliance. A circle with a line indicates that you have partial access.</p> <p>An Appliance with an assignment that is completely outside the user scope is not shown in the drop-down list.</p>
Disconnect currently connected user	<p>Select the checkbox to disconnect immediately and prevent the VPN user from reconnecting.</p> <p>Clear the checkbox to prevent the VPN user from connecting after the current session closes.</p>
Vendor	Select a VPN vendor. The configuration options that follow vary depending on the selected vendor.
Authentication Method	<p>RADIUS or Active Directory</p> <p>The configuration options that follow vary depending on the selected authentication method selected.</p> <p>You may only assign one authentication method type per Appliance. If you edit your configuration on a specific Appliance, the edited change will be applied to all configurations for that Appliance.</p>

5. Select **Next**. The Credentials page of the Add Device wizard opens.

Credentials Page

6. Define access credentials for the VPN device you are configuring.

Cisco Credentials Page

Field Name	Description
Community	Type a unique name for this user group and confirm it
SNMP Params	Type SNMP access parameters. These include the SNMP version (1, 2 or 3) and a community string (for SNMPv1 and SNMPv2c) or user and password (for SNMPv3). The parameters are indicated using the 'snmpwalk' utility format. The VPN Plugin should use only SNMPv1 to handle Cisco VPN3k. Include format (for example): <ul style="list-style-type: none"> ▪ SNMPv1: -v 1 -c <community_name> ▪ SNMPv2: -v 2 -c <community_name> ▪ SNMPv3: -v 3 -u <user> -A <password >

Juniper Credentials Page

Field Name	Description
User	The user logged in to the VPN device.
Password	The password of the user.
Realm	Enter the realm name (group) of the admin user, who is configured here.
Administrative URL Path	Enter a Sign-in administrative URL path.

Administrator URLs	Sign-In Page	Authentication Realm(s)
<input type="checkbox"/> */admin/	Default Sign-In Page	Admin1 Users, Admin Users
<input type="checkbox"/> */admin/	Default Sign-In Page	Admin1 Users
<input type="checkbox"/> */admin/	Default Sign-In Page	Admin Users

Nortel / Cisco ASA Credentials Page

The screenshot shows a configuration window titled "Add Device - Step 2 of 3". On the left, a sidebar lists "General" (with a green checkmark), "Credentials" (selected), and "Radius Authentication". The main content area is titled "Credentials" and contains the following sections:

- Enter access credentials to the VPN.**
- Login Params**
 - User: [text input]
 - Password: [text input]
 - Confirm password: [text input]
- Enable Privileged Params**
 - Enable Privileged Access
 - Use login params: Use login params
 - Password: [text input]
 - Confirm password: [text input]
- Others Params**
 - Group: [text input with "/Base" entered]
 - Connection Method: SSH (dropdown menu)

At the bottom, there are buttons for "Help", "Previous", "Next" (highlighted), "Finish", and "Cancel".

Field Name	Description
User	The user that connects via SSH/telnet to the VPN device.
Password	The password of the user.
Enable Privileged Access	(Cisco ASA only) Select the checkbox to enable privileged access based on the default login parameters defined above, or custom login parameters defined below.
Use login params	Select the checkbox to enable privileged parameters based on the Login parameters defined above.
Password	Enter the privileged password.
Group	(Nortel only) A group name to communicate between the client and VPN. End the entry with a period.
Connection Method	A protocol to be used between the Appliance and the VPN.

The admin user must have permission to change the terminal paging. If this permission is not defined, the plugin configuration test for the VPN device will fail and the plugin cannot manage that VPN device. The plugin uses the following terminal paging commands:

- For Cisco ASA: `terminal pager 0`
- For Nortel: `terminal paging off`

7. Select **Next**. The Radius Authentication page or Active Directory authentication page opens, depending on the authentication method you chose.

Radius Authentication Page

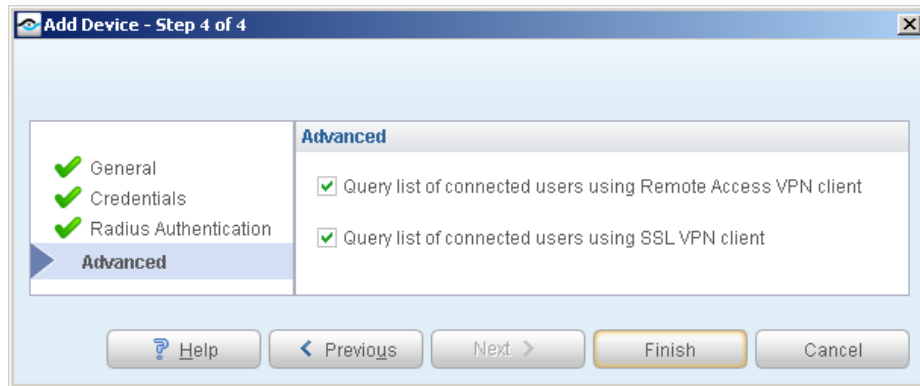
If the Authentication Method is not **RADIUS**, skip this step.

8. Enter credentials required to access the RADIUS or authentication server.

Field Name	Description
Local RADIUS Port	The UDP port for receiving authentication requests from the VPNs. This port must be different from the 802.1x plugin local port.
RADIUS Server Address	The original RADIUS server IP address. This is the RADIUS server the VPN concentrator is initially configured to work with.
RADIUS Server Port	The port for sending authentication requests to the original RADIUS server.
RADIUS Server Secret	The secret for the original RADIUS server.

Cisco ASA – Advanced RADIUS Options

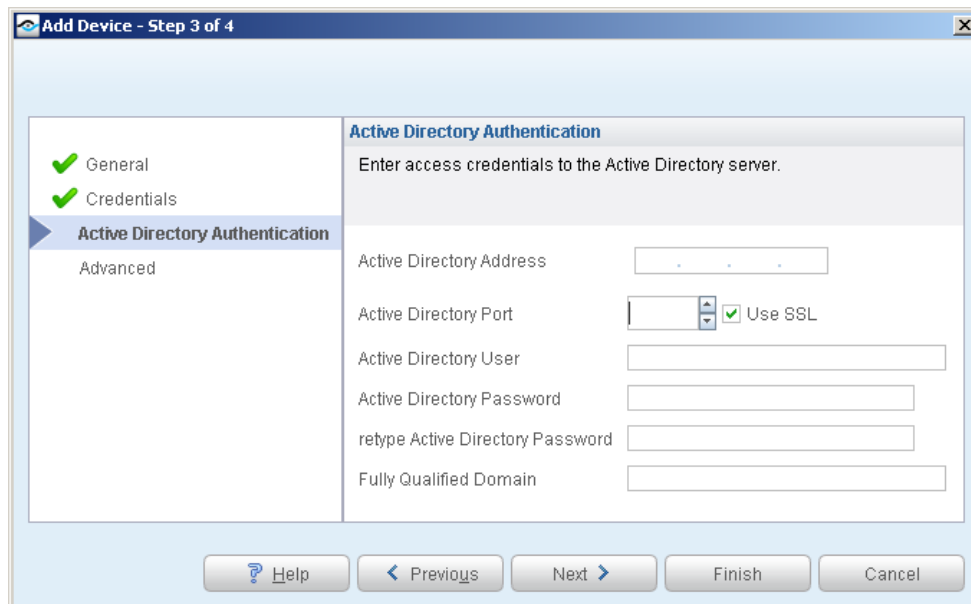
Advanced options are available for Cisco ASA VPN devices that support both Remote Access and SSL connection methods. Disable an option if you do not want the Appliance to be able to block users that connect with that method.



Active Directory Authentication Page

If the Authentication Method is not **Active Directory**, skip this step.

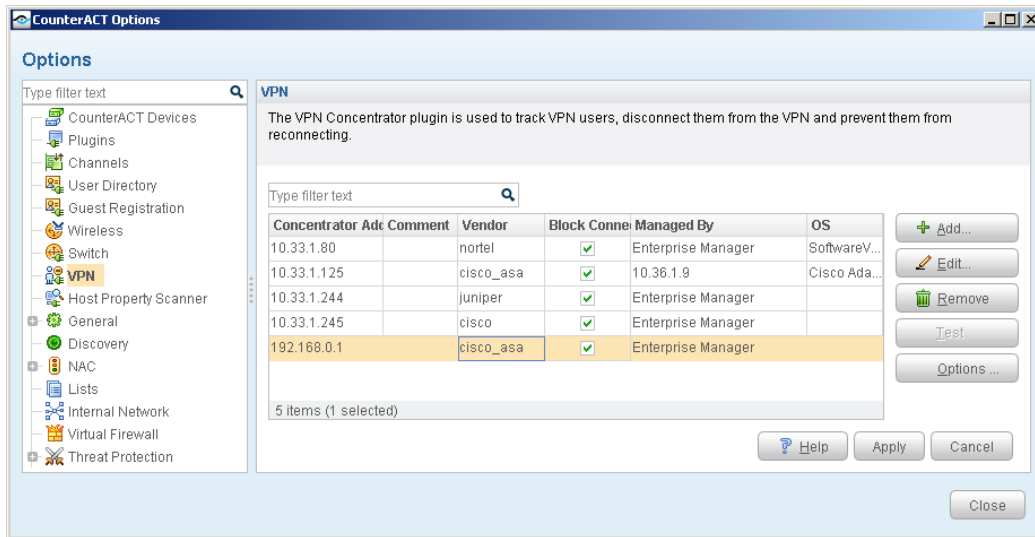
9. Enter credentials required to access the Active Directory server.



Field Name	Description
Active Directory Address	The Active Directory server IP address. This is the server the VPN concentrator is configured to work with.
Active Directory Port	The port used for sending authentication requests to the Active Directory server (default: 389/TCP).
Use SSL	Select this checkbox to apply SSL encryption to communication with the Active Directory server.
Active Directory User	The Active Directory user who is associated with the administrator's or account operator's groups.

Field Name	Description
Active Directory Password	The password of the Active Directory user.
Fully Qualified Domain	The Active Directory domain full name. It is recommend to use upper case letters.

10. Select **Finish** when you are done configuring the VPN device. The configuration appears in the VPN Pane.



The following information is displayed:

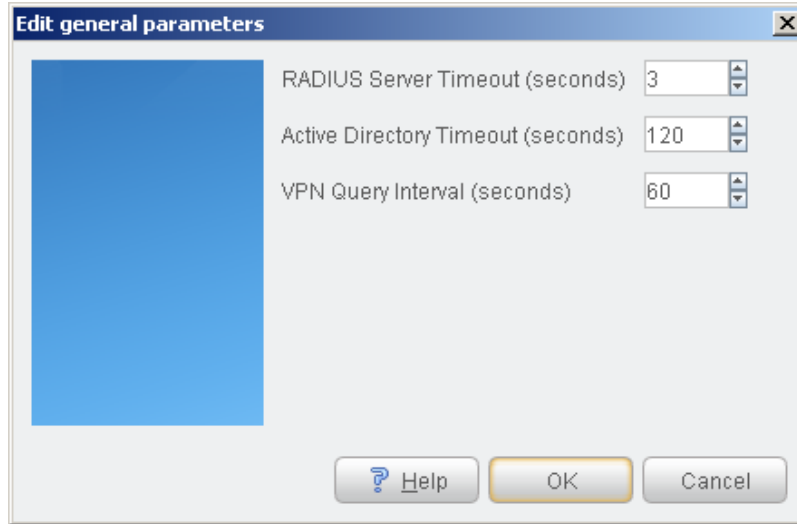
Item	Description
Concentrator Address	The IP address of the VPN device that you added
Comment	Comments that you added
Vendor	The device vendor
Block Connected	Indicates if VPN blocking is enabled
Managed By	The CounterACT component that manages this VPN device
OS	The vendor operating system

Define Global Plugin Timeouts

Define global plugin settings. These settings are applied to all VPN configurations.

To define global plugin parameters:

1. Select **Options** from the VPN pane. The Edit general parameters dialog box opens.



Field Name	Description
RADIUS Server Timeout (seconds)	The time to wait for the original RADIUS server to authenticate a user.
Active Directory Timeout (seconds)	The Active Directory connection timeout.
VPN Query Interval (seconds)	The interval at which to query the VPN for the connected hosts.

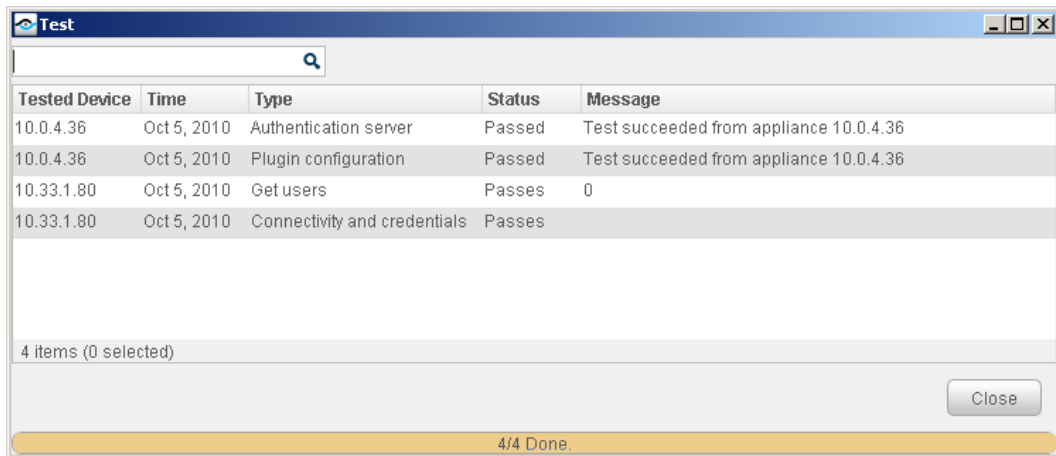
Testing the Configuration


You can check connections, parameters, and access to the Active Directory. Perform this test after adding, editing, or removing VPN parameters.

To test:

1. Select **Options** from the Tools menu.
2. Select **VPN**. The VPN pane opens.
3. Select one or several configurations.
4. Select **Test**.

5. The Test dialog box appears with VPN test parameter information.

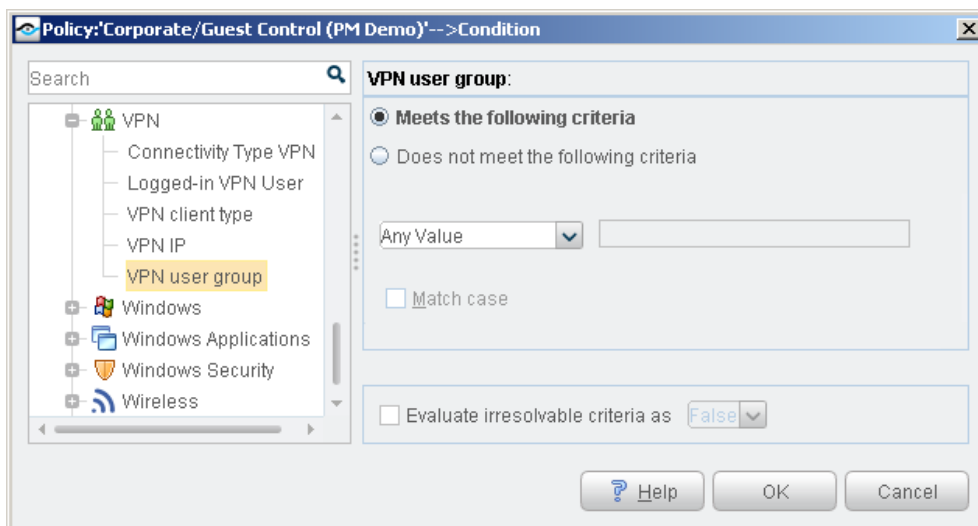


6. Use the **Filter** field to quickly locate a type, for example type **P** and the “Plugin configuration” rows appear on the top of the list.
-  *Even if you do not save the plugin parameter changes, the test uses the edited parameters.*

CounterACT Policies for VPN Management

This section describes host properties and actions provided by the plugin. Use these properties and actions to create CounterACT policies that detect and manage VPN endpoints.


VPN Host Properties

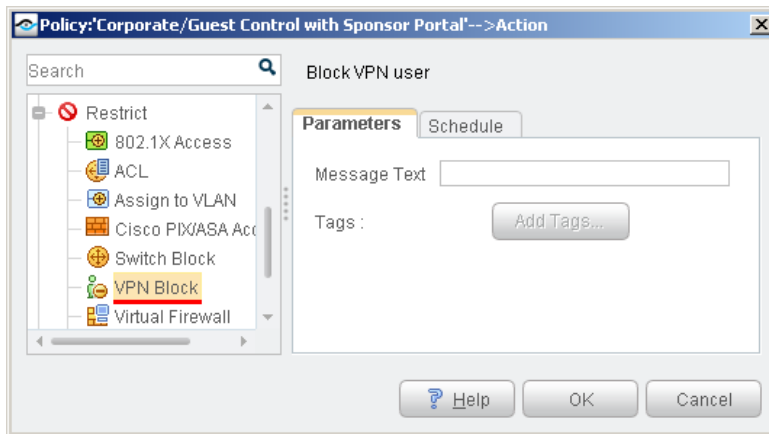


The following host properties report VPN related information.

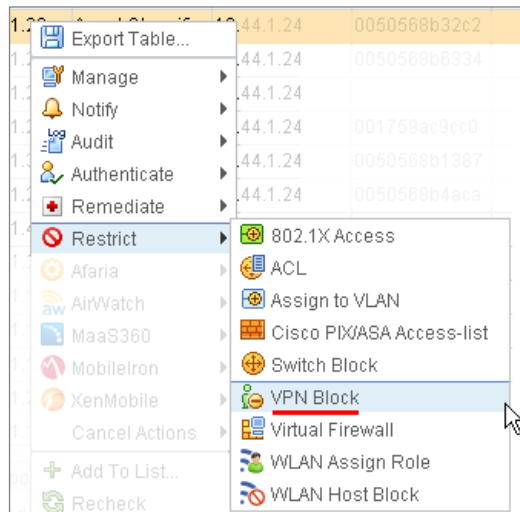
Connectivity Type VPN	A Boolean value that indicates whether the user is connected through a VPN.
Logged-in VPN User	The username under which the host is logged in to the VPN.
VPN client type	The authentication method or tunneling protocol used by the VPN.
VPN IP	The IP of the VPN concentrator to which the endpoint is connected.
VPN user group	The User Group through which the endpoint connects to the corporate network.

The VPN Block Action

The *VPN Block*  action prevents a user from connecting through a VPN.



When the *VPN Block* action is used in a policy rule, each user that matches the conditions of the rule is blocked. You can also apply the action to selected users from the NAC or Inventory views of the Console.



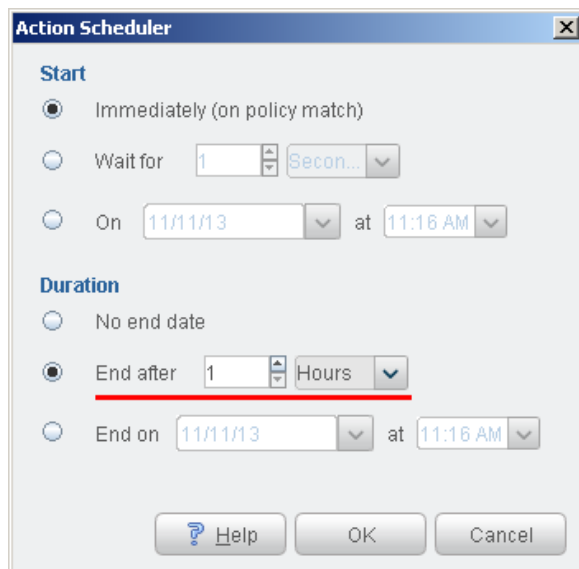
When you use this action, you specify a message text that is displayed to the blocked user if they attempt to reconnect. To include host-specific property values, select **Add Tags** and add Property Tags that resolve to host property values when the message is created. The message text is only seen on the endpoint when attempting to reconnect via Cisco ASA configured with Radius as the *Authentication Method*.

- 📄 *Only add tags that reference single-value properties. You cannot add tags that refer to list or composite properties.*

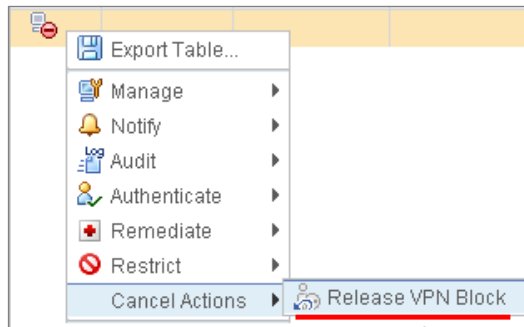
CounterACT must explicitly cancel the VPN block action to allow the user to log in again. Unlike other block actions, this action blocks a *user account* rather than a network endpoint. However, CounterACT policies act on network endpoints. When the blocked user's endpoint device no longer matches the conditions of the blocking rule – for example, if the user removed forbidden file sharing applications – this endpoint device is no longer blocked, but the *user account* still cannot access the network, using this device or any other device.

The *VPN Block* action is enforced until one of the following situations explicitly cancels the VPN block, letting the VPN user access the network again:

- **Schedule settings of the action or policy end the action.** It is recommended to define a duration of 1 hour for this action. This prevents users from accessing the network, but allows them to correct security breaches on their devices and log in again to the network. If a user still matches blocking policy conditions, the *VPN Block* action will be applied each time they log in.



- **An administrator manually cancels the action from the NAC or Inventory views of the Console.**



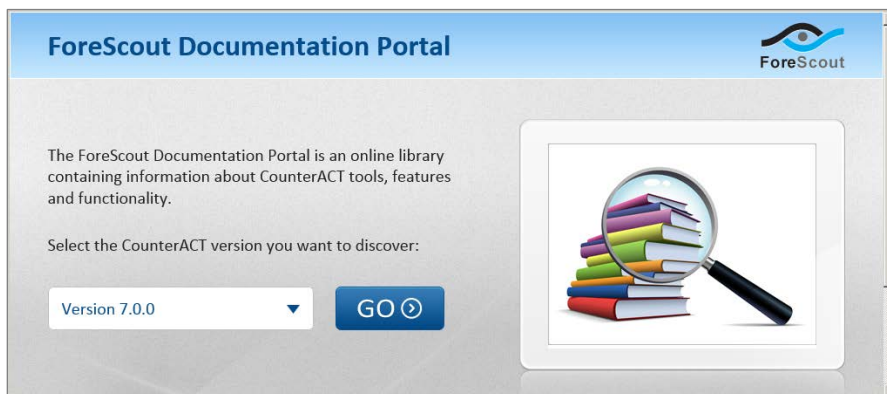
Additional CounterACT Documentation

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:

1. Go to www.forescout.com/kb.
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:

1. Go to <https://updates.forescout.com/support/index.php?url=counteract>.
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 a valid written agreement signed by you and ForeScout that governs the below ForeScout products and services:

- If you have purchased any ForeScout products, your use of such products 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 have purchased any ForeScout Professional Services, the provision of such services is subject to your acceptance of the terms set forth at <http://www.forescout.com/professional-services-agreement/>;
- 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

2017-04-05 14:18