



Forescout

Network Module: VPN Concentrator Plugin

Configuration Guide

Version 4.3.1



Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

<https://www.Forescout.com/support/>

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the Technical Documentation page on the Forescout website for additional documentation: <https://www.Forescout.com/company/technical-documentation/>
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

© 2020 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.

2020-07-09 09:00

Table of Contents

About the VPN Concentrator Plugin.....	4
Overlapping IP Address Support.....	4
Supported Vendor Products	4
Supported Authentication Methods	4
What to Do	4
Requirements.....	5
Forescout Requirements.....	5
Setup Procedures	5
RADIUS Server Setup	5
Active Directory Setup	6
Additional Setup.....	6
Enabling the Plugin.....	6
Cisco VPN3k	6
Configure Read/Write permissions	6
Configuring Forescout to Work with the VPN Device	9
General Page	10
Credentials Page	12
Radius Authentication Page	16
Active Directory Authentication Page.....	17
Define Global Plugin Timeouts.....	19
Certificate Management	20
VPN Pane Display	20
Verify That the Plugin Is Running	21
Test the Plugin Configuration for VPN Device Management	21
Policies for VPN Management.....	22
Property Resolution	22
VPN Block Action	23
Appendix A: CLI Commands for Cisco ASA VPN Devices	26
Network Module Information	27
Additional Forescout Documentation.....	27
Documentation Downloads	27
Documentation Portal	28
Forescout Help Tools.....	28

About the VPN Concentrator Plugin

The VPN Concentrator Plugin is a component of the Forescout® Network Module. See [Network Module Information](#) for details about the module.

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.

Overlapping IP Address Support

The VPN Concentrator Plugin supports working with networks that use overlapping IP addresses. For details about enabling and configuring the Forescout platform's support of overlapping IP address use in an enterprise's network, refer to the *Forescout Working with Overlapping IP Addresses How-to Guide*. See [Additional Forescout Documentation](#) for information on how to access this document.

Supported Vendor Products

The VPN Concentrator Plugin supports working with the following VPN device vendors:

- Cisco
- Pulse Secure (Juniper)
- Nortel

For information about the vendor models (hardware/software) and versions (product/OS) that are validated for integration with this Forescout component, refer to the [Forescout Compatibility Matrix](#).

Supported Authentication Methods

The VPN Concentrator Plugin works with any of the following authentication servers:

- Active Directory
- RADIUS

What to Do

1. Verify that you have met system requirements. See [Requirements](#).
2. Review the set-up instructions described in this document. See [Setup Procedures](#).
3. Configure the plugin. See [Configuring Forescout to Work with the VPN Device](#).
4. Perform the test. See [Test the Plugin Configuration for VPN Device Management](#).

5. At the Console, define the required policy to carry out VPN blocking. See [Policies for VPN Management](#).

Requirements

This section describes the following requirements for running VPN Concentrator Plugin:

- [Forescout Requirements](#)

Forescout Requirements

The following Forescout platform and component versions must be running in your Enterprise Manager and your Appliances:

- Forescout interim release 8.2.1
- Network Module 1.2.1 with the VPN Concentrator Plugin
- If you are using Flexx licensing, ensure that you have a valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the component. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing Flexx licenses.

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 Concentrator 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

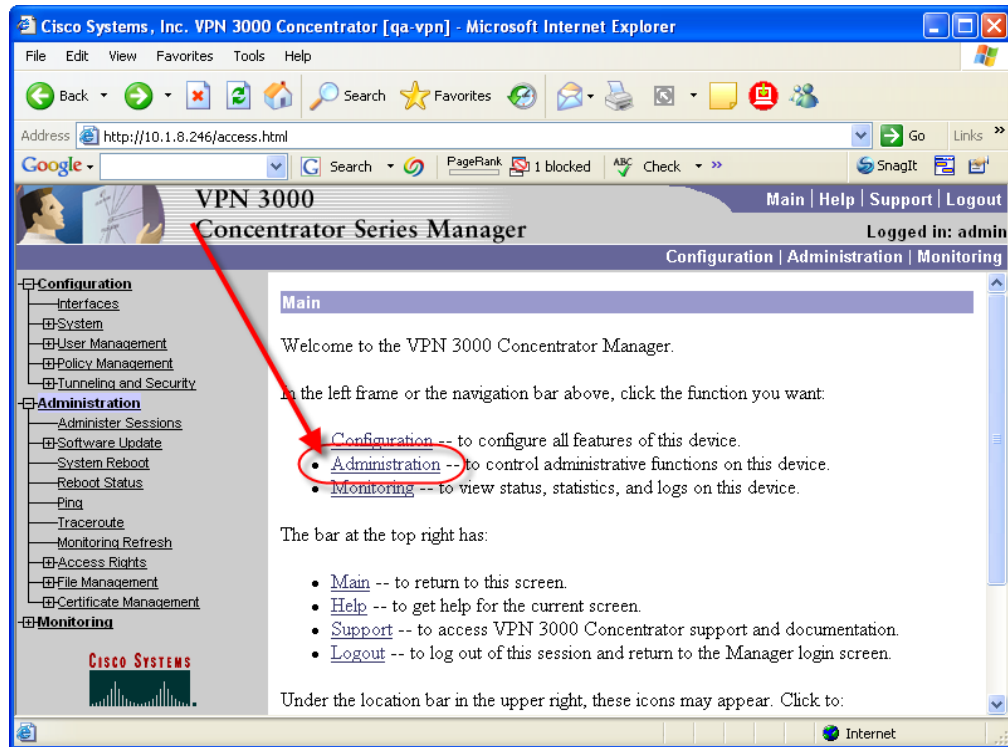
The VPN Concentrator Plugin must only use SNMPv1 to handle Cisco VPN3k.

Configure Read/Write permissions

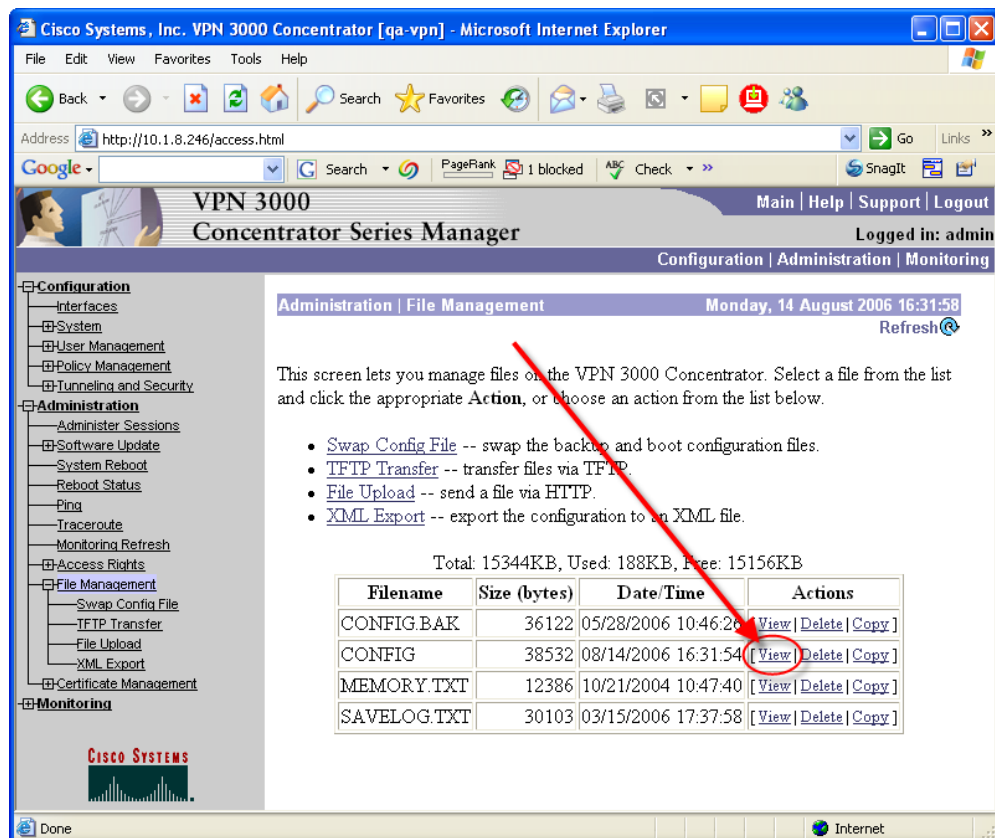
Modify the VPN concentrator SNMP community to support both read and write. This is done by editing the VPN CONFIG file.

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

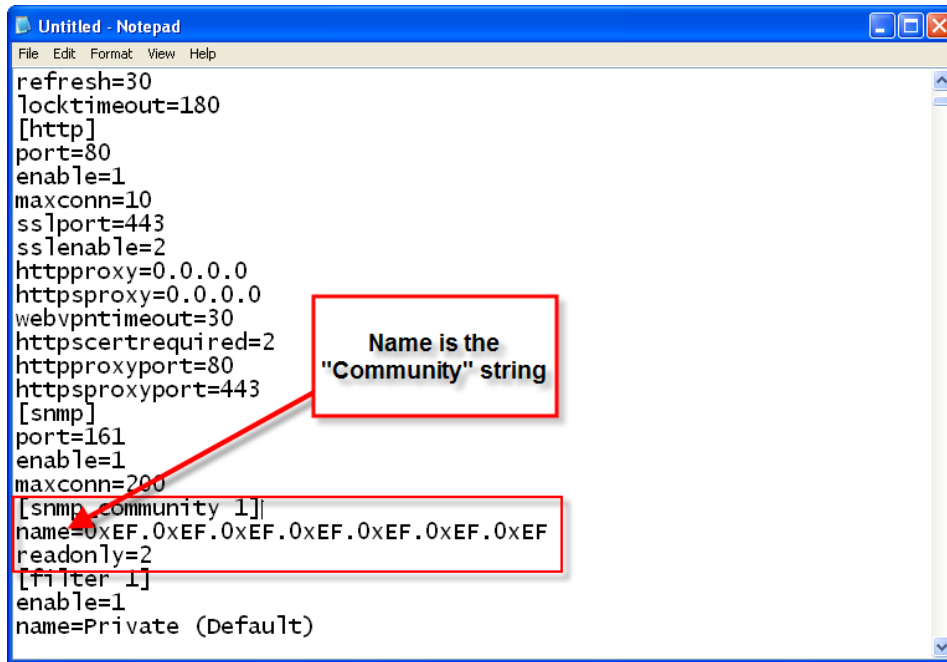
1. Log in to VPN concentrator.
2. Select **Administration > File Management**.



3. View the CONFIG file.

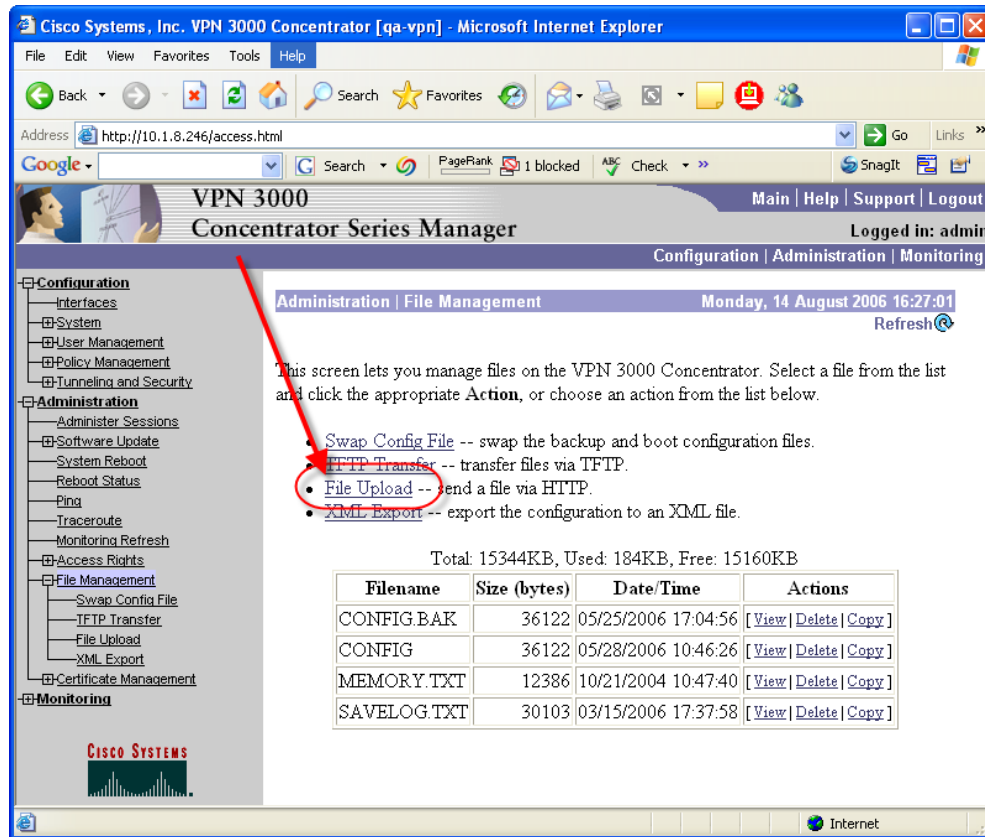


4. Save the file to your local directory as **vpn_config.txt**. It is very important that you save the file with a **.txt** extension; otherwise, the VPN concentrator will not start.



```
refresh=30
locktimeout=180
[http]
port=80
enable=1
maxconn=10
sslport=443
sslenable=2
httpproxy=0.0.0.0
httpsproxy=0.0.0.0
webvpntimeout=30
httpscertrequired=2
httpproxyport=80
httpsproxyport=443
[snmp]
port=161
enable=1
maxconn=200
[snmp community 1]
name=0xEF.0xEF.0xEF.0xEF.0xEF.0xEF
readonly=2
[filter 1]
enable=1
name=Private (Default)
```


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 ForeScout to Work with the VPN Device

This section describes how to configure the VPN Concentrator Plugin to communicate with and manage VPN devices.

-  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 ForeScout Administrator if required.

To define general parameters:

1. From the Console **Tools** menu, select **Options > Modules > Network > VPN > Configure**. The **VPN** pane displays.

VPN
The VPN Concentrator plugin is used to track VPN users, disconnect them from the VPN and prevent them from reconnecting.

Search

Concentrator Address	Comment	Vendor	Block Connected	Managed By	OS	IP Reuse Domain
192.168.2.202@SITE - A		cisco_asa	<input checked="" type="checkbox"/>	192.168.82.43 - Site A	Cisco Adaptive Security A...	SITE - A
192.168.2.202@SITE - B		cisco_asa	<input checked="" type="checkbox"/>	192.168.82.42 - Site B	Cisco Adaptive Security A...	SITE - B

Add **Edit** **Remove** **Test** **Options**

Help **Apply** **Undo**

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

General Page

Enter VPN device information and define the Forescout device (Enterprise Manager or an Appliance) that must communicate with the VPN device. Make sure to synchronize this information with the VPN device.

Add Device - Step 1

General
Enter VPN device information and define the CounterACT component that will communicate with the device.

Address

Comment

Connecting Appliance **Enterprise Manager** ▼

IP Reuse Domain

☒ Disconnect currently connected user when performing VPN block

Vendor **Cisco ASA** ▼

Authentication Method **RADIUS** ▼

Help **Previous** **Next** **Finish** **Cancel**

To configure general information:

1. In the *General* page of the Add Device wizard, define the following:

Field Name	Description
Address	<p>Enter the IP address of the VPN device.</p> <p>When the Forescout platform is enabled to support overlapping IP addresses:</p> <ul style="list-style-type: none"> You can configure the plugin to manage multiple VPN devices all having the same IP address, however for this to be valid, each of these VPN devices must be located within a different IP Reuse Domain (IRD). See the General pane's IP Reuse Domain field.
Comment	Enter comments about the VPN device.
Connecting Appliance	<p>Select from the drop-down list the name of the Forescout device (Enterprise Manager or an Appliance) that must communicate with the 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> appear with either an empty red circle or a red circle with a line through it.</p> <ul style="list-style-type: none"> An empty red circle: Indicates that you do not have access to any IP addresses managed by the Appliance. A circle with a line: Indicates that you have partial access. <p>An Appliance with an assignment that is completely outside the user scope is not shown in the drop-down list.</p>
IP Reuse Domain	<p>This field is view-only field and only appears in the <i>General</i> page/tab when the Forescout platform is enabled to support overlapping IP addresses.</p> <p><i>IP Reuse Domains</i> are used to distinguish several instances of an overlapping IP address. IP addresses are unique in each IP Reuse Domain and cannot overlap within a domain.</p> <p>In order for this field to display an IRD, the following conditions must both be true:</p> <ol style="list-style-type: none"> The selected Connecting Appliance has an IRD assigned to it. The VPN device's IP address is located within the Connecting Appliance's IP segment assignment (scope) that is assigned to the IRD <p>Otherwise, the field displays the value (<i>none</i>) that identifies that the VPN device is not located within an IRD but, rather, is located within the enterprise's default/global network.</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.

Field Name	Description
Authentication Method	<p>Select one of the following authentication methods:</p> <ul style="list-style-type: none"> ▪ RADIUS ▪ Active Directory <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 is applied to all configurations for that Appliance.</p>

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

Credentials Page

Define credentials that the VPN Concentrator Plugin uses to access a plugin-managed VPN device. A unique *Credentials* page displays for the each of following VPN devices:

- [Cisco Credentials Page](#)
- [Juniper/Pulse Secure Credentials Page](#)
- [Nortel/Cisco ASA Credentials Page](#)

Cisco Credentials Page

To configure Cisco credentials:

1. In the *Credentials* page of the Add Device wizard, define the following:

Field Name	Description
Community	Enter a unique name for this user group and confirm it

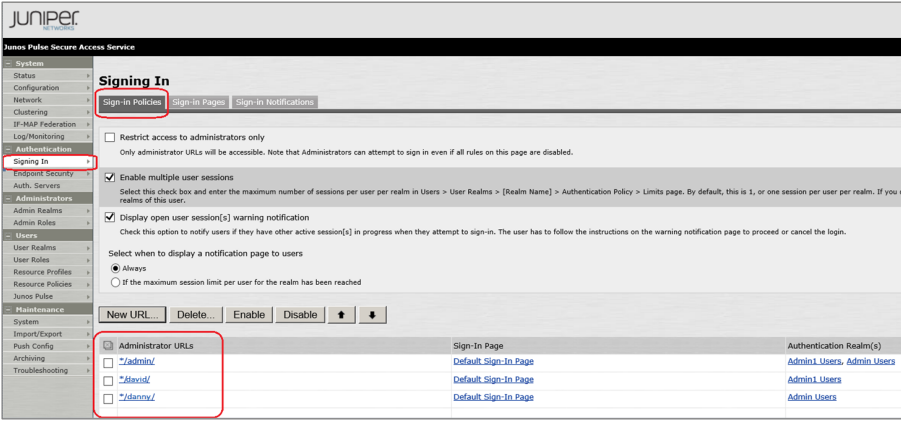
Field Name	Description
SNMP Params	<p>Enter the following SNMP access parameters:</p> <ul style="list-style-type: none"> SNMP version (1, 2 or 3) <p>Note: The VPN Concentrator Plugin must only use SNMPv1 to handle Cisco VPN3k.</p> <ul style="list-style-type: none"> For SNMPv1 and SNMPv2c, a Community string For SNMPv3, a user and password <p>Use the snmpwalk utility format to indicate these parameters.</p> <p>Include format example:</p> <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/Pulse Secure Credentials Page

To configure Juniper/Pulse Secure credentials:

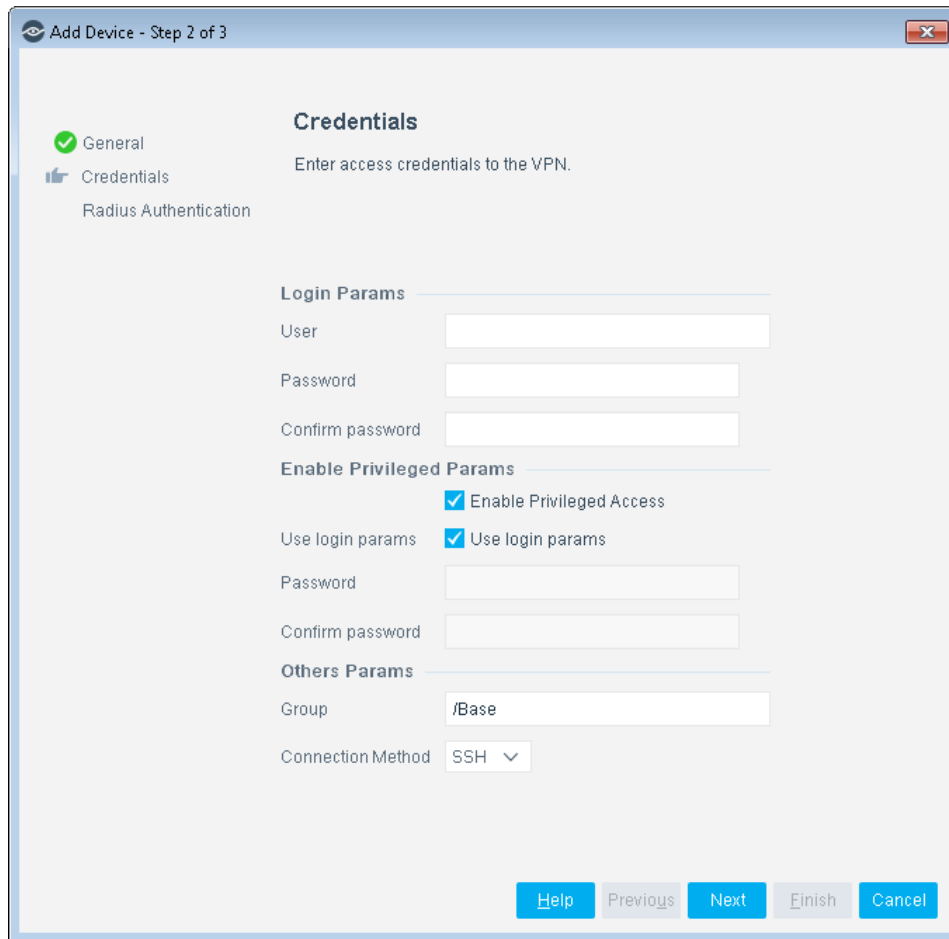
1. In the *Credentials* page of the Add Device wizard, define the following:

Field Name	Description
User	The user logged in to the VPN device.
Password	The password of the user.

Field Name	Description
Realm	Enter the realm name (group) of the admin user, who is configured here.
Administrative URL Path	<p>Enter a Sign-in administrative URL path.</p> 
TLSv1.2	<p>Select this option to instruct the VPN Concentrator Plugin to communicate with the VPN device using TLSv1.2.</p> <ul style="list-style-type: none"> By default, TLSv1.2 is selected. <ul style="list-style-type: none"> If this option is not selected, the plugin uses SSLv2 to communicate with the VPN device. When the Forescout platform runs in Certification Compliance mode, TLSv1.2 is permanently selected. <p>For more information about Certification Compliance mode, refer to the <i>Forescout Installation Guide</i>.</p>

For the certificates required when the plugin is configured to manage a Juniper/Pulse Secure VPN device, see [Certificate Management](#).

Nortel/Cisco ASA Credentials Page



Add Device - Step 2 of 3

Credentials
Enter access credentials to the VPN.

General (checked)
Credentials (selected)
Radius Authentication

Login Params

User:

Password:

Confirm password:

Enable Privileged Params

☒ Enable Privileged Access

Use login params: ☒ Use login params

Password:

Confirm password:

Others Params

Group:

Connection Method:

Help Previous Next Finish Cancel

To configure Nortel/Cisco ASA credentials:

1. In the *Credentials* page of the Add Device wizard, define the following:

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	The connection protocol to be used between the Appliance and the VPN device.

The administrator user must have permission to change the terminal paging. If this permission is not defined, the plugin configuration test for the VPN device fails 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`
2. Select **Next**. Either the Radius Authentication page or the Active Directory authentication page opens, depending on the authentication method you selected in the General page.

Radius Authentication Page

Enter credentials required to access the RADIUS authentication server. If RADIUS is not the authentication method you selected in the *General* page, skip this configuration step.

To configure credentials for plugin access to the RADIUS server:

1. In the *RADIUS Authentication* page of the Add Device wizard, define the following:

Field Name	Description
Local RADIUS Port	The UDP port for receiving authentication requests from the VPNs. This port must be different from the RADIUS 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.

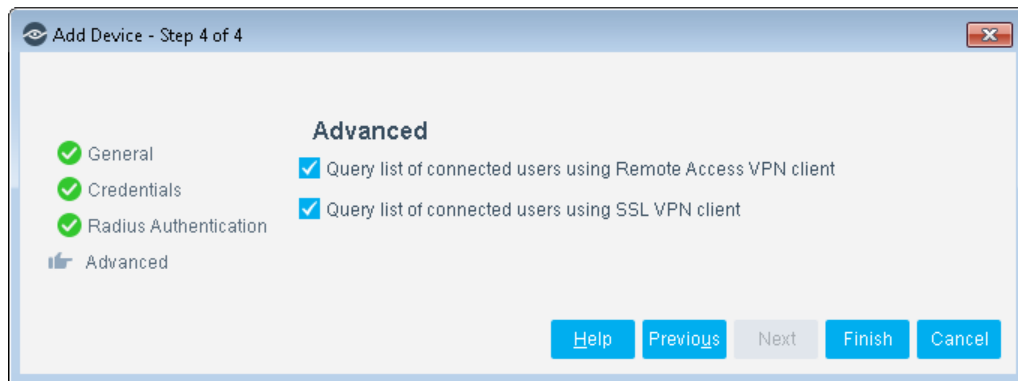
Field Name	Description
RADIUS Server Secret	The secret for the original RADIUS server.

2. Do any of the following:

- a. If you are configuring the plugin to manage a Cisco ASA VPN device using RADIUS as the authentication method, see [Cisco ASA – Advanced RADIUS Options](#).
- b. Select **Finish** when you are done configuring the plugin for management of the VPN device. The configuration appears in the Console *VPN* pane. See [VPN Pane Display](#).

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.



Select **Finish** when you are done configuring the plugin for management of the VPN device. The configuration appears in the Console *VPN* pane. See [VPN Pane Display](#).

Active Directory Authentication Page

Enter credentials required to access the Active Directory server. If *Active Directory* is not the authentication method you selected in the General page, skip this configuration step.

Add Device - Step 3 of 3

Active Directory Authentication
Enter access credentials to the Active Directory server.

☒ General
☒ Credentials
☐ Active Directory Authentication

Active Directory Address:

Active Directory Port: ☒ Use SSL ☐ TLSv1.2

Active Directory User:

Active Directory Password:

retype Active Directory Password:

Fully Qualified Domain:

[Help](#)
[Previous](#)
[Next](#)
[Finish](#)
[Cancel](#)

To configure credentials for plugin access to the Active Directory server:

1. In the Active Directory Authentication page of the Add Device wizard, define the following:

Field Name	Description
Active Directory Address	<p>Specify the Active Directory server that the VPN Concentrator must work with, by entering any of the following:</p> <ul style="list-style-type: none"> ▪ The IPv4 address of the Active Directory server ▪ The FQDN (fully qualified domain name) of the Active Directory server. For example, <i>DCserver1.dom34.mycompany.com</i> <ul style="list-style-type: none"> - When communicating using SSL or TLS, the FQDN entered must match the FQDN that is specified in the Active Directory server's certificate Subject field.
Active Directory Port	<p>Specify the port that the plugin uses to send authentication requests to the Active Directory server. By default, the port value is 636 (TCP)</p>
Use SSL	<p>Select this option to instruct the VPN Concentrator Plugin to apply SSL encryption to communication with the Active Directory server.</p> <ul style="list-style-type: none"> ▪ By default, Use SSL is selected. <ul style="list-style-type: none"> - If this option is not selected, the plugin uses non-encrypted TCP to communicate with the Active Directory server. - If this option is selected and the TLSv1.2 option is not selected, the plugin uses SSLv2/3 to communicate with the Active Directory server. ▪ When the Forescout platform runs in Certification Compliance mode, Use SSL is permanently selected.

Field Name	Description
TLSv1.2	Select this option to instruct the VPN Concentrator Plugin to communicate with the Active Directory server using TLSv1.2. <ul style="list-style-type: none"> By default, TLSv1.2 is selected When the Forescout platform runs in Certification Compliance mode, TLSv1.2 is permanently selected.
Active Directory User	Specify the Active Directory user who is associated with the administrator's or account operator's groups.
Active Directory Password	Specify the password of the Active Directory user.
Fully Qualified Domain	Specify the fully qualified domain name of the Active Directory domain. Forescout recommends using uppercase letters.

For more information about Certification Compliance mode, refer to the *Forescout Installation Guide*.

2. Select **Finish** when you are done configuring the plugin for management of the VPN device. The configuration appears in the Console *VPN* pane. See [VPN Pane Display](#).

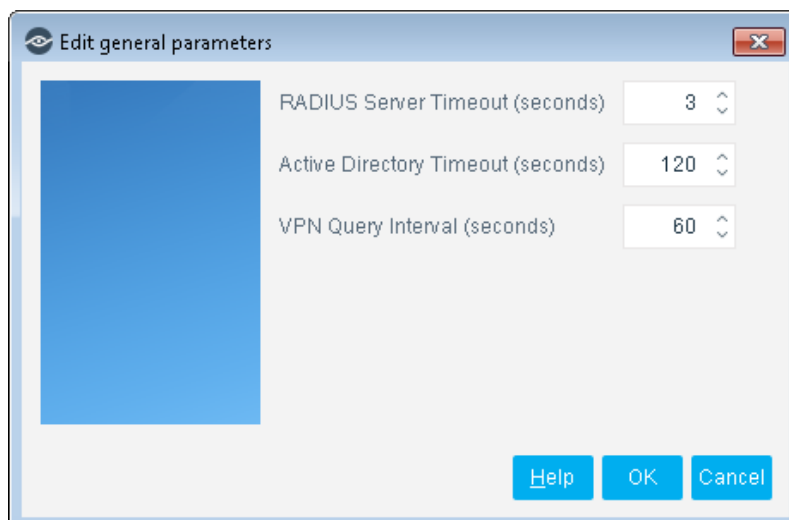
For the certificates required when the plugin is configured to use the Active Directory authentication method, see [Certificate Management](#).

Define Global Plugin Timeouts

Define global plugin settings. These settings apply to all plugin configurations for managing VPN devices.

To define global plugin parameters:

1. In the Console *VPN* pane, select **Options**. The *Edit general parameters* dialog box opens.



2. In the *Edit general parameters* dialog box, modify any of the following fields:

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 device for the connected hosts.

Certificate Management

When the VPN Concentrator Plugin is configured to use either SSL or TLS to establish secure communication connections for the following use cases, you must define certificates:

- The plugin is configured to manage Juniper/Pulse Secure VPN devices. For each Juniper/Pulse Secure VPN device, define that device's trusted certificate chain
- The plugin is configured to use the Active Directory authentication method, define the Active Directory server's trusted certificate chain

Use the Console certificate interface to:

- Configure the certificate authority (CA) trust chain of each plugin-managed Juniper/Pulse Secure VPN device and/or Active Directory server for plugin authentication of these network devices. In the Console, access **Options > Certificates > Trusted Certificates**.

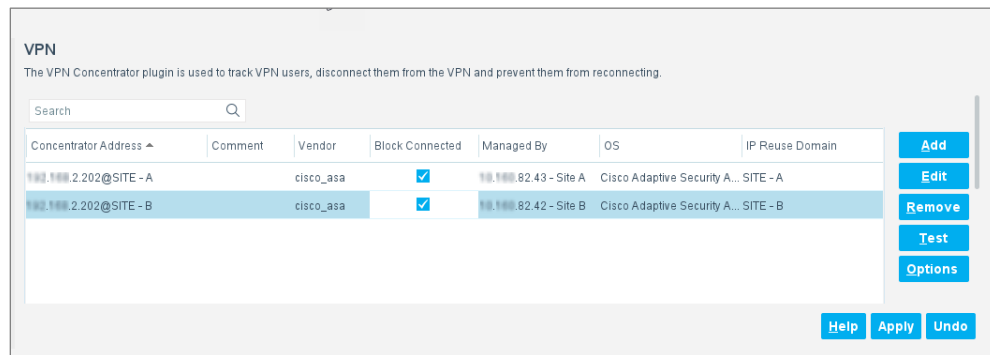
In the *Forescout Administration Guide*, refer to the appendix titled *Configuring the Certificate Interface* for information about working with the Console certificate interface. See [Additional Forescout Documentation](#) for information on how to access this guide.

VPN Pane Display

For each VPN device that the plugin is configured to manage, the Console *VPN* pane displays the following information:

Item	Description
Concentrator Address	The IP address of the managed VPN device. When the VPN device is located within an IP Reuse Domain (IRD), that IRD displays as a suffix of the IP address, in the form <i><IP address>@<IRD></i> . For example, 192.168.2.202@SITE – B.
Comment	Comments that you added.
Vendor	The device vendor.
Block Connected	Identifies whether VPN blocking is enabled or disabled.

Item	Description
Managed By	The Forescout device (Enterprise Manager or an Appliance) defined in the <i>General</i> page/tab, as the <i>Connecting Appliance</i> and that manages/communicates with the VPN device.
OS	The vendor operating system
IP Reuse Domain	This column is only available for display in the VPN pane when the Forescout platform is enabled to support overlapping IP addresses. Displays the IRD in which the VPN device is located. A blank entry identifies that the VPN device is located within the enterprise's default/global network.



Verify That the Plugin Is Running


After configuring the plugin, verify that it is running.

To verify:

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

Test the Plugin Configuration for VPN Device Management


Verify connections, parameters and plugin access to the Active Directory server. Perform this test after adding, editing or removing VPN parameters.

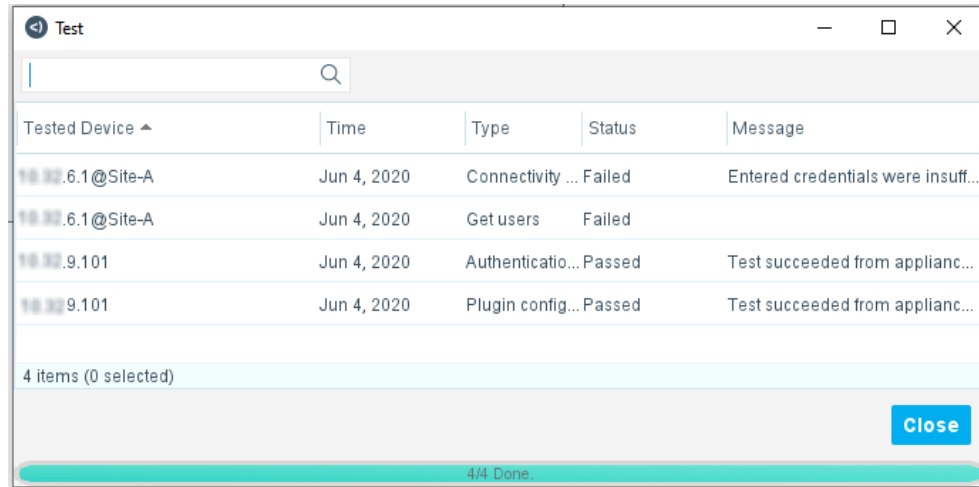
 *Even if you have not yet saved plugin parameter changes, the test uses the edited parameters.*

To test:

1. Select **Options** from the Tools menu.
2. Select **VPN**. The *VPN* pane opens.
3. Select one or multiple configured plugin entries for VPN device management.
4. Select **Test**.

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

 When a tested VPN device is located within an IP Reuse Domain (IRD), its entry in the *Tested Device* column displays that IRD as a suffix of the VPN device's IP address, in the form <IP address>@<IRD>.



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.

Policies for VPN Management

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

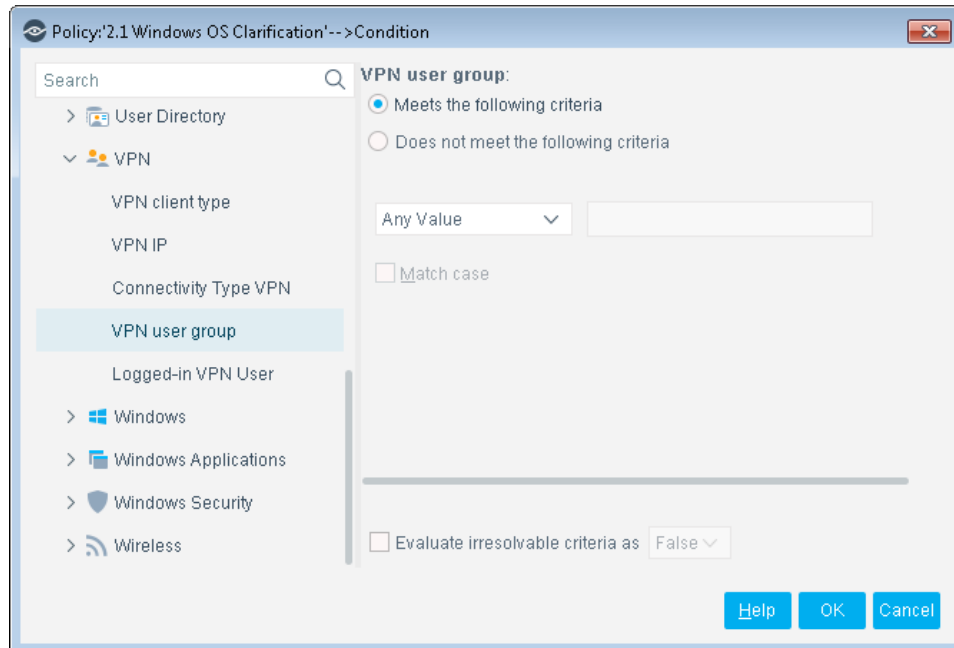
- [Property Resolution](#)
- [VPN Block Action](#)

Property Resolution


The VPN Concentrator Plugin resolves (retrieves) the following properties per plugin-managed VPN device:

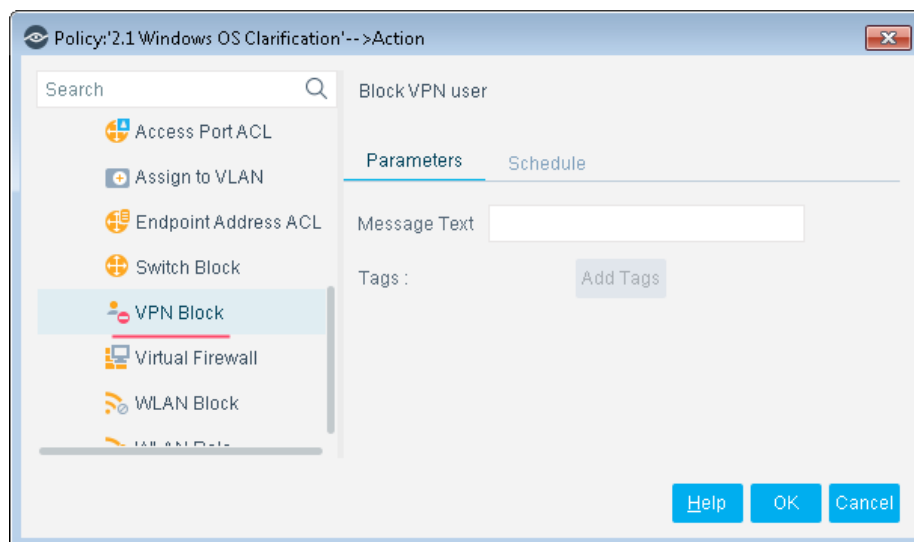
Property	Description
Connectivity Type VPN	A boolean value that identifies whether the user is connected through a VPN.
Logged-in VPN User	The username under which the endpoint is logged in to the VPN.
VPN client type	The authentication method or tunneling protocol used by the VPN.
VPN IP	The IP address of the VPN concentrator to which the endpoint is connected.

Property	Description
VPN user group	The User Group through which the endpoint connects to the corporate network.

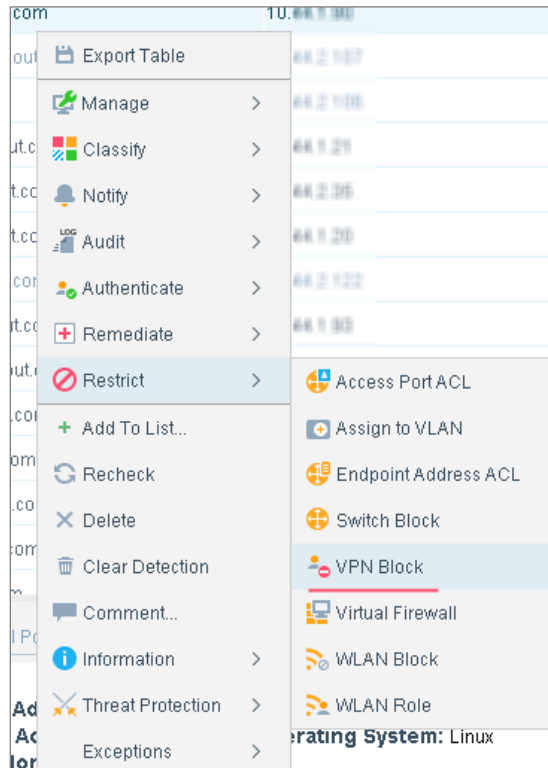


VPN Block Action

The Forescout eyeControl *VPN Block*  action prevents a user from connecting through a VPN. If you are using Flexx licensing, ensure that you have a valid *Forescout eyeControl* license to use this action. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing licenses.



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 manually apply the action on users that you select in either the Console *Home* tab or the *Asset Inventory* tab.



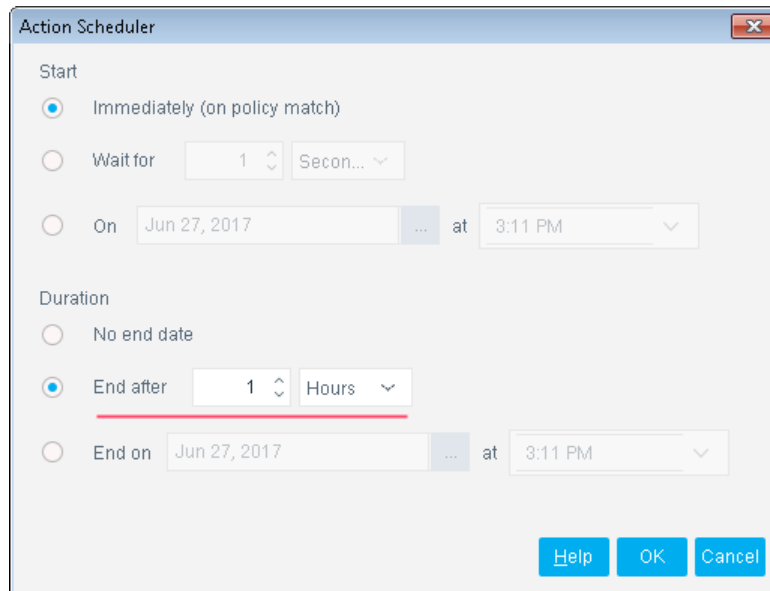
When you use this action, you specify a message text that is displayed to the blocked user if they attempt to reconnect. To include host-specific property values, select **Add Tags** and add Property Tags that resolve to host property values when the message is created. The message text is only seen on an endpoint when the user attempts 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.

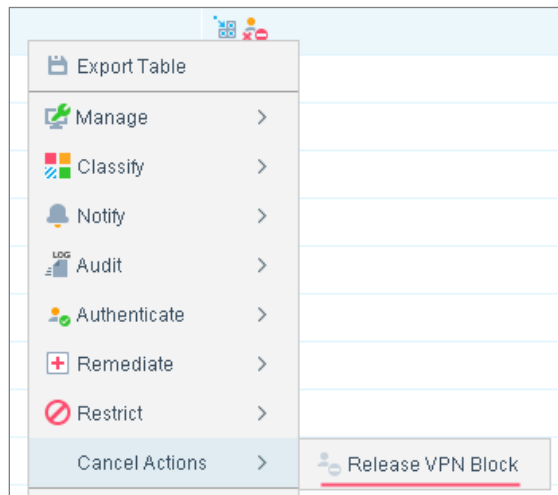
The Fore Scout platform must explicitly cancel the VPN Block action to allow the user to log in again. Unlike other block actions, this action blocks a *user account* rather than a network endpoint. However, Fore Scout platform policies act on network endpoints. When the blocked user's endpoint device 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.

Forescout continues to enforce the applied *VPN Block* action until one of the following situations explicitly cancels the *VPN Block* action, thereby allowing the VPN user to again access the network:

- Schedule settings of the action or policy end the action - Forescout recommends defining a 1 hour duration 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 is applied each time they log in.



- Manual cancellation of the action using the Forescout eyeControl *Release VPN Block* action (This cancellation is initiated from either the Console *Home* tab or the Console *Asset Inventory* tab).



Appendix A: CLI Commands for Cisco ASA VPN Devices

The following CLI commands are available for working with Cisco ASA VPN devices:

Command	Purpose
<code>enable</code>	Enter privileged mode
<code>exit</code>	Close the connection
<code>show version include Version</code>	Display system version
<code>show vpn-sessiondb full remote</code> (for working with version 8.3 or earlier)	Get users - IPSEC
<code>show vpn-sessiondb full ra-ikev1-ipsec</code> (for working with version 8.4 or later)	Get users - IPSEC
<code>show vpn-sessiondb full svc</code> (for working with version 8.3 or earlier)	Get users – SSL
<code>show vpn-sessiondb full anyconnect</code> (for working with version 8.4 or later)	Get users - SSL
<code>ssh -o StrictHostKeyChecking=no -l [user] [vpn ip]</code>	Log in using SSH
<code>telnet [vpn ip]</code>	Log in using Telnet
<code>terminal pager 0</code>	Disable paging of the command output
<code>vpn-sessiondb logoff name \$user\n</code>	To log off a user

Network Module Information

The VPN Concentrator Plugin is installed with the Forescout Network Module.

The Forescout® Network Module provides network connectivity, visibility and control through the following plugin integrations:

- Centralized Network Controller Plugin
- Network Controller Plugin
- Rogue Device Plugin
- Switch Plugin
- VPN Concentrator Plugin
- Wireless Plugin

The Network Module is a Forescout Base Module. Base Modules are delivered with each Forescout release. This module is automatically installed when you upgrade the Forescout version or perform a clean installation of Forescout.

The plugins listed above are installed and rolled back with the Network Module.

Additional Forescout Documentation

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

- [Documentation Downloads](#)
- [Documentation Portal](#)
- [Forescout Help Tools](#)

Documentation Downloads

Documentation downloads can be accessed from the [Technical Documentation Page](#), and one of two Forescout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** – [Product Updates Portal](#)
- **Flexx Licensing Mode** – [Customer Support Portal](#)

 Software downloads are also available from these portals.

To identify your licensing mode:

- From the Console, select **Help > About Forescout**.

Technical Documentation Page

The Forescout Technical Documentation page provides a link to the searchable, web-based [Documentation Portal](#), as well as links to a wide range of Forescout technical documentation in PDF format.

To access the Technical Documentation page:

- Go to <https://www.Forescout.com/company/technical-documentation/>

Product Updates Portal

The Product Updates Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend modules. The portal also provides additional documentation.

To access the Product Updates Portal:

- Go to <https://updates.forescout.com/support/index.php?url=counteract> and select the version you want to discover.

Customer Support Portal

The Downloads page on the Forescout Customer Support Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend modules. Software and related documentation only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Customer Support Portal:

- Go to <https://Forescout.force.com/support/> and select **Downloads**.

Documentation Portal

The Forescout Documentation Portal is a searchable, web-based library containing information about Forescout tools, features, functionality, and integrations.

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/

Forescout Help Tools

You can access individual documents, as well as the [Documentation Portal](#), directly from the Console.

Console Help Buttons

- Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with in the Console.

Forescout Administration Guide

- Select **Administration Guide** from the **Help** menu.

Plugin Help Files

- After the plugin is installed, select **Tools > Options > Modules**, select the plugin, and then select **Help**.

Content Module, eyeSegment Module, and eyeExtend Module Help Files

- After the component is installed, select **Tools > Options > Modules**, select the component, and then select **Help**.

Documentation Portal

- Select **Documentation Portal** from the **Help** menu.