FORESCOUT

Forescout

Network Module: VPN Concentrator Plugin

Configuration Guide

Version 4.2

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

Legal Notice

2019-02-13 17:22

Table of Contents

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. The authentication server can be either a RADIUS server or an Active Directory server.

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 Testing the Configuration.
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
- Supported VPN Devices
- Supported Authentication Methods

Forescout Requirements

The following Forescout version must be running in your Enterprise Manager and your Appliances:

- Forescout 8.1
- (Flexx licensing) A valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the plugin/component. If you do not have this license, these actions will be disabled in the Console. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing Flexx licenses and how to request/purchase this license.

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

Setup Procedures

This section describes the following setup procedures.

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

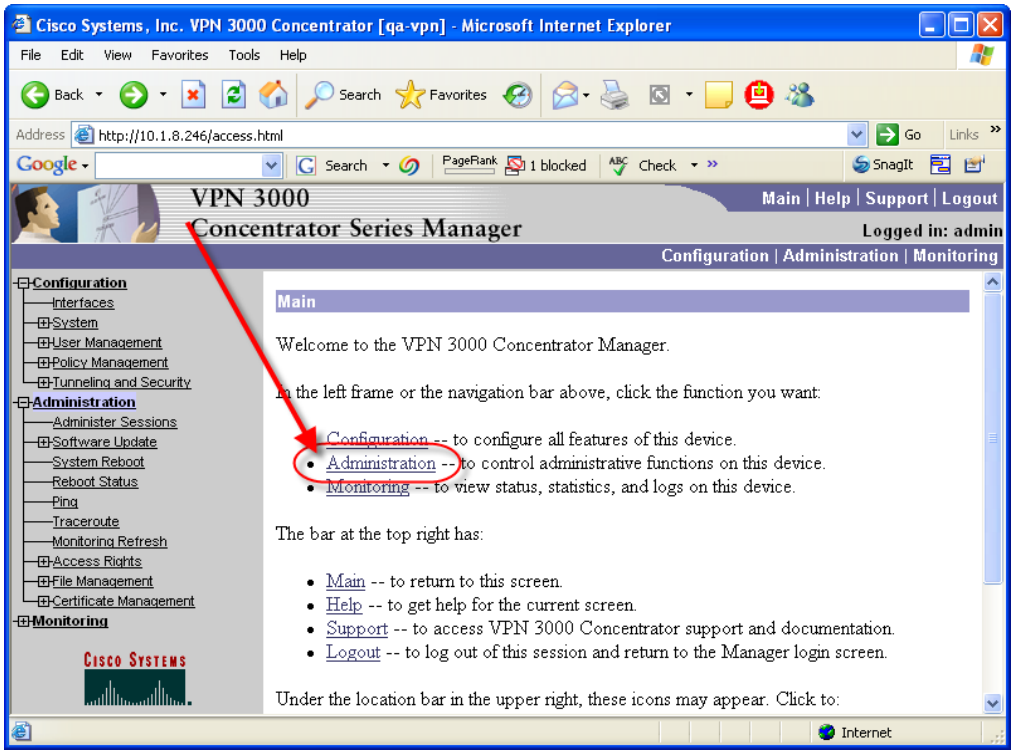
The VPN Concentrator Plugin must only use SNMPv1 to handle Cisco VPN3k.

Configure Read / Write permissions

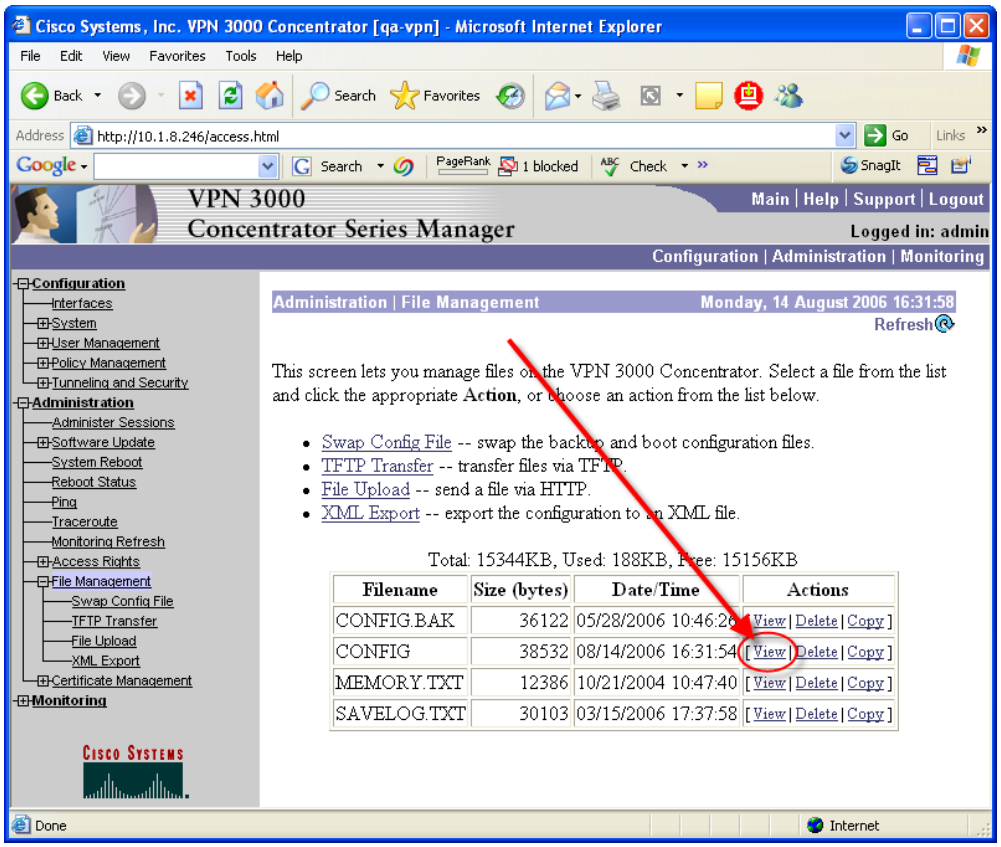
You should modify the VPN concentrator SNMP community to support both read and write. This is done by editing the VPN CONFIG file.

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

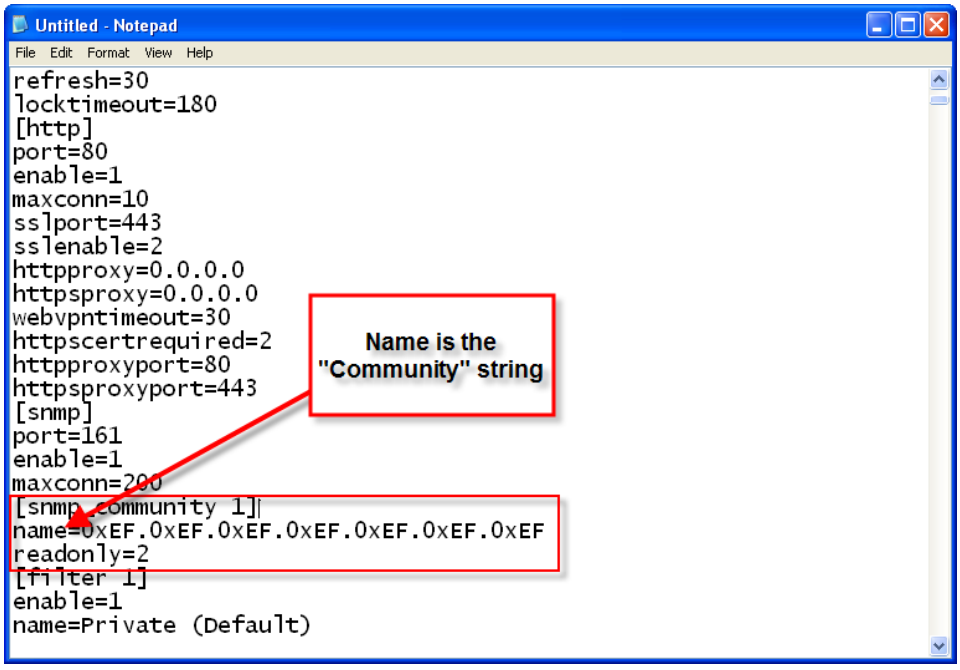
1. Log in to VPN concentrator.
2. Select **Administration** > **File Management**.



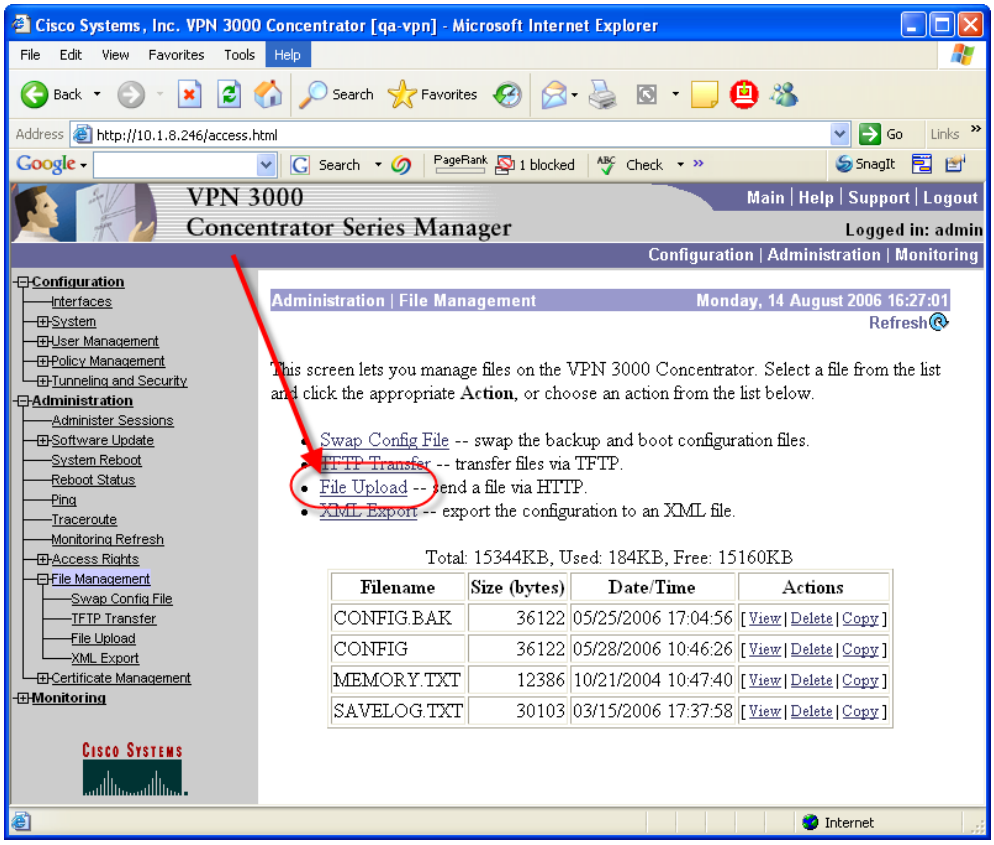
3. View the CONFIG file.



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.

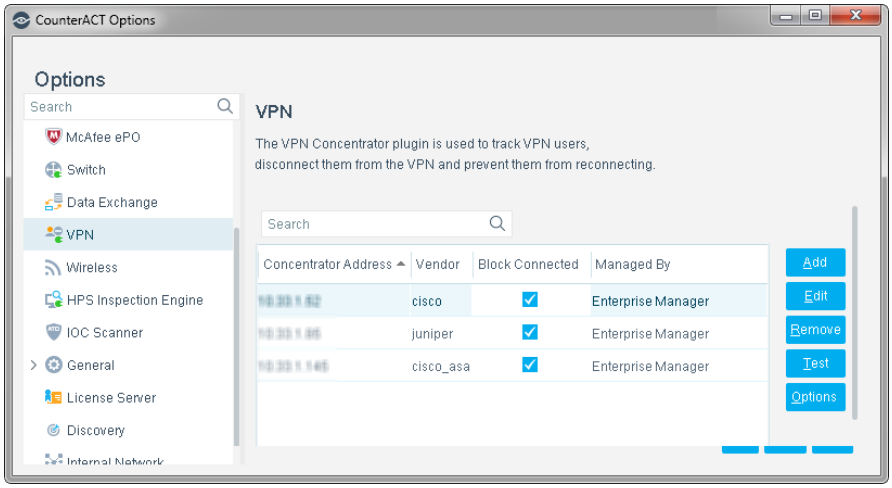
Configuring Forescout to Work with the VPN Device

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:

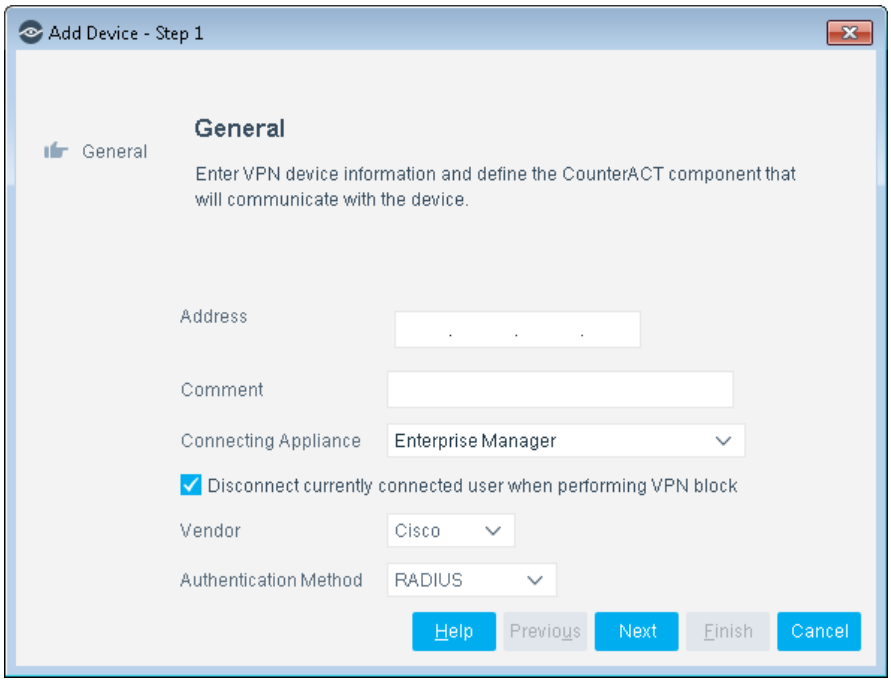
1. From the **Tools** menu, select **Options** > **VPN**.



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

General Page

Enter VPN device information and define the Enterprise Manager/Appliance that must communicate with the VPN device. Make sure to synchronize this information with the VPN device.



To configure general information:

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

Field Name	Description
Address	Enter the IP address of the VPN device.

Field Name	Description
Comment	Enter comments about the VPN device.
Connecting Appliance	Select the name of the Enterprise Manager/Appliance that must communicate with the VPN device. Certain Appliances or certain IP assignments made to a particular Appliance may be out of your user *Scope*. When this happens, you may only view the Appliance configuration and not change it. Appliances that contain Hosts IP assignment out of your *Scope* will appear with an empty red circle or red circle with a line through it. 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. An Appliance with an assignment that is completely outside the user scope is not shown in the drop-down list.
Disconnect currently connected user	Select the checkbox to disconnect immediately and prevent the VPN user from reconnecting. Clear the checkbox to prevent the VPN user from connecting after the current session closes.
Vendor	Select a VPN vendor. The configuration options that follow vary depending on the selected vendor.
Authentication Method	Select one of the following authentication methods: ▪ RADIUS ▪ Active Directory The configuration options that follow vary depending on the selected authentication method selected. 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.

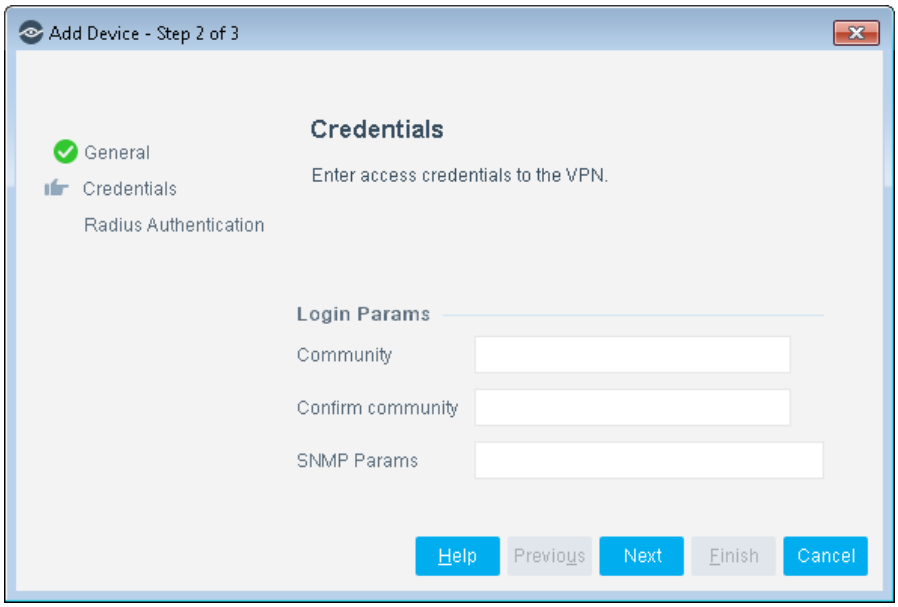
2. Select **Next**. The Credentials page of the Add Device wizard opens.

Credentials Page

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

- Cisco Credentials Page
- Juniper Credentials Page
- Nortel/Cisco ASA Credentials Page

Cisco Credentials Page

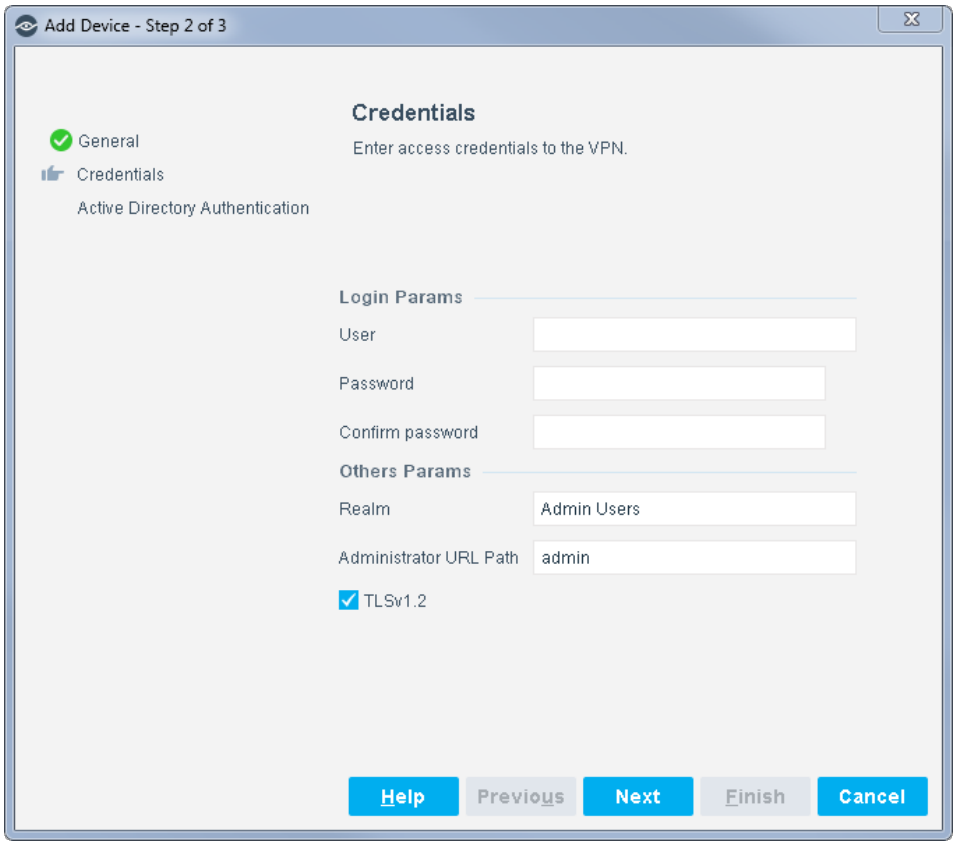


To configure Cisco credentials:

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

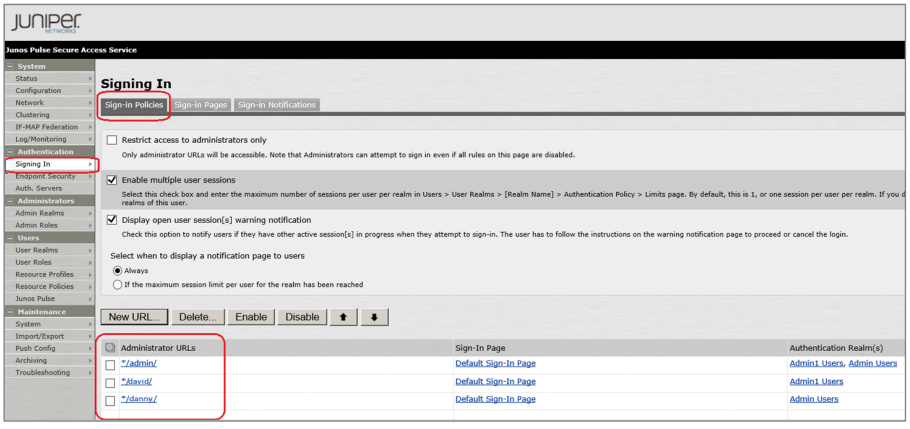
Field Name	Description
Community	Enter a unique name for this user group and confirm it
SNMP Params	Enter the following SNMP access parameters: ▪ SNMP version (1, 2 or 3) ***Note***: The VPN Concentrator Plugin must only use SNMPv1 to handle Cisco VPN3k. ▪ For SNMPv1 and SNMPv2c, a Community string ▪ For SNMPv3, a user and password Use the **snmpwalk** utility format to indicate these parameters. Include format example: - SNMPv1: **-v 1 -c <community_name>** - SNMPv2: **-v 2 -c <community_name>** - SNMPv3: **-v 3 -u <user> -A <password>**

Juniper Credentials Page



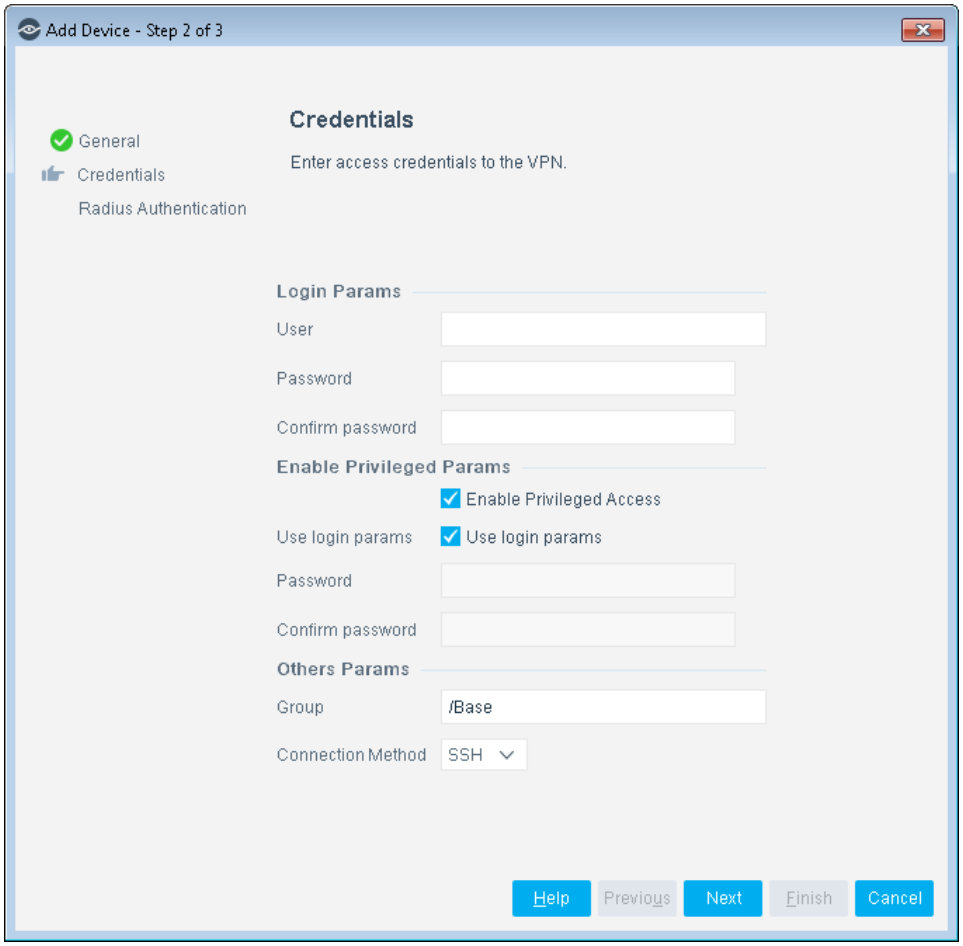
To configure Juniper credentials:

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.
Realm	Enter the realm name (group) of the admin user, who is configured here.
Administrative URL Path	Enter a Sign-in administrative URL path. 

Field Name	Description
TLSv1.2	Select this option to instruct the VPN Concentrator Plugin to communicate with the VPN device using TLSv1.2. ▪ By default, **TLSv1.2** is selected. - 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. For more information about Certification Compliance mode, refer to the *Forescout Installation Guide*.

Nortel/Cisco ASA Credentials Page



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.

Field Name	Description
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.

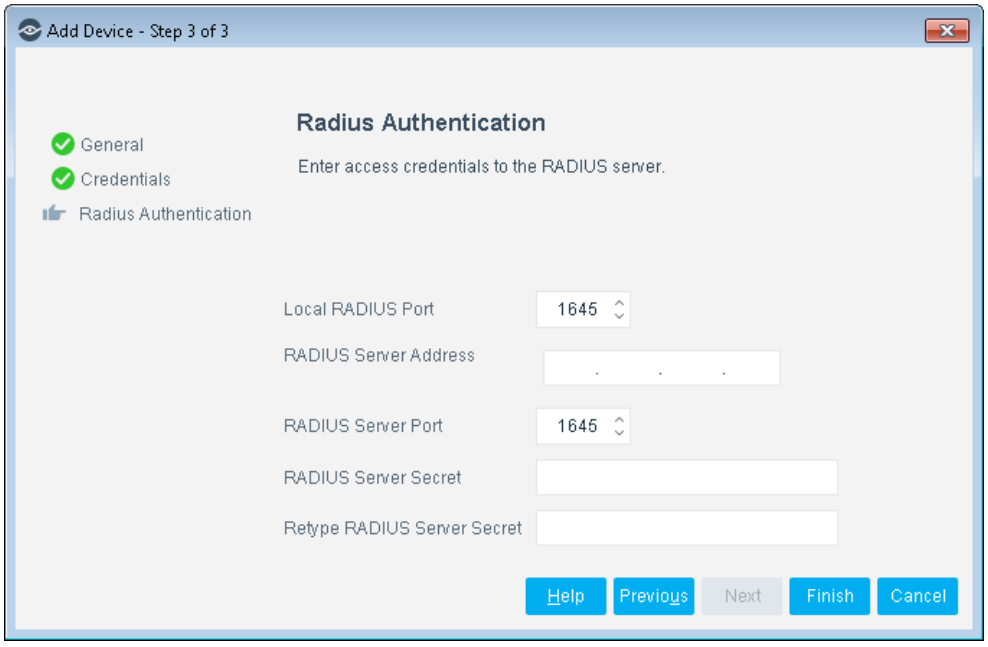
The administrator user must have permission to change the terminal paging. If this permission is not defined, the plugin configuration test for the VPN device fails and the plugin cannot manage that VPN device. The plugin uses the following terminal paging commands:

- 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.



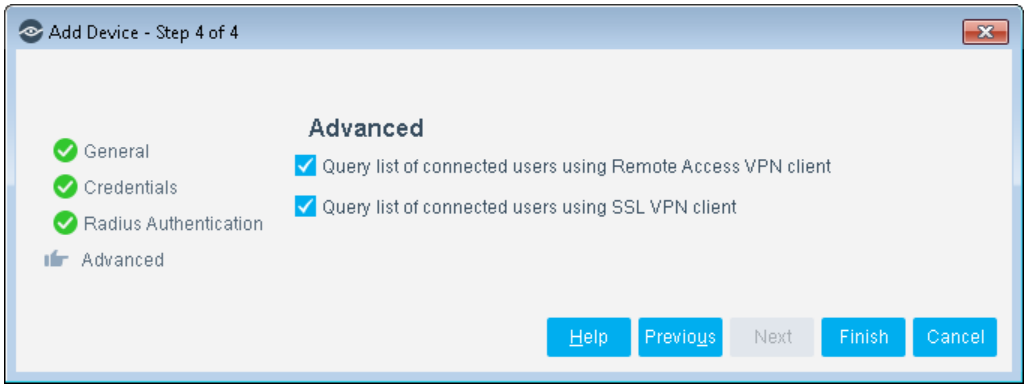
To configure credentials for plugin access to the RADIUS server:

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.
RADIUS Server Secret	The secret for the original RADIUS server.

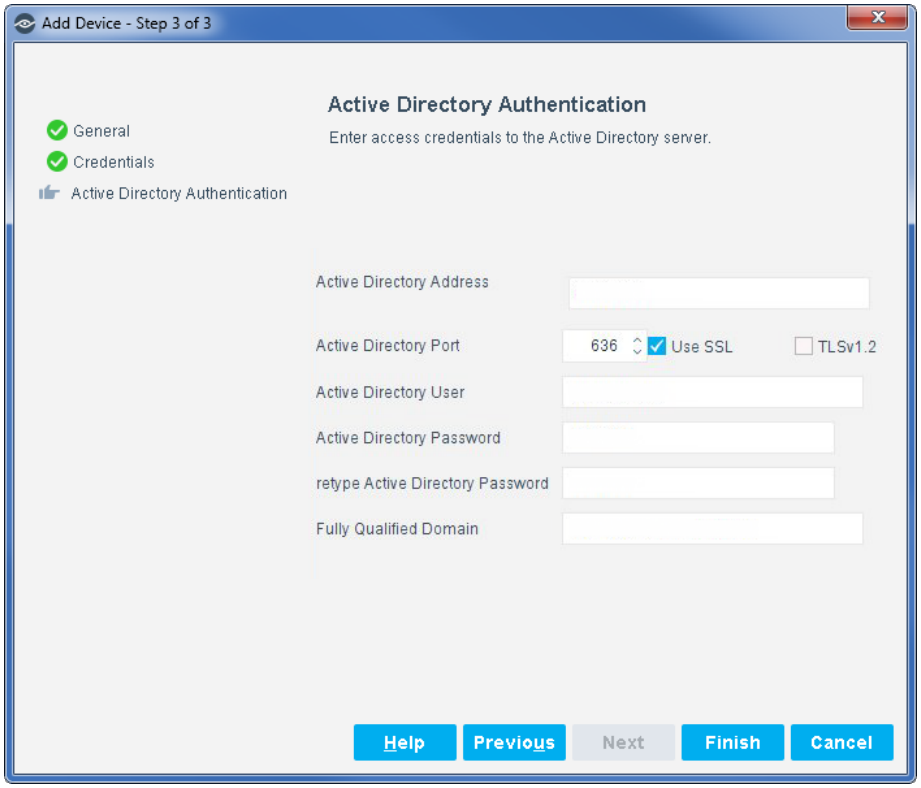
Cisco ASA – Advanced RADIUS Options

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

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



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

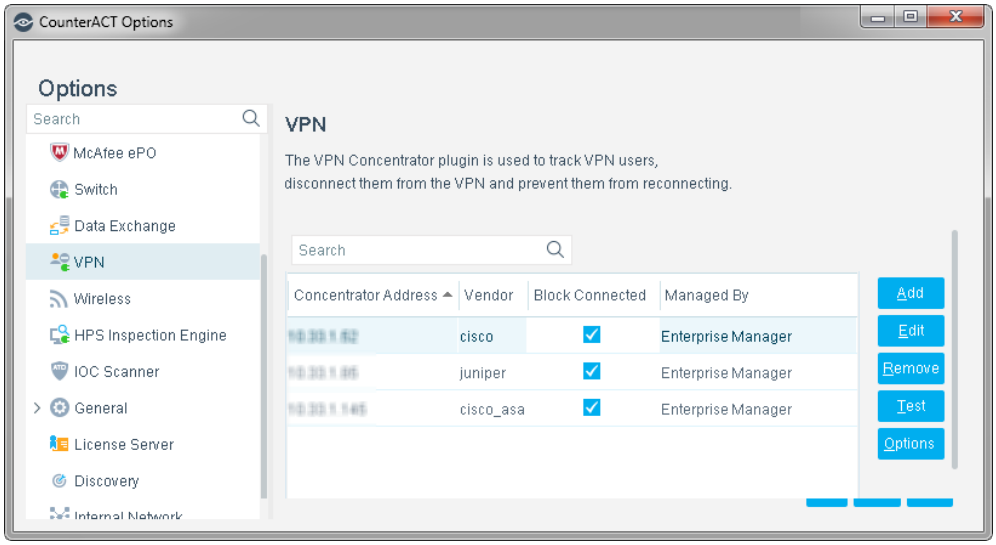
1. In the Active Directory Authentication page of the Add Device wizard, define the following:

Field Name	Description
Active Directory Address	Specify the Active Directory server that the VPN Concentrator must work with, by entering any of the following: ▪ The IPv4 address of the Active Directory server ▪ The FQDN (fully qualified domain name) of the Active Directory server. For example, *DCserver1.dom34.mycompany.com* - 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	Specify the port that the plugin uses to send authentication requests to the Active Directory server. By default, the port value is *636* (TCP)
Use SSL	Select this option to instruct the VPN Concentrator Plugin to apply SSL encryption to communication with the Active Directory server. ▪ By default, **Use SSL** is selected. - 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. ▪ 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 VPN pane.



The Console VPN pane displays the following information about each plugin-managed VPN device:

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

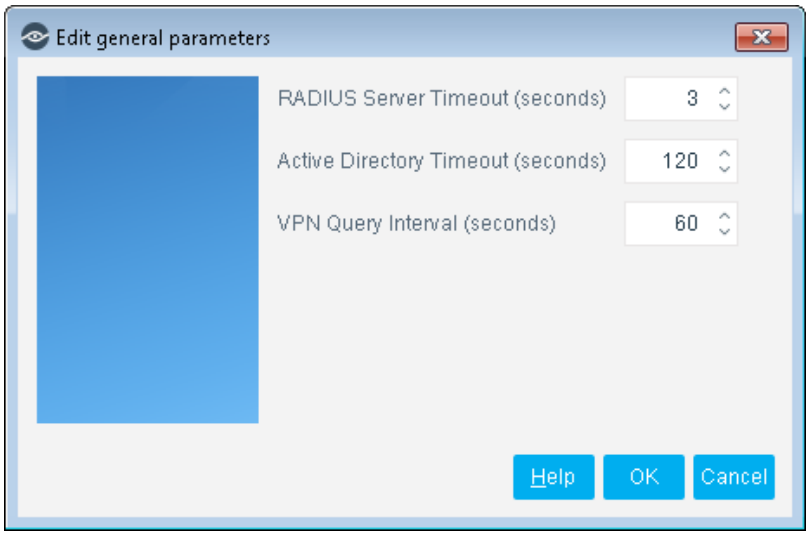
Item	Description
Managed By	The Enterprise Manager/Appliance that manages the VPN device
OS	The vendor operating system

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 Console 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.

Verify That the Plugin Is Running

After configuring the plugin, verify that it is running.

To verify:

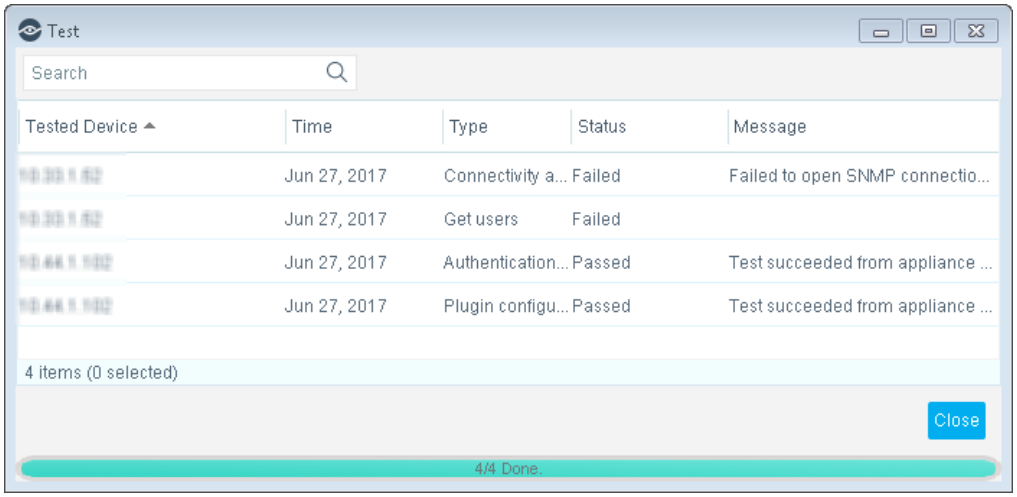
1. Select **Tools**>**Options** and then select **Modules**.
2. Navigate to the plugin and select **Start** if the plugin is not running.

Testing the Configuration

Verify connections, parameters and plugin access to the Active Directory server. 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.



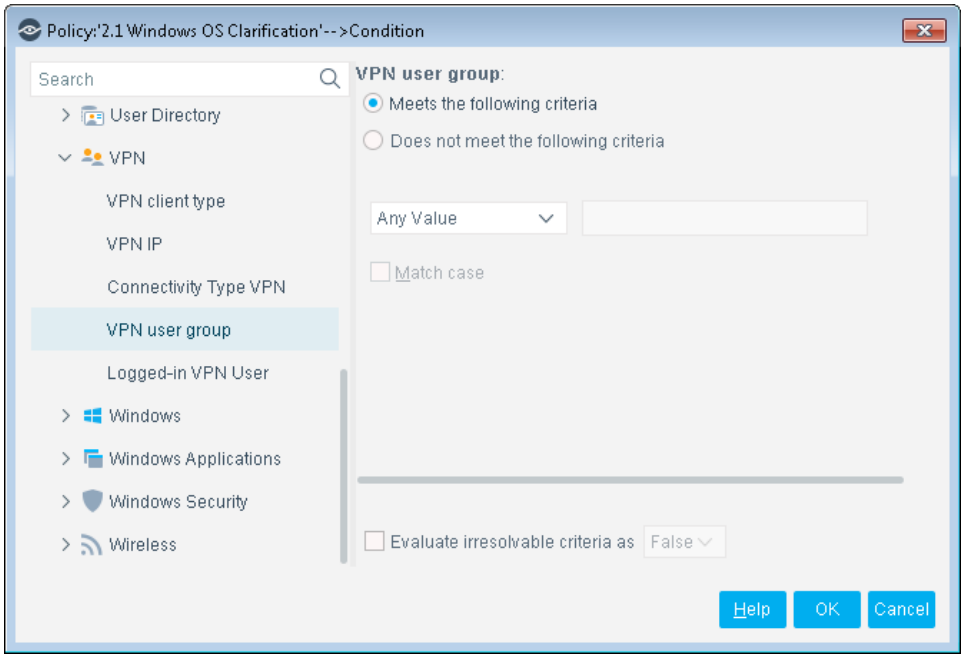
6. Use the **Filter** field to quickly locate a type. For example, type **P** and the "Plugin configuration" rows appear on the top of the list.

Even if you do not save the plugin parameter changes, the test uses the edited parameters.

Policies for VPN Management

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

VPN Host Properties

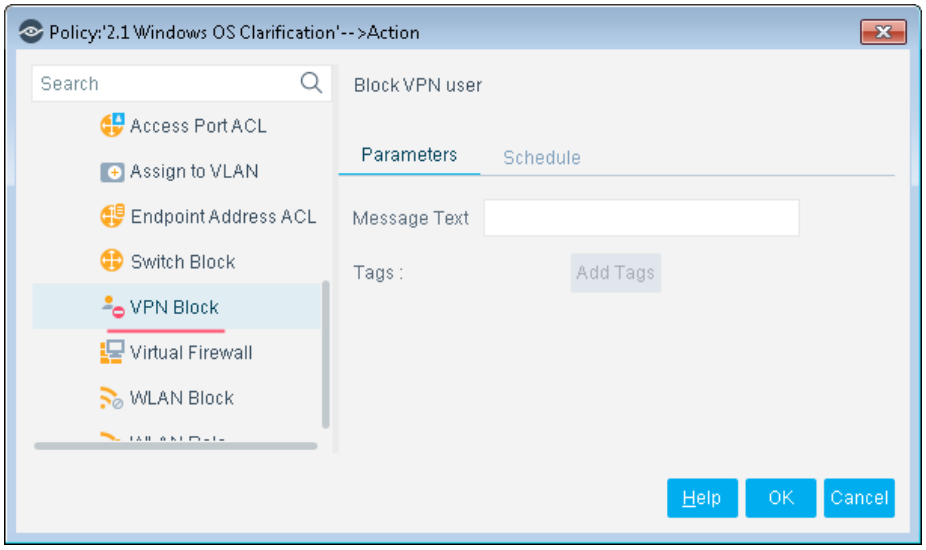


The following host properties report VPN-related information:

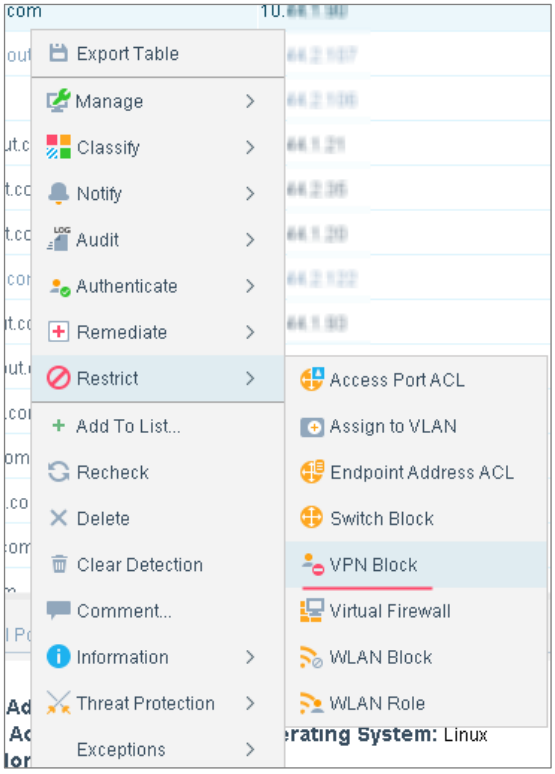
Property	Description
Connectivity Type VPN	A Boolean value that indicates whether the user is connected through a VPN.
Logged-in VPN User	The username under which the host is logged in to the VPN.
VPN client type	The authentication method or tunneling protocol used by the VPN.
VPN IP	The IP of the VPN 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. (Flexx licensing) To use this action, ensure that you have a valid *Forescout eyeControl* license. 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 apply the action to selected users from the Home or Inventory views of the Console.



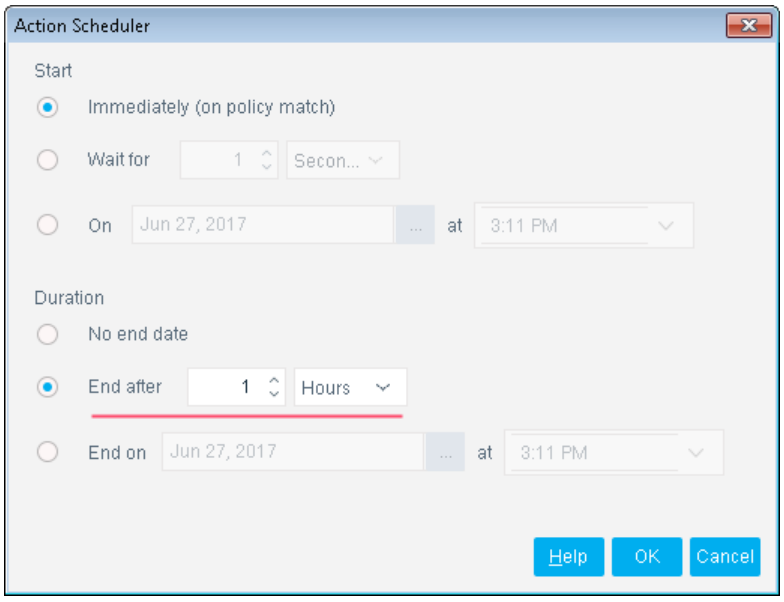
When you use this action, you specify a message text that is displayed to the blocked user if they attempt to reconnect. To include host-specific property values, select **Add Tags** and add Property Tags that resolve to host property values when the message is created. The message text is only seen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

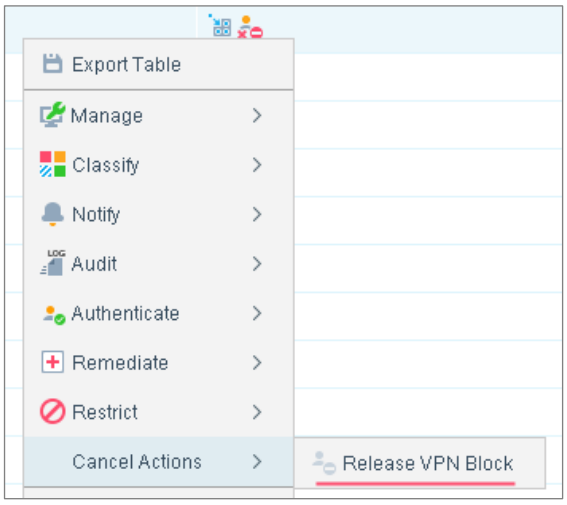
The Forescout platform must explicitly cancel the VPN Block action to allow the user to log in again. Unlike other block actions, this action blocks a *user account* rather than a network endpoint. However, CounterACT policies act on network endpoints. When the blocked user's endpoint device no longer 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.

Forescout continues to enforce the applied *VPN Block* action until one of the following situations explicitly cancels the VPN block, 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 cancelation of the action using the *Release VPN Block* action (user 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
`enable`	Enter privileged mode
`exit`	Close the connection
`show version | include Version`	Display system version
`show vpn-sessiondb full remote` (for working with version 8.3 or earlier)	Get users - IPSEC
`show vpn-sessiondb full ra-ikev1-ipsec` (for working with version 8.4 or later)	Get users - IPSEC
`show vpn-sessiondb full svc` (for working with version 8.3 or earlier)	Get users – SSL
`show vpn-sessiondb full anyconnect` (for working with version 8.4 or later)	Get users - SSL
`ssh -o StrictHostKeyChecking=no -l [user] [vpn ip]`	Log in using SSH
`telnet [vpn ip]`	Log in using Telnet
`terminal pager 0`	Disable paging of the command output
`vpn-sessiondb logoff name $user\n`	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
- 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 Forescout Resources Page, or 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 Portal

Software downloads are also available from these portals.

To identify your licensing mode:

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

Forescout Resources Page

The Forescout Resources Page provides links to the full range of technical documentation.

To access the Forescout Resources Page:

- Go to https://www.Forescout.com/company/resources/, select **Technical Documentation** and search for documents.

Product Updates Portal

The Product Updates Portal provides links to Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. The portal also provides a variety of 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 Portal

The Downloads page on the Forescout Customer Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, 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.

To access documentation on the Forescout Customer 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.

If your deployment is using Flexx Licensing Mode, you may not have received credentials to access this portal.

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/ and use your customer support credentials to log in.

Forescout Help Tools

Access information 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.

Forescout Administration Guide

- Select **Forescout Help** from the **Help** menu.

Plugin Help Files

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

Online Documentation

- Select **Online Documentation** from the **Help** menu to access either the Forescout Resources Page (Flexx licensing) or the Documentation Portal (Per-Appliance licensing).