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 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.
# Table of Contents

**About the VPN Concentrator Plugin** .......................................................... 4
  What to Do .................................................................................................. 4

**Requirements** ......................................................................................... 4
  Forescout Requirements ........................................................................... 4
  Supported VPN Devices .......................................................................... 4
  Supported Authentication Methods ......................................................... 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 ................................................................................... 11
  Radius Authentication Page .................................................................. 15
  Active Directory Authentication Page .................................................. 16
  Define Global Plugin Timeouts ............................................................. 18
  Certificate Management ........................................................................ 19
  Console Display of Plugin Configuration .............................................. 19
  Verify That the Plugin Is Running ......................................................... 20
  Testing the Configuration ..................................................................... 20

**Policies for VPN Management** .............................................................. 21
  VPN Host Properties ............................................................................. 21
  The VPN Block Action .......................................................................... 22

**Appendix A: CLI Commands for Cisco ASA VPN Devices** .................... 25

**Network Module Information** ............................................................... 26

**Additional Forescout Documentation** ................................................... 26
  Documentation Downloads ..................................................................... 26
  Documentation Portal ............................................................................ 27
  Forescout Help Tools ............................................................................. 27
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 8.1.2
- 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.

Supported VPN Devices

The VPN Concentrator Plugin supports the following server packages:

- Cisco ASA VPN 5500 Series Adaptive Security Appliance
- Cisco VPN 3000 software version 4.1.5 or higher
- Juniper 5.5R1 (build 11711) or higher
- Nortel V07_00.062 or higher
- Pulse Connect Secure 8.3R5.1 (Pulse Secure)

Supported Authentication Methods

- RADIUS
- Active Directory

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

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.

![Diagram of VPN Concentrator Manager interface]

This screen lets you manage files on the VPN 3000 Concentrator. Select a file from the list and click the appropriate Action, or choose an action from the list below.

- **Swap Config File** – swap the backup and boot configuration files.
- **TFTP Transfer** – transfer files via TFTP.
- **File Upload** – send a file via HTTP.
- **XML Export** – export the configuration to an XML file.

<table>
<thead>
<tr>
<th>Filename</th>
<th>Size (bytes)</th>
<th>Date/Time</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONFIG</td>
<td>38532</td>
<td>08/14/2006 16:31:54</td>
<td>View/Reset/Upload</td>
</tr>
<tr>
<td>MEMORY.TXT</td>
<td>12386</td>
<td>10/21/2004 10:47:40</td>
<td>View/Reset/Upload</td>
</tr>
<tr>
<td>SAVELOG.TXT</td>
<td>30103</td>
<td>03/15/2006 17:37:58</td>
<td>View/Reset/Upload</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Enter the IP address of the VPN device.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Comment</td>
<td>Enter comments about the VPN device.</td>
</tr>
<tr>
<td>Connecting Appliance</td>
<td>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.</td>
</tr>
<tr>
<td>Disconnect currently connected user</td>
<td>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.</td>
</tr>
<tr>
<td>Vendor</td>
<td>Select a VPN vendor. The configuration options that follow vary depending on the selected vendor.</td>
</tr>
</tbody>
</table>
| 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/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:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community</td>
<td>Enter a unique name for this user group and confirm it</td>
</tr>
<tr>
<td>SNMP Params</td>
<td>Enter the following SNMP access parameters:</td>
</tr>
<tr>
<td></td>
<td>- SNMP version (1, 2 or 3)</td>
</tr>
<tr>
<td></td>
<td>- Note: The VPN Concentrator Plugin must only use SNMPv1 to handle Cisco VPN3k.</td>
</tr>
<tr>
<td></td>
<td>- For SNMPv1 and SNMPv2c, a Community string</td>
</tr>
<tr>
<td></td>
<td>- For SNMPv3, a user and password</td>
</tr>
<tr>
<td></td>
<td>Use the <code>snmpwalk</code> utility format to indicate these parameters.</td>
</tr>
<tr>
<td></td>
<td>Include format example:</td>
</tr>
<tr>
<td></td>
<td>- SNMPv1: -v 1 -c &lt;community_name&gt;</td>
</tr>
<tr>
<td></td>
<td>- SNMPv2: -v 2 -c &lt;community_name&gt;</td>
</tr>
<tr>
<td></td>
<td>- SNMPv3: -v 3 -u &lt;user&gt; -A &lt;password&gt;</td>
</tr>
</tbody>
</table>
## Juniper/Pulse Secure Credentials Page

![Add Device - Step 2 of 3](image)

### To configure Juniper/Pulse Secure credentials:

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

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User</strong></td>
<td>The user logged in to the VPN device.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The password of the user.</td>
</tr>
<tr>
<td><strong>Realm</strong></td>
<td>Enter the realm name (group) of the admin user, who is configured here.</td>
</tr>
<tr>
<td><strong>Administrative URL Path</strong></td>
<td>Enter a Sign-in administrative URL path.</td>
</tr>
</tbody>
</table>

![Admin Directory Authentication](image)
### 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.

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

To configure Nortel/Cisco ASA credentials:

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

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>The user that connects via SSH/telnet to the VPN device.</td>
</tr>
</tbody>
</table>
### Field Name | Description
--- | ---
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:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local RADIUS Port</td>
<td>The UDP port for receiving authentication requests from the VPNs. This port must be different from the RADIUS Plugin local port.</td>
</tr>
<tr>
<td>RADIUS Server Address</td>
<td>The original RADIUS server IP address. This is the RADIUS server the VPN concentrator is initially configured to work with.</td>
</tr>
<tr>
<td>RADIUS Server Port</td>
<td>The port for sending authentication requests to the original RADIUS server.</td>
</tr>
<tr>
<td>RADIUS Server Secret</td>
<td>The secret for the original RADIUS server.</td>
</tr>
</tbody>
</table>

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 VPN pane. See Console Display of Plugin Configuration.

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 VPN pane. See Console Display of Plugin Configuration.

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:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory Address</td>
<td>Specify the Active Directory server that the VPN Concentrator must work with, by entering any of the following:</td>
</tr>
<tr>
<td></td>
<td>- The IPv4 address of the Active Directory server</td>
</tr>
<tr>
<td></td>
<td>- The FQDN (fully qualified domain name) of the Active Directory server. For example, DCserver1.dom34.mycompany.com</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td>Active Directory Port</td>
<td>Specify the port that the plugin uses to send authentication requests to the Active Directory server. By default, the port value is 636 (TCP)</td>
</tr>
<tr>
<td>Use SSL</td>
<td>Select this option to instruct the VPN Concentrator Plugin to apply SSL encryption to communication with the Active Directory server.</td>
</tr>
<tr>
<td></td>
<td>- By default, Use SSL is selected.</td>
</tr>
<tr>
<td></td>
<td>- If this option is not selected, the plugin uses non-encrypted TCP to communicate with the Active Directory server.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- When the Forescout platform runs in Certification Compliance mode, Use SSL is permanently selected.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>TLSv1.2</strong></td>
<td>Select this option to instruct the VPN Concentrator Plugin to communicate with the Active Directory server using TLSv1.2.</td>
</tr>
<tr>
<td></td>
<td>▪ By default, <strong>TLSv1.2</strong> is selected</td>
</tr>
<tr>
<td></td>
<td>▪ When the Forescout platform runs in Certification Compliance mode, <strong>TLSv1.2</strong> is permanently selected.</td>
</tr>
<tr>
<td><strong>Active Directory User</strong></td>
<td>Specify the Active Directory user who is associated with the administrator’s or account operator’s groups.</td>
</tr>
<tr>
<td><strong>Active Directory Password</strong></td>
<td>Specify the password of the Active Directory user.</td>
</tr>
<tr>
<td><strong>Fully Qualified Domain</strong></td>
<td>Specify the fully qualified domain name of the Active Directory domain. Forescout recommends using uppercase letters.</td>
</tr>
</tbody>
</table>

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. See *Console Display of Plugin Configuration*.

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 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.

![Edit general parameters dialog box](image)

RADIUS Server Timeout (seconds) | 9  
Active Directory Timeout (seconds) | 120  
VPN Query Interval (seconds) | 60  

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. See *Console Display of Plugin Configuration*.

For the certificates required when the plugin is configured to use the Active Directory authentication method, see *Certificate Management*.
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS Server Timeout (seconds)</td>
<td>The time to wait for the original RADIUS server to authenticate a user.</td>
</tr>
<tr>
<td>Active Directory Timeout (seconds)</td>
<td>The Active Directory connection timeout.</td>
</tr>
<tr>
<td>VPN Query Interval (seconds)</td>
<td>The interval at which to query the VPN for the connected hosts.</td>
</tr>
</tbody>
</table>

**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.

**Console Display of Plugin Configuration**

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concentrator Address</td>
<td>The IP address of the VPN device that you added</td>
</tr>
<tr>
<td>Comment</td>
<td>Comments that you added</td>
</tr>
<tr>
<td>Vendor</td>
<td>The device vendor</td>
</tr>
<tr>
<td>Block Connected</td>
<td>Indicates if VPN blocking is enabled</td>
</tr>
<tr>
<td>Managed By</td>
<td>The Enterprise Manager/Appliance that manages the VPN device</td>
</tr>
<tr>
<td>OS</td>
<td>The vendor operating system</td>
</tr>
</tbody>
</table>
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.

![Test dialog box](image)

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 VPN Block Action**

**VPN Host Properties**

The following host properties report VPN-related information:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connectivity Type VPN</strong></td>
<td>A Boolean value that indicates whether the user is connected through a VPN.</td>
</tr>
<tr>
<td><strong>Logged-in VPN User</strong></td>
<td>The username under which the host is logged in to the VPN.</td>
</tr>
<tr>
<td><strong>VPN client type</strong></td>
<td>The authentication method or tunneling protocol used by the VPN.</td>
</tr>
<tr>
<td><strong>VPN IP</strong></td>
<td>The IP of the VPN concentrator to which the endpoint is connected.</td>
</tr>
<tr>
<td><strong>VPN user group</strong></td>
<td>The User Group through which the endpoint connects to the corporate network.</td>
</tr>
</tbody>
</table>
The VPN Block Action

The **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 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:

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

Access documentation downloads 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:

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 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 access information about tasks and topics quickly.

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

Plugin Help Files
- After installing the plugin, 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).