Pulse Secure®
Acquired by Ivanti

Pulse Secure Desktop Client Configuration on Pulse Connect Secure

Supporting Pulse Secure Desktop Client 9.1R11

Product Release	**9.1R11**
Published	**February 2021**
Document Version	**1.1**

Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

www.pulsesecure.net

END USER LICENSE AGREEMENT

Contents

PREFACE 1
Document conventions 1
Text formatting conventions 1
Command syntax conventions 1
Notes and Warnings 2
Requesting Technical Support 2
Self-Help Online Tools and Resources 2
Opening a Case with PSGSC 3
Reporting Documentation Issues 3

CONFIGURING PULSE CONNECT SECURE FOR PULSE DESKTOP CLIENT 4
Before You Begin Configuring Pulse Connect Secure 4
Pulse Connect Secure Overview 5
Pulse Client and IVS 6
Pulse Client and Traffic Enforcement 6
Advanced Pulse Client Configuration Feature 6
About Sign-In Notifications 9
Configuring and Implementing Sign-in Notifications 10
Pulse Connect Secure Split Tunneling Overview 11
Split Tunneling Disabled 12
Split Tunneling Enabled 13
Pulse Client Split Tunneling Summary 13
IPv6/IPv4 Split Tunneling 15
Split Tunneling Notes 18
Configuring a Role for Pulse Connect Secure 19
Configuring General Role Options for Pulse Connect Secure 20
Configuring Role Options for Host Checker for Pulse Connect Secure 21
Machine Authentication for Pulse Connect Secure Overview 22
Credential Provider Authentication for Pulse Connect Secure Overview 22
Configuring Role Options for Pulse Connect Secure 23
Configuring User-at-Credprov Credential Provider Authentication for a Pulse Client Connection 26
Configuring Machine-Then-User-at-Credprov Credential Provider Authentication for a Pulse Client Connection 27
Machine and User Authentication through a Pulse Client Connection for Pulse Connect Secure 29
Stealth Mode 30

Scenario 1 31
Scenario 2 33
Configuring Pulse Client for Secure Application Manager 36
Pulse Client Connection Set Options for Pulse Connect Secure 42
Pulse Client Connection Set Options 42
Configuring Client Certificate Selection Option 44
Always-on VPN 46
Configuring Always-on Options 46
Configuring Always-on VPN Options using Wizards 47
Requirement to set up the appropriate GPOs 56
Always-on with Lock-down Mode 57
Lock-down Exception 58
Program-based Resource Access 60
Port-based Resource Access 61
Custom-based Resource Access 62
Retry Button 63
Captive Portal Remediation with Pulse Client Embedded Mini-Browser 63
Policy Secure 802.1X Connection Type Options 65
Trusted Server List (for Policy Secure 802.1X Connection) 66
Connect Secure or Policy Secure (L3) Connection Type Options 66
SRX (for Dynamic VPN) Connection Type Options 68
Pulse Client Connection is Established Options 68
Pulse Client Connection is Established Examples 69
Location Awareness Rules 70
Machine Connection Preferences 71
User Connection Preferences 71
Securing the Connection State on Pulse Client 72
Creating a Client Connection Set for Pulse Connect Secure 72
Pulse Client FIPS Mode for Pulse Connect Secure Overview 74
Endpoint Requirements 74
Configuration Overview 75
Configuring Location Awareness Rules for Pulse Client 76
Component Set Options for Pulse Connect Secure 78
Creating a Client Component Set for Pulse Connect Secure 78
Manage Pulse Client Versions 79
Endpoint Security Monitoring and Management for Pulse Connect Secure 80
Remediation Options 81
Issuing a Remediation Message with Pulse Connect Secure 82
Using SMS/SCCM Remediation with Pulse Connect Secure 83
Pushing Pulse Client Configurations Between Pulse Secure Servers of the Same Type 84

Enabling or Disabling Automatic Upgrades of Pulse Client 85
Upgrading Pulse Client 85
Pulse Collaboration Suite Overview 86
Task Summary: Configuring Pulse Collaboration Suite on Pulse Connect Secure 87
Configuring Pulse Client Connections to Support Meetings 88
Scheduling Meetings Through the Pulse Connect Secure User Web Portal 88
Scheduling Meetings Through Microsoft Outlook 88

Preface

- Document conventions 1
- Requesting Technical Support 2
- Reporting Documentation Issues 3

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Pulse Secure technical documentation.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used in the flow of the text to highlight specific words or phrases.

Format	Description
bold text	Identifies command names
	Identifies keywords and operands
	Identifies the names of user-manipulated GUI elements
	Identifies text to enter at the GUI
italic text	Identifies emphasis
	Identifies variables
	Identifies document titles
`Courier Font`	Identifies command output
	Identifies command syntax examples

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.

Convention	Description
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Non-printing characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, member[member...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.
bold text	Identifies command names, keywords, and command options.

Notes and Warnings

Note, Attention, and Caution statements might be used in this document.

Note: A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

CAUTION
A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

Requesting Technical Support

Technical product support is available through the Pulse Secure Global Support Center (PSGSC). If you have a support contract, file a ticket with PSGSC.

- Product warranties—For product warranty information, visit https://support.pulsesecure.net/product-service-policies/

Self-Help Online Tools and Resources

For quick and easy problem resolution, Pulse Secure provides an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: https://support.pulsesecure.net
- Search for known bugs: https://support.pulsesecure.net
- Find product documentation: https://www.pulsesecure.net/techpubs
- Download the latest versions of software and review release notes: https://support.pulsesecure.net

- Open a case online in the CSC Case Management tool: https://support.pulsesecure.net
- To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://support.pulsesecure.net

For important product notices, technical articles, and to ask advice:

- Search the Pulse Secure Knowledge Center for technical bulletins and security advisories: https://kb.pulsesecure.net
- Ask questions and find solutions at the Pulse Community online forum: https://community.pulsesecure.net

Opening a Case with PSGSC

You can open a case with PSGSC on the Web or by telephone.

- Use the Case Management tool in the PSGSC at https://support.pulsesecure.net.
- Call 1-844 751 7629 (Toll Free, US).

For international or direct-dial options in countries without toll-free numbers, see https://support.pulsesecure.net/support/support-contacts/

Reporting Documentation Issues

To report any errors or inaccuracies in Pulse Secure technical documentation, or to make suggestions for future improvement, contact Pulse Secure Technical Support (https://support.pulsesecure.net). Include a full description of your issue or suggestion and the document(s) to which it relates.

Configuring Pulse Connect Secure for Pulse Desktop Client

This chapter contains the following sections:

- Before You Begin Configuring Pulse Connect Secure 4
- Pulse Connect Secure Overview 5
- About Sign-In Notifications 9
- Configuring and Implementing Sign-in Notifications 10
- Pulse Connect Secure Split Tunneling Overview. 11
- Configuring a Role for Pulse Connect Secure 19
- Machine Authentication for Pulse Connect Secure Overview. 22
- Credential Provider Authentication for Pulse Connect Secure Overview 22
- Configuring User-at-Credprov Credential Provider Authentication for a Pulse Client Connection 26
- Configuring Machine-Then-User-at-Credprov Credential Provider Authentication for a Pulse Client Connection 27
- Machine and User Authentication through a Pulse Client Connection for Pulse Connect Secure 29
- Stealth Mode 30
- Configuring Pulse Client for Secure Application Manager. 36
- Pulse Client Connection Set Options for Pulse Connect Secure. 42
- Securing the Connection State on Pulse Client. 72
- Creating a Client Connection Set for Pulse Connect Secure 72
- Pulse Client FIPS Mode for Pulse Connect Secure Overview. 74
- Configuring Location Awareness Rules for Pulse Client 76
- Component Set Options for Pulse Connect Secure 78
- Endpoint Security Monitoring and Management for Pulse Connect Secure 80
- Issuing a Remediation Message with Pulse Connect Secure 82
- Using SMS/SCCM Remediation with Pulse Connect Secure 83
- Pushing Pulse Client Configurations Between Pulse Secure Servers of the Same Type. . . 84
- Enabling or Disabling Automatic Upgrades of Pulse Client. 85
- Upgrading Pulse Client 85
- Pulse Collaboration Suite Overview 86

Before You Begin Configuring Pulse Connect Secure

Before you begin configuring Pulse Secure Desktop Client (Pulse Client), be sure that you have already configured Pulse Connect Secure server network settings. Also, be sure that you have defined the Authentication settings, including the authentication servers and sign-in settings. The Authentication and Host Checker settings can directly affect a Pulse Client installation because you can define the conditions that an endpoint must meet to be allowed access to protected resources.

Pulse Connect Secure Overview

To enable Pulse Connect Secure, you configure the service so that when users request authentication, they are assigned a role based on the role mappings and optional security profile that you create. Access to specific resources is permitted only for users and devices that provide the proper credentials for the realm, that are associated with the appropriate roles, and whose endpoints meet security restrictions. If a user attempts to connect to the network from an endpoint that does not comply with the security restrictions you have defined, the user cannot access the realm or role.

As you plan your Pulse Client configuration, be sure you know how you want to deploy Pulse Client software. You can use one or more of the following Pulse Client deployment options:

- Use the defaults or make changes to the Pulse Connect Secure default component set and default connection set, and then download and distribute Pulse Client by having users log in to the Pulse Secure server's user Web portal and be assigned to a role. After the installation is complete, users have all the connections they need to access network resources.
- Create the connections that an endpoint needs for connectivity and services, download the settings file (.pulsepreconfig), and download default Pulse Client installation program. For Windows endpoints you run the Pulse Client installation program by using an msiexec command with the settings file as an option. For OS X endpoints, you run the default installer and then import the .pulsepreconfig file using a separate command.
- Distribute Pulse Client with no preconfiguration. You can download the default Pulse Client installation file (.msi format for Windows; .dmg format for Mac) from Pulse Connect Secure, and then distribute the file to endpoints using your organization's standard software distribution methods. Because the installer does not contain preconfigured connections, users must define network connections manually. Or you can create dynamic connections on each Pulse Connect Secure. These connections are automatically downloaded to the installed Pulse Client when users provide their login credentials to the Pulse Secure server's user Web portal, and then starts Pulse Client through the Web portal interface. Dynamic connections are created as manual rather than automatic connections, which means that they are run only when the user initiates the connection or the user browses to a Pulse Connect Secure and launches Pulse Client from the server's Web interface.

Note: For a Windows installation (.msi) that uses an automated distribution mechanism and where the users do not have administrator privileges, you should ensure that the installation is run in the proper context, typically the USER context. To install in USER context, first advertise the .msi while in the SYSTEM context. For example, to advertise the 64-bit Windows installation to all users, use the following msiexec command:

```
msiexec /jm \PulseSecure.x64.msi
```

The advertisement allows the installation to be run in USER context even if the user is a restricted (non-admin) user. The location where the advertisement is run and where the actual installation is run must be the same. If the installation is an upgrade, you must advertise the upgrade version before running it.

Note: It is much easier to upgrade Pulse Client by not disabling the automatic upgrade feature on Pulse Connect Secure.

After the installation is run by the user, Pulse Client will use the correct user certificate and context.

The following tasks summarize how to configure Pulse Connect Secure:

- Create and assign user roles to control who can access different resources and applications on the network. If you are converting your access environment from agentless or a Network Connect environment, you should create new roles that are specific for Pulse Client.
- Define security restrictions for endpoints with Host Checker policies.
- Define user realms to establish authentication domains. If you are converting your access environment from agentless or a NC environment, typically you can use your existing realms.
- Associate the roles with appropriate realms to define your access control hierarchy using role mapping.
- Define Pulse Client component sets, connection sets, and connections.
- Deploy Pulse Client to endpoints.

Pulse Client and IVS

Pulse Connect Secure and Pulse Client do not support Instant Virtual System (IVS) feature anymore.

Pulse Client and Traffic Enforcement

The Traffic Enforcement feature (supported on Windows and macOS) enables the user to prevent the leakage of any packet out of the tunnel as per Pulse Connect Secure tunnel configuration. This is accomplished by applying firewall rules in Pulse Client. These rules are created based on the Pulse Connect Secure tunnel configuration.

For more information on Pulse Connect Secure tunnel configuration policies, refer to the section “Defining Split Tunneling Network Policies” and “Defining the Route Precedence Options” of chapter “VPN Tunneling” of Pulse Connect Secure Administration Guide.

A local program might bypass the routing tables and bind traffic to the physical interface instead of allowing it to go through the Pulse Client virtual interface. If you enable Traffic Enforcement, you ensure that all traffic is bound by the Pulse Connect Secure tunnel configuration. Traffic Enforcement feature is more useful in macOS because of Apple routing behavior.

For example, If SSH session is created using physical adapter before VPN tunnel, the session will continue to use physical adapter even after the tunnel is established because of macOS scoped routing (Apple functionality). If Traffic Enforcement is enabled, the same SSH session gets terminated because firewall rule finds packet leaking out of tunnel from SSH session and it will deny that traffic.

Advanced Pulse Client Configuration Feature

This topic describes the XML advanced Pulse Client configuration that can be used by the Pulse Connect Secure administrator to configure the custom settings, which are meant to solve a specific customer scenario without changing the Pulse Connect Secure admin console. Admin can set these custom settings in the form of XML input through the Advanced Client Configuration UI feature. Pulse Clients supporting these custom settings will consume them when connecting to this Pulse Connect Secure, and the same would be applied on Pulse Client machines. From 9.0R3 release onwards, this feature will minimize the number of changes going into the Pulse Connect Secure admin console to fulfill the requirement of a specific customer.

In the earlier Pulse Client releases, i.e. prior to v5.2R2, the virtual adapter MTU was calculated based on the physical adapter MTU (of the host machine) and the MTU sent by the Pulse Connect Secure.

Basically, the formula used to calculate the virtual adapter MTU is:

MIN (Physical Adapter MTU, MTU from Pulse Connect Secure, TCP MSS value + 40)

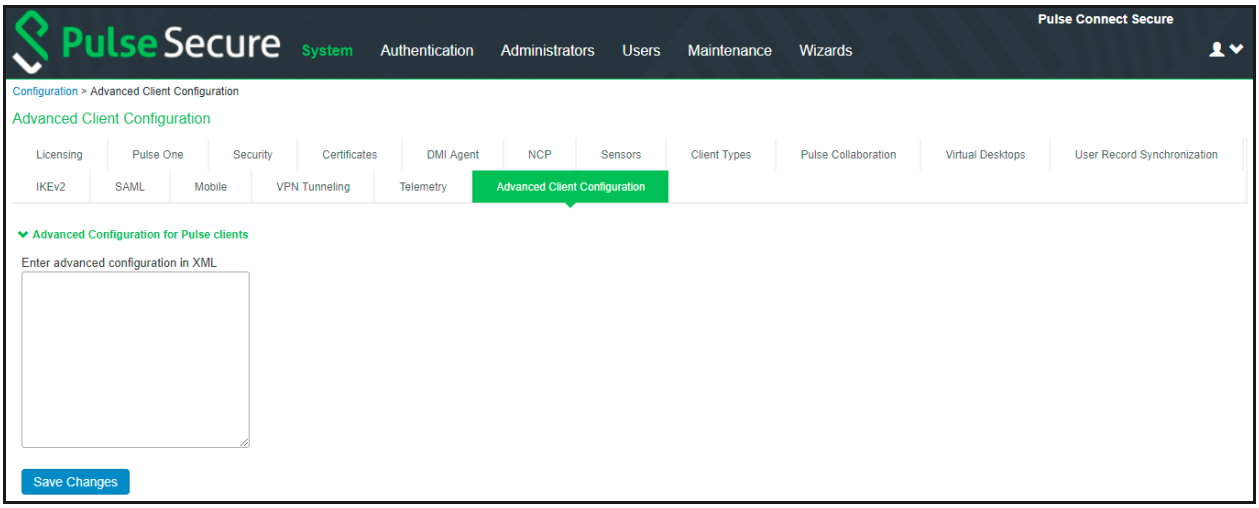
Following is a scenario where Firewall on the data path is stripping the TCP MSS options being advertised by the SA/Pulse Connect Secure to Pulse Client. In this scenario, the TCP MSS value on Pulse Client will default to a minimum value of 536, and as a result the client-side MTU calculation will result in a minimum MTU value of 576. Here, customer wants to ignore the TCP MSS options while calculating the Virtual Adapter MTU calculation.

If the administrator configures the Pulse Connect Secure server with the following XML input in "Advanced Client Configuration for Pulse Clients" option, it will ignore TCP MSS options while calculating the virtual adapter MTU on client side.

1. Select **System > Configuration > Advanced Client Configuration** to display the configuration page.

   Figure 1 shows the configuration page for Pulse Connect Secure.

   Figure 1 Advanced Client Configuration



2. Enter the following XML input in "Advanced Client Configuration for Pulse Clients".

```
<advanced-config>
       <version>9.0.3</version>
        <desktop-client-config>
                 <layer3-connection-config>
                 <adapter-config>
                              <ignore-tcp-mss>TRUE</ignore-tcp-mss>
                 </adapter-config>
                 </layer3-connection-config>
        </desktop-client-config>
   </advanced-config>
```

3. Click **Save Changes**.

The advanced configuration setting "ignore-tcp-mss" is Layer3 Adapter configuration setting and this will be consumed by Pulse Client as part of the IpsecConfig.

Note: This "ignore-tcp-mss" setting is applicable for the virtual adapter MTU calculation only for IPv4. By default the setting is always false, and therefore the TCP MSS options are always considered for MTU by default. Admin has to explicitly set the ignore-tcp-mss setting to TRUE (case-insensitive), to ignore the TCP MSS.

Disabling JNPRNS driver Using Advanced Client Configuration

JNPRNS is a Network Driver Interface Specification (NDIS) based Light Weight Filter (LWF) driver used for certain operations in IPSEC SRX L3 Flow. By default, JNPRNS driver is enabled on all the network adapters associated with PDC. Enabling JNPRNS driver can affect the upload and download performance on normal SSL/ESP L3 VPN. To improve the speed, you can disable JNPRNS driver.

Use any one of the methods to disable JNPRNS driver:

- On windows endpoint, disable JNPRNS driver manually from the network adapter stack using the powershell command
  `Disable-NetAdapterBinding -Name * -DisplayName "Juniper Network Service"`
- On the PCS UI, navigate to **System** --> **Configuration** --> **Advance Client Configuration**. Under, **Advanced Configuration for Pulse Clients**, set the *<disable-jnprns-driver>* flag to **"**True**"** as shown in the figure.

Figure 2 Advanced Client Configuration Settings for JNPRN driver

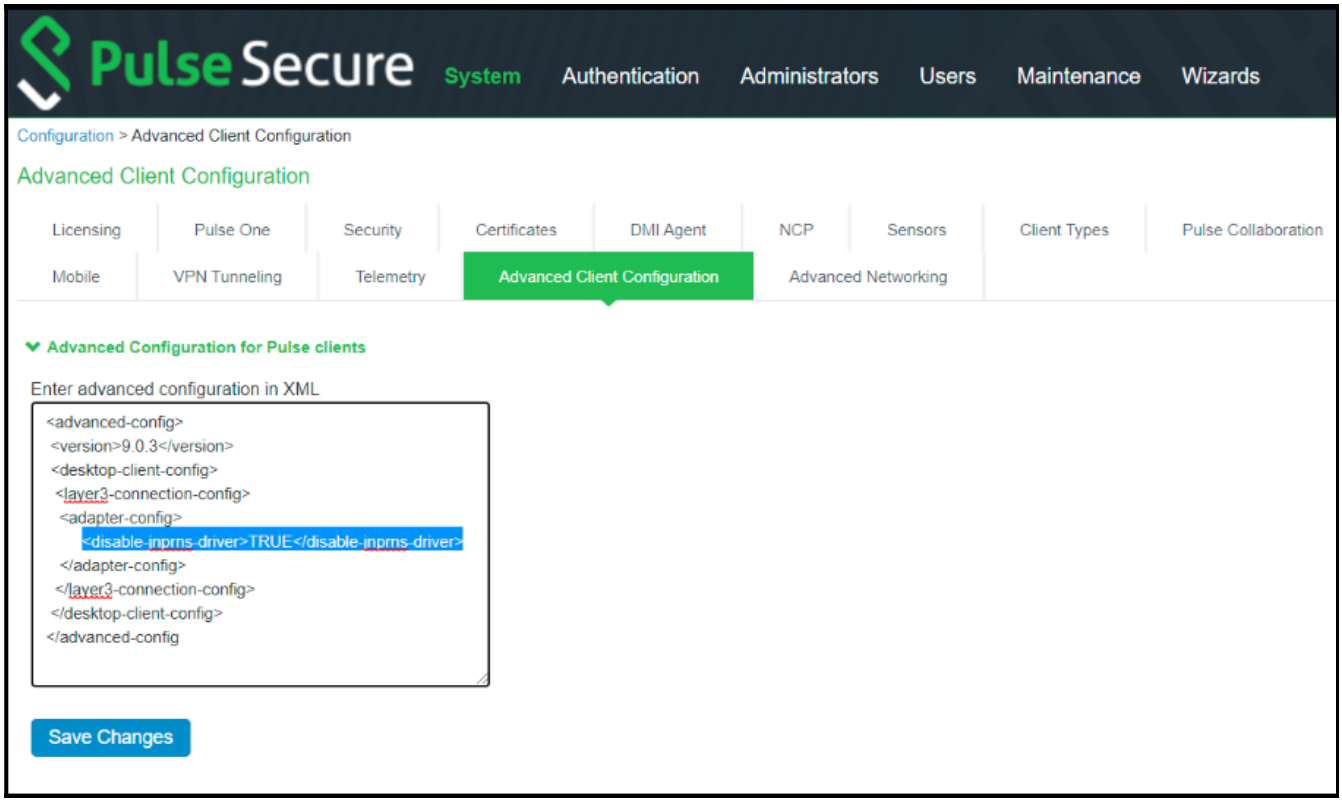
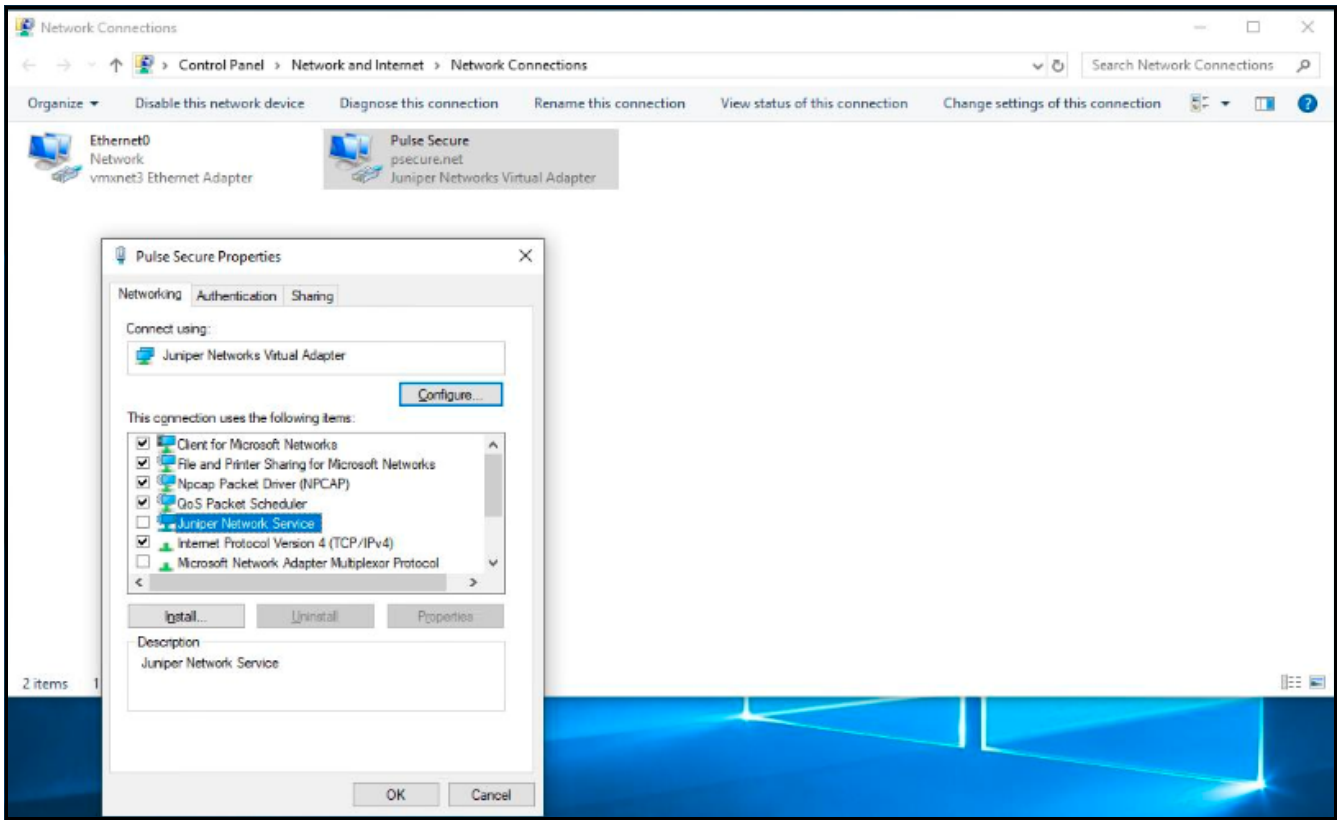


Figure 3 Disable Network Adapter



Note: This setting is applicable for clients running on Windows 10 operating system only.

About Sign-In Notifications

With sign-in notifications, you can create and configure detailed notification messages that appear for Pulse Clients and for agentless access endpoints when the user attempts to sign in. For example, you could configure a notification message that explains terms of use, company-specific policies, a welcome page, an end user license agreement (EULA), or a message of the day (MOTD).

For a browser-based (agentless) login, the notification message appears in a separate page either before (pre-auth) or after (post-auth) user authentication during the sign-in process. For a Pulse Client login, the notification messages appear in a Pulse Client message box. The user is expected to read the content of the sign-in notification message and acknowledge by clicking a Proceed button. The user may indicate disagreement by clicking a Decline button, which ends the login attempt.

You can configure a sign-in policy to use a sign-in notification either as pre-auth or post-auth (or both). In the case of post-auth configuration, you can either use a common message for all roles or use separate messages for each role.

You can create a multi-language sign-in notification package that relies on the language setting of the endpoint. You can customize the sign-in notification page appearance for browser-based logins by modifying the related fields in a sign-in page in the Admin UI or by using a custom sign-in page.

Note: Sign-in notifications are supported on Windows, Mac, and for browser-based access on mobile devices. However, sign-in notifications might not work well with all mobile devices due to device limitations.

Note: Sign-in notifications (including uploaded packages) are included in XML exports.

Note: If a Pulse Client session is resumed or extended, the pre-auth notification message is not shown again. However, if the user switches roles when resuming a session, and that role change results in a new notification, Pulse Client displays the message. You can configure the post-auth message to be skipped if it has already been seen. If the post-auth message is not marked to be skipped, then it always appears.

Configuring and Implementing Sign-in Notifications

Sign-in notifications appear for Pulse Client and for browser-based logins when the user attempts to sign in.

To configure and implement sign-in notifications:

1. In the admin console, select **Authentication > Signing In > Sign-in Notifications**.
2. Click **New Notification**.
3. Specify a Name for the notification. This name appears in the sign-in policies page, and in the UI Options page for a selected role.
4. Select "Text" or "Package" in the **Type** box.
   - If you select Text, type the desired sign-in notification message, or copy and paste the relevant text into the Text field.
   - If you select Package, click the Browse button and navigate to a previously prepared .zip file. A package is typically used to provide different language versions of the notification message.
     - The zip file should include a default.txt file and one or more <language>.txt files (Example: en.txt).
     - Language-abbreviations should be strings that can appear in Accept-Language header of an HTTP request.
     - The character encoding supported is UTF-8.

Note: When you create a zip file, do not add the folder containing the files, but add the files directly.

5. Click **Save Changes**.

To enable sign-in notifications:

1. In the admin console, click **Authentication > Signing In > Sign-in Policies**.
2. Select an existing URL or create a new URL.
3. Under Configure Sign-in Notifications, select the check box for **Pre-Auth Sign-in Notification**, **Post-Auth Sign-in Notification**, or both.
   - After Pre-Auth Sign-in Notification, select a previously configured sign-in notification from the drop-down menu.
   - After Post-Auth Sign-in Notification, select the option for **Use a common Sign-in Notification for all roles** or **Use the Sign-in Notification associated to the assigned role**.
   - If you select **Use a common Sign-in Notification for all roles**, select a previously configured sign-in notification from the drop-down menu.

- If you select **Use the Sign-in Notification associated to the assigned role**, the sign-in notification configured for the assigned role will be used.
- Prevent the Post-Auth sign-in notification from being displayed to users who have seen it before, by selecting the **Skip if already shown** check box. (This is only a hint to the system and might not be honored in all environments.)

4. Click **Save Changes**.
5. You can customize the appearance of the sign-in notification message by selecting **Authentication > Signing In > Sign-in Pages** and creating a sign-in page or using an existing page.
6. Under Sign-in Notification appearance, customize UI options for Pre-Auth Notifications and Post-Auth Notifications by changing the following items:
   - For **Notification Title** enter the text that appears at the top of the sign-in notification page.
   - In the **Proceed Button** box, enter the text for the button that the user clicks to proceed with the sign-in.
   - This text applies to browser-based logins only. A Pulse Client login always displays Proceed.
   - Optionally, clear the check box for **Display "Decline" Button**. If this box is not checked, the user does not have the option to decline.
   - In the **Decline Button** box, enter the text for the button that the user clicks to decline.

     This text applies to browser-based logins only. A Pulse Client login always displays Decline.
   - In the **Message on Decline** box, enter the text that you would like to appear when a user clicks the Decline button.
7. Click **Save Changes**.

Note: If you enabled Use the Sign-in Notification associated to the assigned role you must complete the implementation by selecting the sign-in notification on the **Users > User Roles > Role Name > General > UI Options** page or **Administrators > Admin Roles > Role Name > General > UI Options** page, as applicable.

If more than one role is available to a user, the sign-in notification associated with the first role assigned is displayed.

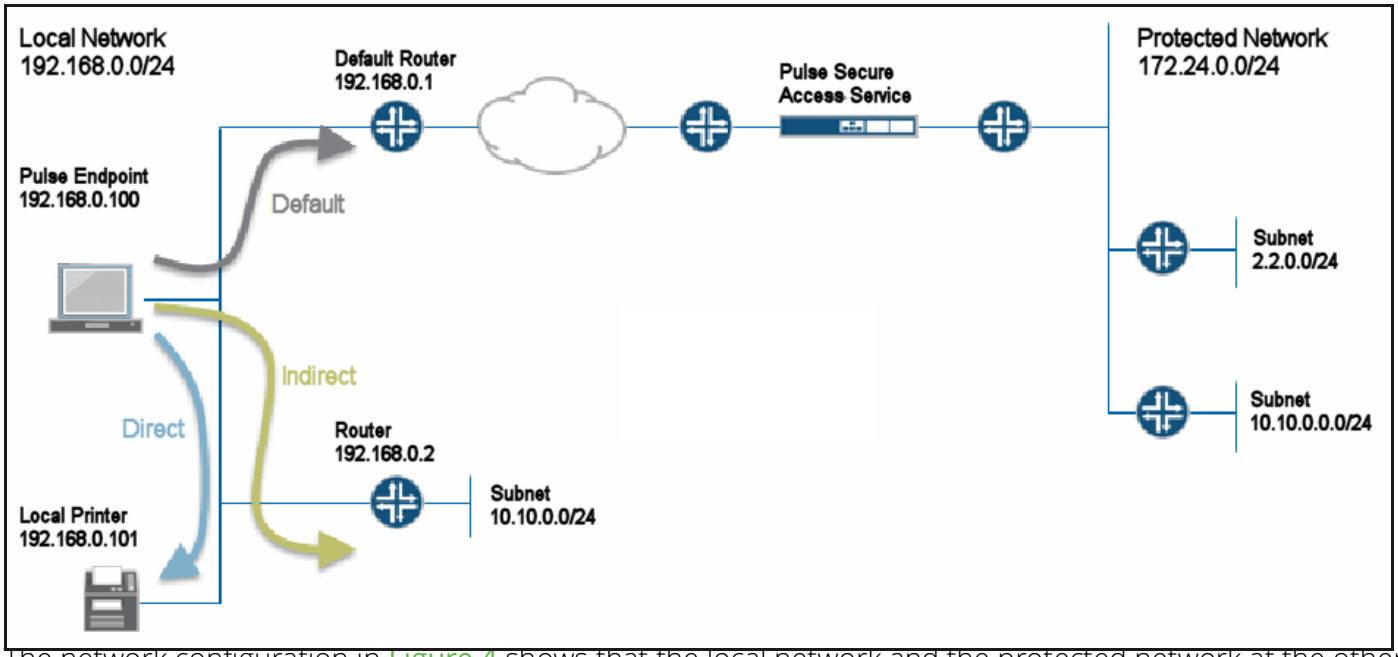
8. Add the sign-in page in which you have customized the sign-in notification appearance to the sign-in policy.

Pulse Connect Secure Split Tunneling Overview

Pulse Clients for Windows, Apple OS X, Google Android, and Apple iOS and the Pulse Secure Network Connect client all support split tunneling. Split tunneling is configured as part of the role that is assigned to a user after authentication. When Pulse Client and Pulse Connect Secure establish a VPN tunnel, Pulse Connect Secure takes control of the routing environment on the endpoint to ensure that only permitted network traffic is allowed access through the VPN tunnel. Split tunneling settings enable you to further define the VPN tunnel environment by permitting some traffic from the endpoint to reach the local network or another connected subnet. When split tunneling is enabled, split tunneling resource policies enable you to define the specific IP network resources that are excluded from access or accessible through the VPN tunnel.

Figure 4 shows a simple network configuration with three possible routes: through the default router, to the local subnet, or to a router connection to an indirectly connected subnet.

Figure 4 Pulse Client Split Tunneling



The network configuration in Figure 4 shows that the local network and the protected network at the other end of the VPN tunnel both have a subnet with the same private IP address, 10.10.0.0/24. In this case, the endpoint needs more information to determine where to send traffic addressed to that IP address range. You use the route precedence setting in the split tunneling settings to define which routing table takes precedence, either the tunnel routes (the routing table associated with the VPN tunnel) or the endpoint route (the routing table associated with the physical interface). If you select tunnel routes for route precedence, traffic addressed to network 10.10.0.0/24 in Figure 4 goes through the VPN tunnel and the 10.10.0.0/24 network available on the local indirect network is not reachable. If you select endpoint routes for route precedence, traffic addressed to network 10.10.0.0/24 goes through the physical adapter and the 10.10.0.0/24 network available through the VPN tunnel is not reachable. Pulse Client restores the original routes when the VPN tunnel is disconnected. However, no matter which way you define route precedence, the endpoint loses connectivity to one of the other of the networks if there are duplicate IP address networks.

Split Tunneling Disabled

When the endpoint has an active VPN tunnel connection, and split tunneling is disabled, the default route is modified to send all network traffic from the endpoint through the VPN tunnel where it is bound by the VPN access control and resource polices. If you set route precedence to endpoint routes, all network traffic goes through the VPN tunnel except traffic that is destined for directly-connected (local) subnets and indirectly connected (routed) subnets. Pulse Clients for Windows and OS X also support the following option to permit limited access to the local network:

- If the Pulse Client connection set is configured to allow the user to override the connection policy, the user can manually suspend the active Pulse Client connection to enable access to the local network. In the network in Figure 4 the user could suspend the Pulse Client connection to access the local printer, which resides on the same subnet as the Pulse Client endpoint. Suspending the Pulse Client connection is a manual method. The user must suspend the connection to access to local subnet and then resume the connection to restore connectivity through the tunnel. While the connection is suspended, no traffic goes through the tunnel.
- You can configure the split tunneling properties to allow access to the local subnet. With split tunneling disabled and local subnet access allowed, network traffic goes through the tunnel except for addresses that are on the local subnet. In the network in Figure 4 the user could print to the local printer but other traffic would go through the default route to the tunnel. No traffic would go through the subnet router 192.168.0.2.

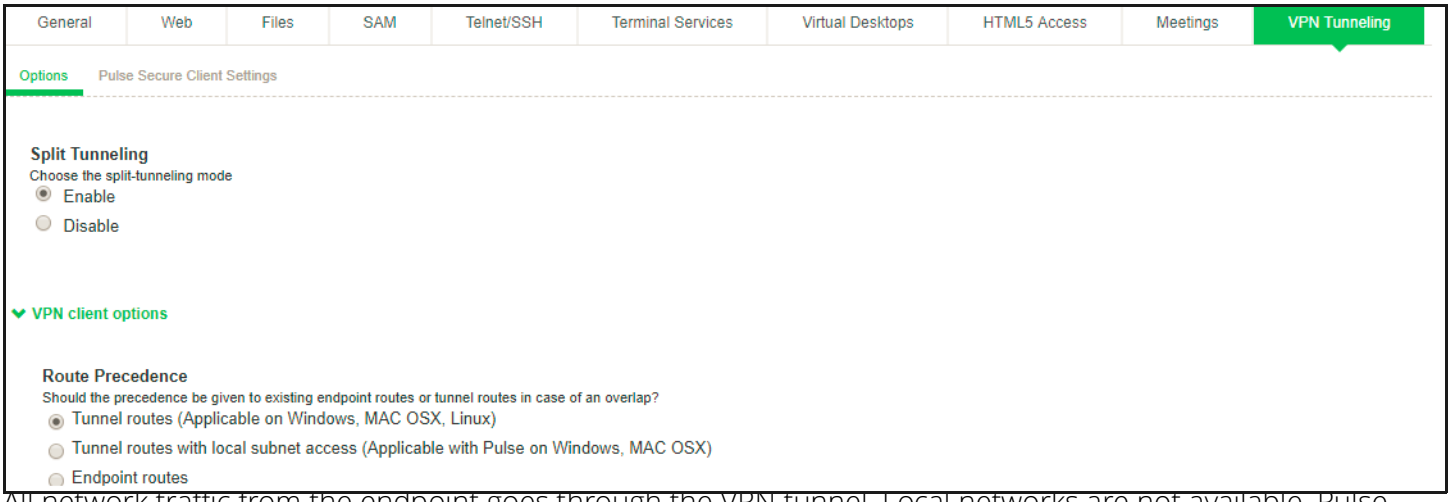
Split Tunneling Enabled

When the endpoint has an active VPN connection, and split tunneling is enabled for the role, Pulse Connect Secure adds or modifies routes on the endpoint so that traffic meant for specific subnets uses the VPN tunnel, and all other traffic goes through the local physical adapter. You specify the subnets that are excluded from access or accessible through the VPN tunnel by defining split tunneling resource policies. In a case where you have identically numbered subnets on both the local network and the tunnel network, (that is, the specified split-tunnel subnet conflicts with an existing endpoint route), the route precedence setting determines the traffic path. The route monitoring option, when enabled, enhances network security by terminating the VPN tunnel if another process on the endpoint makes a change to the routing table.

Pulse Client Split Tunneling Summary

The following scenarios summarize the traffic flows that are possible with each split tunnel configuration. Split tunneling options enable you to control the network traffic on the endpoint so that you can allow the needed connectivity to users while maintaining network security.

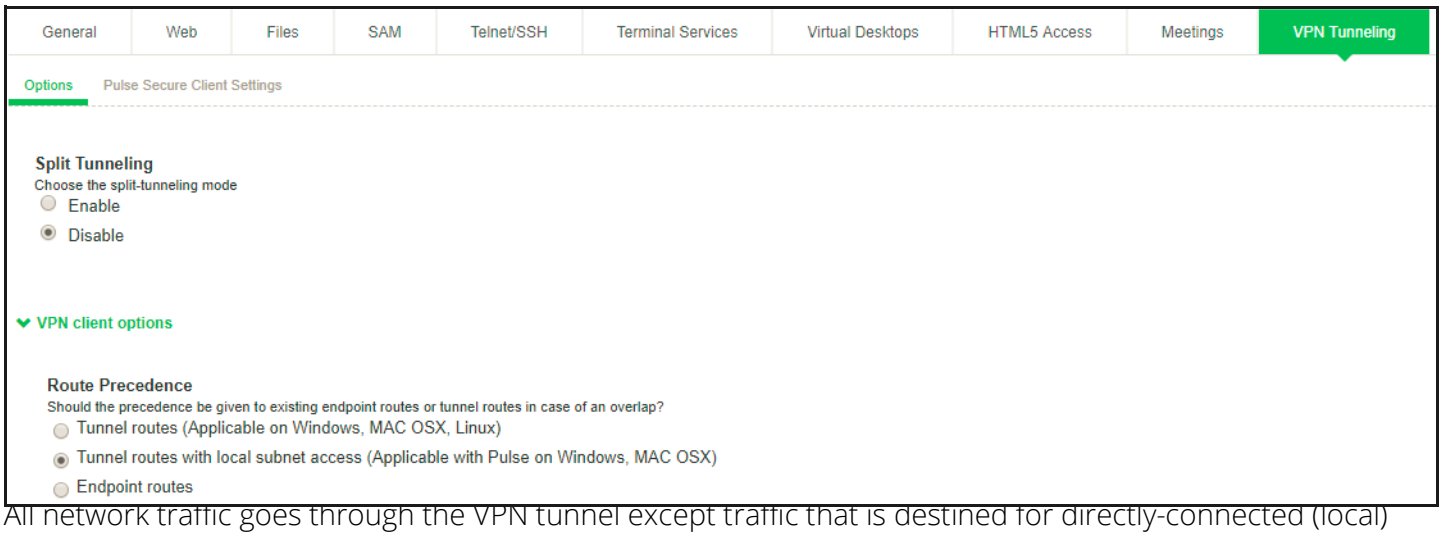
Figure 5 Split Tunneling Enabled



All network traffic from the endpoint goes through the VPN tunnel. Local networks are not available. Pulse Client users may choose to suspend the Pulse Client connection to allow local access if the Pulse Client connection set has the property Allow users to override connection policy enabled. VPN tunneling access control resource policies in effect for the user's role determine which IP resources the user can access. Split tunneling resource policies are not in effect with split tunneling disabled.

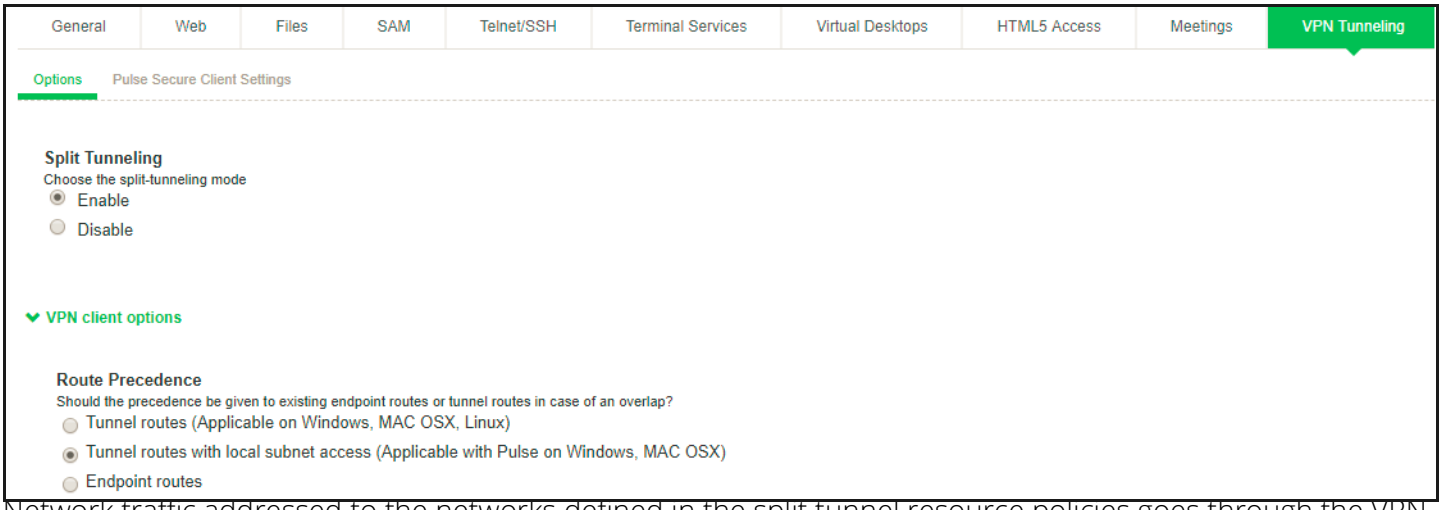
This configuration provides the best security. However, the user has no access to local network resources.

Figure 6 Split tunneling Disabled



All network traffic goes through the VPN tunnel except traffic that is destined for directly-connected (local) subnets. VPN tunneling access control resource policies in effect for the user's role determine which IP resources the user can access. Split tunneling resource policies are not in effect with split tunneling disabled.

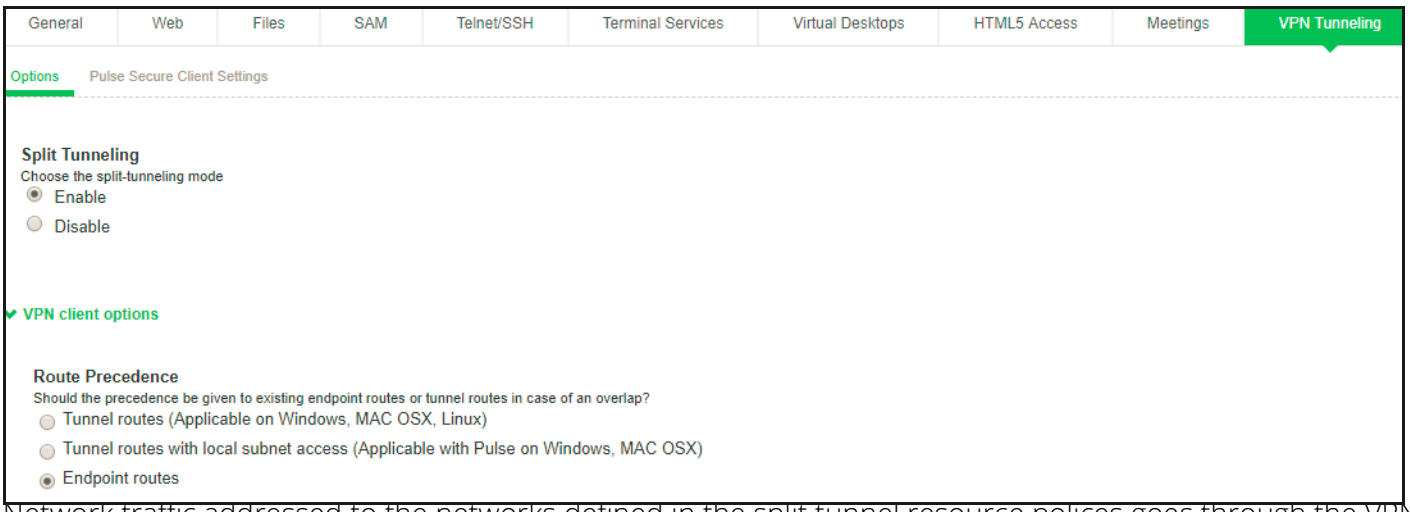
Figure 7 Split tunneling Enabled with Local Subnet Access



Network traffic addressed to the networks defined in the split tunnel resource policies goes through the VPN tunnel.

Network traffic that is addressed to the directly-connected (local) subnet goes to the local subnet. The default route is set to the local subnet so all other network traffic is subject to the original endpoint routing table.

Figure 8 Split Tunneling Enabled with Endpoint Routes



Network traffic addressed to the networks defined in the split tunnel resource polices goes through the VPN tunnel.

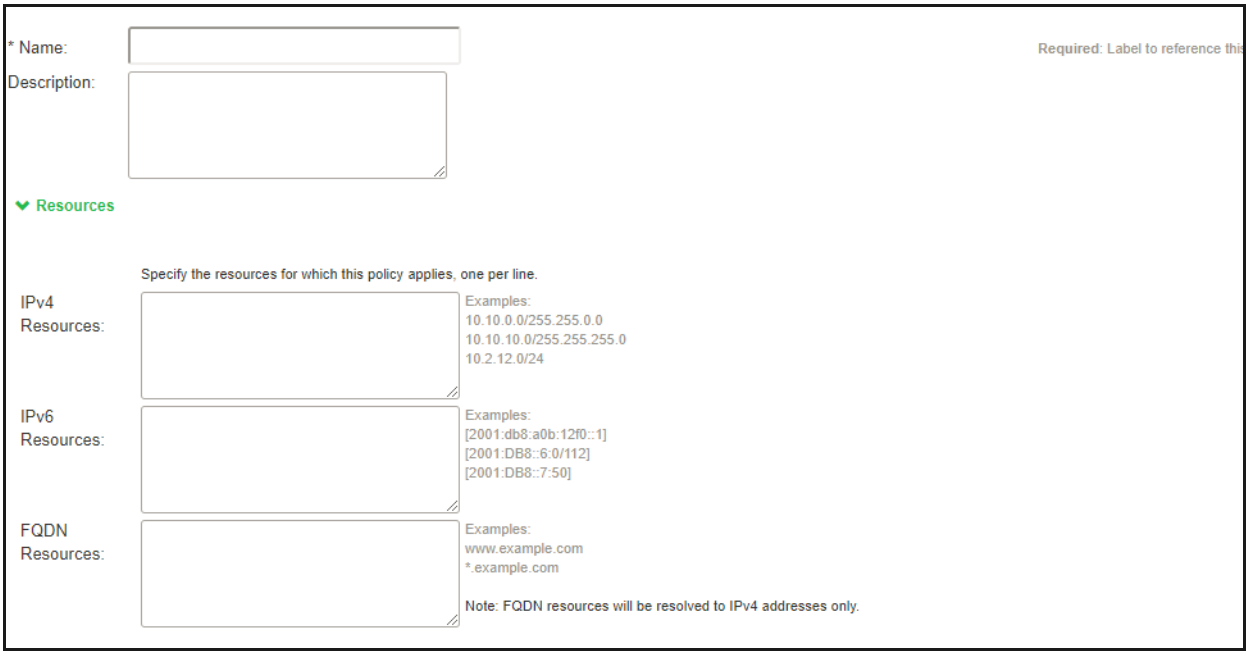
The default route is set to the local subnet so all other network traffic is subject to the original endpoint routing table.

This configuration provides the greatest flexibility for the user.

IPv6/IPv4 Split Tunneling

Pulse Client now allows accessing both IPv4, IPv6 corporate resources from IPv4 and IPv6 endpoints and FQDN resources. It enables client to access both corporate network and local network at the same time. The network traffic designated are directed to tunnel interface for corporate network by configuring route policies, whereas other traffics are sent to direct interface.

Figure 9 IPv6 Split Tunneling



Note: All configurations to IPv6 are similar to IPv4.

Table 1 Split Tunneling Deployment Scenarios

Split Tunnel	IPv4 Tunnel Address	IPv6 Tunnel Address	IPv4 Include Policy	IPv4 Exclude Policy	IPv6 Include Policy	IPv6 Exclude Policy	Expected Client Behavior
Disabled	Yes	No	NA	NA	NA	NA	All IPv4 traffic should go through tunnel.
Disabled	Yes	Yes	NA	NA	NA	NA	Both IPv4 and IPv6 traffics should go through tunnel.
Enabled	Yes	No	IPv4 include subnet Eg: 10.0.2.0/24	IPv4 exclude subnet if any otherwise Empty.	Empty	Empty	All IPv4 include traffic should go through tunnel. All IPv4 exclude traffic should go directly through physical interface.
Enabled	Yes	Yes	IPv4 include subnet Eg: 10.0.2.0/24	IPv4 exclude subnet if any otherwise Empty.	Empty	Empty	All IPv4 include traffic should go through tunnel. All IPv4 exclude traffic should go directly through physical interface. All IPv6 traffic should go through the tunnel.
Enabled	Yes	Yes	Empty	Empty	IPv6 include subnet Eg: [fc00:0:0:2::/64]	IPv6 exclude subnet if any otherwise Empty	All IPv4 traffic should go through the tunnel. All IPv6 traffic included traffic should go through tunnel. All IPv6 exclude traffic should directly go through physical interface.

Split Tunnel	IPv4 Tunnel Address	IPv6 Tunnel Address	IPv4 Include Policy	IPv4 Exclude Policy	IPv6 Include Policy	IPv6 Exclude Policy	Expected Client Behavior
Enabled	Yes	Yes	IPv4 include subnet Eg: 10.0.2.0/24	IPv4 exclude subnet if any otherwise empty	IPv6 include subnet [fc00:0:0:2::/64]	IPv6 exclude subnet if any otherwise Empty	All IPv4 include traffic should go through tunnel. All IPV4 exclude traffic should go directly through physical interface. All IPv6 include traffic should go through tunnel. All IPv6 exclude traffic should go directly through physical interface.
Enabled	Yes	Yes	1st policy: 10.0.2.0/24 2nd policy: empty	Empty Empty	1st policy: Empty 2nd policy: [fc00:0:0:2::/64]	Empty Empty	All IPv4 traffic to 10.0.2.0/24 should go through tunnel. Other IPv4 traffic should directly go through physical adapter. All IPv6 traffic to [fc00:0:0:2::/64] should go through tunnel. Other IPv6 traffic should go to physical adapter.

For FQDN deployment scenarios, refer to FQDN based Split Tunneling Deployment Guide.

Note: FQDN is not supported on IPv6.

Note: FQDN resource has given higher preference than IPv4 resource in case of conflict.

Split Tunneling Notes

- Pulse Connect Secure tries to resolve all DNS requests through the endpoint's physical adapter first, and then routes those that fail to the VPN tunneling adapter.

Configuring a Role for Pulse Connect Secure

A user role defines session settings and options, personalization settings (user interface customization and bookmarks), and access features (Web, file, application, Telnet/SSH, Terminal Services, network, meeting, and e-mail access). A user role does not specify resource access control or other resource-based options for an individual request. For example, a user role can define whether a user can perform Web browsing when the user is connected through the Pulse Connect Secure server Web portal. However, the individual Web resources that a user can access are defined by the Web resource policies that you configure separately.

The following procedure describes the role configuration options.

To create a role for Pulse Client endpoints:

1. Select **Users > User Roles > New User Role** in the admin console.
2. Enter a name for the role and, optionally, a description. This name appears in the list of roles on the Roles page.
3. Under Client Options, select **Pulse Secure**.

   When this option is enabled, the Pulse Secure button appears on the Connect Secure Web portal. When a user clicks it, Pulse Client is downloaded and installed on the user's endpoint.

   Enabling this option alone does not enable Pulse Client for the role. This option works in conjunction with the settings you enable in the Access Features section and then configure on the respective role tabs. The combination of settings determines whether you enable Pulse Client, Pulse Secure Application Manager (SAM), or Network Connect. The following procedures describe how to enable each client option.

   To enable Pulse Client:

   1. In the role's **General > Overview > Options** section select **Pulse Secure**.
   2. This setting applies to both Windows and Apple OS X versions of Pulse Client.
   3. In the Access Features section select **VPN Tunneling**.

      The VPN Tunneling tab enables you to specify split tunnel behavior, specify the Pulse Client component set, and enable 3rd-party software integrations.

   To enable Pulse Secure for SAM:

   1. In the Options section select **Pulse Secure**.
   2. In the Access Features section select **Secure Application Manager** and then select **Windows version**.

      The SAM tab enables you to specify applications and servers secured by SAM.

   To enable Network Connect:

   1. In the Options section make sure **Pulse Secure** is disabled.
   2. In the Access Features section select **VPN Tunneling**.
   3. Click **Save Changes**. Role configuration tabs appear.

Note: When the Pulse Secure option is enabled and no other access method (VPN Tunneling, WSAM) is enabled, then no client will be delivered.

Configuring General Role Options for Pulse Connect Secure

The General tab includes options for detailed control of how Pulse Client interacts with the server and the network. The following describes the options that apply to Pulse Client.

General > Restrictions

- **Source IP**: Control from which IP addresses users can access the Web portal sign-in page, be mapped to a role, or access a resource.
- **Browser**: Allow or deny access to the role based on the browser's user agent string.
- **Certificate**: Allow all users or only users with a signed client-side certificate.
- **Hot Checker**: Select configured Host Checker policies to enforce with this role.

General > VLAN/Source IP

- **VLAN and Select Source IP**: To direct traffic to specific sites based on the role, you can define a source IP alias for each role and then use the alias to configure virtual ports you define for the internal interface source IP address. A back-end device can then direct end user traffic based on the alias. This capability enables you to direct various end users to defined sites based on their roles, even though all of the end user traffic has the same internal interface source IP address.

General > Session Options

- **Idle Timeout**: The maximum time a session can remain idle (no traffic) before the server ends the session.
- **Max. Session Length**: The maximum time for a session before the server ends the session.
- **Reminder Time**: When the Enable Session Extension feature is enabled, the Reminder Time specifies the number of minutes prior to a session end when the server sends a notice through Pulse Client and notifies the user that the session will end soon.
- **Enable Session Extension**: Allows the user to extend the session. The user can choose to extend the session at any time by selecting a menu option in the Pulse Client interface. If the Session Timeout Warning is selected. a notice message appears when the Reminder Time is reached and the user can choose to extend the session from within that notice message.
- **Enable Session Timeout Warning**: Enables or disables the session timeout warning, which notifies the user when their Pulse Client session is close to expiring. The Reminder Time value specifies the point at which the reminder appears.
- **Roaming Session**: Select one of the following options to specify Pulse Client's roaming behavior:
- **Enabled**: A roaming session allows a user to retain connectivity when moving a device, such as a laptop with a dynamic IP address, from one subnet to another. Disable this feature to prevent users from accessing a previously established session from a new source IP address. Disabling roaming can help protect against an attack that spoofs a user's session.

- **Limit to Subnet**: Limit the roaming session to the local subnet specified in the endpoint's IP configuration. Users can sign in from one IP address and continue using their sessions with another IP address as long as the new IP address is within the same subnet.
- **Disabled**: Disable roaming user sessions for users mapped to this role.
- **Browser Session Cookie**: Select Enabled to remove the Connect Secure session cookie and log users out of their Connect Secure web session after Pulse Client is launched. Removing the browser session cookie enhances Pulse Client session security.

General > UI Options

- **UI Options**: The settings on this page define the Pulse Connect Secure Web portal page.

SAM > Applications

- **Add Application**: We recommend that you use resource profiles to specify the applications available to users, but you can use role and resource policy settings instead.

SAM > Options

- **Auto-uninstall Secure Application Manager**: This feature is not applicable to the Windows Phone client. Users must download and install Pulse Client for Windows Phone before the Windows Phone device can connect to the Pulse Connect Secure.
- **Prompt for username and password for intranet sites**: If you enable this option, the Pulse Connect Secure requires users to enter sign-in credentials before connecting to sites on your internal network. This option changes Internet Explorer's intranet zone setting so that Internet Explorer always prompts the user for network sign-in credentials for an intranet site.
- **Auto-upgrade Secure Application Manager**: This feature is not applicable to the Pulse Client for Windows Phone app.
- **Resolve only hostnames with domain suffixes in the device DNS domains**: If you enable this option, users can only browse to Web sites that are part of their login domain.
- **Session start script and Session end script**: This feature is not applicable to the Pulse Client for Windows Phone app.

Configuring Role Options for Host Checker for Pulse Connect Secure

Host Checker options allow you to enable configured Host Checker policies, to choose one or more policies for the role, and to specify whether the endpoint must meet all or just one of the selected Host Checker policies. Before you can assign Host Checker policies for a role, you must have already defined the policies.

To configure Host Checker for a selected role:

1. For a selected role, select **General > Restrictions > Host Checker**.
2. Select the check box **Allow users whose workstations meet the requirements specified by these Host Checker policies**.
3. Click **Add** to move Host Checker policies from the "Available Policies" list to the "Selected Policies" list.
4. Select the check box **Allow access to the role...** to grant access if the endpoint passes any of the selected Host Checker policies.

5. Click **Save Changes**.

Machine Authentication for Pulse Connect Secure Overview

Machine authentication uses machine credentials (machine name and password or machine certificate) to authenticate the endpoint. You can enable machine authentication for Pulse Connect Secure as part of a Pulse Client connection and distribute the connection to endpoints through the normal Pulse Secure distribution methods. You enable machine authentication support on a Pulse Client connection, either Layer 2 or Layer 3.

The following describes the requirements for a machine authentication environment:

- The authentication server used by the Pulse Client connection must be Active Directory/Windows NT for machine name/password authentication or a certificate server for machine certificate authentication.
- The endpoint must be a member of a Windows domain, and the machine credentials must be defined in Active Directory.
- The Pulse Client connection must be configured so that no prompts are presented during the login process. For example, prompts for realm or role selection or for a server certificate trust prompt cause the connection to fail. You can specify a preferred role and realm for the connection, which eliminates realm and role selection dialogs.

Note: If the Pulse Client connection is configured to use a list of Pulse Secure servers, the preferred roles and realms you specify must be applicable to all of those servers.

- For machine certificate authentication, the domain workstation login certificate must be issued by the domain certificate authority. The root certificate must be in the Machine Trusted Certificate store instead of the certificate store for a particular user.

Pulse Secure supports the following machine authentication types:

- **machine-only**: The connection is established using machine credentials when no user is logged in. The connection is maintained after user login.
- **user-after-desktop**: The connection is established using machine credentials when no user is logged in. After user login, the machine connection is disconnected. Once the user logs out, the user connection is disconnected and the machine connection is reestablished.

Credential Provider Authentication for Pulse Connect Secure Overview

When Microsoft introduced Windows Vista, it moved away from a login integration interface based on GINA (Graphical Identification and Authentication) in favor of credential provider authentication. Pulse Client credential provider integration enables connectivity to a network that is required for the user to login to the Windows domain. For example, the domain controller might reside behind a firewall and the endpoint uses credential provider login to connect to Pulse Connect Secure prior to domain login. Pulse Client integrates with Microsoft credential providers to enable password-based login and smart card login. Credential provider login is supported on Windows 8.1 and later Windows platforms.

You can use Pulse Client's support for credential provider to provide single sign-on capabilities. Pulse Client establishes a connection to the network and then uses the same credentials to login the Windows domain.

You enable Pulse Client credential provider support on a Pulse Client connection, (connection type UAC 802.1X (UAC) or SSL VPN (L3)). After the connection has been downloaded to the endpoint through the normal Pulse Client distribution methods, Pulse Client annotates the credential provider tile that appears on the user login screen by adding a Pulse Secure icon in the lower right corner of the tile.

Pulse Client supports the following credential provider types:

- **user-at-credprov**: The connection is established before the user login using credentials collected at the selected credential tile, which provides single-sign-on functionality. The connection is maintained as an active connection on the user's desktop.
- **machine-then-user-at-credprov**: The connection is established using machine credentials when no user is logged in. When a user clicks a login tile and provides user credentials, the machine connection is disconnected and a new connection is established. When the user logs out, the user connection is disconnected and the machine connection is reestablished. In one typical machine-then-user-at-cred prov implementation, the machine connection and the user connection are mapped to different VLANs.

Pulse Client credential provider support usage notes:

- If the endpoint includes more than one Pulse Client Layer 2 connection, Windows determines which connection to use:

  1. If a network cable is attached to the endpoint, Layer 2 wired connections are attempted, and then wireless connections. If there is more than one wireless network available, the order is determined by the scan list specified as a Pulse Client connection option.
  2. After all Layer 2 options are attempted, Pulse Client runs location awareness rules to find one or more eligible Layer 3 connections that are configured for credential provider login. If more than one Layer 3 connection is found, Pulse Client prompts the user to select a connection. A user can cancel the network connection attempt by clicking the cancel button.
  3. After Pulse Client evaluates all configured connection options, Pulse Client returns control to Windows, which enables the user login operation.

- For connections that use user credentials, the Pulse Client connection can be configured so that prompts are presented during the login process, for example, prompts for realm or role selection or a server certificate trust prompt. For connections that use machine credentials, Pulse Client prompts cause the connection to fail because there is no interface to allow a response to the prompts. You can suppress any potential realm and role choice by specifying a preferred realm and role for the connection.
- Pulse Client upgrade notifications and actions are disabled during credential provider login and postponed until the user connection is established. Host Checker remediation notifications are displayed.

Configuring Role Options for Pulse Connect Secure

All of the options for role configuration tabs are described in *User Access Management Framework Feature Guide*.

To configure role options for Pulse Client endpoints:

1. From the Pulse Connect Secure admin console, select **Users > User Roles**.
2. Click the role you want to configure and then click the **VPN Tunneling** tab.

3. Under "Split Tunneling Options", select your options:

   General VPN Options apply to all Layer 3 VPN clients, Pulse Client (Windows, OS X, iOS, and Android), Network Connect, and third-party IKEv2 clients:

   - **Split Tunneling**: Split tunneling options let you define how network traffic flows on the client.

     Enable: Pulse Client modifies routes on the client so that traffic meant for the corporate intranet uses the virtual adapter created by Pulse Client (the Pulse Client tunnel) and all other traffic goes through the local physical adapter.

     Disable: When the client session is established, predefined local subnet and host-to-host routes that might cause split-tunneling behavior are removed, and all network traffic from the client goes through the Pulse Client tunnel. With split tunneling disabled, users cannot access local LAN resources during an active VPN session. However, when you create a Pulse Client connection for users, if you allow users to override you can enable an option that allows the user to suspend their VPN connection. While a Pulse Client connection is in the suspended state, all traffic goes through the local physical adapter.

   Pulse Secure client options apply only to Pulse Client and Network Connect:

   - **Route Precedence**: You can define which routing table takes precedence:

     Tunnel Routes: The route table associated with the Pulse Client virtual adapter takes precedence. Pulse Client overwrites the physical interface routes if there is conflict between the Pulse Client virtual adapter and the physical adapters. Pulse Client restores the original routes when the connection is ended.

     Tunnel Routes with local subnet access (Pulse Client on Windows and macOS only): Network traffic addressed to the networks defined in the split tunnel resource policies goes through the VPN tunnel. Network traffic that is addressed to the directly-connected (local) subnet goes to the local subnet. The default route is set to the local subnet so all other network traffic is subject to the original endpoint routing table.

     Endpoint Routes: The route table associated with the endpoint's physical adapter take precedence.

   - **Route Monitor**: Pulse Client can monitor the route tables and take appropriate action.

     Yes: VPN tunneling ends the connection only if the route change affects the VPN tunnel traffic. For example, if the route metric is changed higher, it should not disconnect VPN tunneling.

     No: Route tables are allowed to change on the client endpoint.

   - **Traffic Enforcement**: When Traffic Enforcement is enabled, Pulse Client creates rules on the endpoint's firewall (macOS and Windows) that ensure that all traffic conforms to the Pulse Connect Secure tunnel configuration.

     A local program might bypass the endpoint's routing tables and bind traffic to the physical interface instead of allowing it to go through the Pulse Client virtual interface. If you enable traffic enforcement, you ensure that all traffic is bound by the Pulse Connect Secure tunnel configuration.

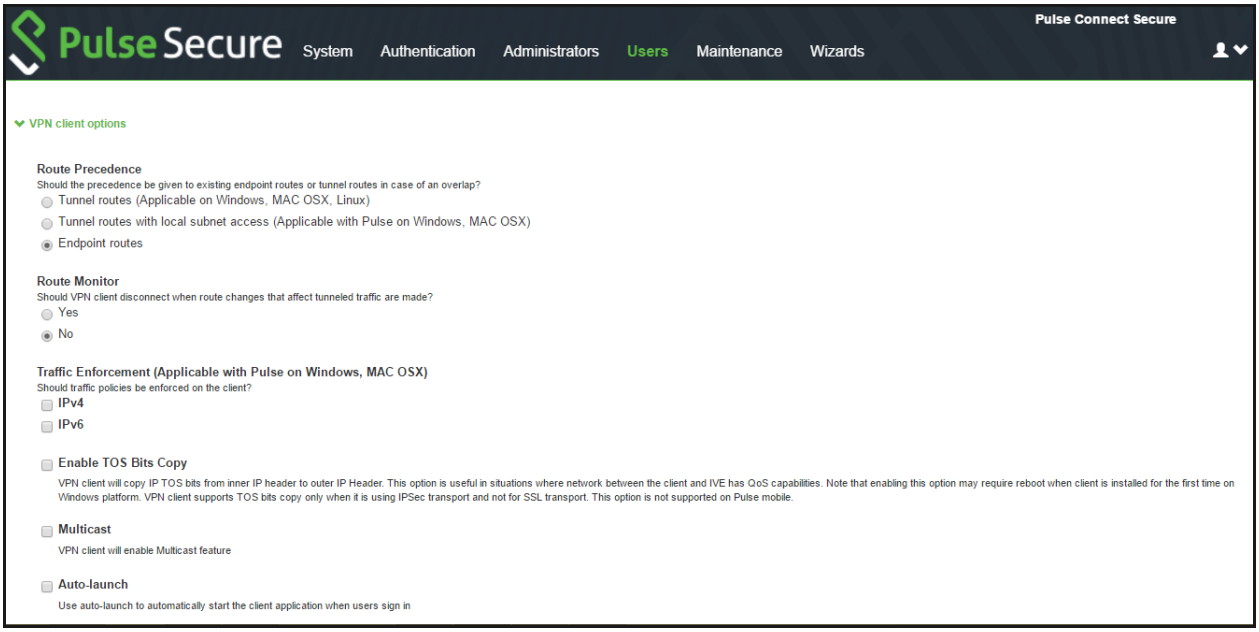
     IPv4: When this check box is selected all IPv4 traffic is bound by the Pulse Connect Secure tunnel configuration.

     IPv6: When this check box is selected all IPv6 traffic is bound by the Pulse Connect Secure tunnel configuration.

Typically, if you wanted to enable traffic enforcement, you would enable both options. Enabling only one option is useful for nested tunnel (tunnel-in-tunnel) configurations. See the *Pulse Secure Supported Platforms Guide* for supported nested tunnel configurations.

- **Enable TOS Bits Copy**: Enables you to control the client behavior in networks that employ Quality of Service (QoS) protocols. When you enable this check box, Pulse Client copies IP Type of Service (TOS) bits from the inner IP header to outer the IP Header. Note that enabling this option might require a reboot of the client endpoint when Pulse Client software is installed for the first time on Windows endpoints. Pulse Clients support TOS bit copy only for IPSec transport and not for SSL transport.
- **Multicast**: Enables the multicast feature on Pulse Client when this option is selected.
- **Auto-launch**: Activates Pulse Client software automatically when the endpoint is started when this option is selected.

Figure 10 VPN Client Options



Options for Pulse Secure client on Windows apply only to Pulse Client and Network Connect on Windows endpoints:

- **Launch client during Windows Interactive User Logon**: When this option is enabled, Pulse Client starts when the user logs into Windows. Note that this setting is not the same as the Pulse Client connection settings that control machine authentication and credential provider authentication. Choose one of the following options:

Require client to start when logging into Windows

Allow user to decide whether to start client when logging into Windows

- **Windows: Session start script**: Specify a script (.bat, .cmd, or .exe) to run for users assigned to the role after Pulse Client connects with Pulse Connect Secure. For example, you can specify a script that maps network drives on an endpoint to shares on protected resources.

- **Windows: Session end script**: Specify a script (.bat, .cmd, or .exe) to run for users assigned to the role after Pulse Client disconnects from Pulse Connect Secure. For example, you can specify a script that disconnects mapped network drives. If there is no start script defined, or the start script has not been run, the end script does not run.
- **Skip if Windows Interactive User Logon Enabled**: Select this option to bypass the specified Windows session start script.
- If the client signs in to their Windows Domain via the Credential Provider automatic sign-in function, a script is executed by the Windows Pulse Client. In this case, the sign-in script might be identical to the specified VPN Tunneling start script. You can use this option, therefore, as a way to avoid executing the same script twice.

Options for Pulse Secure client on Mac apply only to Pulse Client and Network Connect on Apple OS X endpoints:

- **Mac: Session start script**: Specify a script (.bat, .cmd, or .exe) to run for users assigned to the role after Pulse Client connects with Pulse Connect Secure. For example, you can specify a script that maps network drives on an endpoint to shares on protected resources.
- **Mac: Session end script**: Specify a script (.bat, .cmd, or .exe) to run for users assigned to the role after Pulse Client disconnects from Pulse Connect Secure. For example, you can specify a script that disconnects mapped network drives. If there is no start script defined, or the start script has not been run, the end script does not run.

4. In the Session scripts area, optionally specify a location for the following:
   - **Windows: Session start script**: Specify a script (.bat, .cmd, or .exe) to run for users assigned to the role after Pulse Client connects with Pulse Policy Secure. For example, you can specify a script that maps network drives on an endpoint to shares on protected resources. The script must be in a location (either local or on the network) that is accessible by the user.
   - **Windows: Session end script**: Specify a script (.bat, .cmd, or .exe) to run for users assigned to the role after Pulse Client disconnects from Pulse Policy Secure. For example, you can specify a script that disconnects mapped network drives. If there is no start script defined, or the start script has not been run, the end script does not run. The script must be in a location (either local or on the network) that is accessible by the user.
5. Click **Save Changes**.

Configuring User-at-Credprov Credential Provider Authentication for a Pulse Client Connection

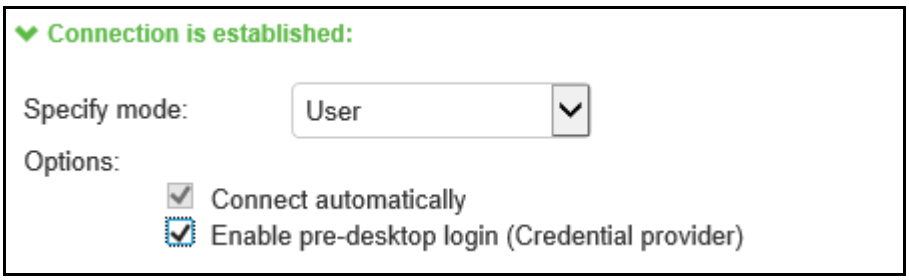
With a user-at-credprov connection, the Pulse Client connection establishes the connection before user login using credentials collected at the selected credential tile, which provides single sign-on functionality. The connection is maintained as an active connection on the user's desktop.

To enable user-at-credprov credential provider support for a Pulse Client connection:

1. Create a Pulse Client connection set for the role (**Users > Pulse Secure > Connections**), and then create a new Pulse Client connection. You can select either a Layer 3 connection type, Connect Secure or Policy Secure (L3), or a Layer 3 connection type, UAC (802.1X).
2. In the Connection is established section, select "User" for the mode.

3. Under Options, select the **Connect automatically** and the **Enable pre-desktop login (Credential provider)** check boxes.

   Figure 11 Connect automatically at user login



4. For a Layer 2 connection that uses machine certificate authentication, make sure that the connection has an entry in the Trusted Server List. To allow any server certificate, type ANY as the Server certificate DN. To allow only one server certificate, specify the server certificate's full DN, for example, C=US; ST=NH; L=Kingston; O=My Company; OU=Engineering; CN=c4k1.stnh.mycompany.net; E=ausername@mycompany.com.

5. Specify **Realm and Role Preferences** to suppress realm or role selection dialogs during the login process:

   - **Preferred User Realm**: Specify the realm for this connection. The connection ignores any other realm that is available for the specific login credentials.

     The following options enable you to allow the user to login using a smart card or a password:

     - **Preferred Smartcard Logon Realm**: Preferred realm to be used when user logs in with a smart card.
     - **Preferred Password Logon Realm**: Preferred realm to be used when user logs in with a password.

Note: Be sure that the authentication realms you specify exist, and that they support the appropriate login credential option.

   - **Preferred User Role Set**: Specify the preferred role or the name of the rule for the role set to be used for user authentication. The role or rule name must be a member of the preferred user realm.

   Note: If the Pulse Client connection is configured to use a list of Pulse Secure servers, the preferred roles and realms you specify must be applicable to all of those servers.

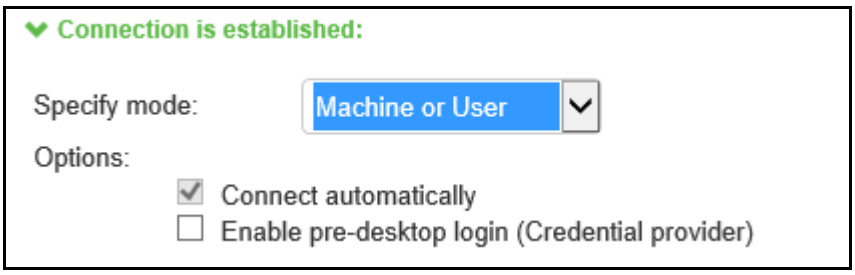
Configuring Machine-Then-User-at-Credprov Credential Provider Authentication for a Pulse Client Connection

With a machine-then-user-at-credprov connection, Pulse Client establishes the connection using machine credentials when no user is logged in. When a user clicks a login tile and provides user credentials, the machine connection is disconnected, and a new connection is established. When the user logs out, the user connection is disconnected, and the machine connection is reestablished. In one typical machine-then-user-at-credprov implementation, the machine connection and the user connection are mapped to different VLANs.

To enable machine-then-user-at-credprov credential provider support for a Pulse Client connection:

1. Create a Pulse Client connection set for the role (**Users > Pulse Secure > Connections**), and then create a new Pulse Client connection. You can select either a Layer 3 connection type, Connect Secure or Policy Secure (L3), or a Layer 2 connection type, Policy Secure (802.1X).
2. In the Connection is established section, select "User or Machine" for the mode.
3. Under Options, select the **Connect automatically** check box.

   Figure 12 Connect automatically when the machine starts. Connection is authenticated again at user login



4. In the Connection is established section, select one of the following options:
5. For a Layer 2 connection that uses machine certificate authentication, make sure that the connection has an entry in the Trusted Server List. To allow any server certificate, type ANY as the Server certificate DN. To allow only one server certificate, specify the server certificate's full DN, for example, C=US; ST=NH; L=Kingston; O=My Company; OU=Engineering; CN=c4k1.stnh.mycompany.net; E=ausername@mycompany.com.
6. Specify Realm and Role Preferences to suppress realm or role selection dialogs during the login process for both machine and user logins:

   - **Preferred Machine Realm**: Specify the realm that this connection uses when establishing the machine connection. The connection ignores any other realm that is available for the specific login credentials.
   - **Preferred Machine Role Set**: Specify the role or the name of the rule for the role set that this connection uses when establishing the machine connection. The role or rule name used must be a member of the preferred machine realm.
   - **Preferred User Realm**: Specify the realm that for this connection that is used when a user logs in to the endpoint. The connection ignores any other realm that is available for the user's login credentials.

   The following options enable you to allow the user to log in using a smart card or a password:

   - **Preferred Smartcard Logon Realm**: Preferred realm to be used when user logs in with a smart card.
   - **Preferred Password Logon Realm**: Preferred realm to be used when user logs in with a password.

   Note: Be sure that the authentication realms you specify exist, and that they support the appropriate login credential option.

   - **Preferred User Role Set**: Specify the preferred role or the name of rule for the role set to be used for user authentication. The role or rule name used must be a member of the preferred user realm.

Note: If the Pulse Client connection is configured to use a list of Pulse Secure servers, the preferred roles and realms you specify must be applicable to all of those servers.

7. Optionally, specify pre-login preferences:
   - **Pre-login maximum delay**: The time period (in seconds) that a Windows client waits for an 802.1X connection to succeed during the login attempt. The range is 1 to 120 seconds.
   - **Pre-login user based virtual LAN**: If you are using VLANs for the machine login, you can enable this check box to allow the system to make the VLAN change.
8. Click **Save Changes**, and then distribute the connection to Pulse Client endpoints.

Machine and User Authentication through a Pulse Client Connection for Pulse Connect Secure

Pulse Client supports certificate authentication for establishing Layer 2 and Layer 3 connections. On Windows endpoints, Pulse Client connection accesses client certificates located in the Local Computer personal certificate store to provide machine authentication or user certificates located in a user's personal certificate store or a smart card for user authentication. A Pulse Client connection can access certificates from only one location. For information on machine authentication, see "Machine Authentication for Pulse Connect Secure Overview" on page 22.

You can create a Pulse Client connection that verifies the identity of both the machine and the user before establishing a connection. There are two options for configuring this dual authentication connection. Both options employ user authentication against a Local System, Active Directory, or ACE server for user authentication and certificate authentication to verify the machine. Both options also use a Pulse Client connection option. The option, Select client certificate from machine certificate store, is part of the User Connection Preferences of a Pulse Client connection.

Option 1: Use an additional authentication server for a realm:

- Create a Pulse Client connection for the target Pulse Secure server. The connection type can be Policy Secure (802.1X) or Connect Secure or Policy Secure (L3). The Connection is established option is typically set to manually by the user or automatically at user login.
- In the User Connection Preferences section of the connection properties, click the check box labeled Select client certificate from machine certificate store. This option enables the Pulse Client connection to perform the machine authentication as part of the connection attempt.
- Create a realm sign in policy that authenticates to a certificate server. When Pulse Client provides the certificate to the server, it uses the certificate from the Local Computer certificate store, which authenticates the machine. If the certificate store holds more than one valid certificate for the connection, Pulse Client opens a dialog box that prompts the user to select a certificate.
- Create a secondary authentication server for the realm. The secondary server can be a Local System, Active Directory, or RSA ACE server. When the machine authentication is successful, the user is prompted to provide authentication credentials for the secondary authentication server.

Option 2 — Use realm authentication to authenticate the user and a certificate restriction on the realm to authenticate the machine.

- Create a Pulse Client connection for the target Pulse Secure server. The connection type can be Policy Secure (802.1X) or Connect Secure or Policy Secure (L3). The Connection is established option is typically set to manually by the user or automatically at user login.
- In the User Connection Preferences section of the connection properties, click the check box labeled Select client certificate from machine certificate store.
- Create a sign-in policy on Pulse Connect Secure that specifies a user realm. The realm authentication server can be a System Local, Active Directory, or RSA ACE server.
- Configure a certificate restriction on the realm to enable Pulse Connect Secure to request a client certificate. Be sure to enable the option labeled only allow users with a client-side certificate signed by Trusted Client CAs to sign in.

Stealth Mode

Stealth mode is the robust solution to provide a seamless authentication to the user without any user interaction when transitioning from one connection to another. This feature supports only on Windows.

Stealth mode is the robust solution to provide a seamless Step-up, Step-down experience to the end-user when transitioning from one connection to another.

Now, while configuring Pulse Connect Secure settings, the following two new checkboxes are added under connection set.

- Enable stealth mode on this connection
- Show stealth connection to user

When **Enable stealth mode** on this connection is enabled, user will not be able to see and control the established connection through the Pulse Client UI. User or machine authentication will happen seamlessly without any user interaction.

When **Show stealth connection to user** is enabled, user will be able to see the Stealth mode connection in the Pulse Client interface. User will be able to see only the connection status in Pulse Client Tray icon and an option to view Advanced Connection details. User will not be able to control any actions.

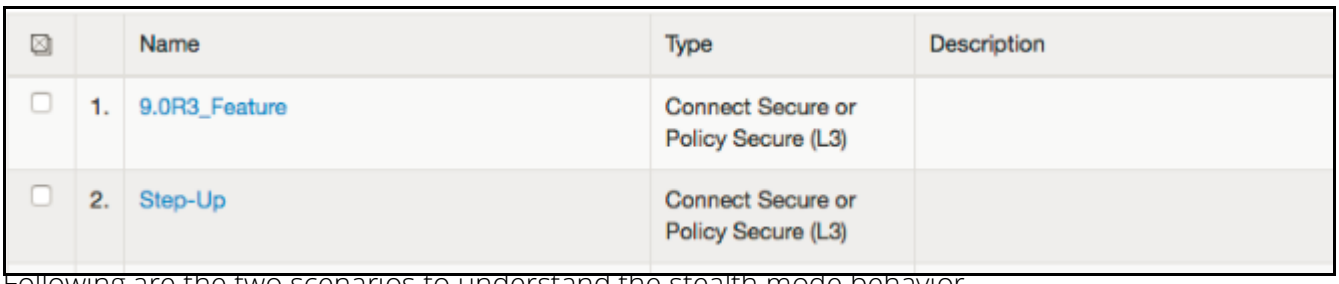
Admin can enable the checkbox **Show stealth connection to user** only when **Enable Stealth mode on this connection** checkbox is checked.

For example, admin wants to configure two connections one by stealth and another connection as non-stealth.

One is stealth enabled connection named "9.0R3_Feature" (by enabling **Enable Stealth** mode on this connection), consider it as Step-down connection.

Second connection is non-stealth configured connection named "Step-Up". Refer the following figure:

Figure 13 Connections



	Name	Type	Description
1.	9.0R3_Feature	Connect Secure or Policy Secure (L3)	
2.	Step-Up	Connect Secure or Policy Secure (L3)	

Following are the two scenarios to understand the stealth mode behavior.

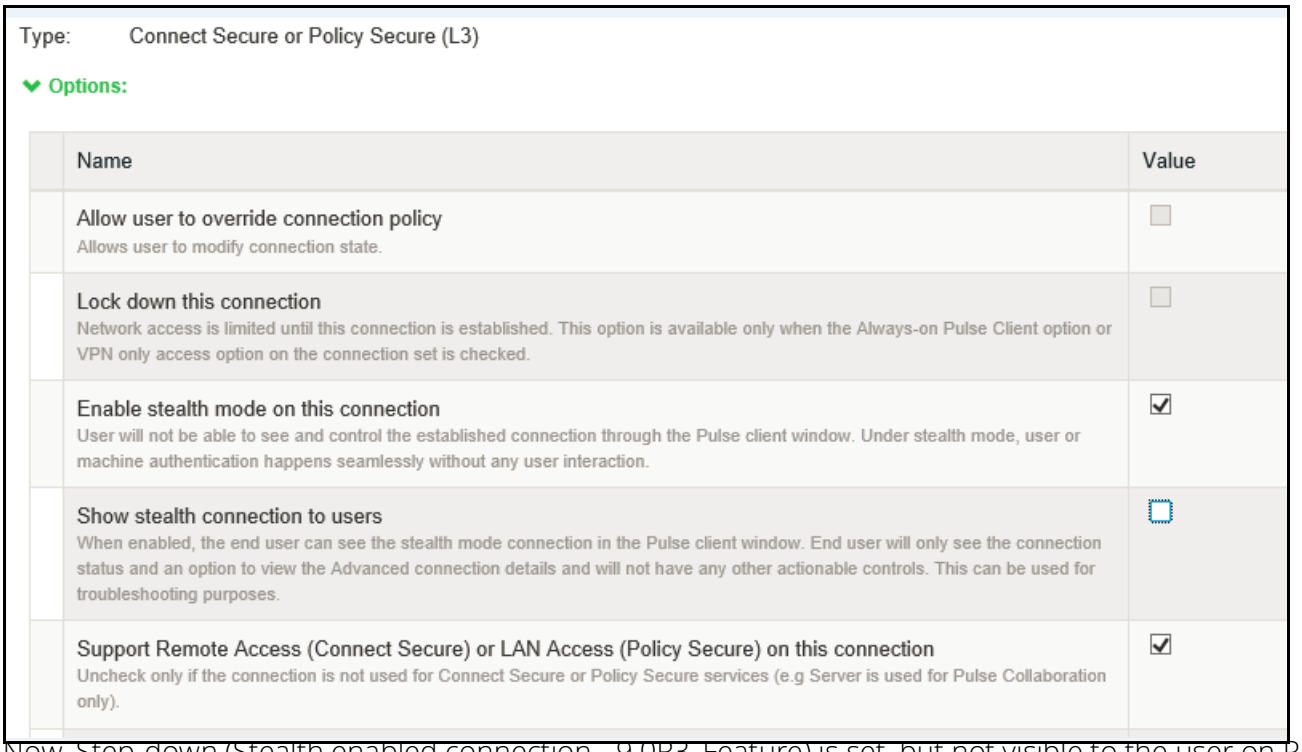
Scenario 1

Enable Stealth mode on this connection: Enabled

Show stealth connection to user: Disabled

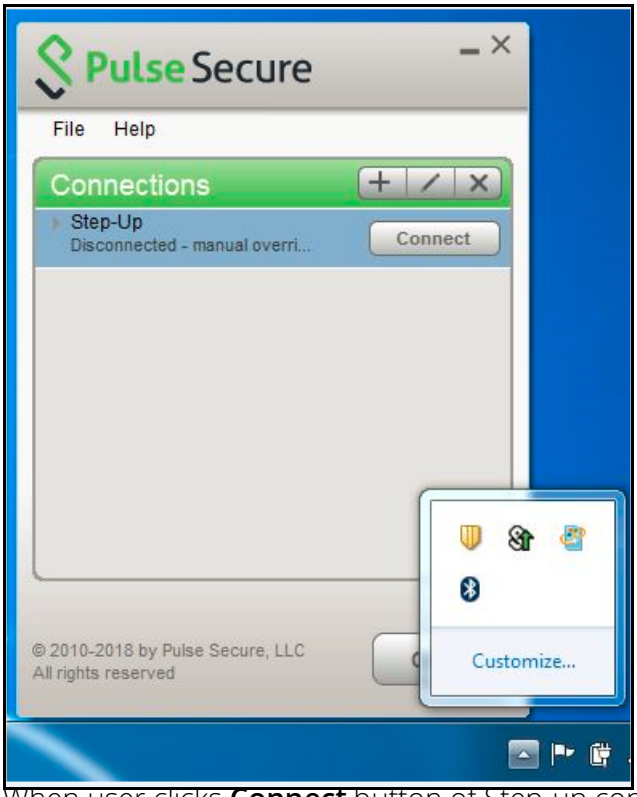
User will not be able to see configured Step-down (Stealth mode connection - 9.0R3_Feature) on Pulse Client UI. Refer to Figure 14 and Figure 15.

Figure 14 Stealth Mode Enabled



Now, Step-down (Stealth enabled connection - 9.0R3_Feature) is set, but not visible to the user on Pulse Client UI. User can only see the connection status in Pulse Client tray icon. Refer the following figure:

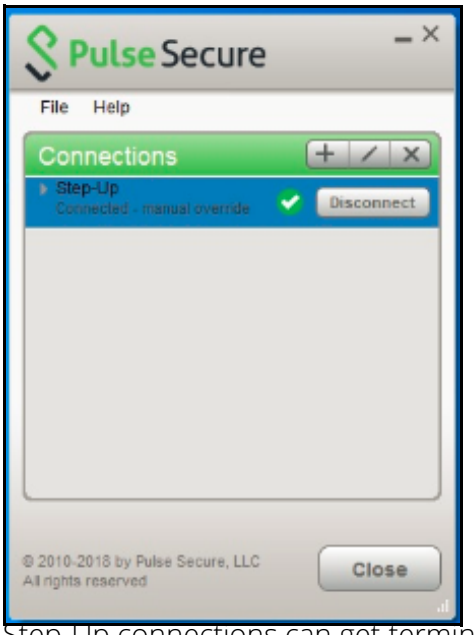
Figure 15 Show Stealth Mode Disabled



When user clicks **Connect** button of Step-up connection, Step-down (Stealth – 9.0R3 feature) gets disconnected and when user clicks **Disconnect** button to disconnect Step-up connection, step-down automatically gets connected.

Refer the following figure:

Figure 16 Step-up connection - Connected



Step-Up connections can get terminated in many scenarios for example:

- When user disconnects Step-Up connection
- Session Timeout (if user does not enter credentials once the timeout happens)
- Location Awareness becomes False

Scenario 2

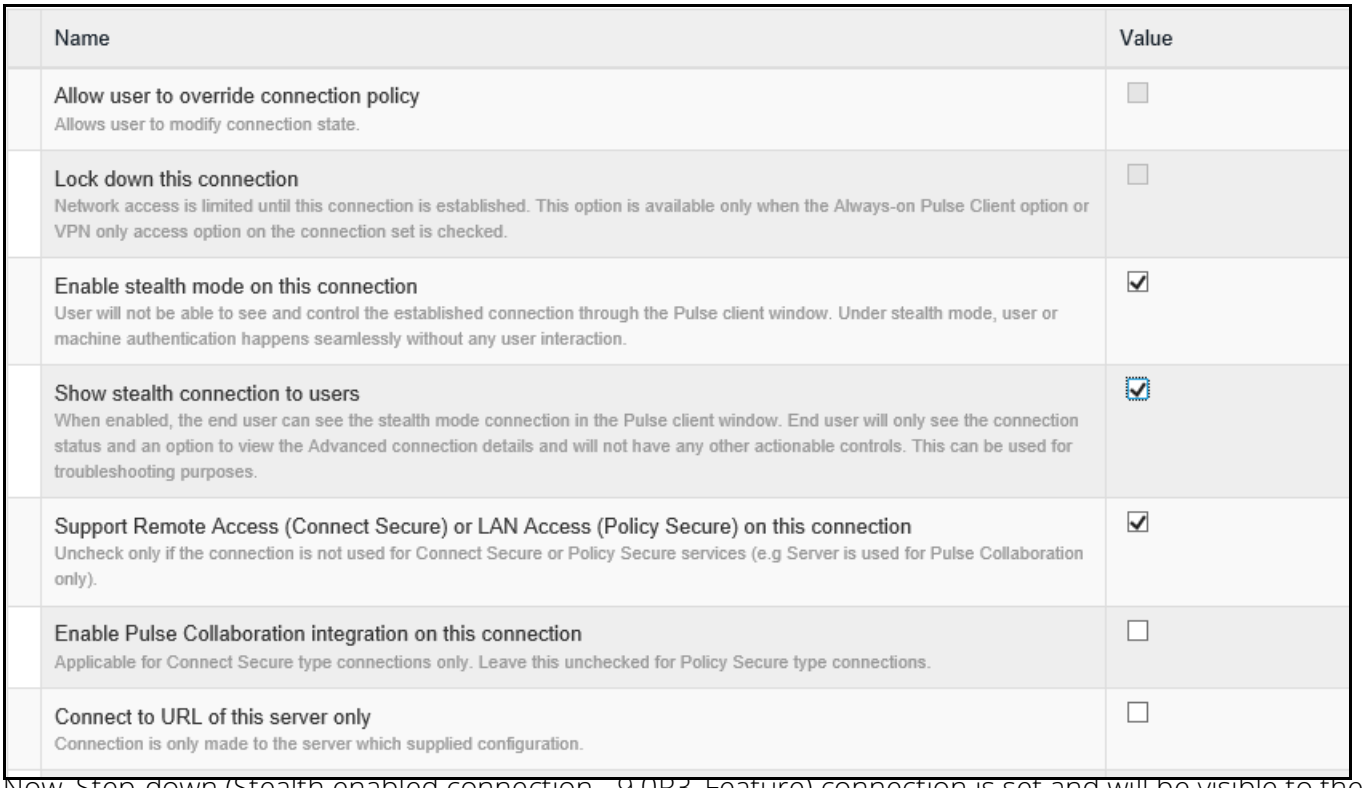
Enable Stealth mode on this connection: Enabled

Show stealth connection to user: Enabled

User will be able to see Step-down (Stealth enabled connection- 9.0R3_Feature) on Pulse Client UI.

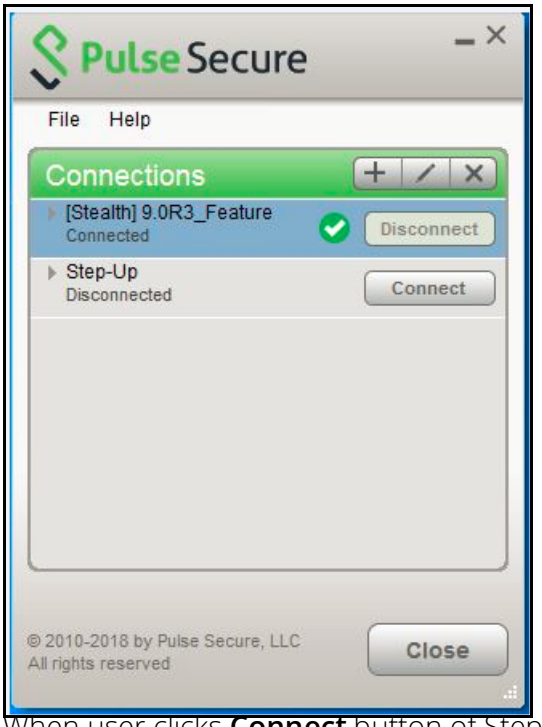
Refer the following figure:

Figure 17 Show stealth connection to users Enabled



Now, Step-down (Stealth enabled connection - 9.0R3_Feature) connection is set and will be visible to the user on Pulse Client UI. Refer the following figure:

Figure 18 Show Stealth Mode Enabled



When user clicks **Connect** button of Step-up connection, Step-down (Stealth – 9.0R3 feature) gets disconnected and when user clicks **Disconnect** button to disconnect Step-up connection, step-down connection automatically gets connected. Refer following figures (Figure 19 and Figure 20).

Figure 19 Step-Up connection - Connected

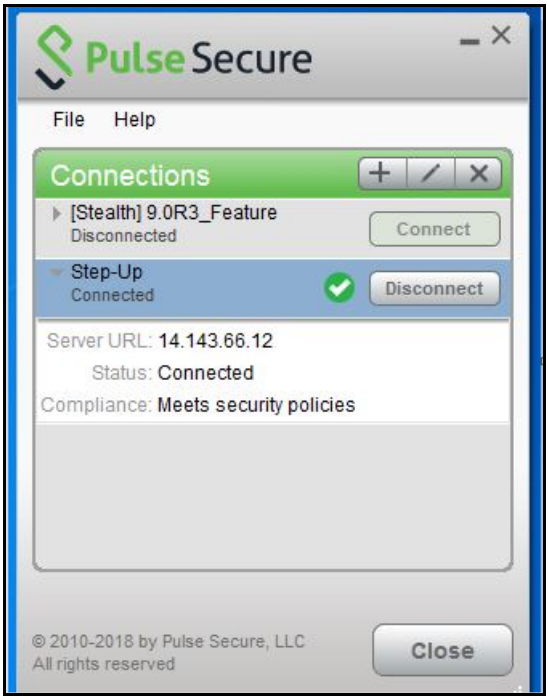
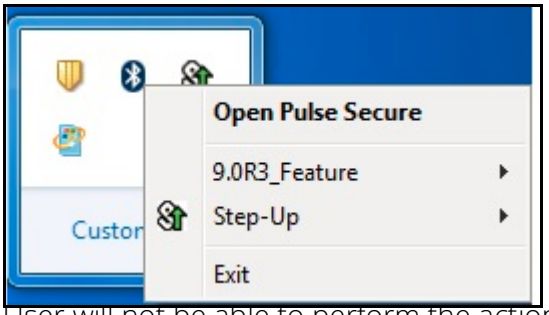


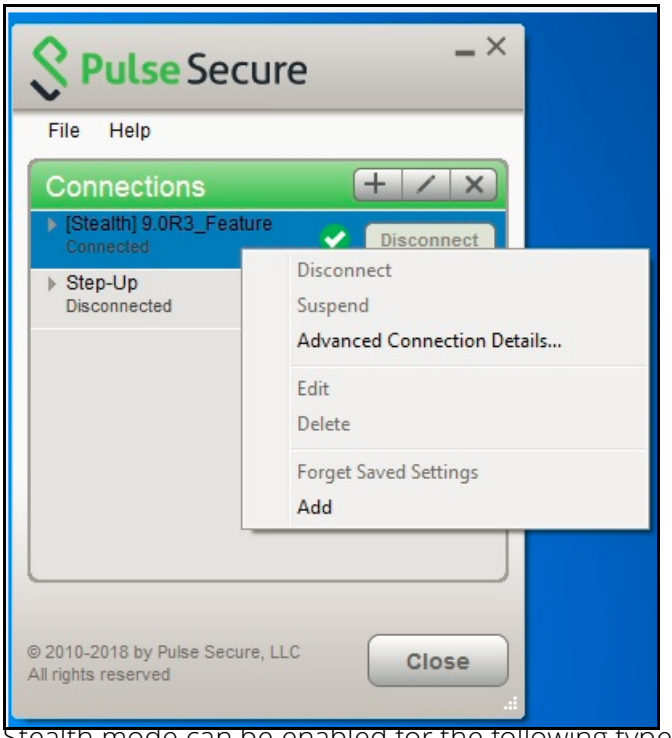
Figure 20 Step-Up connection – Pulse Client Tray icon



User will not be able to perform the actions like Disconnect, Suspend, Cancel, Edit, Delete, Forget Saved Settings. User will be able to see Advanced Connection Details and Add another connection. Refer Figure: Stealth Mode Connection – Actions

Note: When user clicks on **Add** to add another connection, it will not be in Stealth Mode.

Figure 21 Stealth Mode Connection - Actions



Stealth mode can be enabled for the following types of connections:

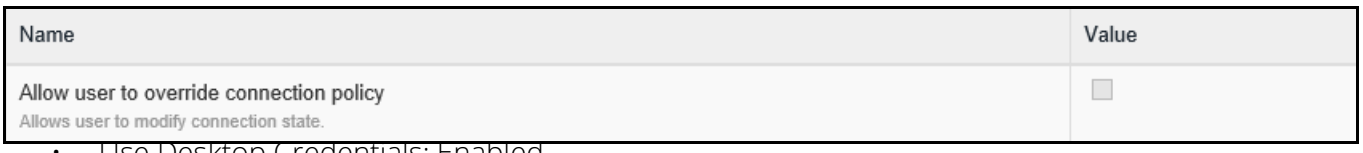
- User connection
- Machine connection
- User or Machine Connection

User would not know that a tunnel is established. Authentication could be done through AD username/ password, Cert-based, Smart-card.

The following connection settings would be non-editable by the user when the Stealth mode is enabled on a connection.

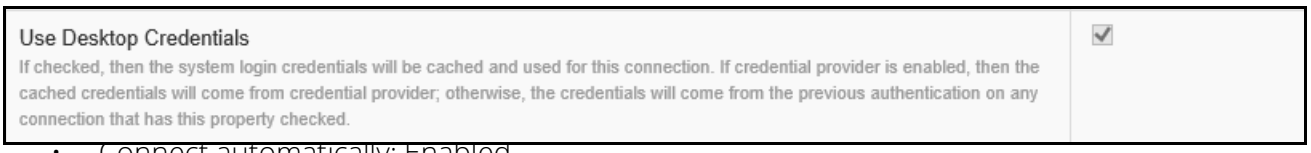
- Allow user to override connection policy: Disabled

Figure 22 Disallowing a User to Override the Connection Policy



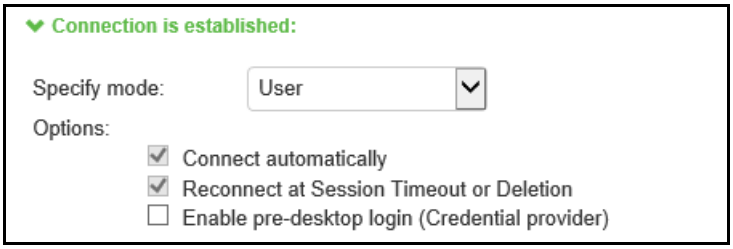
- Use Desktop Credentials: Enabled

Figure 23 Enabling the Use of Desktop Credentials



- Connect automatically: Enabled
- Reconnect at Session Timeout or Deletion: Enabled

Figure 24 Enabling Reconnect at Session Timeout or Deletion



Note: L3 and Pulse SAM Coexistence feature will not work, if L3 is configured Stealth Mode connection.

Configuring Pulse Client for Secure Application Manager

Pulse Client supports Secure Application Manager (SAM). SAM provides remote access using application names and destinations. SAM does not require a virtual adapter or virtual IP address on the endpoint. SAM provides secure access to client/server applications and thin client solutions without provisioning a VPN tunnel.

With Pulse Client R3.0 and later, SAM connectivity is provided through SSL VPN (Pulse Client connection type Connect Secure or Policy Secure (L3)). Prior to Pulse Client R3.0, SAM connectivity was provided through a separate client. Table 2 describes the progression of Pulse Secure/SAM client software.

Table 2 Pulse Client/SAM Client Version Summary

Pulse Client/ SAM Version	Supported Platforms	Description	Notes
Pulse Client R1.0 Included with SSL/ VPN software R7.0 and R7.1	Windows Mobile Windows XP Windows Vista	SAM client that is installed from the Pulse Secure server.	Supports Host Checker.
Pulse Client R2.0	Windows Mobile (6.0, 6.1, and 6.5) Pulse Client R2.0 is supported on touch-based Windows Mobile devices only.	Pulse Client for Windows Mobile smart phone app; available for download from Pulse Secure Technical Support (https://support.pulsesecure.net).	If you install Pulse Client R2.0 on a Windows Mobile device that already has Pulse Client R1.0, the installation detects the presence of the old client and removes it prior to installing the new client. It also detects and removes Host Checker. Host Checker is not supported. If Pulse Client R2.0 for Windows Mobile is installed on a Windows Mobile device, the user should not use a browser to sign into a realm that has Pulse Client R1.0 enabled. Pulse Client R1.0 cannot detect if Pulse Client R2.0 for Windows Mobile is already installed, and so it prompts the user to install Pulse Client R1.0. Note: If Pulse Client R2.0 is installed on a Windows Mobile device, and the user connects to a role that has Host Checker enabled, the user is prompted to install Host Checker. However, if the user allows the installation, nothing happens. To avoid this scenario, you should create a separate role for Pulse Client R2.0 for Windows Mobile devices.
Pulse Client R3.0 and R4.0 Included with Pulse Secure Access Service software R7.2 and later.	Windows XP Windows Vista	Pulse Client incorporates SAM functionality as a native Pulse Client connection method.	Supports Host Checker.
Pulse Client R5.0	Windows XP Windows Vista Windows 8		
Pulse Client R5.1 and later	Windows 8		

This section describes how to configure Pulse Connect Secure to support Windows endpoints. Pulse Connect Secure also supports a Java-based SAM client (JSAM). The JSAM client can be deployed from a Pulse Connect Secure server to any endpoint that supports Java.

To enable SAM for Windows endpoints and configure a role:

1. Log in to the Pulse Connect Secure admin console.
2. Select **User Roles > New User Role**.
3. On the New Role page, specify a name for the role and, optionally, a description. Make note of the name because later in this procedure, you create a realm and map realm users to this role.
4. In the Options section, select "Pulse Secure".

Note: If you leave the Pulse Secure check box cleared, and then enable Secure Application Manager, Windows version in the Access Features section, you enable the Pulse Secure/SAM for the Pulse Client for Windows Mobile smart phone app. The Pulse Secure check box must be selected to enable the role for Pulse Client for Windows endpoints.

5. In the Access Features section of the New Role page, select the **Secure Application Manager** check box and then select **Windows version**.
6. Click **Save Changes** to create the role and to display the role configuration tabs.

The General tab options (Restrictions (which includes Host Checker), VLAN/Source IP, Session Options, and UI Options) are all valid settings for a SAM role.

We recommend that you use resource profiles to specify the applications available to users, but you can use role settings instead.

To specify applications for SAM to secure as part of a role:

1. Open the role you created for Pulse Client/SAM.
2. Click the **SAM** tab.
3. In the Applications section, click **Add Application** or select an existing application in the list and then click **Add Duplicate**.
4. In the Details section, select a type from the **Type** list, and then specify a name and description.

   If you select Custom to specify an application that is not included in the list, the Application Parameters section appears. Specify the following:

   - **Filename**: Specify the name of the file's executable file
   - **Path**: Specify the file's path
   - **MD5 Hash**: Optionally specify the MD5 hash of the executable file. If you enter an MD5 hash value, Pulse Client verifies that the checksum value of the executable matches this value. If the values do not match, Pulse Client notifies the user that the identity of the application could not be verified and does not allow access.

If you select Pick a Resource Profile, and at least one application or destination has been configured as a Resource Profile SAM client application, a selection list appears and you can click a Resource Profile. Then, when you click Save Application or Save + New, the role is added to the profile's list of roles, and the profile's resource polices are updated. If there are no Resource Profile SAM client applications or destinations configured, this option is not available.

5. Click **Save Application** or **Save + New**.

To specify servers for SAM to secure as part of a role:

1. Open the role you created for Pulse Client/SAM.
2. Click the **SAM** tab.
3. In the Applications section, click **Add Server** or select an existing server in the list and then click **Add Duplicate**.

   If you select "Standard", specify a name and a description, and then identify the server by name or IP address.

   If you select "Pick a Resource Profile", a selection list appears and you can click a Resource Profile. Then, when you click **Save Application** or **Save + New**, the role is added to the profile's list of roles, and the profile's resource polices are updated.
4. Click **Save Application** or **Save + New**.

To specify options for the SAM role:

1. Open the role you created for Pulse Client/SAM.
2. Click the **SAM** tab.
3. Click **Options**.
4. Make sure Windows SAM is enabled, and then choose from the following:
   - Secure Application Manager options:
     - **Auto-launch Secure Application Manager**: If you enable this option, Pulse Connect Secure automatically launches Secure Application Manager services when a user signs in through the Connect Secure Web portal. If you do not select this option, users must manually start the Secure Application Manager from the Client Applications Sessions section of the Web portal.
     - **Auto-allow application servers**: If you enable this option, Pulse Connect Secure automatically creates a SAM resource policy that allows access to the servers specified for the role in the SAM tab application and server lists.

- Windows SAM Options:
  - **Auto-uninstall Secure Application Manager**: This setting is a not applicable to Pulse Client R3.0 or later. It applies to the previous WSAM client software only. If you enable it, it is ignored for connections that use Pulse Client R3.0 or later.
  - **Prompt for username and password for intranet sites**: If you enable this option, the Pulse Connect Secure requires users to enter sign-in credentials before connecting to sites on your internal network. This option changes Internet Explorer's intranet zone setting so that Internet Explorer always prompts the user for network sign-in credentials for an intranet site.
  - **Auto-upgrade Secure Application Manager**: This setting is a not applicable to Pulse Client R3.0 or later. It applies to the previous WSAM client software only. If you enable it, it is ignored for connections that use Pulse Client R3.0 or later.
  - **Resolve only hostnames with domain suffixes in the device DNS domains**: If you enable this option, users can only browse to Web sites that are part of their login domain.
  - **Session start script and Session end scripts**: You can specify a script (.bat, .cmd, or .exe) to run on the users endpoint after Pulse Client connects and disconnects. For example, you can specify a script that maps network drives on an endpoint to shares on protected resources when the user connects. The script must be in a location (either local or on the network) that is accessible by the user.

5. Click **Save Changes**.

To use resource profiles to specify the applications available to Pulse Client users:

1. Create resource profiles that enable access to client applications and destinations and configure the appropriate settings. Select **Users > Resource Profiles > SAM > Client Applications**.
2. Click **New Profile**.
3. From the Type list, select "WSAM".
4. From the Application list, select one of the following options:
   - **Custom**: When you select this option, you must manually enter your custom application's executable filename (such as telnet.exe). Additionally, you can specify this file's path and MD5 hash of the executable file (although it is not required that you specify the exact path to the executable). If you enter an MD5 hash value, SAM verifies that the checksum value of the executable matches this value. If the values do not match, SAM notifies the user that the identity of the application could not be verified and does not forward connections from the application to the server.
   - **Lotus Notes**: Select this option to have SAM intermediate traffic from the Lotus Notes fat client application.
   - **Microsoft Outlook**: Select this option to have SAM intermediate traffic from the Microsoft Outlook application.
   - **NetBIOS file browsing**: Select this option to have SAM intercept NetBIOS name lookups in the TDI drivers on ports 137 and 139.

Note: NetBIOS file browsing is not supported for IPv6.

   - **Citrix**: Select this option to have SAM intermediate traffic from Citrix applications.

- **Domain Authentication**: Select this option to allow integrated Windows applications, such as file sharing, Outlook, and so forth to authenticate to the domain controller when the client machine is part of a domain. Before using this option, you must:
  - Specify domain controllers that are reachable through the Pulse Connect Secure in the WSAM Destination list so that LDAP and Kerberos traffic can be proxied and sent to Pulse Connect Secure.
  - Configure a WSAM Access Control Policy to allow access to all domain controllers.

Note: You can configure access to a standard application once per user role. For example, you can enable one configuration of Microsoft Outlook and one configuration of Lotus Notes for the "Users" role.

5. Enter a unique name and optionally a description for the resource profile.
6. In the Autopolicy: SAM Access Control section create supporting auto policies and assign the policies to the role:
   a. If it is not already enabled, select the **Autopolicy: SAM Access Control** check box.
   b. In the **Resource** field, specify the application server to which this policy applies. You can specify the server as a hostname or an IP/netmask pair. You can also include a port.

      If you select "Domain Authentication" from the **Application** list, enter your domain controller server addresses into the Resource field. You can add multiple domain controller servers if more than one is available.
   c. From the **Action** list, select Allow to enable access to the specified server or Deny to block access to the specified server.
   d. Click **Add**.
7. Click **Save and Continue**.
   a. In the **Roles** tab, select the roles to which the resource profile applies and click **Add**.

      The selected roles inherit the autopolicy created by the resource profile. If it is not already enabled, the server also automatically enables the SAM option in the roles **General > Overview** page for all of the roles you select.
   b. Click **Save Changes**.
   c. Select **Users > User Realms > New User Realm**.
   d. Specify a name and, optionally, a description and then click **Save Changes** to create the realm and to display the realm option tabs.
   e. On the Role Mapping tab for the realm, create a new rule that maps all users to the role you created earlier in this procedure.

      You can also use resource profiles to configure destination servers, network subnets and hosts and then add the resource profile to a role.

To use resource profiles to specify the network endpoints available to Pulse Client users:

1. In the admin console, choose **Users > Resource Profiles > SAM > WSAM Destinations**.
2. Click **New Profile**.

3. Enter a unique name and optionally a description for the resource profile.
4. In the WSAM Destinations section, specify which servers you want to secure using WSAM and click **Add**. You can specify the servers as hostname or IP/netmask pairs. You can also include a port.
5. Select the **Create an access control policy allowing SAM access to this server** check box (enabled by default) to enable access to the server specified in the previous step.
6. Click **Save and Continue**.
7. In the **Roles** tab, select the roles to which the resource profile applies and click **Add**.

The selected roles inherit the autopolicy created by the resource profile.

Pulse Client Connection Set Options for Pulse Connect Secure

A Pulse Client connection set contains network options and allows you to configure specific connection policies for client access to any Pulse Secure server that supports Pulse Client. The following sections describe each of the configuration options for a Pulse Client connection set.

Pulse Client Connection Set Options

The following items apply to all connections in a connection set.

- **Allow saving logon information**: Controls whether the Save Settings check box is available in login dialog boxes in Pulse Client. If you clear this check box, Pulse Client always requires users to provide credentials. If you select this check box, users have the option of saving their credentials.

  Pulse Client can retain *learned user settings*. These settings are retained securely on the endpoint, evolving as the user connects through different Pulse Secure servers. Pulse Client can save the following settings:

  - Certificate acceptance
  - Certificate selection
  - Realm
  - Username and password
  - Proxy username and password
  - Secondary username and password
  - Role

Note: If the authentication server is an ACE server or a RADIUS server and authentication is set to Users authenticate using tokens or one-time passwords, Pulse Client ignores the Allow saving logon information option. If the user sees a username and token prompt and the Save settings check box is disabled. Pulse Client supports soft token, hard token, and smart card authentication.

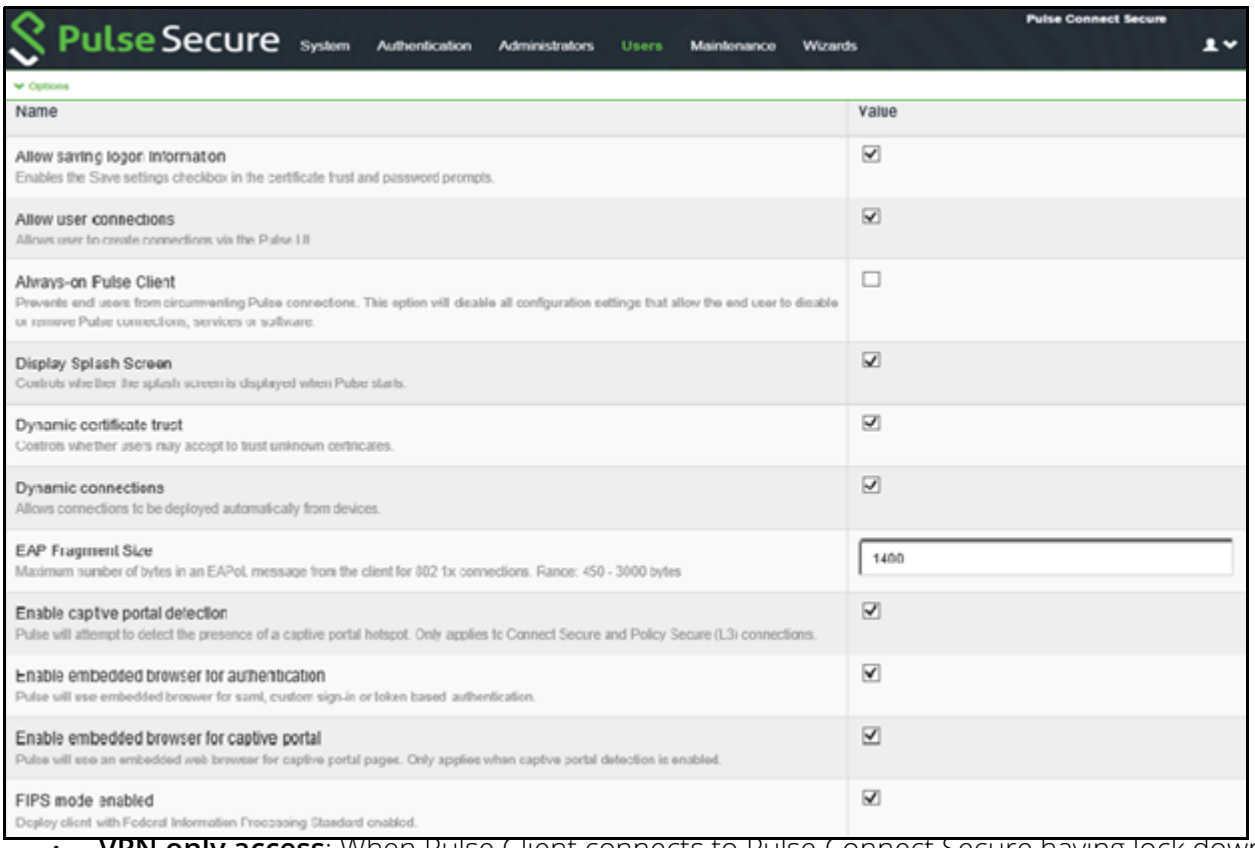
Note: In 5.2R5 Pulse Client introduced two new features to improve the end-user experience during certificate authentication. The administrative console option to configure this feature is now available in 5.3R2. This feature enables the following:

-**Allow user connections**: Controls whether connections can be added by the user.

- **Always-on Pulse Client**: Prevent end users from circumventing Pulse Client connections. This option disables all configuration settings that allow the end user to disable or remove Pulse Client connections, service or software. For more details refer to "Always-on VPN" on page 46.

Note: Checking the "Always-on Pulse Client" option does not prevent end users with administrative privileges from stopping the Pulse Client service on the endpoint device. Create a group policy object (GPO) to prevent users from disabling the Pulse Client service. For more details on how to create GPOs refer to the article found in Microsoft's Website.

Figure 25 Pulse Client Connection Set Options



- **VPN only access**: When Pulse Client connects to Pulse Connect Secure having lock down mode enabled, it will enable lock-down mode and block network if VPN is not in connected state.
  - When VPN only access option is enabled, the Enable captive portal detection and Enable embedded browser for captive portal will be automatically checked and cannot be edited.
- **Display splash screen**: Clear this check box to hide the Pulse Client splash screen that normally appears when Pulse Client starts.
- **Dynamic certificate trust**: Determines whether users can opt to trust unknown certificates. If you select this check box, a user can ignore warnings about invalid certificates and connect to the target Pulse Secure server.

  Note: By default, Dynamic certificate trust check box will be unchecked.

- **Dynamic connections**: Allows connections within this connection set to be automatically updated or added to Pulse Client when the user connects to Pulse Connect Secure through the user Web portal, and then starts Pulse Client through the Web portal interface. Dynamic connections are created as manual rather than automatic connections, which means that they are run only when the user initiates the connection or the user browses to a Pulse Secure server and launches Pulse Client from the server's Web interface.

  If dynamic connections are disabled, and the user logs in through the Web portal of a Pulse Secure server that is not already included in Pulse Client's connection set, then starting Pulse Client from the Web portal does not add a new Pulse Client connection for that Pulse Secure server. If you choose to disable dynamic connections, you can still allow users to manually create connections by enabling Allow User Connections.
- **Enable captive portal detection**: To detect the presence of a captive portal hotspot enable this option. It can be applied only to Pulse Connect Secure and Pulse Policy Secure (L3) connections.
- **Enable embedded browser for captive portal**: When enabled, Pulse Client uses an embedded web browser that the end user can use to traverse captive portal pages and to gain network connectivity for establishing a VPN connection. This applies only when captive portal detection is enabled.
- **Enable embedded browser for authentication**: When enabled, Pulse Client uses an embedded browser for web authentication, rather than external browser.
- **FIPS mode enabled**: Enable FIPS mode communications for all Pulse Client connections in the connection set. The Federal Information Processing Standard (FIPS) defines secure communications for the U.S. government. When a Pulse Client connection is operating in FIPS mode, FIPS On appears in the lower corner of the Pulse Client interface. If your Pulse Connect Secure hardware does not support FIPS mode operations, FIPS mode configuration options are not present in the admin console interface. FIPS mode operations are supported on PSA-V Series Pulse Secure Gateways and some SA series appliances. The device must be running Pulse Policy Secure R5.0 or later or Pulse Connect Secure R8.0 or later.

Note: Users cannot enable FIPS mode from within Pulse Client. You must create FIPS-enabled connections on the server and deploy them.

- **Prevent caching smart card PIN**: Enabling this field will allow system administrators to prevent smart card PIN values from being cached. This feature is applicable only to Windows.
- **Wireless suppression**: Disables wireless access when a wired connection is available. If the wired connection is removed, Pulse Client enables the wireless connections with the following properties:
  - Connect even if the network is not broadcasting.
  - Authenticate as computer when computer information is available.
  - Connect when this network is in range.

Note: Wireless suppression occurs only when the wired connection is connected and authorized. If you enable wireless suppression, be sure to also configure a connection that enables Pulse Client to connect through a wired connection.

Configuring Client Certificate Selection Option

From 9.1R3 release onwards, while Configuring Pulse Connect Secure settings, the following are the new checkboxes added under Client Certificate Selection Option.

- Accept certificates with smartcard logon EKU
- Accept certificate with Custom EKU text
- Accept certificate with Custom EKU OID

The valid certificates get filtered based on the specifications provided by administrator in the above fields.

Only the filtered certificates get displayed in certificate selection prompt.

Enhanced Key Usage (EKU) field, abbreviated as EKU has following two components to it.

- **EKUText** - It is the text which is in human readable format.
- **EKUOID** - It is the OID number which is unique for a given purpose.

The following table defines EKUText and EKUOID variables:

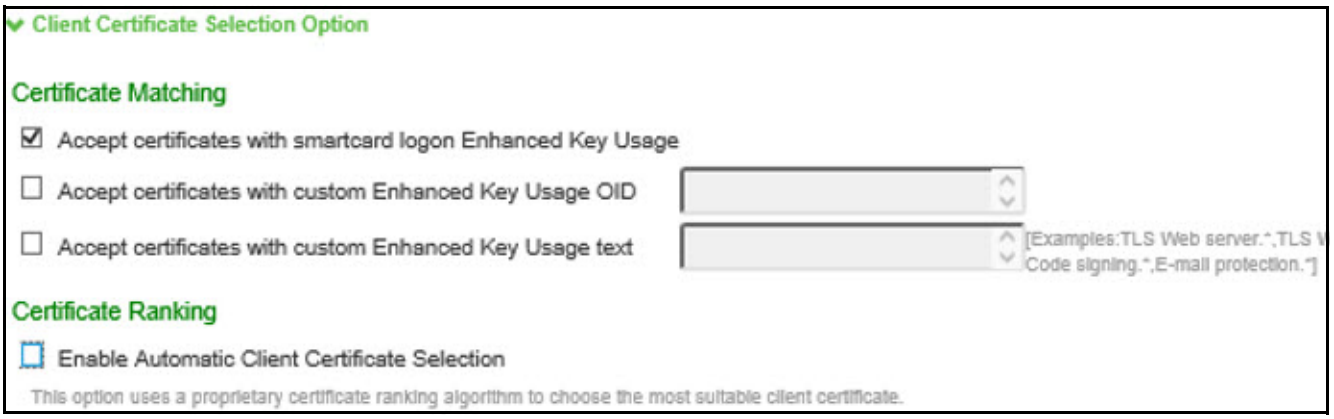
Variable	Description	Examples
EKUText	Format to be given is: EKUText = string or <comma separated string> or string with regular expression. Custom regular expressions need to be given with the following format: certAttr.EKUText = string or <comma separated string> or string with regular expression.	certAttr.EKUText = "TLS Web Server Authentication", "E-mail Protection" ,"TLS Web Client Authentication".
EKUOID	Format to be given is: EKUOID = to a.b.c.d.e.f.g.h.i or <comma separated list of EKUOIDs> or OID with regular expressions. This works in both certificate rule as well as custom expressions. Custom regular expressions need to be given with the following format: certAttr.EKUOID = a.b.c.d.e.f.g.h.i or <comma separated list of EKUOIDs> or OID with regular expressions.	Customer can create certificates with Custom OIDs. Example: certAttr.EKUOID=1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.4,1.3.6.1.5.5.7.3.2

To configure Certificate Matching and Certificate Ranking under Client Certificate Selection Option, the administrator needs to follow the below steps.

1. Log in to admin console.
2. Go to **Users** > **Pulse Secure Client** > **Connections**.
3. Select the connection from the Connections or click **New** to display the New Connection set configuration page.
4. Complete the configuration, as required.

5. Save the configuration.

Figure 26 Client Certificate Selection Option



Note: **Prefer smart card certificate** option can be checked only if Enable Automatic Client Certificate Selection option is checked.

If **Prefer smart card certificate** option is checked, then certificates with client auth EKU set get displayed on the top of the list of certificates and preferred over other certificates.

Accept certificates with smartcard logon Enhanced key Usage option is enabled by default.

Note: **Accept Certificates with smartcard logon Enhanced key Usage** option should be checked to use Yubikey as PIV smart card for VPN authentication.

Based on the EKU configuration settings, Pulse Desktop Client will pick-up the available certificate and make successful connection.

If end-user has more than one certificates, then Pulse Desktop Client will prompt the end-user to select the certificates to make successful connection.

Always-on VPN

By default, Always-on option is disabled. There are many possible configuration options within the Always-on feature. Although some of these options are new for the 5.2r5 Pulse Client (e.g., lock-down mode, embedded browser for captive-portal remediation), some Always-on options existed in previous versions of Pulse Client. To make management of all these options easier, the 8.2r5 Pulse Connect Secure gateway's administrative console provides a simplified way of configuring all the possible Always-on VPN options.

Note the following:

- From 9.0 R1 release onwards, Pulse Client for macOS will support Always-on VPN except Lock-Down Exception function.
- Pulse Client for Linux will not support for Always-on VPN.

Configuring Always-on Options

To configure the Connection set:

1. Login to Pulse Connect Secure admin console
2. Select **Users> Pulse Secure Client > Connections**
3. Click **New** to display the New Connection set configuration page, refer to Figure 25.
4. Complete the configuration as described in Table 3.
5. Save the configuration.

Table 3 Always-on options Settings

Settings	Description
Allow user connection	Controls whether connections can be added by the user.
Always-on Pulse Client	When checked it prevents end users from circumventing Pulse Client connections. This option will disable all configuration settings that allow the end user to disable or remove Pulse Client connections, service or software.
Enable captive portal detection	Controls whether Pulse Client will notify the end user that a VPN connection cannot be established until the requirements of a captive portal are fulfilled.
Enable embedded browser for captive portal	When checked, Pulse Client uses an embedded web browser for captive portal pages.

Note: When Always-on Pulse Client is enabled "VPN Only Access", "Enable captive portal detection" and "Enable embedded browser for captive portal" will be automatically checked and cannot be edited.

Checking this option will modify several checkboxes in both the Connection Set and the Connections within the Connection Set with the effect of:

- Impeding the end user's ability to disconnect or disable VPN connections (Windows and Mac)
- Ensuring that captive portals can still be traversed even when connectivity is locked down (Windows and Mac)

Note: "Always-on" checkbox does not prevent end users (with admin privileges) from stopping endpoint services (the Pulse Client Service and the Base Filtering Engine (BFE)) which are required for VPN connections to be established. If you wish to have the level of protection that comes with prohibiting end users from stopping these services, then it is best to use Group Policy Objects (GPOs).

Configuring Always-on VPN Options using Wizards

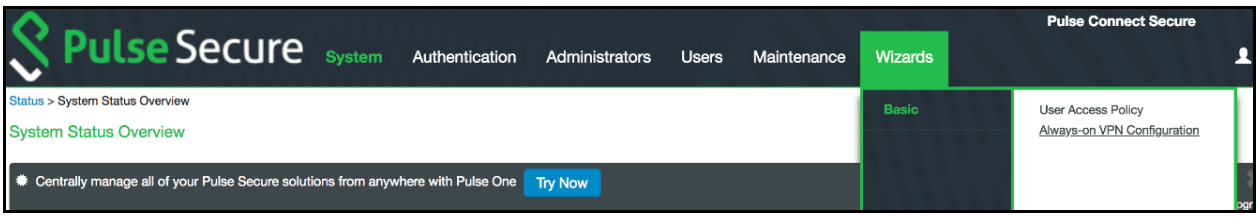
To configure the Always-on VPN Options using wizards.

1. Login to Pulse Connect Secure admin console.
2. Admin can configure Always-on VPN options using Wizards in following two ways:
   - Using Global Wizards
   - Using Connection Set

   Using Global Wizards

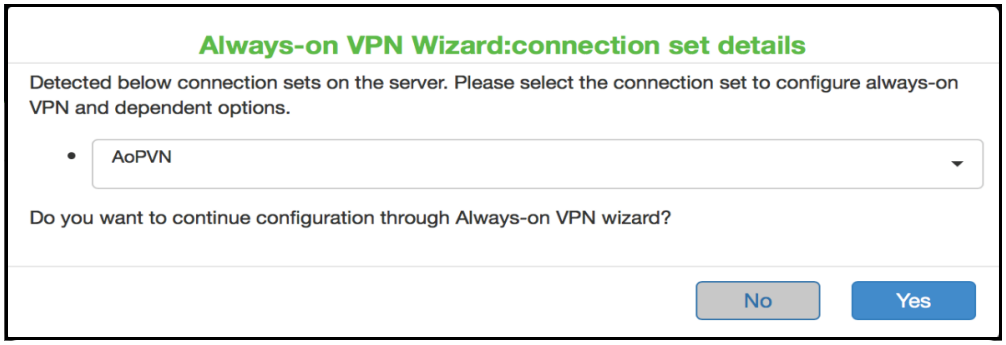
1. Click **Wizards**. Following screen appears:

Figure 27 Wizards Screen



2. Select **Wizard -> Basic -> Always-on VPN Configuration**. Following screen appears:

Figure 28 Always-on VPN connection set details



3. Choose the connection set from the drop-down list of existing connection sets. Figure 30 appears.

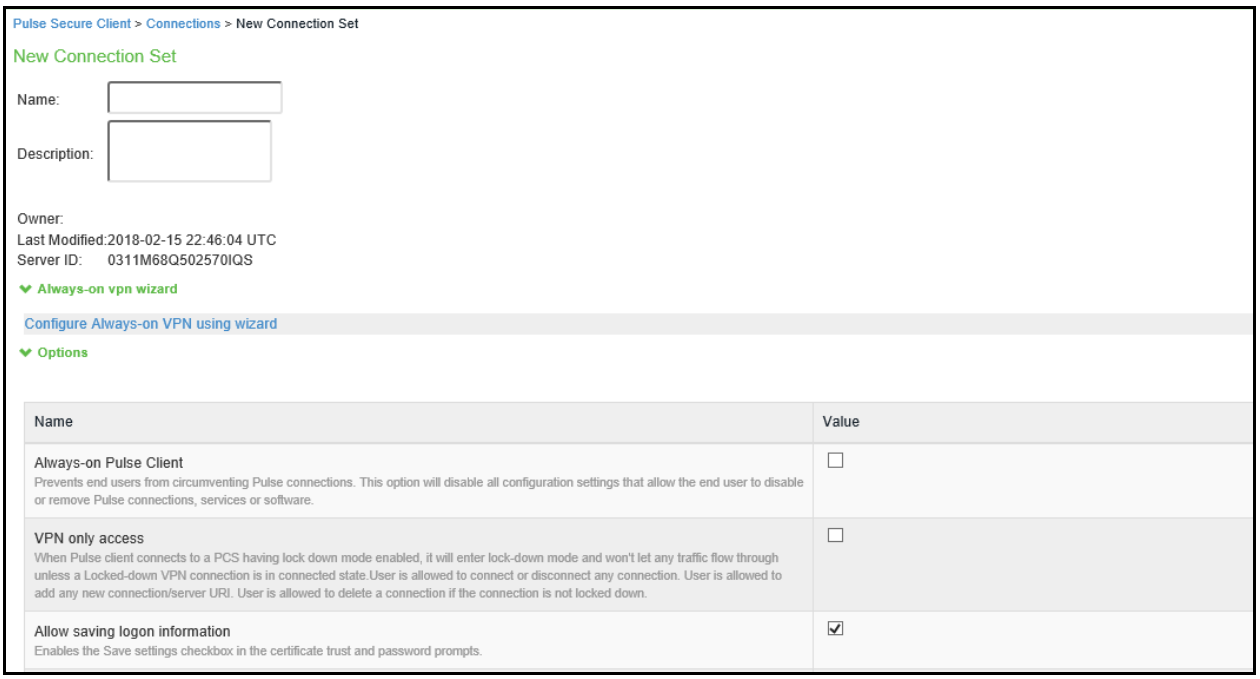
   Go to step 5 to continue with configuration of Always-on VPN.

Using Connection Set

1. Select **Users > Pulse Secure Client > Connections**. Continue to step 3 to continue with configuration of Always-on VPN.

3. Click **New** to display the New Connection set configuration page. The following screen appears:

Figure 29 New Connection Set

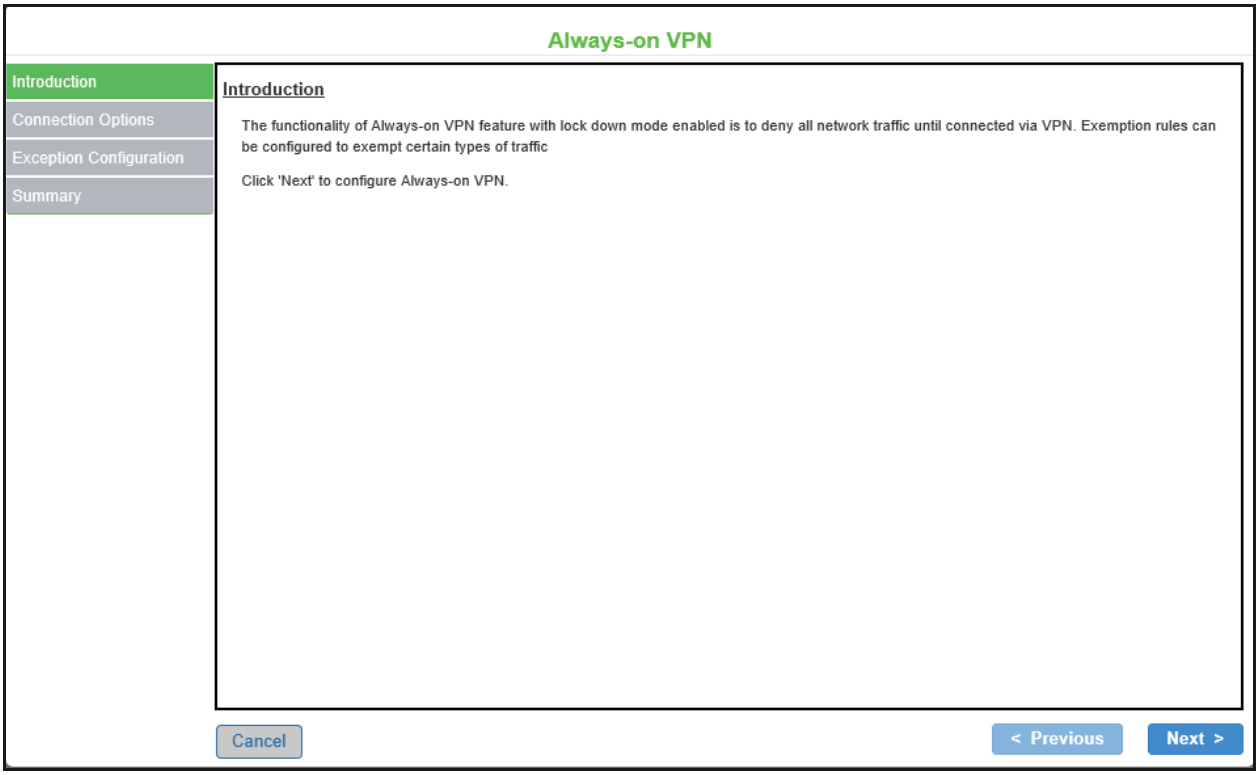


Create new connection set with default values. For more information on Connection set, refer to "Creating a Client Connection Set for Pulse Connect Secure" on page 72.

Note: Admin can edit the existing connection set also.

4. Click **Configure Always-on VPN using wizard**. The following screens appears:

Figure 30 Configure Always-on VPN using wizard



5. If admin has already configured Always-on VPN, the following screen appears:

   Figure 31 Always-on VPN

   Click **TURN-OFF ALWAYS-ON VPN** if you want to disable Always-on VPN option. Also, VPN only access will get disabled.

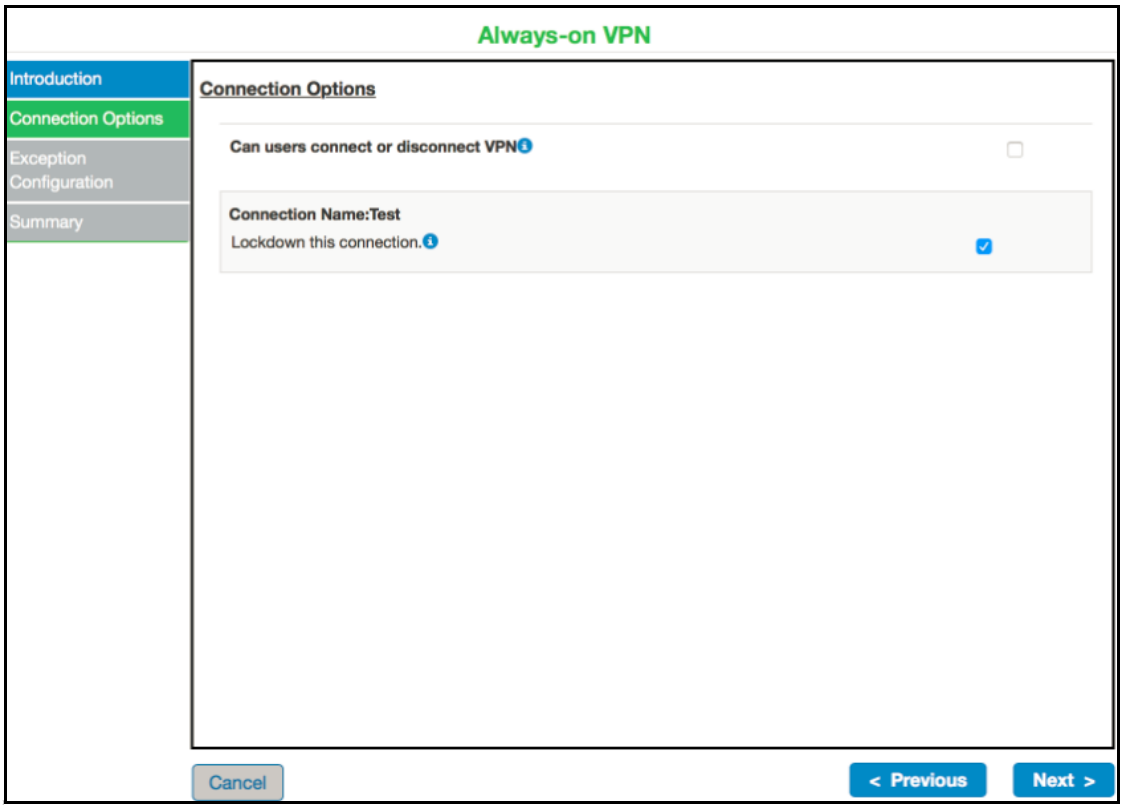
6. Click **Next** to continue with configuration of Always-on VPN. The following screen appears:

Figure 32 Can users connect or disconnect VPN

Check the Lockdown this connection checkbox. Following screen appears:

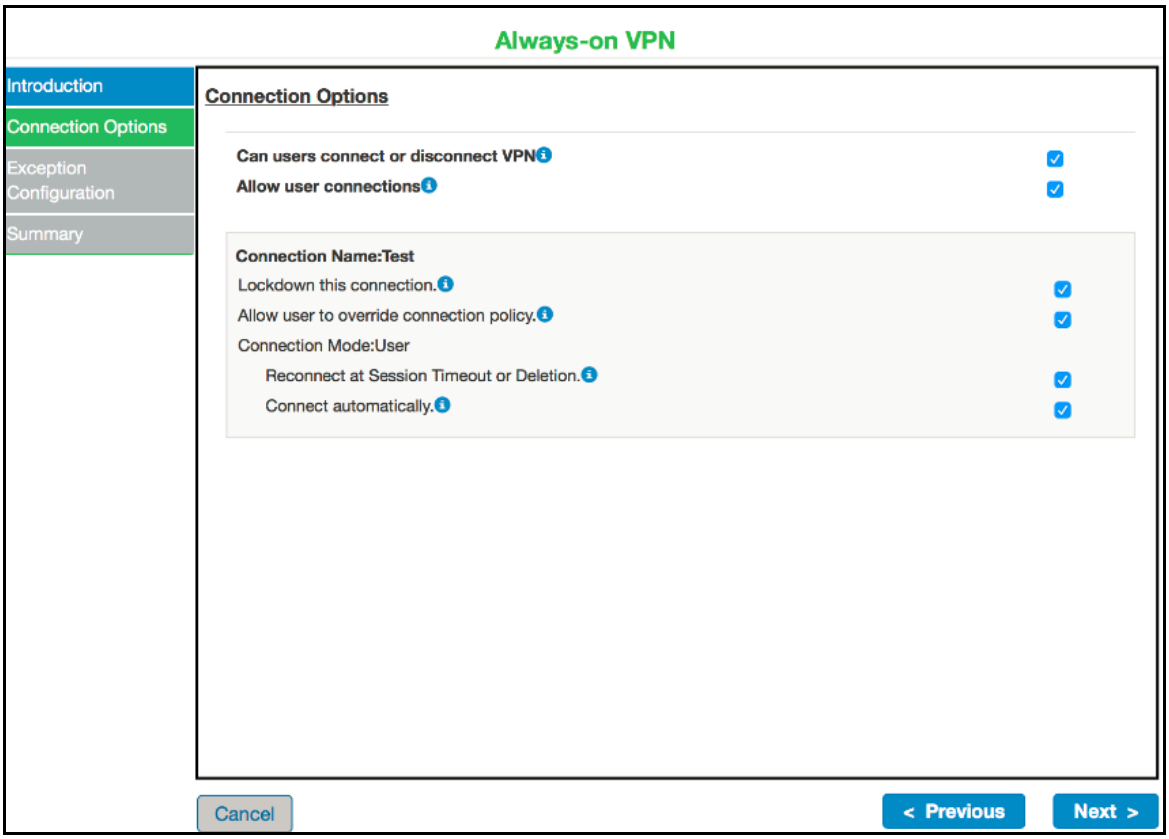
Scenario 1 – Always-on VPN

Figure 33 Can users connect or disconnect VPN (Lockdown mode



Scenario – 2 VPN Only Access

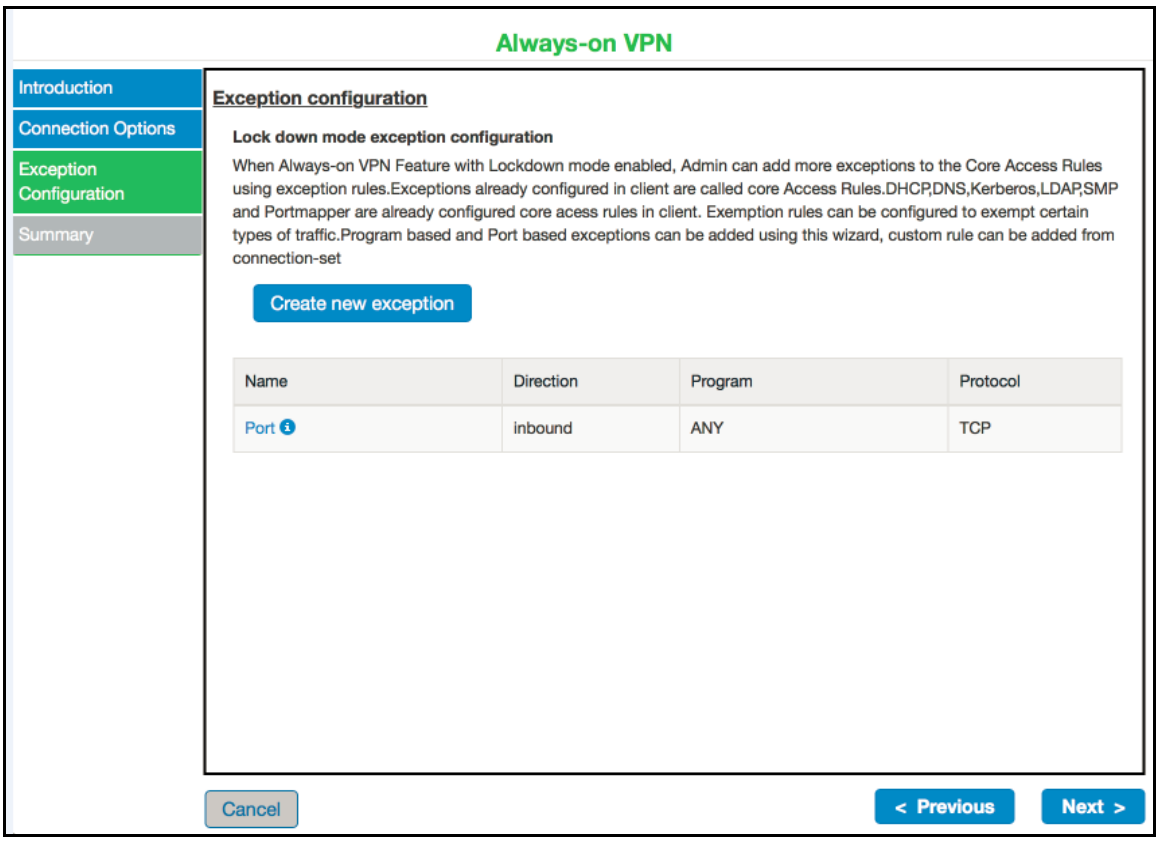
Figure 34 Can users connect or disconnect VPN



7. Check **Can users connect or disconnect VPN** checkbox to continue with Always-on VPN configuration.
8. Click **Next**. The following screen appears:

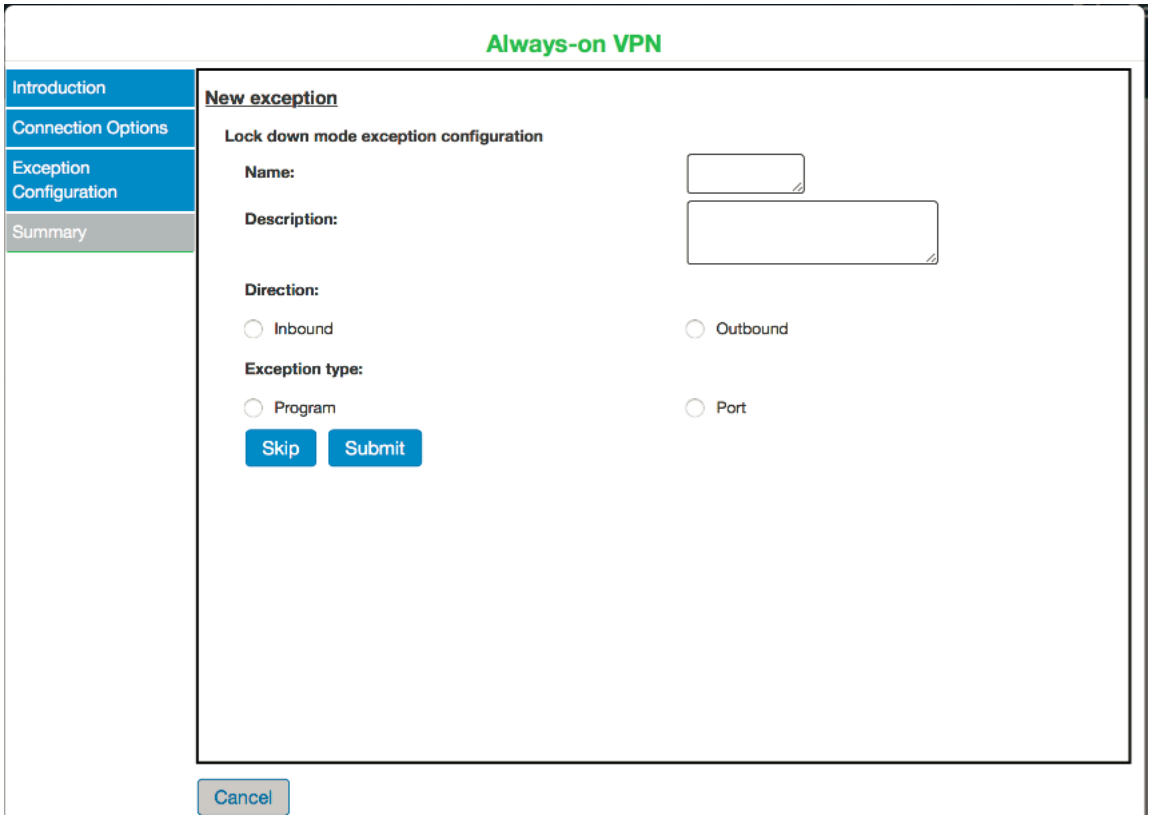
Scenario – 1: Always-on VPN

Figure 35 Lock down mode exception configuration



9. Configure the exception rules. Admin can add more exception rules to the Core Access Rules.
10. Click **Create new exception**. The following screen appears:

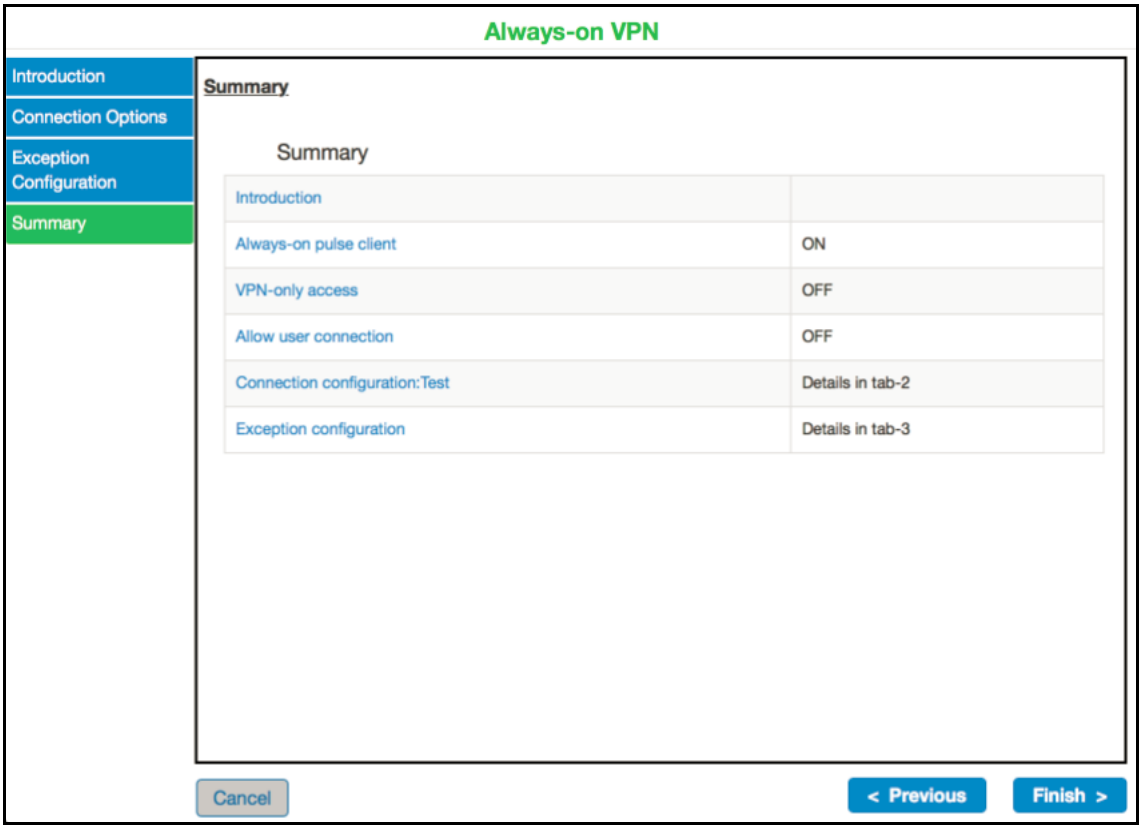
Figure 36 Lock down mode exception configuration



11. Click **Submit**, if exception rules are set.
12. Click **Skip**, if admin wants to change the exception rules.

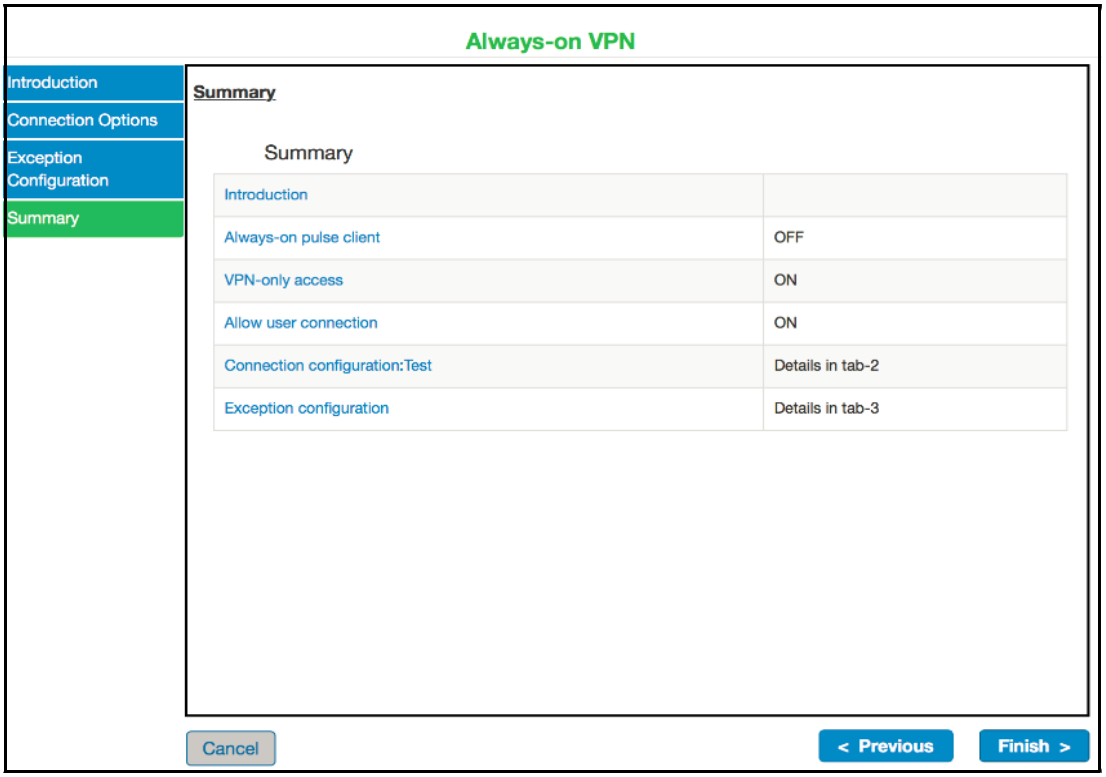
Scenario – 1: Always-on VPN

Figure 37 Summary Screen



Scenario – 2 VPN Only Access

Figure 38 Summary Screen



13. Click **Finish**. "Always-on VPN update successful" message appears on the screen.

Note: "Always-on VPN update successful" message appears along with connection set page (see Figure 29, if Admin is configuring Always-on VPN using Wizards through **Wizard** tab in Pulse Connect Secure console.

Requirement to set up the appropriate GPOs

Setting up GPOs is not required to leverage the benefits of the Pulse Client's Always-on VPN feature. Setting up GPOs would only be necessary if you need the extra security of restricting users with admin privileges from stopping Pulse Client services. As such, setting up GPOs should be considered optional.

Pulse Client should be installed on a box running a server version Microsoft Windows (e.g., Windows server 2008 R2, 2012 R2, 2016).

- The startup type for "Pulse Secure Service" should be set to "Automatic", and permission to start and stop the service should be removed from "Administrators".
- Ensure that "SYSTEM" still retains permission to start and stop the service.
- A "Pulse Secure Admins" should be created on the domain. Permission to start and stop the service should be assigned to this "Pulse Secure Admins". The "Domain Admins" and any other group which should be allowed to start and stop Pulse Client can be made members of the "Pulse Secure Admins" group.
- Disabling the ability to stop the Base Filtering Engine (BFE) should be done in a manner similar to what is described above for the Pulse Client Service.

Installing Pulse Client in Windows Server

To install Pulse Client in Windows Server, follow the below steps:

1. The Pulse Client MSI file should be used for installation.
2. Install Wireless LAN service on Windows 2008 R2, 2012 R2 and 2016 servers before installing Pulse Client to avoid unsuccessful registration during Pulse Client Installation.
3. To enable the Wireless LAN service, follow the below steps:
    a. Open **Server Manager**.
    b. Navigate to **Feature > Add Feature**.
    c. Select the Wireless LAN Service.
    d. Click on **install Wireless LAN Service** for installing.
    e. Click on **Close > Done** once the Wireless LAN Service is installed.

Note: On Windows 2016 servers, even after Wireless LAN Service is installed, an error message will appear during Pulse Client Installation and the error can be accepted and the Pulse Client Installation will be completed.

Note: There is no mechanism within Pulse Client itself to prevent end users with administrative privileges from uninstalling Pulse Client. If this functionality is needed, then it would be best to enforce those restrictions outside of Pulse Client.

Always-on with Lock-down Mode

"Lock-down" mode is a new aspect of Always-on functionality that was added to the 5.2r5 Pulse Client for Windows and 9.0R1 for Mac. Lock-down mode prohibits network communication outside the VPN tunnel when a VPN tunnel is in the process of being created. Lock-down option can be enabled only in conjunction with the "Always-on" and "VPN only access" option. To ensure that end users can easily traverse captive portals in lock-down mode, the "Captive portal remediation with embedded mini-browser" is automatically enabled when lock-down mode is enabled. Lock-down mode is intended for use with Location Awareness rules; this feature can ensure that the user is either:

- Physically on the corporate network.
- Connected to the corporate network through a VPN connection or on the process of creating a VPN connection and cannot access the Internet/local subnet in the meantime.

Location Awareness rules should be set up to automatically initiate a VPN connection when the user is not on the corporate network, and to disconnect the VPN connection when the user is physically on the corporate network. If Location Awareness rules are not configured in this method, then Lock-down mode has very little value, because Lock-down mode prohibits connectivity only when Pulse Client is in the process of creating a network connection. If Pulse Client is not configured to automatically create a Pulse Client connection when off the corporate network, then Lock-down mode will not be automatically invoked when the user leaves the corporate network. For information on configuring Location Awareness rules, refer to "Location Awareness Rules" on page 70.

The lock-down option blocks nearly all network traffic, but there are exceptions for the minimum amount of traffic required to initialize network adapter such that a tunnel can be created. As such, traffic used to get IP addresses, hostnames, etc. (DHCP, DNS, etc.) are permitted even when the machine is locked down.

Note: Lock-down mode is supported only for IPv4 endpoints.

Note: For known third party software issues with Lock-down Mode, refer to the Pulse Secure Knowledge Center article "KB43679" (see https://kb.pulsesecure.net).

To enable the "Lock down this connection" option, follow the below steps:

1. Log in to the Pulse Connect Secure admin console.
2. Select the connection from **Connection Options**.
3. Use a Connect Secure L3 connection for a Layer 3 connection to Pulse Connect Secure.
4. Check **Lock–down this connection** to disable network access when VPN is enabled until connected, see Figure 39.
5. Click on **Save Changes**.

Figure 39 Lock down this connection

Lock-down Exception

When Pulse Client is in Lock-down mode, all network traffic except those defined in Lock-down exception rules will be denied when VPN is not connected.

In the New Configuration section, administrator can add Lock-down mode exceptions rules for Windows and for 9.0R2 release onwards for macOS. Administrator has to configure these rules for which traffic need to be exempted when Lock-down mode has applied at user end.

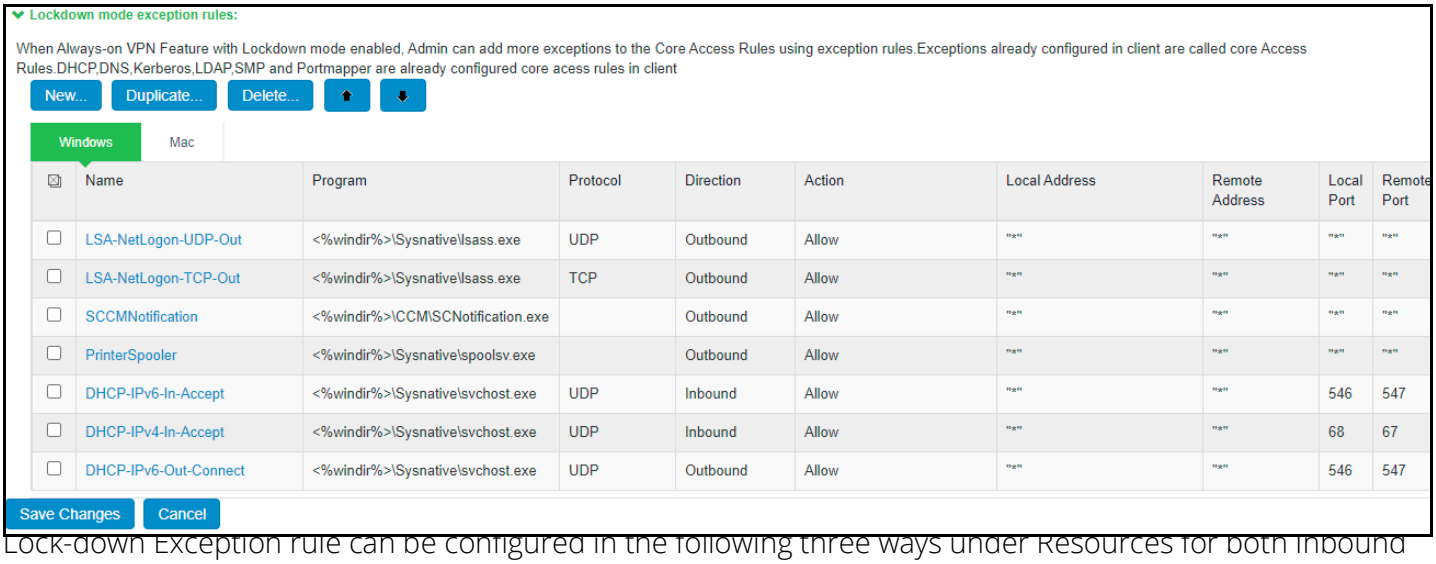
Until 9.1R10, the core access rules using exemption were pre-defined and administrators were not allowed to configure. From 9.1R11 onwards, the PCS populates the list of core access rules depending on the platforms. Administrators are allowed to modify and reorder the list. Administrators can also configure the exception rules with allow/deny option.

To configure exception rules, an administrator needs to follow the below steps.

1. Log in to admin console.
2. Go to **Users > Pulse Secure Client**.
3. Select **Connections**.
4. Select **Options > Enable Always-on Pulse Client & VPN only access**.

Lock-down Exception can be enabled by selecting Always-on Pulse Client alone or VPN only Access.

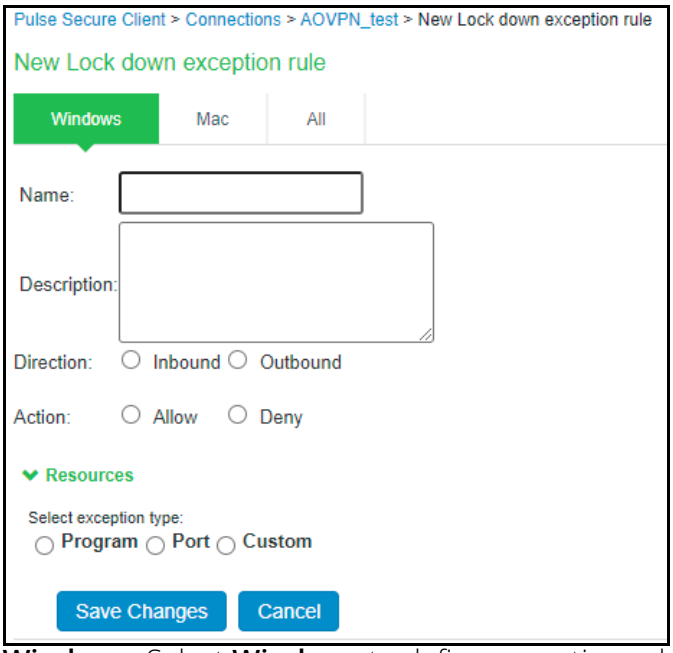
Figure 40 Connections



Lock-down Exception rule can be configured in the following three ways under Resources for both Inbound and Outbound traffic separately.

- “Program-based Resource Access” on page 60
- “Port-based Resource Access” on page 61
- “Custom-based Resource Access” on page 62

Figure 41 New Always-on VPN Exception Rules



Windows: Select **Windows** to define exception rules for only Windows.

Mac: Select **Mac** to define exception rules for only Mac.

All: Select **All** to define exception rules for both Windows and Mac.

Inbound traffic is always directed towards user’s machine (Example: RDP).

Outbound traffic is always directed towards outside the machine (Example: Skype for Business Application).

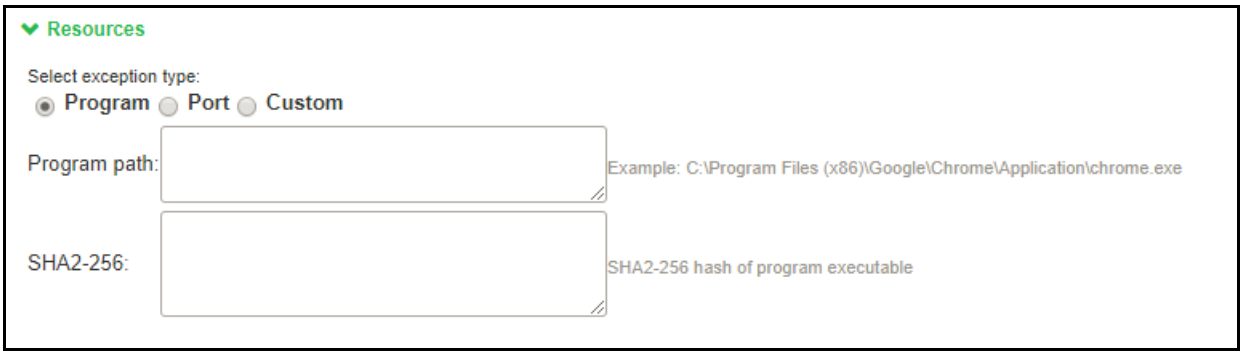
Allow or Deny allows to configure the exception rules.

Program-based Resource Access

To configure Program-based resource access, administrator needs to select **Program**. Then the following configuration UI appears.

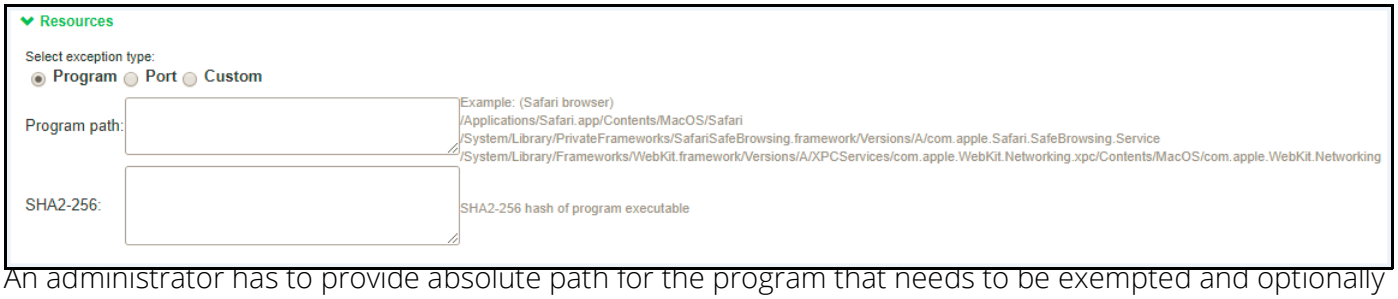
Windows – Program based Resource Access

Figure 42 Windows - Program-based Resource Access



macOS – Program based Resource Access

Figure 43 macOS - Program-based Resource Access



An administrator has to provide absolute path for the program that needs to be exempted and optionally provide SHA-256 checksum.

Following are the examples for Lockdown Exception rules for macOS.

1. MAC Update program path:

   /Applications/App Store.app/Contents/MacOS/App Store
   /System/Library/PrivateFrameworks/StoreXPCServices.framework/Versions/A/XPCServices/
   com.apple.appstore.PluginXPCService.xpc/Contents/MacOS/com.apple.appstore.PluginXPCService
   /System/Library/Frameworks/ApplicationServices.framework/Versions/A/Frameworks/
   HIServices.framework/Versions/A/XPCServices/com.apple.hiservices-xpcservice.xpc/Contents/MacOS/
   com.apple.hiservices-xpcservice
   /System/Library/CoreServices/Software Update.app/Contents/Resources/softwareupdated
   /System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/
   com.apple.WebKit.Networking.xpc/Contents/MacOS/com.apple.WebKit.Networking

2. Safari browser program path:

/Applications/Safari.app/Contents/MacOS/Safari
/System/Library/PrivateFrameworks/SafariSafeBrowsing.framework/Versions/A/com.apple.Safari.SafeBrowsing.Service
/System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.Networking.xpc/Contents/MacOS/com.apple.WebKit.Networking

/System/Library/StagedFrameworks/Safari/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.Networking.xpc/Contents/MacOS/com.apple.WebKit.Networking -> Mac 11 & Mac 12

3. Facetime program path:

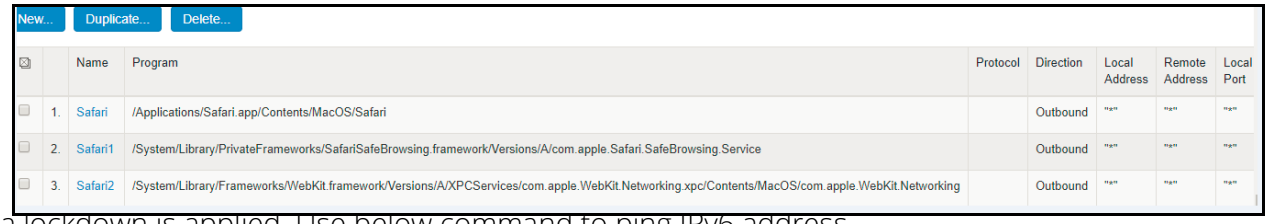
   /System/Library/PrivateFrameworks/ApplePushService.framework/apsd
   /Applications/FaceTime.app/Contents/MacOS/FaceTime
   /System/Library/PrivateFrameworks/AuthKit.framework/Versions/A/Support/akd
   /System/Library/PrivateFrameworks/IDS.framework/identityservicesd.app/Contents/MacOS/identityservicesd
   /System/Library/PrivateFrameworks/AOSKit.framework/Versions/A/XPCServices/com.apple.iCloudHelper.xpc/Contents/MacOS/com.apple.iCloudHelper
   /usr/libexec/avconferenced
   /usr/libexec/nsurlsessiond

4. Symantec Norton security program path:

   /Applications/Norton Security.app/Contents/MacOS/Norton Security
   /Library/Application Support/Symantec/Silo/NFM/Daemon/SymDaemon.bundle/Contents/MacOS/SymDaemon
   /Library/Application Support/Symantec/Silo/NFM/LiveUpdate/com.symantec.SymLUHelper
   /Library/Application Support/Symantec/Silo/NFM/SymUIAgent/Norton.app/Contents/MacOS/Norton

   Each process needs to configure with different process rules, and not with single process.

   Figure 44 Lockdown Exception Rules - Safari



When a lockdown is applied. Use below command to ping IPv6 address.

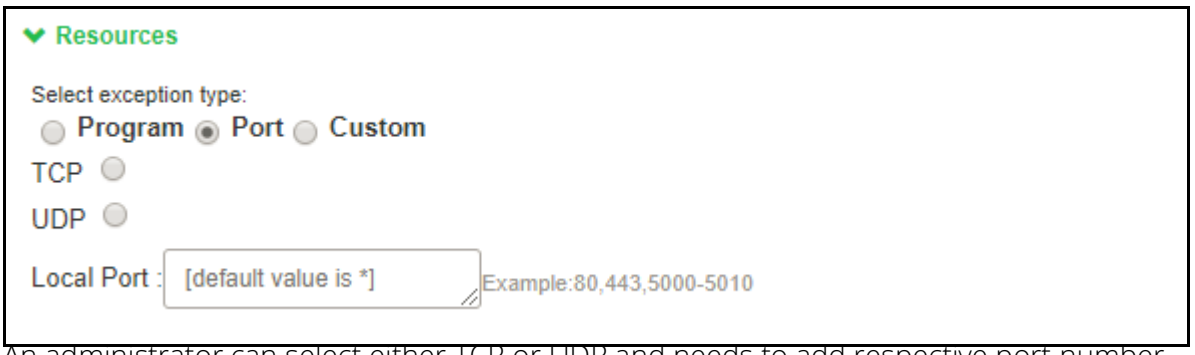
```
ping6 -S (Source IPv6) (destination IPv6)
```

Port-based Resource Access

To configure Port-based resource access, administrator needs to select **Port**. Then the following configuration UI appears.

Windows and macOS Port based Resource Access:

Figure 45 Port-based Resource Access

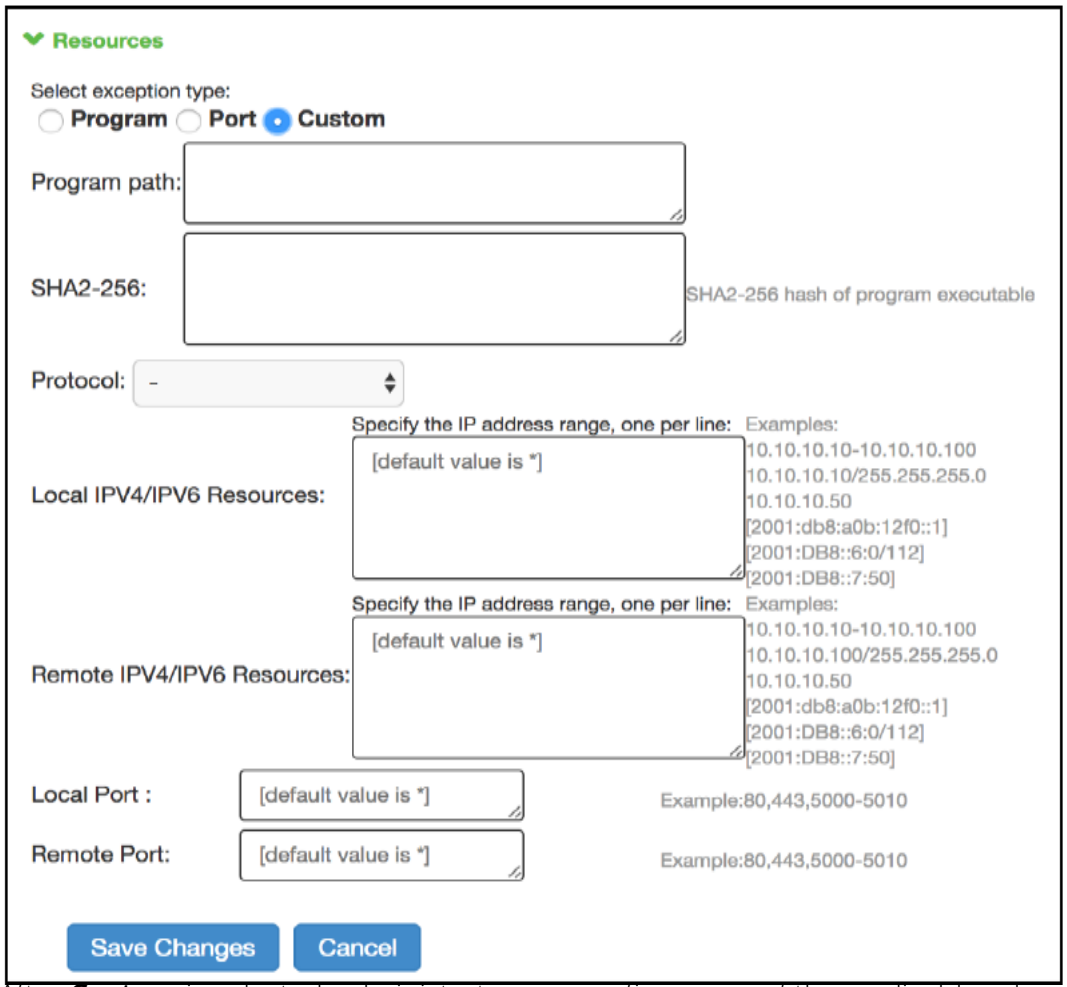


An administrator can select either TCP or UDP and needs to add respective port number.

Custom-based Resource Access

To configure Custom-based resource access, administrator needs to select **Custom**. Then following configuration UI appears.

Figure 46 Custom-based Resource Access



After **Custom** is selected, administrator can configure any of the applicable rules. (Example: administrator can configure Local or Remote IPv4/IPv6 addresses or Ports or Absolute Program Path or Type of protocol).

Note the following:

- In custom-based resource access, it is not mandatory to configure all the options. Default value for all configurable fields are "*".
- After a Pulse Client upgrade, user has to make at least one successful connection to the Pulse Connect Secure, so that the configured Lock-down exceptions can be applied on the client machine.

Retry Button

The Retry button allows the user to reconnect the connection after a time out or failure. When an authentication has failed, Always-on VPN attempts to reestablish the connection to activate the session if the session time is still open or user can reconnect to new VPN session by clicking on Retry button.

The retry option can be found in the Pulse Client user interface:

1. Open Pulse Client.
2. Click on **File > Connections > Retry to reconnect**.

Captive Portal Remediation with Pulse Client Embedded Mini-Browser

The "Enable embedded browser for captive portal" option makes it easy for end users to satisfy captive portals (for example, when in a coffee-shop that requires either credit-card payment or acceptance of an acceptable-use policy before gaining Wi-Fi access). By default, support for captive portal remediation is disabled.

To enable Embedded Browser:

1. Log in to Pulse Connect Secure admin console.
2. Select **Users> Pulse Secure Client > Connections**.
3. Click **New** to display the New Connection set configuration page.
4. Complete the configuration as described in Table 4.
5. Save the configuration.

Table 4 Pulse Client Embedded Mini-Browser Settings

Settings	Guidelines
Enable Captive Portal detection	If this option is checked, Pulse Client will detect if connectivity is hampered by a captive portal, then Pulse Client will automatically display an embedded browser (not an external browser, like IE or Chrome or Safari) so that the end user can traverse the captive portal and gain the network connectivity needed to establish a VPN connection.
Enable embedded browser for captive portal	Pulse Client will use an embedded browser for captive portal pages, applicable only if Captive Portal detection is enabled.

Although this feature can be used as a convenience independent of the Always-on VPN and VPN only access feature, it is essential (and is enabled automatically) when using lock-down mode. The embedded browser is part of Pulse Client's internal processes, and is therefore exempt from the lock-down connectivity restrictions placed on external browsers. Lock-down mode prevents external browsers from communicating before the VPN is established, so external browsers cannot be used for captive-portal remediation with lock-down mode enabled. The embedded browser is the only option for remediating a captive portal in lock-down mode.

For macOS, Captive Portal Remediation using external browser needs admin privileges if system proxy settings are configured. Embedded browser will bypass proxy settings automatically without admin privileges.

For Windows OS, user can bypass proxy settings and perform captive portal remediation using external browser.

Pulse Client's embedded browser is restricted to ensure that end users cannot use it for purposes other than traversing captive portals. Furthermore, certain web-browser functionality is disabled to make the embedded browser more secure.

The following table describes features which are enabled and disabled:

Table 5 Enabled and Disabled features

Features	Enabled
Display of images & playing of sound	Yes
Running scripts	Yes
Display of script errors	Yes
Display popup windows and dialogs	Yes
Running JAVA	No
Downloading or running ActiveX	No
Downloading Files	No

Policy Secure 802.1X Connection Type Options

Use this connection type to define authenticated connectivity to 802.1X devices, wired or wireless. Users cannot create 802.1X connections from the Pulse Client interface. Users see 802.1X connections in the Pulse Client interface only when the connection has been deployed from the server and the specified network is available.

- **Adapter type**: Specifies the type of adapter to use for authentication: wired or wireless.
- **Outer username**: Enables a user to appear to log in anonymously while passing the actual login name (called the inner identity) through an encrypted tunnel. As a result, the user's credentials are secure from eavesdropping, and the user's inner identity is protected. In general, enter anonymous, which is the default value. In some cases, you might need to add additional text. For example, if the outer identity is used to route the user's authentication to the proper server, you might be required to use a format such as "anonymous@acme.com".

Note: If you leave the box blank, Pulse Client passes the user's or the machine's Windows login name as the outer identity.

- **Scan list**: If you selected wireless as the adapter type, the scan list box is available to specify the SSIDs, including non-broadcast SSIDs, to connect to in priority order. If you leave the list empty, the user can connect to any available wireless network.
- **Support Non-broadcast SSID**: Allows a user to connect to a non-broadcast wireless network from within the Pulse Client interface. Selecting this field enables the following options:
  - **Wireless Security Cipher**: Specify the type of encryption used by the non-broadcast network:
    - TKIP
    - AES

If the non-broadcast SSID options are configured, the Pulse Client connection configuration includes the values and they are used to configure the wireless profile on the endpoint.

Trusted Server List (for Policy Secure 802.1X Connection)

FQDN criteria for 802.1X/EAP server certificates (with wildcard support) can be specified in the Trusted Server List of the Pulse Connect Secure admin console. In the name field, you can enter a fully-qualified-domain name (FQDN) that can be either an exact FQDN or an FQDN that begins with a "." and/or can contain wildcards ("*").

Note the Following:

- The "ANY" entry matches any server certificate name.
- An entry that contains "=" requires an exact Subject:DN (Distinguished Name) match.
- An entry that is neither "ANY" nor contains "=" is an FQDN. It can be either an exact value or include wildcards and/or begin with a "." character. This value will be checked against FQDNs in the server's certificate (Subject:DN:CN=..., SAN:DNS=...).
  - An entry that begins with "." will wildcard only the first subdomain (domain component) in the FQDN. For example, ".mycompany.com" will match "foo.mycompany.com" but not "foo.bar.mycompany.com". As such, a FQDN beginning with "." is equivalent to the same FQDN beginning with "." (e.g., ".mycompany.com" is equivalent to ".mycompany.com"). Note that this mechanism is more restrictive than what is described in RFC 5280.
  - FQDN may contain at most one wildcard per domain component (DC). For example, "a.mycompany.com" is not allowed and will always result in authentication failure.
  - A wildcard matches 1 or more characters (but not zero characters). For example, "f*r.mycompany.com" will match "foo-bar.mycompany.com" but not "fr.mycompany.com".
  - See RFC 2818 and RFC 6125 for more details and security implications of wildcards.
  - Be careful when mixing wildcard FQDN entries with certificates that contain wildcards in their names. For example, the entry "foo*.mycompany.com" will match a certificate with the name "*bar.mycompany.com".
  - This wildcarding mechanism does not work with server certificates that contain the "?" character in their names. (This is not a common occurrence.)
- You can choose any server certificate's issuing certificate authority (CA) from the drop-down list. It could be the direct issuer or any CA at higher level in the certificate chain, up to the root.

Connect Secure or Policy Secure (L3) Connection Type Options

Use a Connect Secure or Policy Secure (L3) connection for a Layer 3 connection to Pulse Connect Secure or Pulse Policy Secure.

- **Allow user to override connection policy**: Allows a user to override the connection policy by manually connecting or disconnecting. Typically, you leave this option selected to make sure that a user can establish a connection under all conditions. If you disable this check box, the user cannot change the endpoint's connection status, suspend/resume a connection to Pulse Connect Secure or shut down Pulse Client.
- **Lock-down this connection**: When enabled, this option limits network connectivity while Pulse Client is in the process of creating a VPN connection. When used in conjunction with Location Awareness rules, this option ensures that end users cannot access network resources outside of a VPN tunnel.

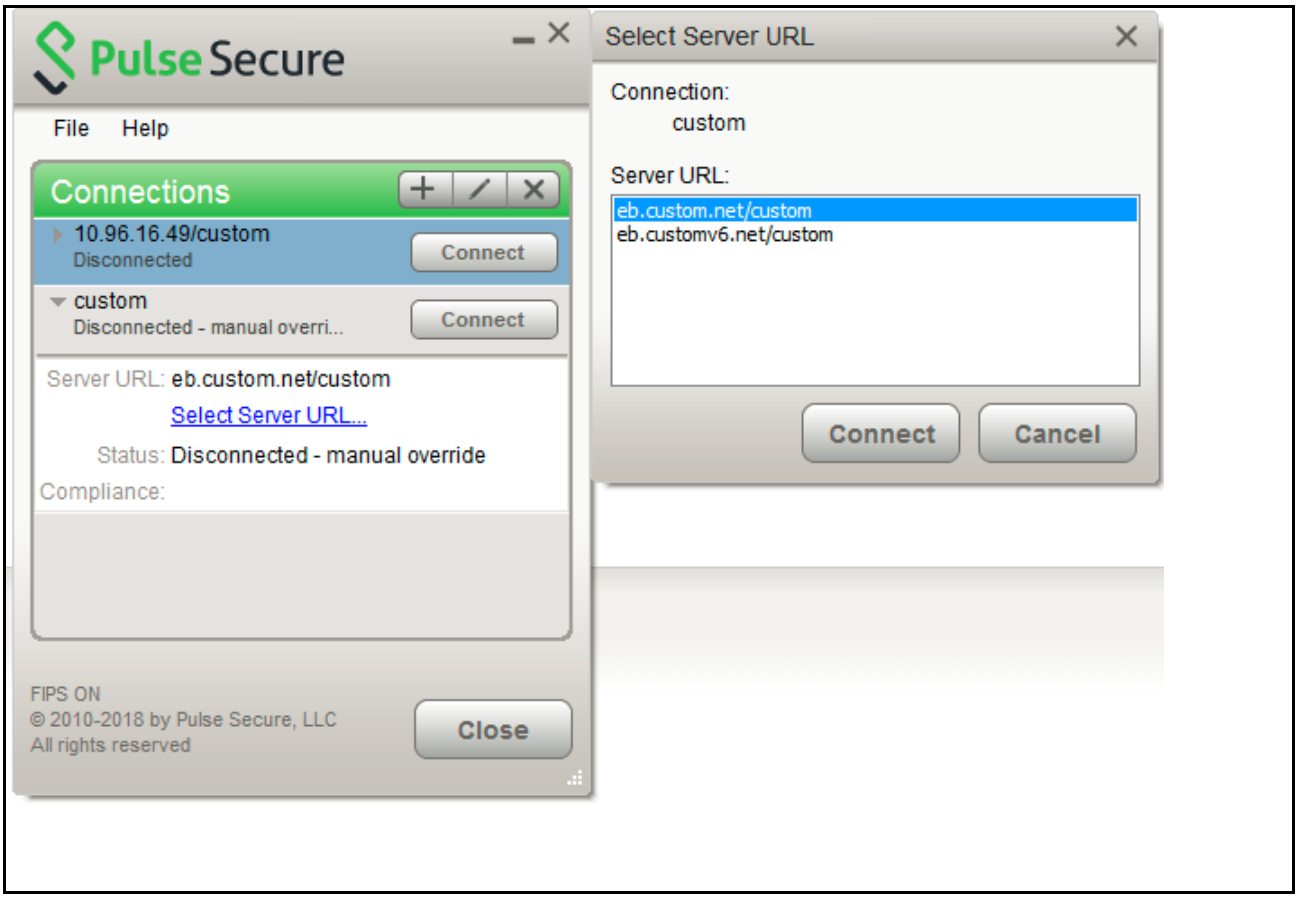
Note: Lock-down this connection feature exists in Pulse Client for Windows only.

- **Support Remote Access (SSL VPN) or LAN Access (UAC) on this connection**: This option must be selected if this connection is for Pulse Policy Secure. If the connection is for Pulse Connect Secure, you can disable this check box and use the connection for accessing Pulse Collaboration meetings only by also selecting Enable Pulse Collaboration integration on this connection.
- **Enable Pulse Collaboration integration on this connection**: This option must be disabled if this connection is for Pulse Policy Secure. If the connection is for Pulse Connect Secure, you can enable this check box and use the connection for accessing Pulse Collaboration meetings.
- **Connect to URL of this server only**: Specifies whether the endpoint connects to this Pulse Secure server exclusively or if it can connect to the any of the servers listed in the list of connection URLs. Disable this check box to enable the List of Connection URLs.
- **List of Connection URLs**: Allows you to specify a list of Pulse Secure servers (Pulse Policy Secure or Pulse Connect Secure) for this connection. Pulse Client attempts to reach each server in the list, in the order listed, until it succeeds. You can specify up to 8 Pulse Secure servers.

Note: IF-MAP federation must be configured to ensure that a suspended session can be resumed to a different URL. When this feature is used with Pulse Policy Secure, all Pulse Secure devices in the list must be configured for failover, so that any one of them can provision the firewall enforcer.

Figure 47 shows how the Pulse Client user can select a server from the connection's list of URLs.

Figure 47 Pulse Client for Windows with a List of Connection URLs



- **Attempt most recently connected URL first**: If you have specified a list of connection URLs, you can select this check box to have Pulse Client always attempt the most recent successful connection. If that connection is not successful, Pulse Client then starts at the top of the list. The most recently connected URL is saved across reboots.
- **Randomize URL list order**: If you have specified a list of connection URLs, select this check box to have Pulse Client ignore the order in which the servers are listed. You can select this option to spread the connection load across multiple Pulse Secure servers.

  If you enabled Attempt most recently connected URL first, then Pulse Client attempts that connection first. If the connection attempt fails, Pulse Client chooses randomly from the list for the next connection attempt. During a credential provider connection attempt, Pulse Client chooses the URL automatically. It does not display a window to let the user choose a URL. Connections that use machine authentication ignore this option and always use the ordered list of connection URLs. Any preferred roles and realms you specify must be applicable to all of those servers. In the case of an interrupted connection, such as temporarily losing the WiFi link, Pulse Client always tries to reconnect to the most recently connected URL.

  The Pulse Secure servers should be configured for IF-MAP federation to ensure that a session can be resumed to a different URL. If the Pulse Secure servers are not federated, then Pulse Client might prompt for credentials.

SRX (for Dynamic VPN) Connection Type Options

Use an SRX connection for a dynamic VPN connection to an SRX Series Services Gateway.

- **Address**: Specifies the IP address of the SRX Series device.
- **Allow user to override connection policy**: Allows users to override the connection policy by manually connecting or disconnecting. Typically, you leave this option selected to make sure that a user can establish a connection under all conditions. If you disable this check box, the user cannot change the endpoint's connection status or shut down Pulse Client.

Pulse Client Connection is Established Options

For all connection types, specify how the connection is established. The options vary according to the type of connection. Automatic connections include machine authentication and credential provider connections. Connections can be established using the following options.

Note: All connections that are configured to start automatically attempt to connect to their target networks at startup time. To avoid multiple connection attempts, be sure that only one connection is configured to start automatically, or configure location awareness rules.

- Modes:
  - **User**: Enables user authentication.
  - **Machine**: Enables machine authentication, which requires that Active Directory is used as the authentication server and that machine credentials are configured in Active Directory. A machine connection is, by default, an automatic connection.
  - **Machine or user**: Enables machine authentication for the initial connection. After user authentication, the machine authentication is dropped. When the user logs out, the machine authentication connection is restored.

- Options:
  - **Connect automatically**: Connections are attempted when the conditions specified in the location awareness rules are true, and disconnected when the conditions are no longer true.
  - **Reconnect at Session Timeout or Deletion**: If this option is enabled, user initiated sessions automatically attempt to reconnect upon a session timeout or deletion. If this option is disabled, then user initiated sessions remain disconnected upon a session timeout or deletion.
  - **Enable pre-desktop login (Credential provider)**: Enables Pulse Client interaction with the credential provider software on the endpoint. The user credentials are used to establish the authenticated Pulse Client connection to the network, login to the endpoint, and login to the domain server.

Pulse Client Connection is Established Examples

The following configurations show how to select the Connection is established options of a Pulse Client connection set for specific user login behavior:

Figure 48 Connect manually

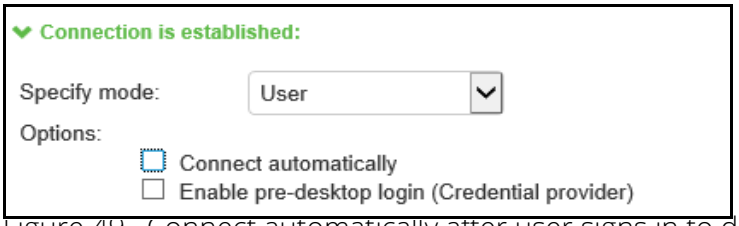


Figure 49 Connect automatically after user signs in to desktop

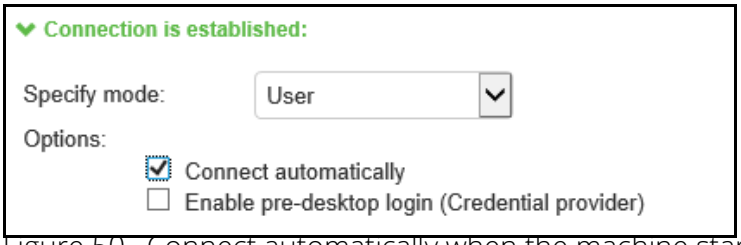
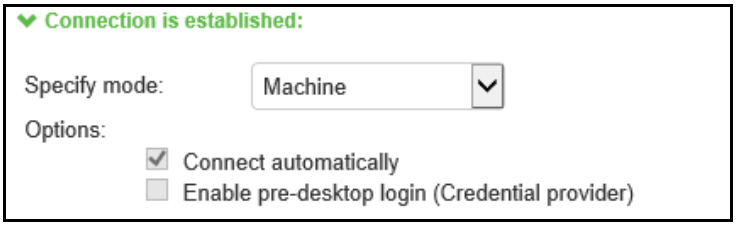


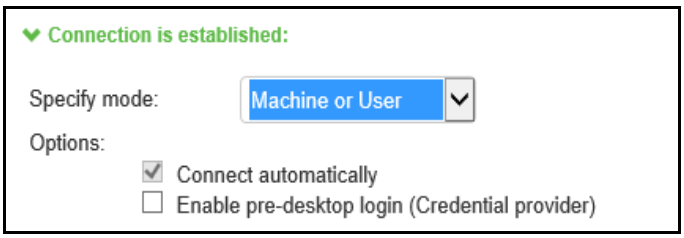
Figure 50 Connect automatically when the machine starts; machine credentials are used for authentication



Note: When you use machine credentials for authentication and no user credentials, Pulse Client cannot perform user-based tasks. The following tasks can be run only when the user is logged in:

- Run session scripts
- Detect or modify proxy settings
- Run automatic Pulse Client upgrade
- Install or upgrade Pulse Client components

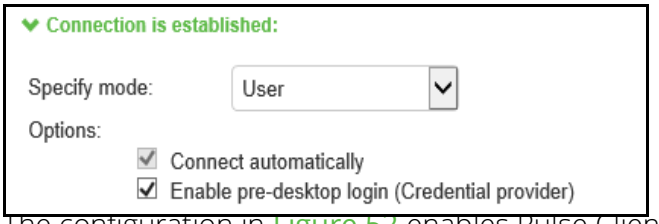
Figure 51 Connect automatically when the machine starts; the connection is authenticated again when the user signs in to the desktop



The configuration in Figure 51 enables machine authentication for the initial connection. After the user connects with user credentials, the machine authentication is dropped. When the user logs out, the machine authentication connection is restored. In one typical use case, the machine credentials provide access to one VLAN, and the user credentials provide access to a different VLAN.

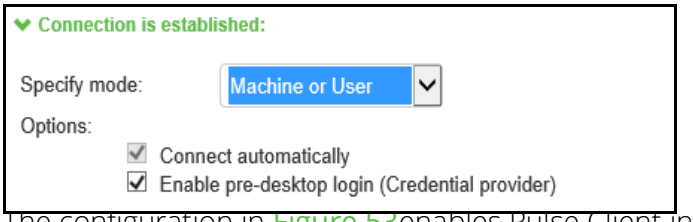
Note: If the machine and user have different roles, each role should map to the same connection set. Otherwise, after the user connects, the existing connection set might be replaced.

Figure 52 Connect automatically at user login



The configuration in Figure 52 enables Pulse Client interaction with the credential provider software on the endpoint. The user credentials are used to establish the authenticated Pulse Client connection to the network, to log in to the endpoint, and to log in to the domain server.

Figure 53 Connect automatically when the machine starts; connection is authenticated again at user login



The configuration in Figure 53enables Pulse Client interaction with the credential provider software on the endpoint. Machine credentials are used to establish the authenticated Pulse Client connection to the network. When the user provides user credentials, the connection is authenticated again. In one typical use case, the machine credentials provide access to one VLAN, and the user credentials provide access to a different VLAN.

Location Awareness Rules

For Connect Secure or Policy Secure (L3) and SRX connections, you can define location awareness rules that enable an endpoint to connect conditionally. If you do not have location awareness rules defined, Pulse Client attempts to connect with each connection that is defined as an automatic connection until it connects successfully. Location awareness rules allow you to define an intelligent connection scheme. For example, the endpoint connects to Pulse Policy Secure if it is connected to the company intranet, or it connects to Pulse Connect Secure if it is in a remote location.

A Pulse Client connection uses the IP address of a specified interface on the endpoint to determine its network location. Each location awareness rule includes the following settings:

- **Name**: A descriptive name, for example, "corporate-DNS." A name can include letters, numbers, hyphens, and underscores.
- **Action**: The method the connection uses to discover the IP address. Choose one of the following values:
  - **DNS Server**: Allows the endpoint to connect if the endpoint's DNS server on the specified interface is set to one of the specified values. Use the Condition box to specify IP addresses or address ranges.
  - **Resolve Address**: Allows the endpoint to connect if the hostname specified in the DNS Name box can be resolved by the DNS server for the specified interface. If one or more address ranges are specified in the Address Range box, the address must resolve to one of the ranges to satisfy the expression.
  - **Endpoint Address**: Allows the endpoint to connect if the IP address of the specified interface is within a range specified in the IP Address Range box.

Note: To create a negative location awareness rule, you first create the positive state and then use rule requirement logic to use the rule as a negative condition.

Machine Connection Preferences

The Machine Connection Preferences appear if you have selected one of the machine authentication options for how the connection is established. Normally Pulse Client presents a selection dialog box if more than one realm or role is available to the user. However, a connection that is established through machine authentication fails if a dialog box is presented during the connection process. To suppress the selection dialogs, either ensure that only one role and realm is available to users, or specify a preferred realm and role for this connection.

- **Preferred Machine Realm**: Specify the realm that this connection uses when establishing the machine connection. The connection ignores any other realm available for the specified login credentials
- **Preferred Machine Role Set**: Specify the role or the name of rule for the role set that this connection uses when establishing the machine connection. The role or rule name used must be a member of the preferred machine realm.

User Connection Preferences

The User Connection Preferences options enable you to specify a realm and role for automatic connections that would otherwise present a selection dialog box to the user. To suppress the selection dialogs, either ensure that only one role and realm is available to users, or specify a preferred realm and role for this connection.

- **Preferred User Realm**: Specify the realm for this connection that is used when a user logs onto the endpoint. The connection ignores any other realm available for the user's login credentials

  If one of the credential provider connection options is enabled, the following options are available:

  - **Preferred Smartcard Logon Realm**: Preferred realm to be used when user logs in with a smart card.
  - **Preferred Password Logon Realm**: Preferred realm to be used when user logs in with a password.

Note: Be sure that the authentication realms you specify exist, and that they support the appropriate login credential option.

- **Preferred User Role Set**: Specify the preferred role or the name of the rule for the role set to be used for user authentication. The role or rule name used must be a member of the preferred user realm.
- **Select client certificate from machine certificate store**: Enables you to specify the location of the client certificate on a Windows endpoint as part of a Pulse Client connection that verifies the identity of both the machine and the user before establishing a connection. When this check box is selected, the Pulse Client connection looks at client certificates located in the Local Computer personal certificate store. When this check box is not selected, the connection accesses the user certificate store as a Windows endpoint. For more information, see "Machine and User Authentication through a Pulse Client Connection for Pulse Connect Secure" on page 29.

Securing the Connection State on Pulse Client

To disable user interaction with Pulse Client connections on the endpoint, you can configure Pulse Client Connections so that when they are deployed to the endpoint, users cannot shut down a connection, suspend or resume a connection, or shut down Pulse Client. Disabling user interaction with Pulse Client enables the administrator to control how endpoints connect to the network without allowing the user to override administrative control. For example, if you use machine authentication, the connection from endpoint to server is established automatically. By locking down the Pulse Client endpoint, users cannot change their connection.

To secure the Pulse Client endpoint:

1. Click **Users > Pulse Secure Connections**.
2. Edit or create a new connection.
3. Disable the check box labeled **Allow user to override connection policy**.

Creating a Client Connection Set for Pulse Connect Secure

To create a Pulse Client Connection:

1. From the admin console, select **Users > Pulse Secure > Connections**.
2. Click **New**.
3. Enter a name and, optionally, a description for this connection set.

Note: You must enter a connection set name before you can create connections.

4. Click **Save Changes**.
5. From the main Pulse Client Connections page, select the connection set.
6. Under Options, select or clear the following check boxes:

- **Allow saving logon information**: Controls whether the **Save Settings** check box is available in login credential dialog boxes in Pulse Client. If you clear this check box, Pulse Client always requires users to provide credentials. If you select this check box, users have the option of saving their credentials.
- **Allow user connections**: Controls whether connections can be added by the user through the Pulse Client interface.
- **Display splash screen**: Clear this check box to hide the Pulse Client splash screen that normally appears when Pulse Client starts.
- **Dynamic certificate trust**: Determines whether users can opt to trust unknown certificates. If you select this check box, a user can ignore warnings about invalid certificates and connect to the target Pulse Secure server.

  Note: By default, Dynamic certificate trust check box will be unchecked.

- **Dynamic connections**: Allows new connections to be added automatically to Pulse Client when the user logs into a Pulse Secure server through the server's Web portal, and then starts Pulse Client though the Web portal interface.
- **FIPS mode enabled**: Enable FIPS mode communications for all Pulse Client connections in the connection set. The Federal Information Processing Standard (FIPS) defines secure communications for the U.S. government. When a Pulse Client connection is operating in FIPS mode, **FIPS On** appears in the lower corner of the Pulse Client interface.

Note: If the Pulse Connect Secure hardware does not support FIPS mode operations, FIPS mode configuration options are not present in the admin console interface. FIPS mode operations are supported on PSA-V Series Pulse Secure Gateways and some SA series appliances. The device must be running Pulse Policy Secure R5.0 or later or Pulse Connect Secure R8.0 or later.

Note: Users cannot enable FIPS mode for connections that are created on Pulse Client. You must deploy connections with FIPS mode enabled using a pre-configured connection set with FIPS mode enabled or have users establish a browser session to the FIPS-enabled Pulse Connect Secure.

- **Wireless suppression**: Disables wireless access when a wired connection is available. Wireless suppression occurs only when the wired connection is connected and authorized.

7. Under Connections, click New to define a new connection.
8. Enter a name and, optionally, a description for this connection.
9. Select a type for the connection and then specify the connection. Type can be any of the following:
   - **Policy Secure (802.1X)**: Select this type if the connection establishes connectivity to an 802.1X wired or wireless device.
   - **Connect Secure or Policy Secure (L3)**: Select this type to define a connection for Pulse Connect Secure or Pulse Policy Secure.
   - **SRX**: Select this type to define a connection to an SRX Series Services Gateway.
10. The connection configuration options that appear depend on the connection type you select.

After you have created the client connection set, create a client component set and select this connection set.

Pulse Client FIPS Mode for Pulse Connect Secure Overview

The United States Federal Information Processing Standard (FIPS) defines security and interoperability requirements for computer systems that are used by the U.S. government. Pulse Client for Windows, Mac, iOS (32-bit iOS devices only), and Android support FIPS mode operations when communicating with Pulse Connect Secure and Pulse Client for Windows and Mac support FIPS mode operations when communicating with Pulse Policy Secure. When it is operating in FIPS mode, **FIPS On** appears in the bottom corner of the Pulse Client for Windows and Mac.

If the Pulse Secure server hardware does not support FIPS mode operations, FIPS mode configuration options are not present in the admin console interface. FIPS mode operations are supported on PSA-V Series Pulse Secure Gateways and some SA series appliances. The device must be running Pulse Policy Secure R5.0 or later or Pulse Connect Secure R8.0 or later.

You enable FIPS mode operations when you configure Pulse Client connections on the server. You enable FIPS mode operations for a connection set. That connection set can include any or all types of Pulse Client connection:

- **Policy Secure (802.1X)**: Pulse Client uses FIPS mode cryptography for authentication but it uses default Microsoft cryptography for the WEP/WPA wireless encryption.
- **Connect Secure or Policy Secure (L3)**: FIPS mode cryptography is supported.
- **SRX**: FIPS mode cryptography is not supported.

Note: Users cannot enable FIPS mode for connections that are created on Pulse Client. You must deploy connections with FIPS mode enabled using a pre-configured connection set with FIPS mode enabled or have users establish a browser session to the FIPS-enabled Pulse Connect Secure.

From release 9.1R11 onwards, Pulse Client in FIPS mode is not available for download from Pulse Connect Secure or Pulse Policy Secure. The Pulse Client installer for FIPS mode is available for download at https://support.pulsesecure.net. Pulse Client package can be uploaded to server for end users access. Upgrading the Pulse Client in FIPS mode to non-FIPS mode is not supported.

Endpoint Requirements

Pulse Client supports FIPS mode on Windows Vista and later Windows versions. FIPS is not supported by the Pulse Client for OS X.

To support client certificate private key operations, the security policy on the endpoint must have FIPS enabled. To verify that FIPS is enabled, use the Microsoft Management Console (MMC). Make sure that the Group Policy Snap-in is installed, and then navigate to **Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options**.

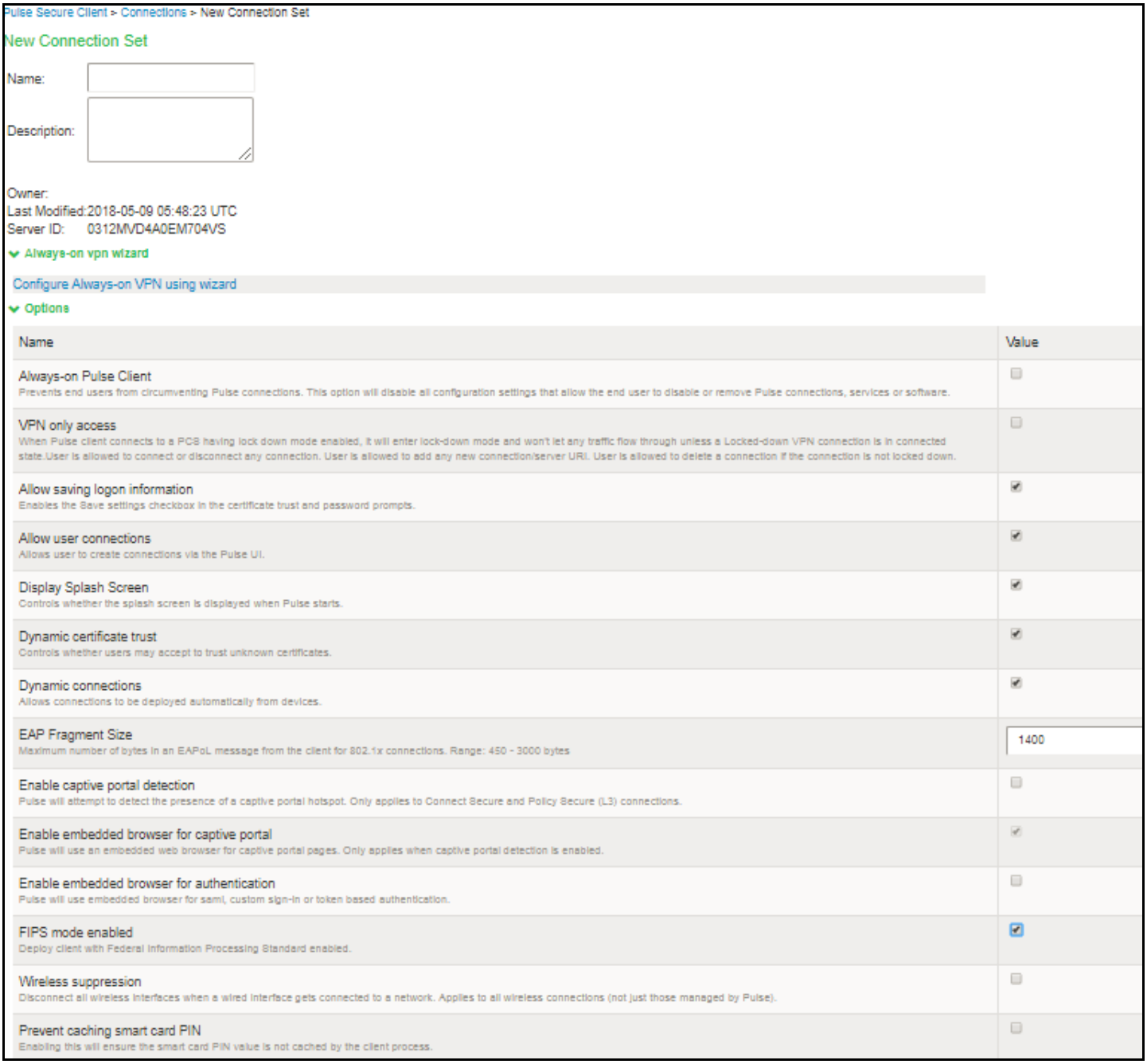
Scroll through the Policy list and make sure that the following policy is enabled:

"System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing"

Configuration Overview

Pulse Client includes all components required for FIPS mode communications. To enable FIPS mode communications, deploy one or more connections to a Pulse Client that is FIPS enabled. Figure 54 shows the check box in the Pulse Connect Secure connection set configuration screen that enables FIPS mode operations for all connections in the connection set.

Figure 54 Enabling FIPS Mode for Pulse Client Connections



Note: If the Pulse Secure server hardware does not support FIPS mode operations, FIPS mode configuration options are not present in the admin console interface. FIPS mode operations are supported on PSA-V Series Pulse Secure Gateways and some SA series appliances. The device must be running Pulse Policy Secure R5.0 and later or Pulse Connect Secure R8.0 and later.

Configuring Location Awareness Rules for Pulse Client

The location awareness feature enables Pulse Client to recognize its location and then make the correct connection. For example, you can define rules so that a Pulse Client that is started in a remote location automatically establishes a VPN connection to Pulse Connect Secure, and then that same client automatically connects to Pulse Policy Secure when it is started in the corporate office. If Pulse Client detects that it is connected to the corporate LAN and it already has a VPN connection (for example, the VPN connection was suspended when the computer was put into hibernation), it first discovers that the VPN location awareness rules are no longer true, disconnects that VPN connection, and then evaluates the location awareness rules for the other configured connections.

Location awareness relies on rules you define for each Pulse Client connection. If the conditions specified in the rules resolve to TRUE, Pulse Client attempts to make the connection. If the conditions specified in the rules do not resolve to TRUE, Pulse Client tries the next connection. To set up the location awareness rules that select among many connections, you must define location awareness rules for each connection. Each location awareness rule is based on the endpoint's ability to reach an IP address or resolve a DNS name over a specified network interface.

The following location awareness example includes two connections. Each connection is configured to connect to only one target server. The first connection is a Pulse Policy Secure connection that resolves to TRUE when the endpoint is connected to the corporate LAN. The second connection is a Pulse Connect Secure connection that resolves to TRUE when the endpoint is located in a remote location. If Pulse Client detects that it is connected to the corporate LAN and it already has a VPN connection, it disconnects that VPN connection.

Pulse Policy Secure connection

- If the DNS server that is reachable on the endpoint's physical network interface is one of your organization's internal DNS servers, then establish the connection.

Pulse Connect Secure connection

- If the DNS server that is reachable on the endpoint's physical network interface is not one of your organization's internal DNS servers, and the DNS name of your Pulse Connect Secure device resolves to the external facing IP address of the Pulse Connect Secure device, then establish the connection.

Note: Connections can be set to manual, automatic, or controlled by location awareness rules. When the user logs in, Pulse Client attempts every connection in its connections list that is set to automatic or controlled by location awareness rules.

Note: To create a negative location awareness rule, you first create the positive state and then use rule requirement logic to use the rule as a negative condition.

To configure location awareness rules:

1. If you have not already done so, create a connection or open an existing connection.

   You can configure location awareness rules for SRX connections and Connect Secure or Policy Secure (L3) connections. Location awareness rules do not apply to UAC (802.1X) connections.

2. Click the **Mode** list, and then select one of the options, "User", "Machine", or "Machine or user".
3. If you selected "User" as the Mode, Under Options, select **Connect automatically**. If you selected "Machine" or "Machine or User", **Connect automatically** is enabled by default.

4. Under Location awareness rules, click **New**.

   Alternatively, you can select the check box next to an existing rule, and then click **Duplicate** to create a new rule that is based on an existing rule.

5. Specify a name and description for the rule.

6. In the Action list, select one of the following:

   - **DNS server**: Connect if the DNS server associated with the endpoint's network properties is (or is not) set to a certain value or set of values. Specify the DNS server IP address in the IP address box. Also specify a network interface on which the condition must be satisfied:
     - **Physical**: The condition must be satisfied on the physical interfaces on the endpoint.
     - **Pulse Secure**: The condition must be satisfied on the virtual interface that Pulse Client creates when it establishes a connection.
     - **Any**: Use any interface.
   - **Resolve address**: Connect if the configured hostname or set of hostnames is (or is not) resolvable by the endpoint to a particular IP address. Specify the hostname in the DNS name box and the IP address or addresses in the IP address box. Also specify a network interface on which the condition must be satisfied.

Note: Pulse Client evaluates IP and DNS policies on network interface changes. DNS lookups occur on DNS configuration changes or when the time-to-live setting (10 minutes) expires for a particular host record. If Pulse Client cannot resolve the host for any reason, it polls the configured DNS server list every 30 seconds. If the host had been resolved successfully previously and the time-to-live timer has not expired, the polling continues until the timer expires. If the host had not been resolved successfully previously, the resolution attempt fails immediately.

   - **Endpoint Address**: Connect if a network adapter on the endpoint has an IP address that falls within or outside of a range or a set of ranges. Specify the IP address or addresses in the IP address box. Also specify a network interface on which the condition must be satisfied.

7. Click **Save Changes**.

After you create the rule or rules, you must enable each rule you want to use for the connection. To enable a negative form of a rule, use a custom version of the rule. To enable location awareness rules:

1. In the list of connection awareness rules for a connection, select the check box next to each rule you want to enable.

2. To specify how to enforce the selected location awareness rules, select one of the following options:

   - **All of the above rules**: The condition is TRUE and the connection is attempted only when all selected location awareness rules are satisfied.
   - **Any of the above rules**: The condition is TRUE and the connection is attempted when any select location awareness rule is satisfied.
   - **Custom**: The condition is TRUE and the connection is attempted only when all selected location awareness rules are satisfied according to the Boolean logic you specify in the Custom box. Use the Boolean condition to specify a negative location rule. For example, connect to Pulse Connect Secure when Rule-1 is false and Rule-2 is true. The Boolean logic in the custom box would be: "NOT Rule-1 AND Rule-2". The accepted Boolean operators are AND, OR, NOT, and the use of ( ).

3. Click **Save Changes**.

Component Set Options for Pulse Connect Secure

A Pulse Client component set includes specific software components that provide Pulse Client connectivity and services.

Note: Client component set options affect Web-based installations only.

- **All components**: Supports all Pulse Client connection types.
- **No components**: Updates existing Pulse Client configurations, for example, to add a new connection. Do not use this setting for a new installation.

Creating a Client Component Set for Pulse Connect Secure

A Pulse Client component set includes specific software components that provide Pulse Client connectivity and services.

Note: Client component set options affect Web-based installations only.

To create a Pulse Client component set:

1. From the admin console, select **Users > Pulse Secure > Components**.
2. Click **New** to create a new component set.
3. If you have not yet created a client connection set, select **Users > Pulse Secure > Connections** and create a new connection set. Or you can use the default client configuration, which permits dynamic connections, supports the outer username anonymous, and allows Pulse Client to automatically connect to Pulse Policy Secure or Pulse Connect Secure.
4. Specify a name for the client component set.
5. (Optional) Enter a description for this client component set.
6. Select a connection set that you have created, or use the default connection set.
7. For Pulse Client components, select one of the following options:
   - **All components**: Supports all Pulse Client connection types.
   - **No components**: Updates existing Pulse Client configurations, for example, to add a new connection. Do not use this setting for a new installation.
8. Click **Save Changes**.
9. After you create a component set, distribute Pulse Client to users through a role. When users access the role, the installer automatically downloads to the endpoint. The installer components and connections are applied to the endpoint client.

   If client connections associated with the component set for a role are changed even though the list of components has not, the existing configuration on the endpoint is replaced immediately if the endpoint is currently connected, or the next time the endpoint connects.

If a user is assigned to multiple roles and the roles include different component sets, the first role in an endpoint's list of roles is the one that determines which client (component set) is deployed.

Manage Pulse Client Versions

This feature is supported for Pulse Client on macOS and Windows. From 9.1R2 release onwards, this feature is supported for iOS Mobile Client and Android Mobile Client also.

Note: From 9.1R2 onwards, this feature will not be applicable for Windows Universal App.

This feature allows admin to configure a minimum client version. If the client has version lower than the configured minimum version, then the PCS server will reject the client connection.

If the client is older than the configured minimum client version, then PCS gateway will reject the connection. User can upgrade it later through browser or SCCM server.

For example, the gateway can host Pulse Client 5.2r3, but the minimum version could be Pulse Client 5.2r2.

Similarly, if Pulse Client 5.2r2 is connected to the gateway it would prompt for an upgrade, if the active version is greater than the Pulse Client version.

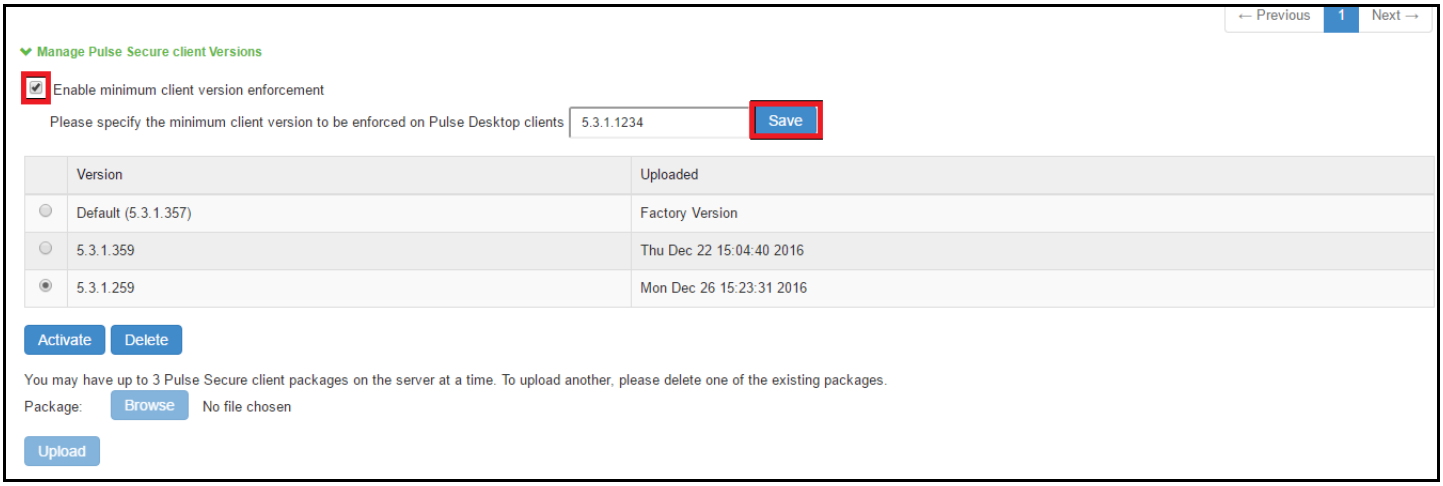
For Pulse Client 5.2r1, the connectivity would be rejected and will display an appropriate error message.

Note: This feature is qualified only for PCS.

To enable this feature on Pulse Connect Secure:

1. From the admin console, select **Users > Pulse Secure > Components**.
2. Select the **Enable minimum client version enforcement** checkbox (see Figure 55). The following options appear:
   - Pulse Desktop Clients
   - Android Mobile Clients
   - iOS Mobile Clients

Figure 55 Minimum Client Version Enforcement



3. Specify the minimum client version to be enforced on Pulse Client. For example, 5.2R1.

If the minimum client version is not specified for any specific type of client, any version of the client is allowed to connect to PCS without any minimum client version enforcement for that specific client.

4. Click **Save**.
5. Select a Version to **Activate** or **Delete** the version details.
6. Click **Browse** to select a Pulse Client package.
7. Click **Upload** to add packages.

Note: Pulse Client allows you to add up to three packages on the server at a time. To add new packages, delete an existing package.

Note: Observe the following:

- Minimum Client Version Enforcement is not supported on Linux clients. Enforcement is not applicable when Pulse Client for Linux connects to a PCS with minimum client version enforcement enabled.

- Minimum Client Version Enforcement is not supported by Pulse Policy Secure.

- Minimum Client Version Enforcement is not supported for a client session launched from a user browser session.

Endpoint Security Monitoring and Management for Pulse Connect Secure

You can configure and enable Host Checker policies to perform an endpoint security assessment before allowing the endpoint to connect. Host Checker is supported on the following operating systems:

- Windows (including 8.1 and later versions of Windows RT and Windows Phone)
- macOS
- Google Android
- Apple iOS

You can invoke Host Checker at the role level or the realm level to specify access requirements for endpoints seeking authentication. Host Checker policies that are implemented at the realm level occur before the user is authenticated. Host Checker policies at the role level are implemented after authentication but before the user is permitted to access protected resources. When an endpoint first connects to Pulse Connect Secure, the latest version of the IMC is downloaded to the host computer. The initial check can take 10-20 seconds to run. Outdated IMC files are automatically updated at subsequent checks.

Note: The first time an endpoint connects to Pulse Connect Secure that has a patch assessment policy, if the connection is a Layer 2 connection, the IMC cannot download. In this case, you should configure a remediation role that displays instructions to direct the user to retry with a Layer 3 connection or to contact the administrator.

Note: If a realm has a Host Checker policy enabled that is for Pulse Clients, and a mobile device user employs a browser on the mobile device to connect to the Web portal, the login is denied because the desktop Host Checker program is not compatible with the mobile client OS. If Pulse Client mobile users are mapped to multiple roles, the login operation assigns them to a role where Host Checker is not enabled if possible. If all the roles have Host Checker enabled, the mobile users will not be allowed to login from the browser. You can create and enable Host Checker policies that are specific to each mobile operating system and then Host Checker runs when Pulse Client connects to the server.

For patch management on Windows systems, Host Checker uses a list of the most current patch versions from the vendor for predefined rules in the Host Checker policy. Host Checker does not scan for non-security patches. Server and Host Checker manage the flow of information between the corresponding pairs of TNC-based integrity measurement collectors (IMCs) and integrity measurement verifiers (IMVs). IMCs are software modules that run on the endpoint and collect information such as antivirus, antispyware, patch management, firewall, and other configuration and security information about the host. IMVs are software modules that run on the server and verify a particular aspect of a host's integrity. Each IMV works with the corresponding IMC on Pulse Client to verify that the endpoint meets the Host Checker rules. IMCs scan the endpoint frequently for changes in security status. For example, if the user turns off virus checking, the IMC can detect this and then trigger a new check to make sure the modified system complies with the requirements of the Host Checker policy. You can configure Host Checker to monitor third-party IMCs installed on client computers by using third-party IMVs that are installed on a remote IMV server.

You obtain the most current patch version information from a Pulse Secure staging site. You can manually download and import the list into the Pulse Connect Secure server, or you can automatically import the list from the Pulse Secure staging site or your own staging site at a specified interval.

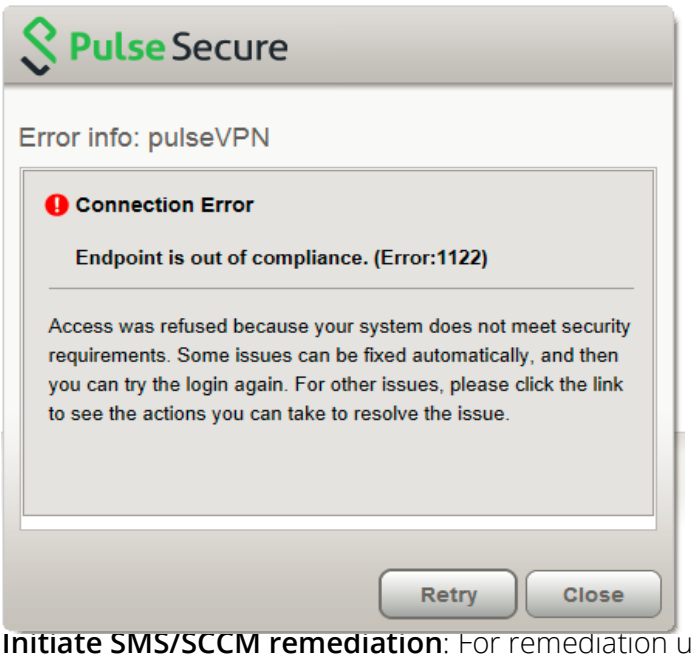
Monitoring is based on one or more specified products or on specific patches, though not in the same policy. For example, you could check for Internet Explorer Version 7 with one policy, and Patch MSOO-039: SSL Certificate Validation Vulnerabilities with a second policy. Then, apply both policies to endpoints at the role or realm level to ensure that the user has the latest browser version with a specific patch. In addition, for Microsoft products, you can specify the severity level of patches that you want to ignore. For example, you could ignore low or moderate threats.

Remediation Options

Host Checker can identify issues on an endpoint. However, Host Checker and Pulse Connect Secure cannot resolve issues, that is, perform remediation tasks, on non-compliant endpoints. To repair those issues Pulse Connect Secure supports the following remediation options:

- **Instructions to the user**: The Pulse Secure gateway can send a message to the user describing the non-compliant patches or software and a link to where the user can obtain the required software. Figure 56 shows a typical Pulse Client remediation message.

Figure 56 Pulse Client Remediation Instructions



- **Initiate SMS/SCCM remediation**: For remediation using Microsoft System Center Configuration Manager (ConfigMgr or SCCM), formerly Systems Management Server (SMS), a preinstalled SMS/SCCM client on the endpoint is triggered by Host Checker to get patches from a preconfigured SMS/SCCM server. This mechanism installs only those patches that are published on the SMS/SCCM server.

Issuing a Remediation Message with Pulse Connect Secure

If a Host Checker policy finds that an endpoint is not in compliance, Host Checker can display a message through the Pulse Client interface that includes custom instructions and reason strings on how to bring the endpoint into conformance. The user must perform the steps described in the message before the endpoint is allowed to access protected resources.

To enable a remediation message for a Host Checker policy:

1. In the admin console, select **Authentication > Endpoint Security > Host Checker**.
2. In the Policies section, click **New** to create a new Host Checker policy.
3. As part of the Host Checker Policy, select **Enable Custom Instructions**.

   When you select this option, a text box appears. Enter the instructions to display to the user on the Host Checker remediation page. You can use the following HTML tags to format text and to add links to resources such as policy servers or web sites: <i>, <b>,
, <font>, and <a href>. For example:

   ```
   You do not have the latest signature files.
   <a href="www.company.com">Click here to download the latest signature files.</a>
   ```

4. Optionally, select **Send reason strings**. Select this option to display a message to users (called a reason string) that is returned by Host Checker or IMV and that explains why the client does not meet the Host Checker policy requirements. Reason strings describe to users what the IMV is checking on the client. This option applies to predefined rules, to custom rules, and to third-party IMVs that use extensions in the Pulse Secure TNC SDK.

5. Click **Save Changes**.

Be sure to include the Host Checker policy in the realm or role you configure for Pulse Client users.

Using SMS/SCCM Remediation with Pulse Connect Secure

Pulse Client supports the Microsoft System Center Configuration Manager (ConfigMgr or SCCM), formerly Systems Management Server (SMS) download method for patch deployment. If Pulse Connect Secure is configured for the SMS/SCCM method for patch deployment, the Pulse Client endpoint must have the SMS/SCCM client already installed on the endpoint, otherwise remediation fails.

Endpoints configured with SMS/SCCM for software management typically poll the server for updates every fifteen minutes or longer. In a worst-case scenario, clients that are not in compliance with existing Host Checker software requirements might have to wait until the next update interval to login. Using the SMS/SCCM download method, you can force the client to initiate the software update immediately after the patch assessment check. If a user attempts to log in, and the endpoint does not have a required software version for compliance with a Host Checker patch assessment policy, Host Checker immediately notifies the client to poll the server for an immediate update. The client receives notification that an SMS/SCCM update has started.

To configure SMS/SCCM to update the client when notified, set the advertisement time on the SMS/SCCM to As soon as possible.

You assign clients to a particular group or collection on the SMS/SCCM server and then server can advertise patches for that collection. You can configure roles that correspond to collections and SMS/SCCM can send the appropriate patches for a particular role.

You must have the SMS/SCCM client installed and configured correctly on endpoints, and the SMS/SCCM server must be reachable. In a Layer 2 network, Host Checker is performed before the endpoint is connected to the network. Host Checker can obtain the IP address of the SMS/SCCM server configured for the client. If the endpoint is out of compliance and remediation is necessary, Host Checker pings the server IP address every 15 seconds until the server can be notified to update the client.

You should inform users of the expected behavior if this feature is enabled, as there is no notification to the user until the SMS/SCCM sends back the advertisement.

To enable SMS/SCCM assessment and remediation:

1. In the admin console, select **Authentication > Endpoint Security > Host Checker**.
2. In the Policies section, click **New** to create a new Host Checker policy.
3. Under Patch Remediation Options, select **SMS/SCCM Patch Deployment**.
4. Click **Save Changes**.

Be sure to include the Host Checker policy in the realm or role you configure for Pulse Client users.

Pushing Pulse Client Configurations Between Pulse Secure Servers of the Same Type

You can use the Push Configuration feature to centrally manage Pulse Client Connections, components, and uploaded Pulse Client packages. The Push Configuration feature enables you to copy all configuration settings or selected configuration settings from one Pulse Secure server to another Pulse Secure server of the same type, for example, from one Pulse Connect Secure server to another Pulse Connect Secure server.

The following notes apply to pushing configurations:

- You can push to a single Pulse Secure server or to multiple Pulse Secure servers in one operation. You can push up to 8 targets per push operation. You can run up to 25 push operations simultaneously. The maximum number of targets is 200. If a push to a target Pulse Secure server fails, the operation proceeds to the next target until all identified targets are updated. The results page displays the status and any problems encountered during the process.
- You can push to a Pulse Secure server that is a member of a cluster as long as the target Pulse Secure server is not a member of the same cluster as the source.
- Target Pulse Secure servers can refuse pushed configuration settings. The default is to accept.
- After an update, the target Pulse Secure server restarts its services. Brief interruptions might occur while the service restarts. We recommend that you push to targets when they are idle or when you can accommodate brief interruptions.
- Target Pulse Secure servers do not display a warning message when they receive a pushed configuration.
- The target Pulse Secure server automatically logs out administrators during the push process.
- The source and target Pulse Secure servers must have the same build version and number.
- The administrator account on the source Pulse Secure server must sign in to the target Pulse Secure server without any human intervention. For example, you cannot have dynamic credentials or multiple roles that are not merged as these both require manual interaction.

Before you use Push Configuration, you must configure your system according to the following conditions:

- You must map to the .Administrators role, thereby creating a “super administrator” with full administration privileges. Modify **Authentication > Auth Servers > Administrator Server > Users settings** to add yourself to the .Administrators role.
- The target Pulse Secure server administrator account must use static password authentication or two-factor tokens that do not use challenge/response type authentication. For example, certificates, Soft ID, and Defender Authentication are not supported. Modify **Administrators > Admin Realms > [Administrator Realm] > General settings** to select the proper authentication server for the administrator realm.
- Do not configure the administrator account in a way that requires the administrator to select a role to sign in to the target Pulse Secure server. For example, do not map a single user to multiple roles, including the Push Configuration administrator role, and then fail to merge those roles. We recommend creating an account exclusively for Push Configuration administrators to guarantee that the administrator does not need to choose a role during the sign-in process and to clearly distinguish the actions of Push Configuration administrators in your log files. Use the **Administrators > Admin Realms > [Administrator Realm] > Role Mapping** settings to set the appropriate role-mapping rules.

To push Pulse Client configurations from one Pulse Secure server to other Pulse Secure servers of the same type:

1. If you have not already done so, define the targets by selecting **Maintenance > Push Config > Targets**.
2. From the admin console, select **Maintenance > Push Config > Push Configuration**.
3. In the "What to push" box, select **Selected configuration** to display the configuration categories.
4. Scroll down the list and expand the item labeled "Pulse Secure".
5. Select the **Select All Configurations** check box to push all Pulse Client configurations on this Pulse Secure server. Or choose none, all, or selected items from the following categories:
   - **Pulse Secure Connections**: Connection sets and connections.
   - **Pulse Secure Components**: Component sets.
   - **Pulse Secure Versions**: Pulse Client packages that were uploaded to the Pulse Secure server.
6. Add the targets to the **Selected Targets** box.
7. Click **Push Configuration**.

Enabling or Disabling Automatic Upgrades of Pulse Client

After you deploy Pulse Client software to endpoints, software updates occur automatically. If you upgrade the Pulse Client configuration on your Pulse Connect Secure server, updated software components are pushed to a client the next time it connects.

Note: If you configure Pulse Client to make 802.1X based connections, a reboot might be required on Windows endpoints when Pulse Client is upgraded.

Note: A bound endpoint receives connection set options and connections from its binding server, but it can have its Pulse Client software upgraded from any Pulse Secure server that has the automatic upgrade option enabled. During a Pulse Client software upgrade the client loses connectivity temporarily.

Pulse Client software upgrades are enabled by default. To change the behavior of Pulse Client upgrades:

1. From the admin console, select **Maintenance > System > Options**.
2. Set or clear the **Enable automatic upgrade of Pulse Secure Clients** check box.
3. Click **Save Changes**.

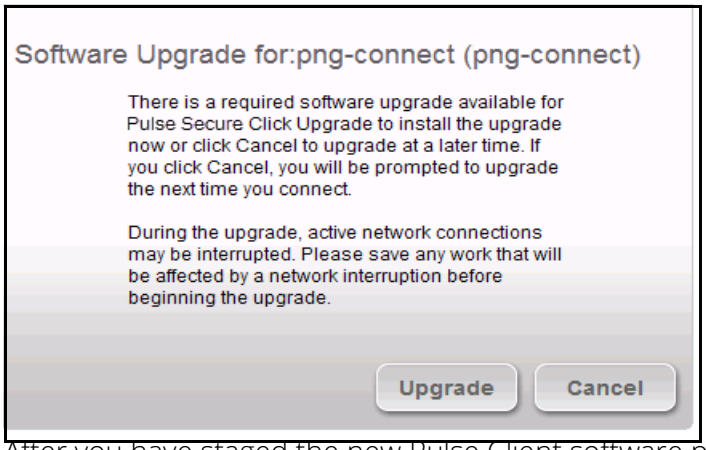
Upgrading Pulse Client

The software image for each supported Pulse Secure server includes a Pulse Client software package. When a newer version of Pulse Client is available, you can upload the new software to the Pulse Secure server. You can have more than one version of Pulse Client on a Pulse Secure server but only one Pulse Client package can be active. If you activate a new version of Pulse Client, and if the Pulse Secure server's automatic upgrade option is enabled, connected Pulse Clients display an upgrade prompt to the user. The user can choose to install the upgrade or cancel the operation. If a user cancels, the upgrade prompt appears each time the client connects to the server. During a Pulse Client software upgrade the client machine loses connectivity temporarily.

Note: The automatic update feature is supported on Pulse Connect Secure and Pulse Policy Secure servers only. SRX gateways do not support automatic Pulse Client software updates.

Note: If you configure Pulse Client to make 802.1X based connections, a reboot might be required on Windows endpoints when Pulse Client is upgraded.

Figure 57 Pulse Client Upgrade Message



After you have staged the new Pulse Client software package in a location accessible to the Pulse Secure server, use the following procedure to upload the software to the Pulse Secure server:

1. In the device administrator console, select **Users > Pulse Secure > Components**.
2. In the section labeled “Manage Pulse Secure Client Versions”, click **Browse**, and then select the software package.
3. Click **Upload**.

Only one Pulse Client package can be active at a time. After you upload a new package, you need to enable it.

To enable a Pulse Client package as the default:

1. In the admin console, select **Users > Pulse Secure > Components**.
2. In the section labeled "Manage Pulse Secure Client Versions", select the radio button next to a version, and then click **Activate**.

Pulse Collaboration Suite Overview

Pulse Collaboration Suite (formerly Secure Meeting) allows users to schedule and attend secure online meetings. In meetings, users can share their desktops and applications with one another over a secure connection. Meeting attendees can collaborate by enabling remote-control of their desktops and through text chatting. Users can schedule meetings through the Pulse Connect Secure user Web portal or, if they have the Microsoft Outlook Plug-in installed, through Microsoft Outlook.

In addition to regular meetings, Pulse Collaboration Suite supports Instant Meetings and Support Meetings. Instant meetings allow you to create meetings with static URLs for that particular type of meeting (for example, weekly status meetings). You do not need to schedule these types of meetings. The conductor starts the meeting and the invitees enter the URL to attend the meeting.

You can enable Pulse Collaboration Suite integration as part of a Pulse Client connection and push the connection to Pulse Clients through an installer package or a configuration update. The Connect Secure or Policy Secure (L3) connection type includes a check box that enables Pulse Collaboration integration on the connection. When the check box is selected, Pulse Clients that have installed that connection display new menu items that enable users to access Pulse Collaboration Suite functions. A connection that is enabled for meetings can serve as a normal SSL VPN connection or it can be dedicated to meetings only. When a Pulse Client user clicks the tray icon menu item for meetings, Pulse Client launches a browser window and connects to the server's user Web portal.

Task Summary: Configuring Pulse Collaboration Suite on Pulse Connect Secure

The following summarizes how to enable a Pulse Connect Secure server as a meeting server for Pulse Collaboration Suite meetings.

To configure Pulse Collaboration Suite:

1. In the Pulse Connect Secure admin console, click **System > Network > Overview** and specify a network identity for the server. Pulse Collaboration Suite uses this hostname when constructing meeting URLs for e-mail notifications.
2. Configure role-level settings:
   - To enable Pulse Collaboration Suite at the role level, click **Users > User Roles > Role Name > General**.
   - To configure role-level meeting restrictions, click **Users > User Roles > Role Name > Meetings > Options**.
3. Configure the authentication settings:
   - To specify the authentication servers meeting creators can access and search click **Users > User Roles > [Role Name] > Meetings > Auth Servers**.
   - To allow meeting creators to invite users from an LDAP server, click **Authentication > Auth. Servers > Select LDAP Server> Meetings**.
4. Configure meeting sign-in policies:
   - To customize the user Web portal pages that meeting attendees see when they sign into a meeting, click **Authentication > Signing In > Sign-in Pages**.
   - To define the URL that meeting participants use to join a meeting, click **Authentication > Signing In > Sign-in Policies > [Meeting Policy]** You also use this page to associate a meeting page with the URL.
   - To associate your meeting sign-in policy with a user sign-in policy, click **Authentication > Signing In > Sign-in Policies > [User Policy]**. The Pulse Connect Secure server applies the specified meeting URL to any meeting created by a user who signs into the associated user URL.
5. To configure system-level meeting settings, include session time-outs, SMTP server information, time zone settings, and color-depth settings, click **System > Configuration > Pulse Collaboration Suite** page of the admin console.
6. To enable client-side logging, click **System > Log/Monitoring > Client Logs > Settings**.

7. To view the logs that users push to the Pulse Connect Secure server, click **System > Log/Monitoring > Uploaded Logs**.

Configuring Pulse Client Connections to Support Meetings

When you configure a Pulse Client Connection to support Pulse Collaboration Suite meetings, Pulse Client users on Windows endpoints can access meeting functions from the Pulse Secure tray icon. When the user clicks Start Meeting in the tray icon menu, Pulse Client launches a browser window that provides access to the meeting functions. The browser shows the Meetings page of the server's user Web portal, which a user can also access by using a browser to login to the Pulse Secure Access server.

The tray icon for Pulse Collaboration Suite access is available when a Pulse Client connection is enabled as a meeting server connection. Pulse Client users cannot enable the meeting function for a connection. This task must be performed by the Pulse Connect Secure administrator on a connection defined on the server, and then installed on endpoints through normal methods of distributing and updating Pulse Client software.

The following steps summarize how to create a Pulse Client connection that enables Pulse Collaboration Suite functions.

1. In a Pulse Client connection set, create a new Pulse Client connection or edit an existing connection set.

   Pulse Collaboration Suite is available with SSL VPN connections (connection type Connect Secure or Policy Secure (L3)) only.

2. Select the check box labeled **Enable Pulse Collaboration integration on this connection**.

3. Distribute the connection to endpoints through normal methods of distributing and updating Pulse Client software.

Scheduling Meetings Through the Pulse Connect Secure User Web Portal

If you enable meeting creation abilities at the role level, users can create meetings through the Meetings page of the Pulse Connect Secure user Web portal. The user scheduling the meeting must specify all of the standard meeting details such as the meeting name, description, start time, start date, recurrence pattern, duration, password, and a list of invitees. Additionally, the user must categorize all invitees into one of two categories:

- **Pulse Connect Secure invitees**: A user who signs into the same Secure Access server or cluster as the meeting creator, also called an in-network invitee. When inviting an in-network user to a meeting, the meeting creator must specify the user's username and authentication server.
- **Non-Pulse Connect Secure invitees**: A user who signs into a different Secure Access server or cluster as the meeting creator, also called an our-of-network invitee. When inviting an out-of-network user to a meeting, the meeting creator must specify the user's email address.

Note: If an in-network invitee uses the meeting URL instead of the Meetings page in the Pulse Connect Secure user Web portal to join a meeting, Pulse Collaboration Suite classifies the user as an out-of-network invitee.

Scheduling Meetings Through Microsoft Outlook

If you enable meeting creation abilities at the role level, Pulse Connect Secure users can create meetings through the Microsoft Outlook calendar using the Pulse Collaboration Suite Outlook plug-in.

When installing the Pulse Collaboration Suite plug-in on Microsoft Outlook 2000, the following message appears, "The form you are installing may contain macros." Since the Pulse Collaboration Suite form does not contain macros it does not matter whether you click Disable Macros or Enable Macros.

Note: You must use the same Outlook profile to remove the Pulse Collaboration Suite plug-in for Outlook as the one used to install the plug-in. Switching profiles between the installation and removal of the Plug-In is not supported.

To use this plug-in, the user must:

1. Install the plug-in from the Meetings page in the Pulse Connect Secure user Web portal.
2. Open the Pulse Collaboration Suite scheduling form in Outlook by choosing **New > Pulse Collaboration Suite**.
3. Use the Pulse Collaboration Suite tab to enter details about the Pulse Secure Access server on which the meeting should be scheduled as well as the user's sign-in credentials, realm, and a meeting password.

Note: Due to limitations with Microsoft Outlook, not all meeting details cross-populate between Microsoft Outlook and Pulse Connect Secure. For a complete list of restrictions, see the Pulse Collaboration Suite for Outlook information available from the user help system available on the Pulse Connect Secure user Web portal as well as the Pulse Collaboration Suite for Outlook plug-in installer.

4. Use the Scheduling and Appointment tabs to schedule the meeting and add invitees using standard Outlook functionality. Note that Pulse Collaboration Suite supports creating standard or recurring meetings through Outlook.

Note: The Appointment tab has a check box labeled This is an online meeting using. This check box is not related to the Meeting Server or the Pulse Collaboration Suite Outlook Plug-in and cannot be used by a third-party plug-in.

5. Save the calendar entry to send the information to the Pulse Collaboration Suite server. Note that when saving a meeting, the user might see a certificate warning because the plug-in is communicating with a secure server.
6. Outlook sends invitation e-mails to the invitees using the text and meeting URL link constructed by the Pulse Collaboration Suite Outlook plug-in. Outlook also adds the meeting to the Outlook calendars of meeting invitees. This calendar item includes all of the standard information recorded by Outlook as well as an additional Pulse Collaboration Suite tab containing the information specified by the meeting creator in the Pulse Collaboration Suite tab. Note that the Pulse Secure Access server does not send an additional e-mail using the SMTP server.
7. To delete a meeting, click **Delete Meeting from Server** on the Pulse Collaboration Suite tab. Clicking Delete from the Outlook form does not delete the meeting.