



Pulse Secure Desktop Client: Always-on VPN and VPN Only Access

Deployment Guide

Published

February 2021

Document Version

6.0

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

www.pulsesecure.net

© 2021 by Pulse Secure, LLC. All rights reserved.

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Pulse Secure Desktop Client: Always-on VPN and VPN Only Access

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at <http://www.pulsesecure.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Revision History

The following table lists the revision history for this document.

Document Version	Date	Description
6.0	February 2021	Updated Lock-down exception enhancements.
5.0	September 2020	Added "System Extensions Support".
4.0	October 2019	Updated "Prerequisites" and "Related Features" section.
3.0	July 2019	Added "Updating Pulse Secure Client with New Connection Set" section.
2.0	May 2019	Initial Publication - 9.0Rx
1.0	December 2017	Initial Publication

Contents

REVISION HISTORY	3
PURPOSE OF THIS GUIDE	1
PREREQUISITES.....	1
OVERVIEW	2
ALWAYS-ON VPN	2
VPN ONLY ACCESS	2
RELATED FEATURES.....	2
CONFIGURATION	4
ENABLING ALWAYS-ON VPN	4
ENABLING VPN ONLY ACCESS	6
ALWAYS-ON VPN AND VPN ONLY ACCESS OPTIONS SETTINGS.....	8
CONFIGURING LOCK-DOWN MODE	10
CONFIGURING LOCK-DOWN EXCEPTION RULES.....	10
CONFIGURING LOCK-DOWN EXCEPTION TYPES.....	12
CONFIGURING LOCATION AWARENESS RULES	15
SYSTEM EXTENSIONS SUPPORT	16
ACTIVATING PULSE SECURE SYSTEM EXTENSIONS	17
SYSTEM EXTENSIONS DURING PULSE CLIENT UNINSTALLATION	19
UPDATING PULSE SECURE CLIENT WITH NEW CONNECTION SET	20

Purpose of This Guide

This guide describes how to configure Always-on VPN and VPN Only Access features on the Pulse Desktop Client using the Pulse Connect Secure administrator console.

Prerequisites

This guide assumes you are familiar with the use of the following products or documents and their related terminology.

- Windows Operating System
- macOS Operating System
- Pulse Desktop client
- Pulse Secure Desktop Client Administration Guide

Overview

Always-on VPN

Always-on VPN feature allows the Pulse Desktop Client to establish a VPN connection that is always active, and all traffic passes through the VPN tunnel. If the VPN tunnel is disconnected, for any reason, the machine has limited connectivity required to re-establish the VPN tunnel. The feature restricts the users to manually connect/disconnect a tunnel or disable/uninstall the Pulse Secure service.

The administrator controls and manages all the user activities.

VPN Only Access

VPN Only Access feature is an enhancement to the Always-on VPN feature.

This feature allows the users to connect/disconnect a connection and add/delete a connection.

Note: Delete option is applicable only to the manually added connections.

Related Features

Always-on VPN and VPN Only Access features work well along with the following additional features:

- **Lock-down mode:** Lock-down mode is applicable to connections where Always-on VPN or VPN Only Access features are enabled. Lock-down mode prohibits network communication outside the VPN tunnel when a VPN tunnel is in the process of being created.
Note: “Lock-down” mode is a new aspect of Always-on functionality that was added to 5.2r5 Pulse Desktop Client for Windows and to 9.0R1 Pulse Desktop Client for macOS.
- **Location Awareness Rules:** The location awareness rules enable an endpoint to connect conditionally. If the location awareness rules are not defined, Pulse Desktop Client attempts to connect to each connection that is defined as an automatic connection until it connects successfully.

For example, you can define rules to enable Pulse Desktop client to automatically establish a secure tunnel to the corporate network through Pulse Connect Secure when the user is at home, and to establish a Pulse Policy Secure connection when the user is in the office and connected to the corporate network over the LAN. Pulse does not re-establish a VPN tunnel when the endpoint re-enters the trusted/corporate network. Location awareness rules are based on the client's IP address and network interface information.

Lock-down mode is intended to use along with Location Awareness rules to ensure that the user is connected over VPN when the end machine is not plugged in with the corporate network.

- **Lock-down Exception Rules:** Lock-down exception rules allow the administrator to configure the rules for which traffic needs to be exempted when Lock-down mode is applied at the user end. Until 9.1R11, the exemption rules were pre-defined and was not allowed to configure. From 9.1R11 onwards, the PCS populates the list of 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.

For example, when a Lock-down exception rule is defined for NetLogon, the user can login to the domain even when Lock-down mode is enabled, and the user is not connected to VPN.

Note: “Lock-down Exception Rules” was added to 5.1R3 Pulse Desktop Client for Windows and to 9.0R2 Pulse Desktop Client for macOS.

- **Captive Portal Detection and Enable Embedded Browser:** Captive Portal Detection feature helps to detect if connectivity is hampered by a captive portal. The Pulse Desktop Client then automatically displays an embedded browser so that the end user can traverse the captive portal to obtain the network connectivity required to establish a VPN connection.

When the Always-on VPN or the VPN Only Access feature is enabled, the Enable captive portal detection and Enable embedded browser for captive portal are automatically checked and cannot be edited.

- **Machine Authentication:** Machine authentication uses machine credentials (machine name and password or machine certificate) to authenticate the endpoint. On Windows endpoints, a Pulse client connection accesses client certificates to provide machine authentication. The certificates are available in the Local Computer personal certificate store, or in a user’s personal certificate store, or on a smart card.

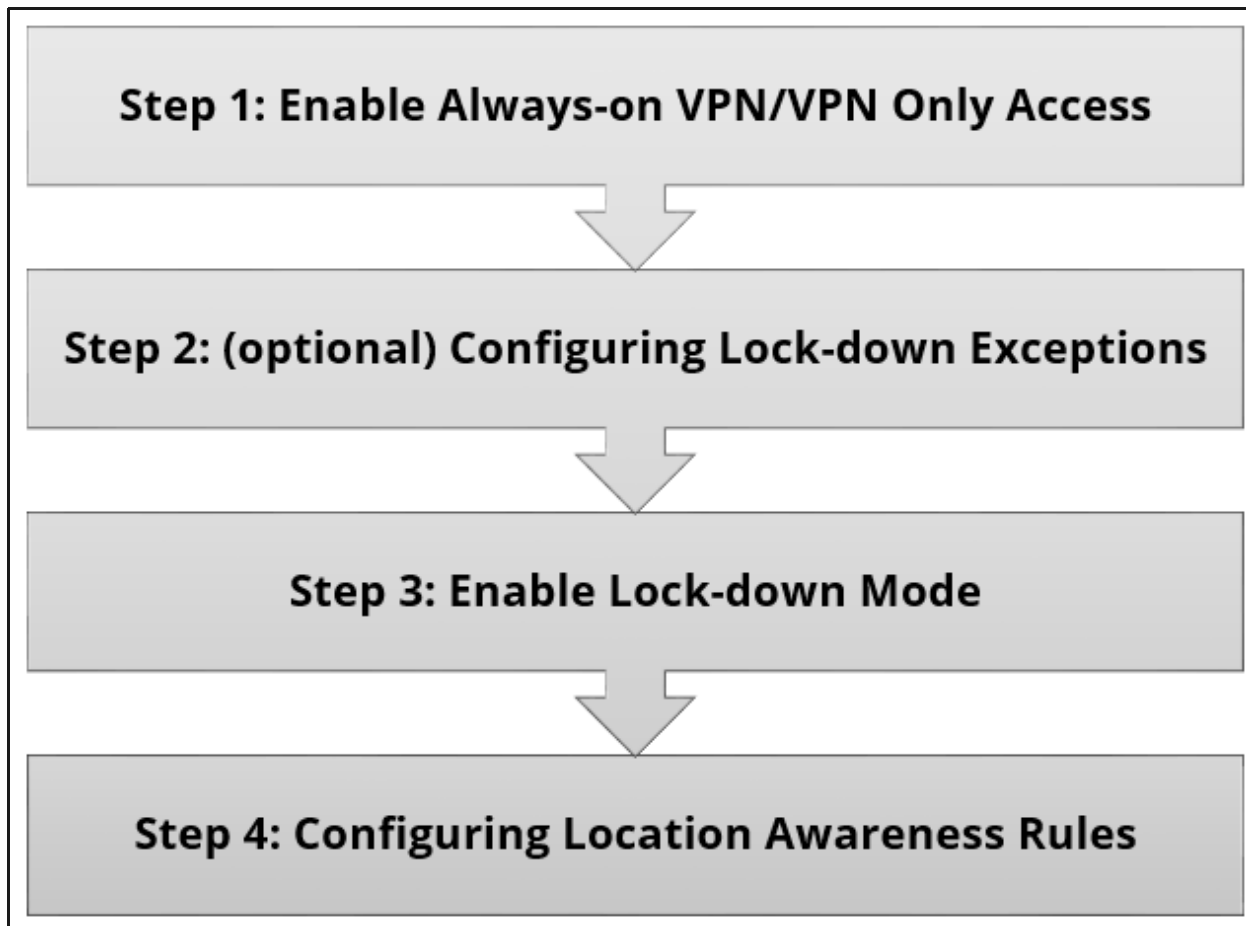
Pulse supports the following machine authentication types:

- **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 re-established.

For more detailed information on the related features, refer to [Pulse Secure Desktop Client Administration Guide](#).

Configuration

A high-level overview of the configuration steps to set up Always-on VPN or VPN Only Access feature is shown below. Click each step to directly jump to the related instructions.



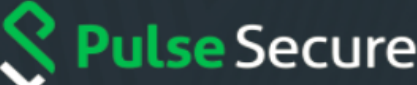
Enabling Always-on VPN

By default, the Always-on VPN option is disabled. There are many possible configuration options within the Always-on feature.

To configure the Connection Set, use the following steps:

1. Log in to Pulse Connect Secure administrator console.
2. Select **Users > Pulse Secure Client > Connections**.
3. Click **New** to display the **New Connection set** configuration page.

Figure 1 New Connection Set Configuration for Always-on VPN



Pulse Secure System Authentication Administrators **Users** Maintenance Wizards

Pulse Secure Client > Connections > New Connection Set

New Connection Set

Name:

Description:

Owner: qa.psecure.net
 Last Modified: 2017-12-06 09:28:49 UTC
 Server ID: 0312MKLQ502W50IQS

▼ Options

Name	Value
Always-on Pulse Client Prevents end users from circumventing Pulse connections. This option will disable all configuration settings that allow the end user to disable or remove Pulse connections, services or software.	<input checked="" type="checkbox"/>
VPN only access When Pulse client connects to a PCS having lock down mode enabled, it will enter lock-down mode and won't let any traffic flow through unless a Locked-down VPN connection is in connected state. User is allowed to connect or disconnect any connection. User is allowed to add any new connection/server URI. User is allowed to delete a connection if the connection is not locked down.	<input checked="" type="checkbox"/>
Allow saving logon information Enables the Save settings checkbox in the certificate trust and password prompts.	<input checked="" type="checkbox"/>
Allow user connections Allows user to create connections via the Pulse UI.	<input type="checkbox"/>
Display Splash Screen Controls whether the splash screen is displayed when Pulse starts.	<input checked="" type="checkbox"/>
Dynamic certificate trust Controls whether users may accept to trust unknown certificates.	<input checked="" type="checkbox"/>
Dynamic connections Allows connections to be deployed automatically from devices.	<input checked="" type="checkbox"/>
EAP Fragment Size Maximum number of bytes in an EAPoL message from the client for 802.1x connections. Range: 450 - 3000 bytes	<input type="text" value="1400"/>
Enable captive portal detection Pulse will attempt to detect the presence of a captive portal hotspot. Only applies to Connect Secure and Policy Secure (L3) connections.	<input checked="" type="checkbox"/>
Enable embedded browser for captive portal Pulse will use an embedded web browser for captive portal pages. Only applies when captive portal detection is enabled.	<input checked="" type="checkbox"/>
FIPS mode enabled Deploy client with Federal Information Processing Standard enabled.	<input type="checkbox"/>
Wireless suppression Disconnect all wireless interfaces when a wired interface gets connected to a network. Applies to all wireless connections (not just those managed by Pulse).	<input type="checkbox"/>
Prevent caching smart card PIN Enabling this will ensure the smart card PIN value is not cached by the client process.	<input type="checkbox"/>

> Connections
 > Lockdown mode exception rules:

4. Select **Always-on Pulse Client** and complete other **Machine Setting** configurations as described in [Table 1](#).
5. Configure the **Connections** and **Lockdown mode exception rules**. For more information see, ["Configuring Lock-down Mode" on page 10](#) and ["Configuring Lock-down Exception Rules" on page 10](#).
6. Click **Save Changes**.

Note: Admin can configure Always-on VPN options using wizards also. For more information, refer to [Configuring Always-on VPN Options using Wizards](#) section in [Pulse Secure Desktop Client Administration Guide](#).

Note: Lock-down mode exceptions rules are not supported for Configuring Always-on VPN options using wizards for only Mac and All.

Enabling VPN Only Access

By default, the VPN only access option is disabled. There are many possible configuration options within the feature.

To configure the Connection Set, use the following steps:

1. Log in to Pulse Connect Secure administrator console.
2. Select **Users > Pulse Secure Client > Connections**.
3. Click **New** to display the **New Connection Set** configuration page.

Figure 2 New Connection Set Configuration for VPN Only Access

Pulse Secure System Authentication Administrators **Users** Maintenance Wizards

Pulse Secure Client > Connections > New Connection Set

New Connection Set

Name:

Description:

Owner:
 Last Modified: 2017-12-07 10:53:34 UTC
 Server ID: 0312MVD4A0EM704VS

▼ Options

Name	Value
Always-on Pulse Client Prevents end users from circumventing Pulse connections. This option will disable all configuration settings that allow the end user to disable or remove Pulse connections, services or software.	<input type="checkbox"/>
VPN only access When Pulse client connects to a PCS having lock down mode enabled, it will enter lock-down mode and won't let any traffic flow through unless a Locked-down VPN connection is in connected state. User is allowed to connect or disconnect any connection. User is allowed to add any new connection/server URI. User is allowed to delete a connection if the connection is not locked down.	<input checked="" type="checkbox"/>
Allow saving logon information Enables the Save settings checkbox in the certificate trust and password prompts.	<input checked="" type="checkbox"/>
Allow user connections Allows user to create connections via the Pulse UI.	<input checked="" type="checkbox"/>
Display Splash Screen Controls whether the splash screen is displayed when Pulse starts.	<input checked="" type="checkbox"/>
Dynamic certificate trust Controls whether users may accept to trust unknown certificates.	<input checked="" type="checkbox"/>
Dynamic connections Allows connections to be deployed automatically from devices.	<input checked="" type="checkbox"/>
EAP Fragment Size Maximum number of bytes in an EAPoL message from the client for 802.1x connections. Range: 450 - 3000 bytes	<input type="text" value="1400"/>
Enable captive portal detection Pulse will attempt to detect the presence of a captive portal hotspot. Only applies to Connect Secure and Policy Secure (L3) connections.	<input checked="" type="checkbox"/>
Enable embedded browser for captive portal Pulse will use an embedded web browser for captive portal pages. Only applies when captive portal detection is enabled.	<input checked="" type="checkbox"/>
FIPS mode enabled Deploy client with Federal Information Processing Standard enabled.	<input type="checkbox"/>
Wireless suppression Disconnect all wireless interfaces when a wired interface gets connected to a network. Applies to all wireless connections (not just those managed by Pulse).	<input type="checkbox"/>
Prevent caching smart card PIN Enabling this will ensure the smart card PIN value is not cached by the client process.	<input type="checkbox"/>

► Connections

► Lockdown mode exception rules:

Save Changes **Cancel**

4. Select **VPN only access** and complete other **Machine Setting configurations** as described in [Table 1](#).
5. Configure the **Connections** and **Lockdown mode exception rules**. For more information see, [“Configuring Lock-down Mode” on page 10](#) and [“Configuring Lock-down Exception Rules” on page 10](#).
6. Click **Save Changes**.

Always-on VPN and VPN Only Access Options Settings

The Pulse Connect Secure (PCS) administrator console provides a simplified way to configure the possible Always-on VPN and VPN Only Access options. Enabling some options restricts or automatically modifies several other options in the Machine Settings.

Table 1 Machine Settings Configuration

Settings	Description	When Always-on VPN is enabled	When VPN Only Access is enabled
Always-on Pulse Client	Prevents end users from circumventing Pulse connections. This option disables all configuration settings that allow the end user to disable or remove Pulse connections, services, or software. Default: Disabled	Enabled; Editable	Disabled; Editable
VPN Only Access	Prevents any traffic flow through unless a Locked-down VPN connection is in connected state. Default: Disabled	Enabled; Not editable	Enabled; Editable
Allow saving logon information	Saves the certificate trust and password information. Default: Enabled	Enabled; Editable	Enabled; Editable
Allow user connection	Allows to add user connections. Default: Disabled	Disabled; Not editable	Disabled; Editable
Display Splash Screen	Displays the splash screen on Pulse connection. Default: Enabled	Enabled; Editable	Enabled; Editable
Dynamic certificate trust	Allows to trust unknown certificates. Default: Enabled	Enabled; Editable	Enabled; Editable
Dynamic connections	Allows devices to automatically deploy connections. Default: Enabled	Enabled; Editable	Enabled; Editable

Settings	Description	When Always-on VPN is enabled	When VPN Only Access is enabled
EAP Fragment Size	Indicates the maximum number of bytes in an EAPoL message from the Pulse Desktop client for 802.1x connections. Range: 450 - 3000 bytes Default: 1400	Enabled; Editable	Enabled; Editable
Enable captive portal detection	Allows the Pulse Desktop client to notify the end user that a VPN connection cannot be established until the requirements of a captive portal are fulfilled. Default: Disabled	Enabled; Not editable	Enabled; Not editable
Enable embedded browser for captive portal	Allows the Pulse Desktop Client to use an embedded web browser for captive portal pages. Default: Enabled and not editable when Enable captive portal detection is enabled.	Enabled; Not editable	Enabled; Not editable
FIPS mode enabled	Deploy Pulse Desktop Client with FIPS enabled. Default: Disabled	Disabled; Editable	Disabled; Editable
Wireless suppression	Disconnects all wireless interfaces when a wired interface gets connected to a network. Default: Disabled	Disabled; Editable	Disabled; Editable
Prevent caching smart card PIN	Ensures the smart card PIN value is not cached by the Pulse Desktop Client process. Default: Disabled	Disabled; Editable	Disabled; Editable

Note: When **Always-on Pulse Client** is enabled, **VPN Only Access** option is automatically enabled in machine settings and cannot be edited.

When **Always-on Pulse Client** is enabled, the **Connection Set** and the **Connections** have the following effects.

- Impeding the end user's ability to disconnect or disable VPN connections
- Ensuring that captive portals can still be traversed even when connectivity is locked-down.
- "Always-on Pulse Client" check box does not prevent end users (with administrator privileges) from stopping endpoint services (the Pulse Secure Service and the Base Filtering Engine (BFE)) which are required to establish the VPN connections.

Configuring Lock-down Mode

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

1. On the **Pulse Connect Secure administrator console**, select **Users > Pulse Secure Client > Connections**.
2. Click a Name and select a connection from the list of **Connections**.
For example, use a **Connect Secure L3 connection** for a Layer 3 connection to Pulse Connect Secure.
3. Select the **Lock down this connection** option to disable network access when VPN is enabled until connected.
4. Under **Connection is established**, select the mode. By default, user is selected.
5. Create Location Awareness rules. See [“Configuring Location Awareness Rules” on page 15](#).
6. Click **Save Changes**.

Figure 3 Lock-down Connection Mode

The screenshot shows the Pulse Secure administrator console interface. The breadcrumb trail is 'Pulse Secure Client > Connections > Default > SA'. The connection name is 'SA' and the description is 'Default server connection'. The type is 'Connect Secure or Policy Secure (L3)'. Under the 'Options' section, there is a table with the following rows:

Name	Value
Allow user to override connection policy <small>Allows user to modify connection state.</small>	<input type="checkbox"/>
Lock down this connection <small>Network access is limited until this connection is established. This option is available only when the Always-on Pulse Client option or VPN only access option on the connection set is checked.</small>	<input checked="" type="checkbox"/>
Support Remote Access (Connect Secure) or LAN Access (Policy Secure) on this connection <small>Unchecked only if the connection is not used for Connect Secure or Policy Secure services (e.g. Server is used for Pulse Collaboration only).</small>	<input checked="" type="checkbox"/>
Enable Pulse Collaboration integration on this connection <small>Applicable for Connect Secure type connections only. Leave this unchecked for Policy Secure type connections.</small>	<input type="checkbox"/>
Connect to URL of this server only <small>Connection is only made to the server which supplied configuration.</small>	<input checked="" type="checkbox"/>
List of Connection URLs <small>List of server URLs to which Pulse should attempt to connect.</small>	<div></div>

Note: Administrator can enable **Allow user to override connection policy** only when VPN Only Access is selected.

Configuring Lock-down Exception Rules

Lock-down exception rules section is enabled by selecting Always-on Pulse Client or VPN Only Access options.

In the New Configuration section, administrator can add Lock-down mode exception rules for Windows and for 9.0R2 release onwards for macOS. Administrator must 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 Lock-down exception rules, use the following steps. This feature is supported from PCS 8.3R3/ PDC 5.3R3 onwards.

1. On the Pulse Connect Secure administrator console, select **Users > Pulse Secure Client > Connections**.
2. Click a **Name** and select **New** under **Lock-down mode exception rules**.

Figure 4 Connection Settings

Lockdown mode exception rules:

When Always-on VPN Feature with Lockdown mode enabled, Admin can add more exceptions to the Core Access Rules using exception rules. Exceptions already configured in client are called core Access Rules. DHCP, DNS, Kerberos, LDAP, SMP and Portmapper are already configured core access rules in client

New... Duplicate... Delete... ↑ ↓

Windows Mac

<input type="checkbox"/>	Name	Program	Protocol	Direction	Action	Local Address	Remote Address	Local Port	Remote Port
<input type="checkbox"/>	LSA-NetLogon-UDP-Out	<%windir%>\System32\lsass.exe	UDP	Outbound	Allow	Any	Any	Any	Any
<input type="checkbox"/>	LSA-NetLogon-TCP-Out	<%windir%>\System32\lsass.exe	TCP	Outbound	Allow	Any	Any	Any	Any
<input type="checkbox"/>	SCCMNotification	<%windir%>\CCM\SCNotification.exe		Outbound	Allow	Any	Any	Any	Any
<input type="checkbox"/>	PrinterSpooler	<%windir%>\System32\spoolsv.exe		Outbound	Allow	Any	Any	Any	Any
<input type="checkbox"/>	DHCP-IPv6-In-Accept	<%windir%>\System32\svchost.exe	UDP	Inbound	Allow	Any	Any	546	547
<input type="checkbox"/>	DHCP-IPv4-In-Accept	<%windir%>\System32\svchost.exe	UDP	Inbound	Allow	Any	Any	68	67
<input type="checkbox"/>	DHCP-IPv6-Out-Connect	<%windir%>\System32\svchost.exe	UDP	Outbound	Allow	Any	Any	546	547

Save Changes Cancel

3. Enter the rule **Name** and **Description**. Select the traffic type.
 - 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).
 - Select Allow or Deny actions to configure the exception rules.

Figure 5 New Lock down exception rule

Pulse Secure Client > Connections > AOVPN_test > New Lock down exception rule

New Lock down exception rule

Windows Mac All

Name:

Description:

Direction: ☐ Inbound ☐ Outbound

Action: ☐ Allow ☐ Deny

▼ Resources

Select exception type:

☐ Program ☐ Port ☐ Custom

Save Changes Cancel

4. Select the exception type from **Resources**. Fill in appropriate details. For more information, see [“Configuring Lock-down Exception Rules” on page 10](#).
5. Click **Save Changes**.

Configuring Lock-down Exception Types

The Lock-down exception rules can be configured in the following ways for both Inbound and Outbound traffic separately.

- **Program-based Resource Access:** Select Program in the New Always-on VPN exception rules page. Enter the absolute path for the program that needs to be exempted and optionally provide SHA-256 checksum.

Figure 6 Windows - Program-based Resource Access

▼ Resources

Select exception type:

☒ Program ☐ Port ☐ Custom

Program path: Example: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

SHA2-256: SHA2-256 hash of program executable

Figure 7 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 8 macOS - Program-based Resource Access

New... Duplicate... Delete...								
<input type="checkbox"/>	Name	Program	Protocol	Direction	Local Address	Remote Address	Local Port	
<input type="checkbox"/>	1. Safari	/Applications/Safari.app/Contents/MacOS/Safari		Outbound	any	any	any	
<input type="checkbox"/>	2. Safari1	/System/Library/PrivateFrameworks/SafariSafeBrowsing.framework/Versions/A/com.apple.Safari.SafeBrowsing.Service		Outbound	any	any	any	
<input type="checkbox"/>	3. Safari2	/System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.Networking.xpc/Contents/MacOS/com.apple.WebKit.Networking		Outbound	any	any	any	

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

ping6 -S (Source IPv6) (destination IPv6)

- **Port-based Resource Access:** Select Port in the New Always-on VPN exception rules page. Select TCP or UDP and enter the respective port number.

Figure 9 Port-based Resource Access

✓ Resources

Select exception type:

☐ Program
 ☒ Port
 ☐ Custom

TCP ☐

 UDP ☐

Local Port : Example: 80,443,5000-5010

- **Custom-based Resource Access:** Select Custom in the New Always-on VPN exception rules page. Configure the rules as applicable.

Figure 10 Custom-based Resource Access

Resources

Select exception type:
☐ Program ☐ Port ☒ Custom

Program path:

SHA2-256: SHA2-256 hash of program executable

Protocol:

Local IPv4/IPv6 Resources: Examples:
 10.10.10.10-10.10.10.100
 10.10.10.10/255.255.255.0
 10.10.10.50
 [2001:db8:a0b:12f0::1]
 [2001:DB8::6:0/112]
 [2001:DB8::7:50]

Remote IPv4/IPv6 Resources: Examples:
 10.10.10.10-10.10.10.100
 10.10.10.100/255.255.255.0
 10.10.10.50
 [2001:db8:a0b:12f0::1]
 [2001:DB8::6:0/112]
 [2001:DB8::7:50]

Local Port : Example:80,443,5000-5010

Remote Port: Example:80,443,5000-5010

Once 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: In custom-based resource access, it is not mandatory to configure all the options. Default value for all configurable fields are "*".

Note: Post Pulse Desktop Client upgrade, user needs to make at least one successful connection to the Pulse Connect Secure, so that the configured Lock-down exception rules can be applied on the client machine.

Configuring Location Awareness Rules

To configure location awareness rules, use the following steps.

1. If not already created, create a connection or open an existing connection.

Location Awareness rules are applicable 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 select the mode, **User**, **Machine**, or **Machine** or **user**.
3. For **User** Mode, manually select **Connect automatically** under options. For **Machine** or **User** or **Machine** modes, **Connect automatically** option is enabled by default.

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

Alternatively, 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 and specify a network interface as **Physical**, **Pulse Secure**, or **Any**.
 - **DNS server**—Specify the DNS server IP address in the IP address box.
 - **Resolve address**—Specify the hostname in the DNS name box and the IP address or addresses in the IP address box.
 - **EndpointAddress**—Specify the IP address or addresses in the IP address box. Also specify a network interface on which the condition must be satisfied.

1. Click **Save Changes**.

2. Enabling Location Awareness Rules

To enable location awareness rules, use the following steps.

1. Specify how to enforce the selected location awareness rules by selecting one of the following options:
 - **All of the above rules**—The connection is attempted only when all selected location awareness rules are satisfied.
 - **Any of the above rules**—The connection is attempted when any of the selected location awareness rules is satisfied.
 - **Custom**—The connection is attempted only when all selected location awareness rules are satisfied according to the Boolean logic you specify in the Custom box. The accepted Boolean operators are AND, OR, NOT, and ().
For example, connect to Pulse Connect Secure where Rule-1 and Rule-2 are defined. To set a custom rule where, Rule-1 is false and Rule-2 is true. The Boolean logic in the custom box would be **NOT Rule-1 AND Rule-2**.
2. Click **Save Changes**.

System Extensions Support

Apple introduced the concept of System Extensions (SysExt) as an alternate to Kernel Extensions (Kext). System Extensions / Network Extensions allow to extend the functionality of macOS without requiring kernel-level access.

This feature is applicable for Pulse Client version 9.1R8.2 and above and version Catalina onwards. This feature is applicable when Traffic enforcement and Lockdown mode are enabled.

When installing Pulse Client version previous to 9.1R8.2 a message displays when installing the PulseSecure.dmg. MacOS cannot recognise the PulseSecure.pkg and displays that the package could be a malicious software.

Pulse Client 9.1.R8.2 and later versions are notarized and Pulse Client installation do not display this warning on MacOS.

Click **Open** to install the package despite the warning.

Figure 11 Malicious Software warning

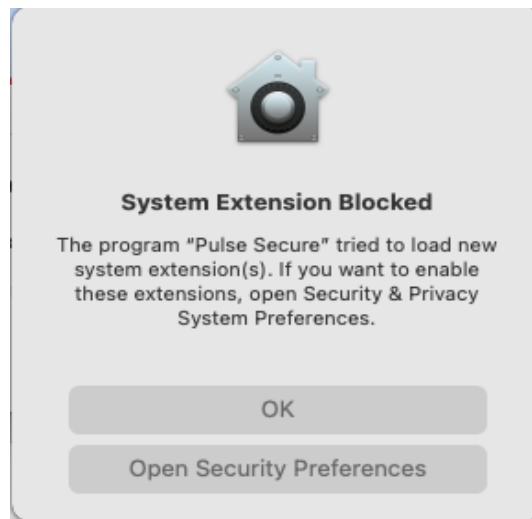


Activating Pulse Secure System Extensions

The following procedure provides steps to activate Pulse Secure System extensions on MacOS when Traffic enforcement and Lockdown mode are enabled. Pulse Client release 9.1R8.2 includes support to System Extension-based firewall required to use network filtering.

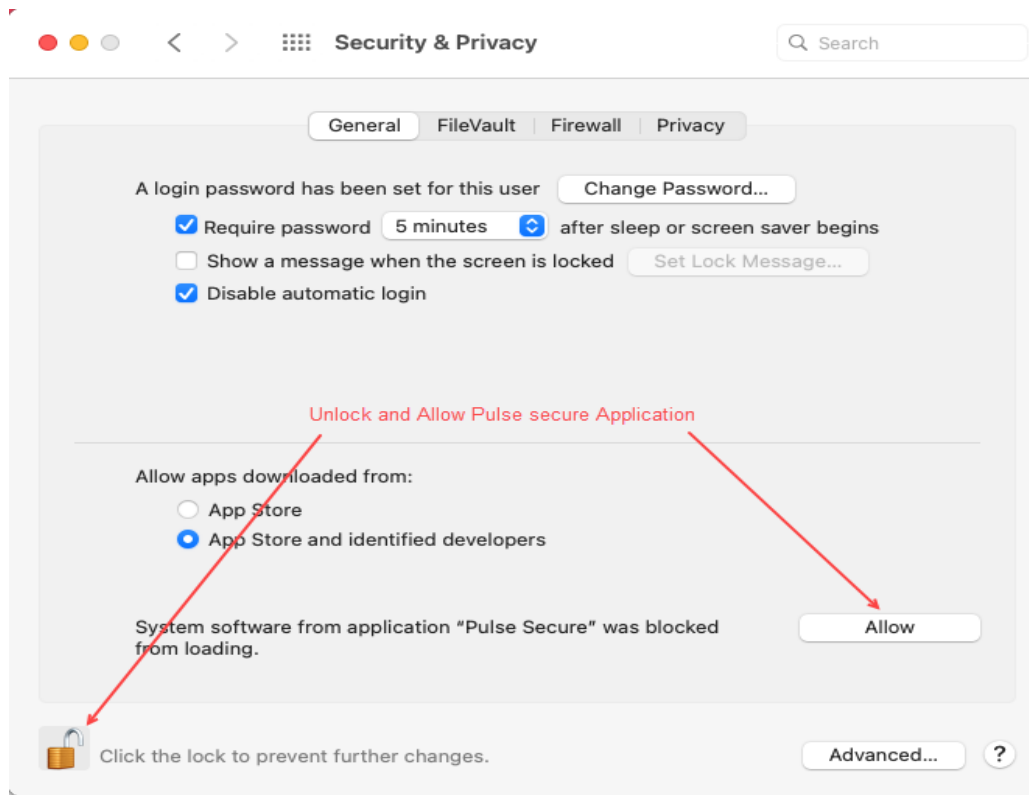
1. When adding new connections, few warnings may appear. On the **System Extension Blocked** message, click **Open security Preferences**.

Figure 12 System Extension Warning



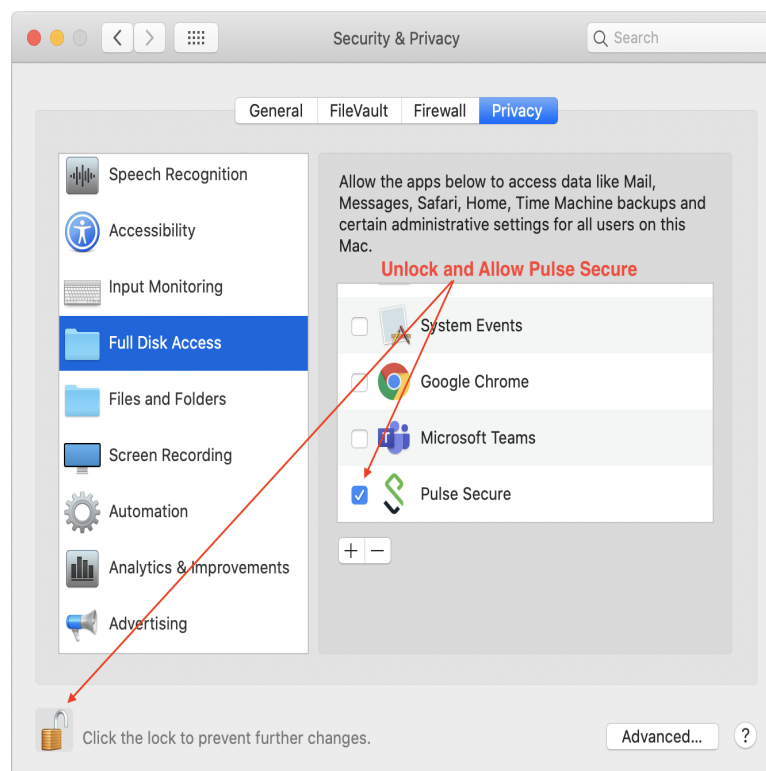
2. Under General tab, unlock permissions to make changes and click **Allow** to unblock the software.

Figure 13 Security and Privacy settings



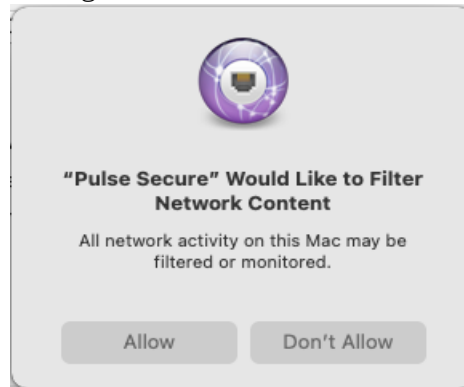
3. Under Privacy tab, unlock permissions to make changes and Select Pulse Secure.

Figure 14 Privacy Settings



4. On setting the system extensions and when Traffic Enforcement and Lock-down mode are enabled, the following message appears when establishing a connection. Click **Allow** to filter Network Content

Figure 15 Filter confirmation during Network Connection



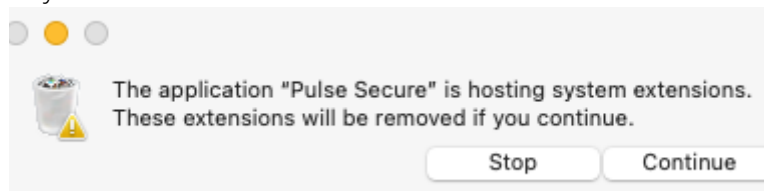
To ensure system extensions are activated and enabled on a terminal, use the following command:

```
systemextensionsctl list | grep pulse
```

System Extensions during Pulse Client Uninstallation

When uninstalling the Pulse Client, the system extensions are also removed. The following confirmation message appears, click **Continue** to remove system extension settings.

Figure 16 Remove System Extension



Updating Pulse Secure Client with New Connection Set

To deploy the above mentioned configuration at end-user machine, please refer to the section “Deploying Pulse Secure Client” of [Pulse Secure Desktop Administrator Guide](#).