Pulse Secure Client
Linux Quick Start Guide
# Revision History

The following table lists the revision history for this document.

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.7</td>
<td>April 2020</td>
<td>No documentation updates for 9.1R5 release.</td>
</tr>
<tr>
<td>1.6</td>
<td>January 2020</td>
<td>No documentation updates for 9.1R4 release.</td>
</tr>
<tr>
<td>1.5</td>
<td>November 2019</td>
<td>Added <a href="#">Reconnecting VPN Connection</a> section.</td>
</tr>
<tr>
<td>1.4</td>
<td>November 2019</td>
<td>Updated <a href="#">Supported Features</a> section.</td>
</tr>
<tr>
<td>1.3</td>
<td>October 2019</td>
<td>Updated links for 9.1R3 Pulse Desktop Client SPG.</td>
</tr>
<tr>
<td>1.2</td>
<td>July 2019</td>
<td>Updated links for 9.1R2 Pulse Desktop Client SPG.</td>
</tr>
<tr>
<td>1.1</td>
<td>July 2019</td>
<td>Updated links for 9.1R1 Pulse Desktop Client SPG.</td>
</tr>
<tr>
<td>1.0</td>
<td>May 2019</td>
<td>No documentation updates for 9.1R1 Release.</td>
</tr>
</tbody>
</table>
Contents

REVISION HISTORY ........................................................................................................................................................................3
REQUESTING TECHNICAL SUPPORT ..............................................................................................................................................6
PART 1 ...........................................................................................................................................................................................7
  OVERVIEW ............................................................................................................................................................8
  SUPPORTED PLATFORMS ...........................................................................................................................................8
  SERVER PLATFORM COMPATIBILITY .............................................................................................................................8
  SUPPORTED FEATURES ........................................................................................................................................8
  LIMITATIONS ...........................................................................................................................................................8
PART 2 ........................................................................................................................................................................................10
CONFIGURING SERVER VPN POLICY ......................................................................................................................................11
INSTALLING PULSE SECURE CLIENT FOR LINUX ................................................................................................................12
USING PULSE LINUX CLIENT UI ...........................................................................................................................................13
  ADDING VPN CONNECTIONS ........................................................................................................................................14
  MODIFYING VPN CONNECTION ..................................................................................................................................15
  DELETING VPN CONNECTION ....................................................................................................................................16
  LAUNCHING VPN CONNECTION ....................................................................................................................................17
  Initiating VPN Connection ........................................................................................................................................17
  TERMINATING VPN CONNECTION ..................................................................................................................................18
  RECONNECTING VPN CONNECTION ..............................................................................................................................19
  DIAGNOSTICS AND STATUS ........................................................................................................................................20
    Uploading the Pulse Secure Client Log Files ..............................................................................................................20
    Advanced Connection Details ......................................................................................................................................23
    About Pulse Linux Client ........................................................................................................................................23
USING PULSE LINUX CLIENT COMMAND LINE ....................................................................................................................25
  INITIATING VPN CONNECTION .......................................................................................................................................25
  LAUNCH THE COMMAND LINE CLIENT .........................................................................................................................25
  TERMINATING VPN CONNECTION .......................................................................................................................................25
  DIAGNOSTICS AND STATUS ........................................................................................................................................25
    Uploading Pulse Secure Client Log Files ......................................................................................................................25
    Checking Pulse Secure Client Status ...........................................................................................................................26
MANAGING CERTIFICATES ON LINUX .......................................................................................................................................27
HOST CHECKING SUPPORT ON LINUX ..................................................................................................................................29
  CONFIGURING PCS HOST CHECKER POLICY FOR PULSE LINUX CLIENT ........................................................................29
DIAGNOSTICS AND STATUS ...................................................................................................................................................31
SAML SUPPORT ........................................................................................................................................................................32
CERTIFICATE AUTHENTICATION SUPPORT ..............................................................................................................................33
  CONFIGURING CLIENT CERTIFICATE IN PULSE CONNECT SECURE ................................................................................33
  CONFIGURING AUTHENTICATION WITH THE CERTIFICATE SERVER ........................................................................34
  CLIENT CERTIFICATE INSTALLATION ..................................................................................................................................36
  CERTIFICATE TYPES SUPPORTED .......................................................................................................................................36
  Public Certificates ..................................................................................................................................................................36
Requesting Technical Support

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

- Product warranties—For product warranty information, visit https://www.pulsesecure.net
- Find product documentation: https://www.pulsesecure.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: https://www.pulsesecure.net/support

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://www.pulsesecure.net/support
- Call Phone: 1-844-751-7629 (Toll Free, US)

For international or direct-dial options in countries without toll-free numbers, see https://www.pulsesecure.net/support
Part 1

- Overview
- Supported Platforms
- Server Platform Compatibility
- Supported Features
- Limitations
Overview

Pulse Secure client for Linux provides secure connectivity between a device running Linux and Pulse Connect Secure. Pulse Secure client for Linux is available from the PCS Admin Installers Page. After installing the Pulse Secure client VPN package on a Linux device, the user can configure a connection and establish Layer 3 VPN communications.

Configuration on the Pulse Connect Secure gateway to support Pulse Secure clients for Linux is the same as that of Pulse for Windows and macOS. Use the sign-in policies, authentication realms, roles and VPN tunnel policies to define authentication and access permissions. A typical Pulse server configuration for Linux access is to create a realm, a role and a remediation role that are designed for Linux users.

Supported Platforms

This topic provides the browser platforms that were tested with the current release of the Pulse Secure Desktop Clients for Linux.

For more information, refer to section Platform and Browser Compatibility of Pulse Secure Desktop Client Supported Platforms Guide.

Server Platform Compatibility

This topic provides the server platforms that were tested with the current release of the Pulse Secure Desktop Clients for Linux.

For more information, refer to section Server Platform Compatibility of Pulse Secure Desktop Client Supported Platforms Guide.

Note: 8.0Rx and 7.4RX with Host Checker is not supported.

Supported Features

The following features are supported by the Pulse Secure Client for Linux:

- Pulse Linux Client Usability Improvements
  - The Pulse Linux client will now remain connected if the UI is closed. When the UI is re-launched, updated statistics are presented.
- SAML support for Linux
- Java Free Pulse Linux Client Support
- 64-bit Operating Systems Support
- Multi-Factor Authentication (MFA) Support
- Host Checker
- Session Timeout Warning Feature
- Command Line Support
- RPM/DEB Package Manager Support
- Pre- and post-authentication sign-in notification messages
- Client Certificate Authentication Support.
- VPN tunneling connections for IPv4 resource access

Limitations

The following are the limitations to the Pulse Secure Client for Linux.
• Refer to KB40238 for Pulse Secure Linux on CentOS clients cannot connect using TLS 1.2
FIPS or NDcPP mode is not supported on Pulse Linux Clients

⚠️ Note: The certificate authentication through UI will be supported only on the machines using libsoup 2.48 and above. Centos 6.4 and Ubuntu 14.04 doesn't meet the above requirements.
Part 2

- Configuring Server VPN Policy
- Installing Pulse Secure Client for Linux
- Using Pulse Linux Client UI
- Using Pulse Linux Client Command Line
- Managing Certificates on Linux
- Host Checking Support on Linux
- SAML Support
- Certificate Authentication Support
Configuring Server VPN Policy

The Pulse Secure client enables you to secure your company resources using authentication realms, user roles and resource policies. For complete information on the Pulse Connect Secure gateway, see the Pulse Connect Secure documentation.

The Pulse Connect Secure gateway checks the authentication policy defined for the authentication realm. The user must meet the security requirements that are defined for a realm's authentication policy. At the realm level, you can specify security requirements based on various elements, such as the user's source IP address or the possession of a client-side certificate. If the user meets the requirements specified by the realm's authentication policy, the gateway forwards the user's credentials to the appropriate authentication server. If this server successfully authenticates the user, then the gateway evaluates the role-mapping rules defined for the realm to determine which roles to assign to the user.

The following is a generalized example of configuring a Pulse Connect Secure gateway for the Pulse Client for Linux.

1. Click **Users > User Roles** and then either select an existing role (preferred) or create a new role.
2. If creating a new role, specify a name and optional description for the role, for example: Linux Users Role, Linux Users VPN Role.
3. Enable **VPN Tunneling** and **Save Changes**.
4. Click **Users > User Realms** to create new realm or select an existing realm.
5. Configure and save your options on the General and Authentication Policy tabs.
6. To Sign In, enable primary/secondary authentication by selecting Servers from Authentication Server list.
7. On the Role Mapping tab, click New Rule to create a new role-mapping rule.
8. One option for a role-mapping rule is to create a custom expression that uses the user agent string to identify a Linux device. The Pulse Secure client for Linux user agent string has a form like this: 
   ```
   DSClient; PulseLinux
   ```
   You can use all or part of the string in a custom expression that uses the userAgent variable. For example:
   ```
   userAgent = '*PulseLinux*' 
   ```
   9. Select the role that you created earlier for the Linux users, add it to the Selected Roles list.
   10. Click **Save Changes**.

User sign-in policies determine the realm(s) that users can access.

1. To create a new sign-in policy, click New URL. Or, to edit an existing policy, click a URL in the User URLs column.
2. Modify an existing sign-in page or create a new one using options in the **Authentication > Signing In > Sign-in Pages** page of the admin console.
3. Specify a sign-in policy that associates a realm, sign-in URL, and sign-in page using settings in the **Authentication > Signing In > Sign-in Policies** page of the admin console. To create or configure user sign-in policies, Click **New URL** in **Authentication > Signing In > Sign-in Policies**.
4. Under Authentication realm, specify which realm(s) map to the policy, and how users and administrators should pick from amongst realms.
5. Click **Save Changes**.
Installing Pulse Secure Client for Linux

The Pulse Secure client for Linux currently is designed only for CLI-based installation.

The Installation Command:
- Debian – based installation
  ```bash
dpkg -i <package name>
  ```
- RPM – based installation
  ```bash
rpm -ivh <package name>
  ```

The Upgrade Command:
- Debian – based installation
  ```bash
dpkg -i <package name>
  ```
- RPM – based installation
  ```bash
rpm -Uvh <package name>
  ```

The Uninstallation Command:
- Debian – based installation
  ```bash
dpkg -r <package name>
  ```
- RPM – based installation
  ```bash
rpm -e <package name>
  ```

The Dependencies Installation Command:
- 64 bit machines
  ```bash
/usr/local/pulse/PulseClient_x86_64.sh install_dependency_packages
  ```
- 32 bit machines:
  ```bash
/usr/local/pulse/PulseClient.sh install_dependency_packages
  ```

**Note:** On Ubuntu distributions, installing through Ubuntu Software Center is supported.
Using Pulse Linux Client UI

To launch UI from the Desktop

Pulse Linux Client UI can be launched by searching for Pulse Secure Icon under Applications List.

Figure 1 Pulse Secure Client for Linux Application

To launch UI from the Terminal

1. Append /usr/local/pulse to LD_LIBRARY_PATH
   ```
   export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/local/pulse
   ```
2. Launch the UI by executing the below command
   ```
   /usr/local/pulse/pulseUi
   ```
Adding VPN Connections

To create a Pulse Secure VPN connection on a Linux device:

1. Click on the Add (+) option on the top-right-hand corner of the main Pulse Secure Linux client screen.
2. In the Name field, specify the name for the Pulse Connect Secure gateway.
3. In the URL field, specify the URL for the Pulse Connect Secure gateway.

   You can identify the server using the server IP address, the hostname, or a URL that optionally specifies the port the connection uses and the specific sign-in page. To specify an URL, use the following format:

   https://hostname[:port][/][sign-in page]

   The brackets indicate options. If you specify a specific sign-in page, make sure that the name you specify matches what is defined on the Pulse Connect Secure gateway. (Authentication > Signing in > Sign-in pages.)

4. New VPN connection appears in the VPN list after user click the save button on the above screen.

   The user can tap connect to initiate a VPN connection. The VPN connection state is indicated in the VPN dropdown menu on the VPN list.
Modifying VPN Connection

To modify a Pulse Secure VPN connection on a Linux device:

**Figure 3 Modifying VPN Connection**

- Select the VPN connection and click on the edit (J) option on the top-right-hand corner of the main Pulse Secure Linux client screen.
  1. In the Name field, specify the name for the Pulse Connect Secure gateway.
  2. In the URL field, specify the URL for the Pulse Connect Secure gateway.

    You can identify the server using the server IP address, the hostname, or a URL that optionally specifies the port the connection uses and the specific sign-in page. To specify an URL, use the following format:
    
    `https://hostname[:port][/][sign-in page]
    
    The brackets indicate options. If you specify a specific sign-in page, make sure that the name you specify matches what is defined on the Pulse Connect Secure gateway. (Authentication > Signing in > Sign-in pages.)

- Modified VPN connection appears in the VPN list after user click the save button on the above screen

  The user can tap connect to initiate a VPN connection. The VPN connection state is indicated in the VPN dropdown menu on the VPN list.
Deleting VPN Connection

To delete a Pulse Secure VPN connection on a Linux device:

**Figure 4 Deleting VPN Connection**

1. Select the VPN connection and click on the delete (-) option on the top-right-hand corner of the main Pulse Secure Linux client screen.
2. VPN connection is removed from the VPN list after user click the **OK** button on the above screen.
Launching VPN Connection

Initiating VPN Connection

To initiate a Pulse Secure VPN connection on a Linux device:

Figure 5 Initiating VPN Connection

1. Select the VPN connection and click on the **Connect** button of the VPN connection entry in the Main Pulse Secure Linux client screen.

2. New window opens to continue authentication process based on the authentication method configured for the realm.
Terminating VPN Connection

To terminate a Pulse Secure VPN connection on a Linux device:

**Figure 6 Terminating VPN Connection**

Select the VPN connection and click on the **Disconnect** button of the VPN connection entry in the Main Pulse Secure Linux client screen.
Reconnecting VPN Connection

To reconnect a Pulse Secure VPN connection on a Linux device:

Figure 7 Reconnecting VPN Connection

Reconnecting button, in the above screen is disabled. Pulse Secure Linux Client will automatically attempt to reconnect in case of an interrupted connection, such as temporarily losing the Wi-Fi link.
Diagnostics and Status

Uploading the Pulse Secure Client Log Files

The Pulse Secure desktop client for Linux makes it easy to transmit diagnostic log bundles to PCS gateways for analysis by system administrators.

The Pulse Connect Secure admin must enable which clients can send log files by traversing the following menus in the admin console and clicking on the Pulse Client:

- System > Log/Monitoring > Client Logs > Settings

Figure 8 Enabling Upload logs Admin Option

The Pulse Connect Secure admin must enable upload logs feature by traversing the following menus in the admin console and clicking on the Checkbox:

- User Roles -> <Role> -> General -> Session Options
Figure 9 Enabling Upload logs Admin Option

Pulse Secure Linux allows user to select normal/detailed logs to store for organizing issues.

To change the log level, run the following step from the desktop client user interface:

- File -> Logs -> Log Level
To send a log bundle to the PCS, when a VPN connection is selected, run the following step from the desktop client user interface:

- File -> Logs -> Upload.

Once this work is done, the system administrator can view uploaded logs in the administrative console here:
• System > Log/Monitoring > Client Logs > Uploaded Logs

Figure 12 Admin Uploaded logs page

Advanced Connection Details
Advanced connection details page shows the status of the selected VPN connection from the list.

To view advanced connection details, click on File > Connections > Advanced Status Details.

Figure 13 Advanced Connection Details

Note: To upload logs to the VPN server, the user needs to be authenticated with an active session.

About Pulse Linux Client
To view Pulse Linux client details:
1. Click on About button on main Pulse Linux client UI.
Figure 14 About Pulse Linux client
Using Pulse Linux Client Command Line

Initiating VPN connection

Pulse Secure CLI client can be launched from Linux terminals. The usage information is also available in the readme file inside the package.

The following command gives the usage of the various options of the command line client:
/usr/local/pulse/PulseClient.sh –H

In the case of 64 bit machines, please execute the following command:
/usr/local/pulse/PulseClient_x86_64.sh –H

The PulseClient.sh script will install the 32 bit dependent packages if these packages are not already installed.

Prerequisites to Run the Command Line Client:

- Pulse Connect Secure (PCS, formerly SA/IVE) IP address or hostname
- VPN user name and password
- PCS certificate (Contact PCS administrator to get certificate in DER format)
- PCS sign-in URL
- Proxy details, if applicable, (IP address/hostname, proxy username and password)
- Realm name to connect

Launch the Command Line Client

Use the following command format to launch the command line client:
/usr/local/pulse/PulseClient.sh -h <PCS appliance IP/hostname> -u <vpn username> -p <vpn password> -r <realm>

Example:
/usr/local/pulse/PulseClient.sh -h vpn.pulsesecure.net -u user1 -p PulseSecure -r users

Terminating VPN connection

Run the following command to terminate the command line client to terminate the VPN connection.
/usr/local/pulse/PulseClient.sh -K

Diagnostics and Status

Uploading Pulse Secure Client Log Files

Use the following command format to launch the command line client:
/usr/local/pulse/PulseClient.sh -h <PCS appliance IP/hostname> -u <vpn username> -p <vpn password> -r <realm> -g

Example:
/usr/local/pulse/PulseClient.sh -h vpn.pulsesecure.net -u user1 -p PulseSecure -r users -g

Note: -g option connects to Pulse Connect Secure (PCS) with the provided credentials and uploads the logs into Pulse Connect Secure.
Checking Pulse Secure Client Status

Run the following command to see the status of the VPN connection:
```bash
/usr/local/pulse/PulseClient.sh -S
```

ℹ️ **Note:** The above command could take up to 30 seconds to reflect the current state of the Pulse client.
Managing Certificates on Linux

Pulse Secure Linux clients verify server certificate with trusted Certificate Authorities (CA) store in the system. Follow the instructions to add issuing CA certificate to store.

Note: CA certificates to be stored as PEM format in trusted CA store. Following command is used to convert CA certificates to PEM format from DER format.
openssl x509 -in cert.crt -inform der -outform pem -out cert.pem

Linux (Ubuntu, Debian)

To add CA certificate into system store:
1. Install the ca-certificate package
   ```shell
   sudo apt-get install ca-certificates
   ```
2. Copy the CA certificate which has been used to sign the device certificate, to `/usr/local/share/ca-certificates` directory:
   ```shell
   sudo cp device-ca.crt /usr/local/share/ca-certificates/device-ca.crt
   ```
3. Copy the CA certificate which has been used to sign the certificate of Identity Provider (IdP) (in case of SAML authentication), to `/usr/local/share/ca-certificates` directory:
   ```shell
   sudo cp idp-ca.crt /usr/local/share/ca-certificates/idp-ca.crt
   ```
4. Update the CA store:
   ```shell
   sudo update-ca-certificates
   ```

Linux (CentOS/RHEL/Fedora)

To add CA certificate into system store:
1. Become Super User of the machine using the following command:
   ```shell
   su-
   ```
2. Install the ca-certificate package:
   ```shell
   yum install ca-certificates
   ```
3. Enable the dynamic CA configuration feature:
   ```shell
   update-ca-trust force-enable
   ```
4. Copy the CA certificate which has been used to sign the device certificate, to `/usr/local/share/ca-certificates` directory:
   ```shell
   sudo cp device-ca.crt /etc/pki/ca-trust/source/anchors/
   ```
5. Copy the CA certificate which has been used to sign the certificate of Identity Provider (IdP) (in case of SAML authentication), to `/usr/local/share/ca-certificates` directory:
   ```shell
   sudo cp idp-ca.crt /usr/local/share/ca-certificates/idp-ca.crt
   ```
6. Use command:
   ```shell
   update-ca-trust extract
   ```

Note: Pulse Secure Linux client command line “-f” option is deprecated from 8.1R8 release.

Note: From 9.0 R1 release onwards, web browser invoked for establishing connections will display
following error message, if the user visits or forwarded to the websites which have certificates not trusted by the machine.

Figure 15 Error Message

Unable to load page
Problem occurred while loading the URL https://10.209.113.207/cert_auth
Unacceptable TLS certificate
Try again
Host Checking Support on Linux

All Host Checker rules are implemented through IMCs and IMVs based on the TNC open architecture. IMCs are software modules that Host Checker runs on the client machine. IMCs are responsible for collecting information, such as antivirus, antispyware, patch management, firewall, and other configuration and security information for a client machine.

Configuring PCS Host Checker Policy for Pulse Linux Client

To configure a Host Checker policy, perform these tasks:

1. Create and enable Host Checker policies through the Authentication > Endpoint Security > Host Checker page of the admin console.
2. In the admin console, select Authentication > Endpoint Security > Host Checker.
4. Enter a name in the Policy Name field and then click Continue. (Users see this name on the Host Checker remediation page if you enable custom instructions for this policy.)
5. Create one or more rules to associate with the policy.
6. Configure additional system-level options on the Authentication > Endpoint Security > Host Checker page of the admin console as necessary:
   a. If you want to display remediation information to users if they fail to meet the requirements of a Host Checker policy, configure remediation options through the Authentication > Endpoint Security > Host Checker page of the admin console.
   b. To change default Host Checker settings, configure settings through the Authentication > Endpoint Security > Host Checker page of the admin console.
7. Determine the level you that you want to enforce Host Checker policies:
   a. To enforce Host Checker policies when the user initially accesses the device, implement the policy at the realm level by selecting the policy at the Users > User Realms > Select Realm > Authentication Policy > Host Checker page of the admin console.
   b. To allow or deny users access to specific roles based on compliance with Host Checker policies, implement the policies at the role level by using the Users > User Roles > Select Role > General > Restrictions > Host Checker page of the admin console.
   c. To map users to roles based on their compliance with Host Checker policies, use custom expressions in the Users > User Realms > Select Realm > Role Mapping page of the admin console.
   d. To allow or deny users access to individual resources based on their compliance with Host Checker policies, use conditions in the Users > Resource Policies > Select Resource > Select Policy > Detailed Rules > Select | Create Rule page of the admin console.

Pulse Linux Client supports Files, Ports and Processes IMCs currently

• **Ports**—Use this rule type to control the network connections that a client can generate during a session. This rule type ensures that certain ports are open or closed on the client machine before the user can access the device. In the Ports configuration page:
  1. Enter a name for the port rule.
  2. Enter a comma delimited list (without spaces) of ports or port ranges, such as: 1234,11000-11999,1235.
  3. Select Required to require that these ports are open on the client machine or Deny to require that they are closed.
  4. Click Save Changes.
• **Process**—Use this rule type to control the software that a client may run during a session. This rule type...
ensures that certain processes are running or not running on the client machine before the user can access resources protected by the system. In the Processes configuration page:

1. Enter a name for the process rule.
2. Enter the name of a process (executable file), such as: good-app.exe.

**Note:** For Linux systems, the process that is being detected must be started using an absolute path. You can use a wildcard character to specify the process name.

For example: `/usr/local/bin/pulseUI`

3. Select Required to require that this process is running or Deny to require that this process is not running.
4. Specify the MD5 checksum value of each executable file to which you want the policy to apply (optional). For example, an executable may have different MD5 checksum values on a desktop, laptop, or different operating systems. On a system with OpenSSL installed—many Linux systems have OpenSSL installed by default—you can determine the MD5 checksum by using this command: `openssl md5 <processFilePath>`
5. Click Save Changes.

- **File**—Use this rule type to ensure that certain files are present or not present on the client machine before the user can access the device. You may also use file checks to evaluate the age and content (through MD5 checksums) of required files and allow or deny access accordingly. In the Files configuration page:

1. Enter a name for the file rule.
2. Enter the name of a file (any file type), such as: `/tmp/bad-file.txt`.
   a. You can use a wildcard character to specify the file name.
      
      For example: `*.txt`
   b. You can also use an environment variable to specify the directory path to the file. (You cannot use a wildcard character in the directory path.) Enclose the variable between the `<%` and `%>` characters.
      
      For example: `FILEPATH\bad-file.txt`
3. Select Required to require that this file is present on the client machine or Deny to require that this file is not present.
Diagnostics and Status

Pulse Linux Client updates the status of host checker in the VPN connection window.

**Figure 16 Host Checker Status on VPN Connection Window**

Pulse Linux Client shows compliance status for connected session when user clicks on drop down option for the same VPN connection entry.

**Figure 17 Host Checker Compliance Status Window**
SAML Support

SAML is an XML-based framework for communicating user authentication, entitlement and attribute information. It is used primarily to implement Web browser single sign-on (SSO). This feature allows users to authenticate over SAML. This feature has been tested and qualified for the following Identity Providers (IdPs):

- G Suite
- Okta

For more information on SAML Support, see Pulse Secure Linux Client SAML Deployment Guide.
Certificate Authentication Support

This feature enables users to login to the client using their certificates. The supported scenario is “certificate based login only” the Pulse Linux Client setup is now switched to this authentication method. In a typical enterprise environment, each user will be provided with certificate which can be used for VPN login. This mechanism can be used as a primary or secondary authentication mechanism.

Configuring Client Certificate in Pulse Connect Secure

To configure trusted client CA certificate:

1. Select System > Configuration > Certificates > Trusted Client CAs.

2. Click Import CA Certificate to display the configuration page.

3. Browse to the certificate file and select it.

4. Click Import Certificate to complete the import operation.

5. Click the link for the Trusted Client CA to configure.
Configuring Authentication with the Certificate Server
To configure authentication with the certificate server follow the steps below:

1. Select Authentication > Auth Servers.
2. Select Certificate Server and Click New Server to display the configuration page.

3. Complete the configuration as described in Table 1.
Table 1: Certificate Server Settings

<table>
<thead>
<tr>
<th>Settings</th>
<th>Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify a name to identify the server within the system</td>
</tr>
<tr>
<td>User Name Template</td>
<td>Specify a username template. Specify how the system should construct a username. You may use any combination of certificate variables contained in angle brackets and plain text. NOTE: This value populates the &lt;USER&gt; and &lt;USERNAME&gt; session variables for use throughout the rest of the system configuration.</td>
</tr>
<tr>
<td>User Record Synchronization</td>
<td>This applies only to Connect Secure</td>
</tr>
<tr>
<td>Enable User Record Synchronization</td>
<td>Select this option to retain the bookmarks and individual preferences regardless of which system you log in to.</td>
</tr>
<tr>
<td>Logical Auth Server Name</td>
<td>Specify a logical authentication server name.</td>
</tr>
</tbody>
</table>

Figure 22 Configuring Certificate Server

4. Save the configuration.
Client Certificate Installation

The installation of the certificates can be facilitated through a script. Client certificates can be installed using utility script “PulseClient.sh”. An example on how to install the certificate are shown below:

- To install the certificate from pfx file:
  `/usr/local/pulse/PulseClient.sh install_certificates -inpfx /mnt/hgfs/shared_dir/10.30.113.196.pfx`

- Using separate private and public certificate:
  `/usr/local/pulse/PulseClient.sh install_certificates -inpriv /mnt/hgfs/shared_dir/certs/flowerCert.key -inpub /mnt/hgfs/shared_dir/certs/flowerCert.pem`

- To list the certificate from Certificate Store:
  `/usr/local/pulse/PulseClient.sh list_installed_certificates`

- To delete the Certificate from certificate store:
  `/usr/local/pulse/PulseClient.sh delete_certificates -certName <certificate name>`

Certificate Types Supported

Public Certificates

<table>
<thead>
<tr>
<th>Extensions</th>
<th>Certificate Formats</th>
</tr>
</thead>
<tbody>
<tr>
<td>der, cer</td>
<td>DER</td>
</tr>
<tr>
<td>pem, crt, key, pub</td>
<td>PEM</td>
</tr>
</tbody>
</table>

Private Keys

<table>
<thead>
<tr>
<th>Extensions</th>
<th>Certificate Formats</th>
</tr>
</thead>
<tbody>
<tr>
<td>der, cer</td>
<td>DER</td>
</tr>
<tr>
<td>pem, crt, key</td>
<td>PEM</td>
</tr>
</tbody>
</table>

PFX file (Contains both Private Key and Public Keys)

<table>
<thead>
<tr>
<th>Extensions</th>
<th>Certificate Formats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pfx, p12</td>
<td>PFX</td>
</tr>
</tbody>
</table>

Note: Other formats like p7b, p7c, pk8 are not currently supported. All of the above formats will be converted from PEM format to store it in GNOME-keyring.
Default Certificate Selection

If multiple certificates are available for a connection, the certificates will be listed and user can select the certificate for establishing the connection. Once user selects the certificate, that certificate will be stored as preferred certificate for the corresponding connection and this will be used for subsequent authentications to all the corresponding connection.

**Figure 23 Cert_list**

The above **Figure 23** shows that when user clicks on connect the multiple client certificate will be displayed to continue authenticating for connection. On clicking the view, the certificate details can be viewed by the user (refer **Figure 24**).
Figure 24 Certs_details_onclicking view

Note:

- The certificate authentication through UI will be supported only on the machines using libsoup 2.48 and above. Centos 6.4 and Ubuntu 14.04 doesn't meet the above requirements.
- The user cannot save the certificate selection. Save credentials will not be supported.
- Client certificate authentication through smart cards is not supported.