



# Pulse Secure Client for Linux

Security Assertion Markup Language (SAML)

Deployment Guide

Document Version

**1.0**

Published

**November 2017**

Pulse Secure, LLC  
2700 Zanker Road, Suite 200  
San Jose, CA 95134  
[www.pulsesecure.net](http://www.pulsesecure.net)

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 Client for Linux Security Assertion Markup Language (SAML) Deployment Guide*

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 [www.pulsesecure.net](http://www.pulsesecure.net). By downloading, installing or using such software, you agree to the terms and conditions of that EULA."

# Contents

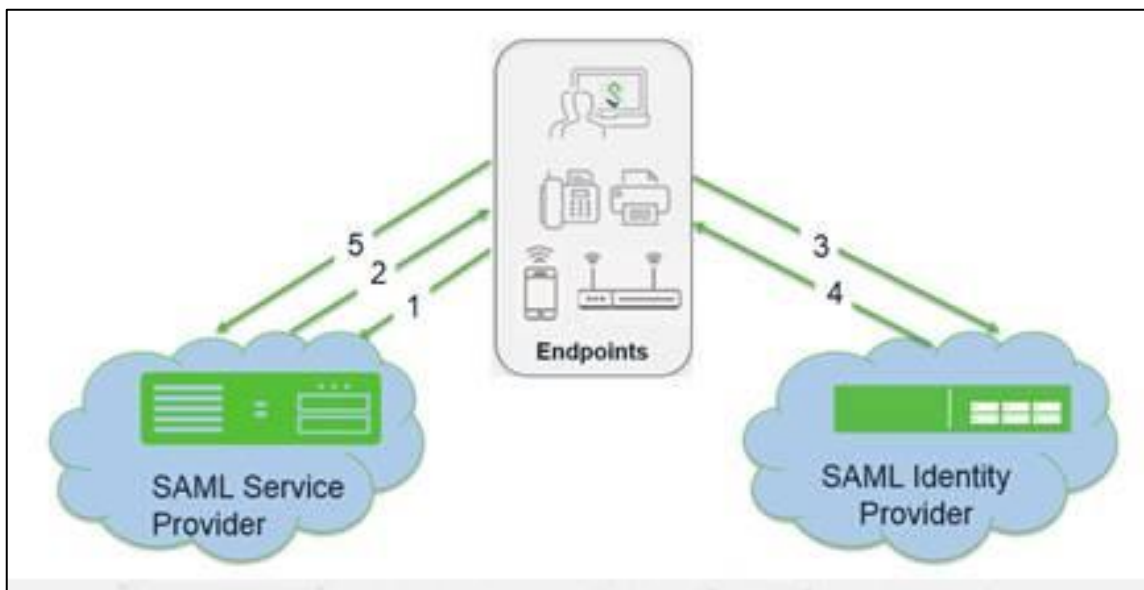
Introduction .....	4
Initial Configuration .....	5
SAML IdP Configuration .....	5
Authentication Server Configuration .....	6
Role Creation .....	7
New User Realm Creation .....	8
New Sign-In Policy Creation .....	10
VPN Client Connectivity Configuration .....	11
Log in to Pulse Secure Linux Client .....	13

# Introduction

SAML is an XML-based framework for communicating user authentication, entitlement, and attribute information. The standard defines the XML-based assertions, protocols, bindings, and profiles used in communication between SAML entities. SAML is used primarily to implement Web browser single sign-on (SSO). SAML enables businesses to leverage an identity-based security system like Pulse Connect Secure to enforce secure access to websites and other resources without prompting the user with more than one authentication challenge.

Pulse Secure supports SAML authentication using Linux version of the client. There are numerous SAML based Identity Provider (IdP) services which help users authenticate using SAML, for example, GSuite, Okta, SimpleSamlPhp, etc.

The following figure illustrates the basic SAML workflow. The numbers indicate the request and acknowledgement flow.



A high-level overview of the configuration steps needed to set up and run the SAML for the Linux version of the client is shown below. Click each step to directly jump to the related instructions.



## Initial Configuration

1. Configure the SAML IdP application on the IdP provider website.
2. Either manually copy the SSO URL, the Entity ID and download the certificate, or download the IdP Metadata XML file and save it on the local drive.

## SAML IdP Configuration

1. Navigate to **System > Configuration > SAML**.
2. Click **Settings**.
3. Enter the **Host FQDN for SAML** and click **Save Changes**.
4. Navigate back to **System > Configuration > SAML**.
5. Under **New Metadata Provider**, enter the **Name**.
6. Under **Metadata Provider Location Configuration**, click **Browse** beside **Upload Metadata File** and select the IdP Metadata XML file you have saved on the local drive.
7. If the signing information is not available in the IdP Metadata XML file, under **Metadata Provider Verification Configuration**, select **Accept Unsigned Metadata**.
8. Under **Metadata Provider Filter Configuration**, select **Identity Provider** as the Role.
9. Click **Save Changes**.

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

### New Metadata Provider

Name:  Label to reference metadata provider.

**Metadata Provider Location Configuration**

Location:  Local  Remote Location of metadata provider. In case of Local, metadata file needs to be uploaded by admin. In case of Remote Location, metadata file is fetched by Connect Secure from the configured download url.

Upload Metadata File:  No file chosen  
Current File: None

**Metadata Provider Verification Configuration**

Accept Unsigned Metadata If checked Connect Secure accepts unsigned metadata.

Signing Certificate:  
 Issued To:  
 Issued By:  
 Valid:  
 Details:

Upload Certificate:  No file chosen   
 Enable Signing Certificate status checking  
(Uses configuration in Trusted Client CAs. This applies to the certificate configured above as well as the one comes along with the Metadata.)

**Metadata Provider Filter Configuration**

Roles:  Identity Provider  Service Provider  Policy Decision Point Roles which Connect Secure looks for in the metadata file.

Entity Ids to import:  List of entity ids to be imported. (one per line). If left empty all entity ids in the file are imported.

## Authentication Server Configuration

1. Navigate to **Authentication > Auth. Servers**.
2. Select **SAML Server** under **New** field and click **New Server**.
3. Enter the **Server Name**.
4. Under **Settings**, select **Metadata** as **Configuration Mode**.
5. Select **Identity Provider Entity Id** and **Identity Provider Single Sign On Service URL** specific to the IdP service.
6. Under **SSO method**, select the IdP specific certificate for **Select Certificate**.
7. Under **Service Provider Metadata Settings**, enter **Metadata Validity** as 365.
8. Click **Save Changes**.

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

Auth Servers > New SAML Server

### New SAML Server

Server Name:

**Settings**

\*SAML Version:  1.1  2.0

\*Connect Secure Entity Id:  Unique SAML identifier of the SAML Auth Server. Uses host name configured at [SAML Settings](#).

\*Configuration Mode:  Manual  Metadata Uses metadata files configured at [SAML Metadata](#) for metadata file based configuration.

\*Identity Provider Entity Id:  Unique SAML identifier of the Identity Provider.

Identity Provider Single Sign On Service URL:  User is redirected to this URL in destination first scenario. Select "Not Applicable" if destination first scenario is not required.

User Name Template:  Example: <assertionNameDN.uid>, uid from X509SubjectName. The entire assertion name identifier if not specified; Or <userAttr.attr>, attr from AttributeStatement attributes.

Allowed Clock Skew (minutes):  0 - 9999 minutes

Support Single Logout If checked, Connect Secure supports sending and receiving single logout requests.

**SSO Method**

Artifact  Post

Response Signing Certificate:  
 Issued To:  
 Issued By:  
 Valid:  
 Details: [Other Certificate Details](#)

Select Certificate:  [Delete](#)

Enable Signing Certificate status checking  
 (Uses configuration in [Trusted Client CAs](#). This applies to the certificate configured above as well as the one comes along with the SAML response.)

Select Device Certificate for Signing:  Certificate used for signing the Requests initiated by Connect Secure for the SAML Auth Server. Select "Not Applicable" if Request signing is not required.

Select Device Certificate for Encryption:  Certificate used by the IdP for wrapping encryption keys for the SAML Auth Server. Select "Not Applicable" if encryption is not required.

Select Requested Authn Context Classes to be sent in the AuthRequest:  
 Available: SmartcardPKI, Unspecified, SoftwarePKI, Telephony, NomadTelephony, PersonalTelephony  
 Selected: (none)

Comparison Method for Authentication Classes:

**Service Provider Metadata Settings**

Metadata Validity:  days 1 - 9999. Specifies the time in days after which metadata for the SAML Auth Server should be refreshed by the Identity Provider. This is used to populate the cache duration field in the generated metadata.

Do Not Publish Connect Secure Metadata Prevents the Metadata for the SAML Auth Server to be published at the location specified by the Connect Secure Entity Id.

[Download Metadata](#)

## Role Creation

1. Navigate to **Users > User Roles > New User Role**.
2. Enter **Name**.
3. Under **Options**, select **Pulse Secure Client**.
4. Under **Access Features**, select **VPN Tunneling**.
5. Click **Save Changes**.

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

User Roles > New Role

### New Role

Name:

Description:

**Options**

Session and appearance options are specified in [Default Options](#). Check the following if this role should override these defaults.

- VLAN/Source IP
- Session Options
- UI Options
- Pulse Secure client Dynamically deliver Pulse Secure client to Windows and MAC OSX users

**Access Features**

Check the features to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles assigned to the user.

- Web
- Files, Windows
- Files, UNIX/NFS
- Telnet/SSH
- Secure Application Manager
  - Windows version Note: On Windows Mobile, Pulse Secure client is delivered via WSAM
  - Java version
- Terminal Services
- Virtual Desktops
- HTML5 Access
- Meetings
- VPN Tunneling (Includes IKEv2)
- Secure Mail

**Save Changes**

## New User Realm Creation

1. Navigate to **Users > User Realms > New User Realm**.
2. Enter **Name**.
3. Under **Servers**, select the applicable SAML Authentication Server that you configured in [Authentication Server Configuration](#) as **Authentication server**.
4. Click **Save Changes**.



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

User Realms > New Authentication Realm

### New Authentication Realm

Name:

Description:

When editing, start on the Role Mapping page

**Servers**

Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication:

User Directory/Attribute:

Accounting:

Device Attributes:

**Additional Authentication Server**

Enable additional authentication server

**Dynamic policy evaluation**

Enable dynamic policy evaluation

**Save Changes**

5. In the Role Mapping screen, click **New Rule**.

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

Created realm successfully. Add role mapping rules here. ✕

User Realms > test > Role Mapping

### Role Mapping

General Authentication Policy **Role Mapping**

Specify how to assign roles to users when they sign in. Users that are not assigned a role will not be able to sign in.

**New Rule...** **Duplicate** **Delete**   **Save Changes**

	When users meet these conditions	assign these roles	Rule Name	Stop
<input type="checkbox"/>				

When more than one role is assigned to a user:

- Merge settings for all assigned roles
- User must select from among assigned roles
- User must select the sets of merged roles assigned by each rule

Note: Users that do not meet any of the above rules will not be able to sign into this realm.

6. Enter **Name**.

7. Under **Rule: If username**, select **is** and type `"*"` without the quotes in the text box.

8. From the list of **Available Roles**, select the related IdP role and click **Add**.
9. Click **Save Changes**.

The screenshot shows the 'Role Mapping Rule' configuration page in the Pulse Secure interface. The page has a dark header with the Pulse Secure logo and navigation tabs: System, Authentication, Administrators, Users (highlighted), Maintenance, and Wizards. The main content area is titled 'Role Mapping Rule' and contains the following elements:

- 'Rule based on:' dropdown set to 'Username' with an 'Update' button.
- 'Name:' text input field.
- 'Rule: if username...' section with a dropdown set to 'is' and a text area for defining the rule. A note states: 'If more than one username should match, enter one username per line. You can use \* wildcards.'
- 'then assign these roles' section with two columns: 'Available Roles' and 'Selected Roles'.
  - 'Available Roles' list: Active Directory Role, Certificate Authentication Role, DUO Role, employee, GSuite HC Role, HC Role.
  - 'Add ->' and 'Remove' buttons between the columns.
  - 'Selected Roles' list: (none).
- 'Stop processing rules when this rule matches' checkbox (unchecked).
- Link: 'To manage roles, see the [Roles](#) configuration page.'
- 'Save Changes' and 'Save + New' buttons at the bottom.

## New Sign-In Policy Creation

1. Navigate to **Authentication > Signing In > Sign-In Policies**.
2. Click **New URL**.
3. Type the **Sign-In URL** for the SAML SP service (For example: \*/saml).
4. Click **User picks from a list of authentication realms**.
5. From the list of **Available Realms**, select the applicable realm specific to the SAML IdP and click **Add**.
6. Click **Save Changes**.

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

Signing In > Sign-in Policies > New Sign-In Policy

### New Sign-In Policy

User type:  Users  Administrators  Meeting  Authorization Only Access

Sign-in URL:  Format: -host-[path]-C. Use \* as wildcard in the beginning of the host name.

Description:

Sign-in page:  To create or manage pages, see [Sign-in pages](#).

Meeting URL:

**Authentication realm**

Specify how to select an authentication realm when signing in.

**User types the realm name**  
The user must type the name of one of the available authentication realms.

**User picks from a list of authentication realms**  
The user must choose one of the following selected authentication realms when they sign in. If only one realm is selected, it is automatically used (the sign-in page will not display the list). To create or manage realms, see the [User Authentication](#) page or the [Administrator Authentication](#) page.

Available realms:   
Certificate Authentication Realm  
Dual Authentication Realm  
Duo Realm  
employee

Selected realms:

Buttons: Add, Remove, Move Up, Move Down

**Configure SignIn Notifications**

Pre-Auth Sign-in Notification  
 Post-Auth Sign-in Notification

## VPN Client Connectivity Configuration

1. Navigate to Users > Resource Policies > VPN Tunneling > Connection Profiles.
2. Click New Profile.
3. Under IPv4 Address Management, set the DHCP Server.
4. Under Connection Settings, set the transport mode to ESP or SSL.
5. (optional). Under Roles, select the applicable role to apply to the policy.
6. Click Save Changes.

PulseSecure
System Authentication Administrators **Users** Maintenance Wizards

Resource Policies > VPN Tunneling Connection Profiles > New Profile

### New Profile

\* Name:

Description:

**IPv4 address assignment**

Specify how IPv4 addresses are assigned to clients.

**DHCP servers**  
Specify the name or IPv4 address for up to 3 DHCP servers

**DHCP options**  
Specify any DHCP options that should be sent to the DHCP Server. Enter the option number, option value, and option value type. Option values can be token replaced values. Note: Please refer to Admin Guide for more details.

<input type="checkbox"/>	Option Number	Option Value	Option Type	
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	String	<input type="button" value="Add"/>

**IPv4 address pool**  
Specify the assignable IPv4 address ranges for this profile, one per line. Note: Please refer to Admin Guide for details.

Examples:  
10.10.1.1-10.10.5.200  
10.10.10.10-100  
10.10.10.50

**IPv6 address assignment**

**Connection Settings**

Transport:  **ESP (maximize performance)**  
ESP mode of transportation and encryption is not applicable in FIPS enabled role.

UDP port:  (This is IPv4 specific settings)

For IPv6 please go to: [IPv6 UDP settings](#)

ESP to SSL fallback timeout:  seconds (15-65535 seconds)

Key lifetime (time based):  minutes (20-86400 minutes)

Key lifetime (bytes transferred):  bytes (0 implies no limits)

Replay Protection:

ESP Transport Only (No SSL fallback, this setting is for the Pulse client only):

Encryption:

- AES128/MD5 (MD5 is insecure. Option is not recommended)
- AES128/SHA1**
- AES256/MD5 (MD5 is insecure. Option is not recommended)
- AES256/SHA1
- AES256/SHA256 (maximize security)

**SSL (maximize compatibility)**  
SSL mode is FIPS compliant on FIPS appliances.

**DNS Settings**

**Proxy Server Settings**

**Roles**

- Policy applies to ALL roles
- Policy applies to SELECTED roles
- Policy applies to all roles OTHER THAN those selected below

Available roles:

- Active Directory Role
- Certificate Authentication Role
- DUO Role
- GSuite HC Role
- HC Role

Selected roles: (none)

## Log in to Pulse Secure Linux Client

1. Launch Pulse Secure Linux Client.
2. Create a connection specific to SAML, and enter the URL `https://<IP or FQDN of PCS Box>/saml`, for the connection. Click **Connect**.  
Note that a Webkit based browser opens and you are redirected to the IdP.
3. Enter the credentials on the redirected web page. Upon successful authentication, the Webkit based browser closes and creates a Tunnel.