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

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**.** By downloading, installing or using such software, you agree to the terms and conditions of that EULA."

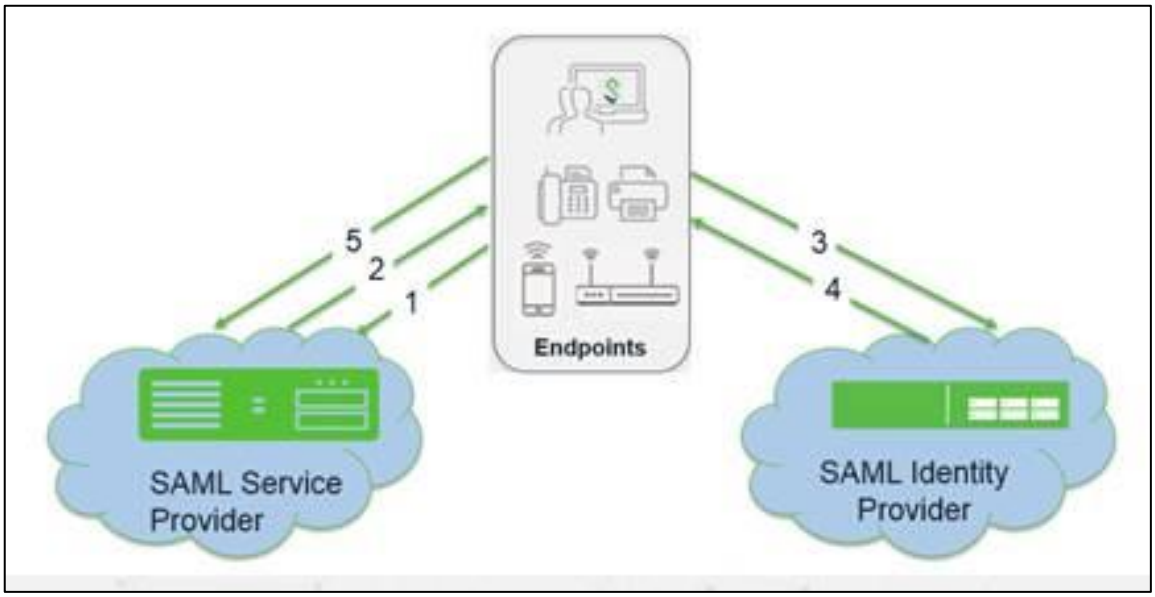
Contents

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.



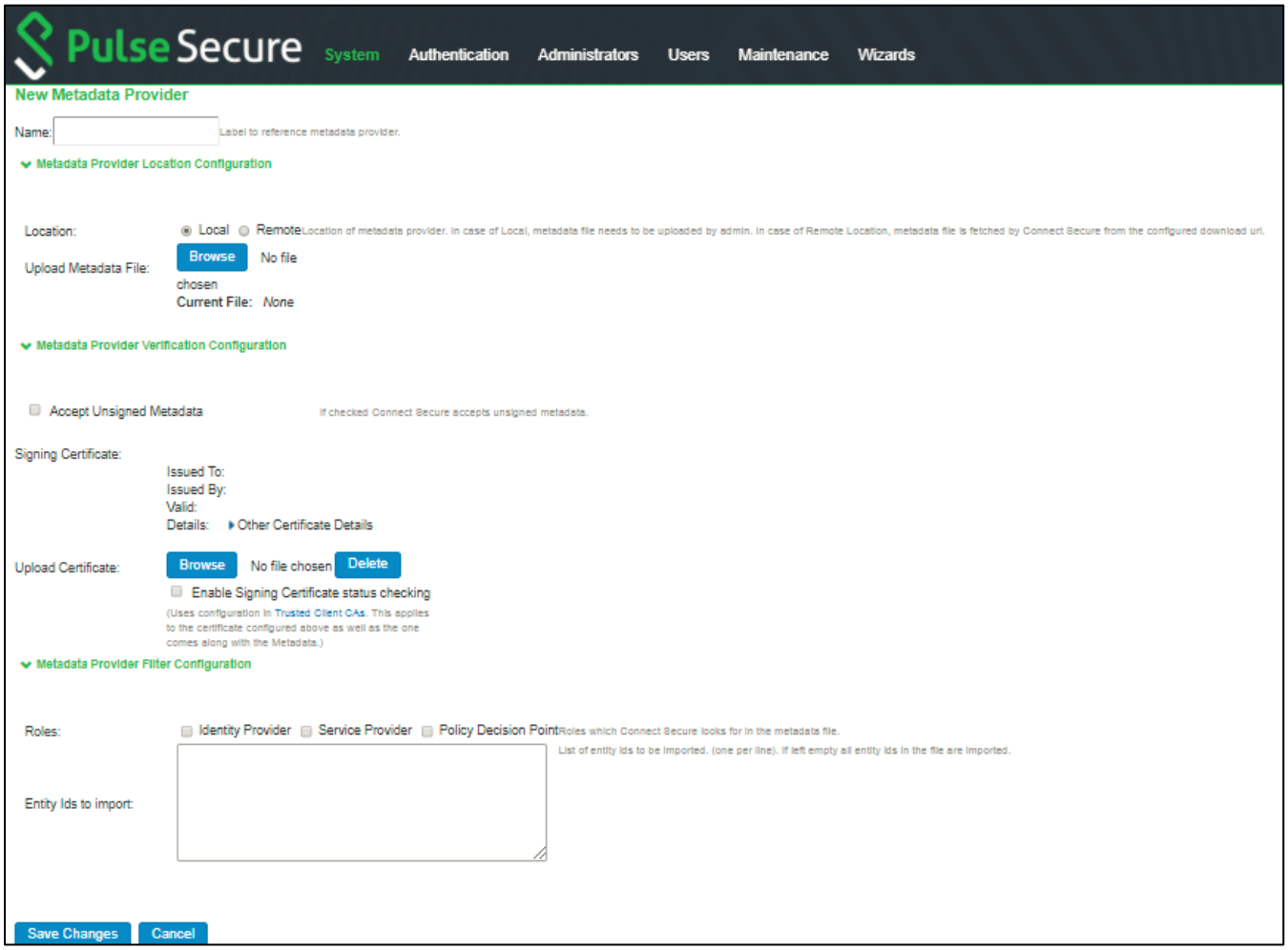
A high-level overview of the configuration steps needed to set up and run the SAML for the Linux version of the client is shown below. Click each step to directly jump to the related instructions.

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.

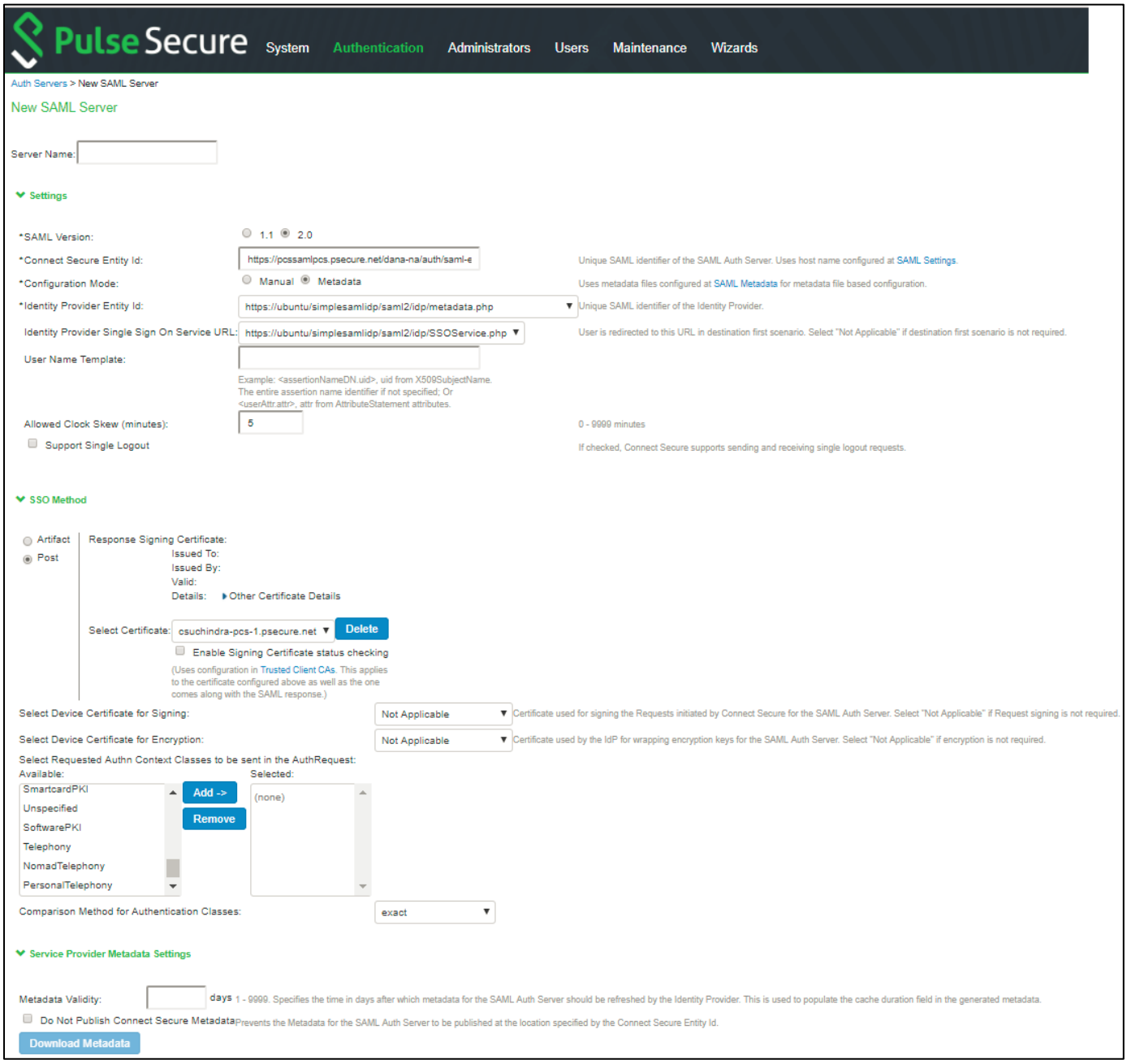
SAML IdP Configuration

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**.



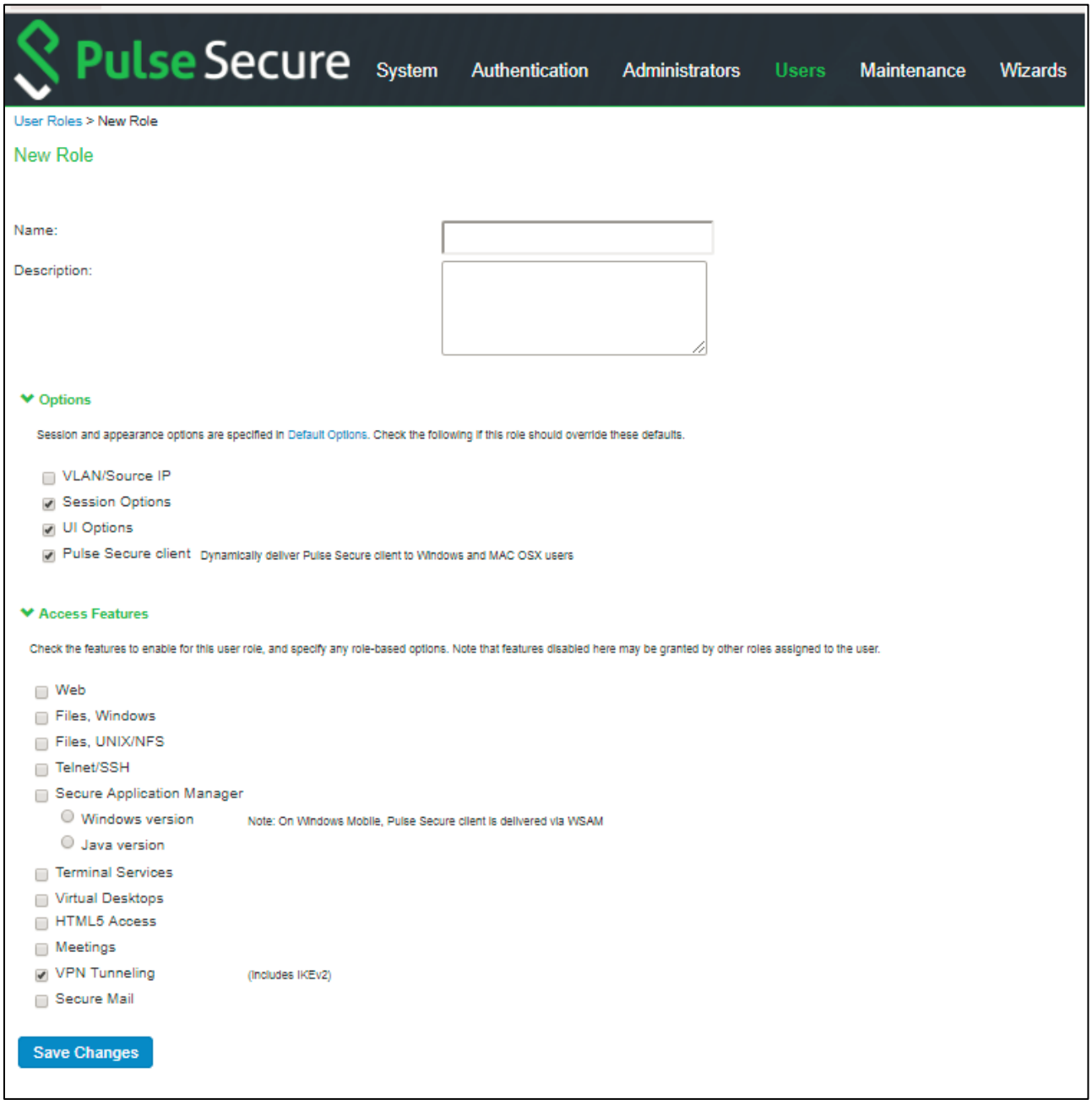
Authentication Server Configuration

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**.



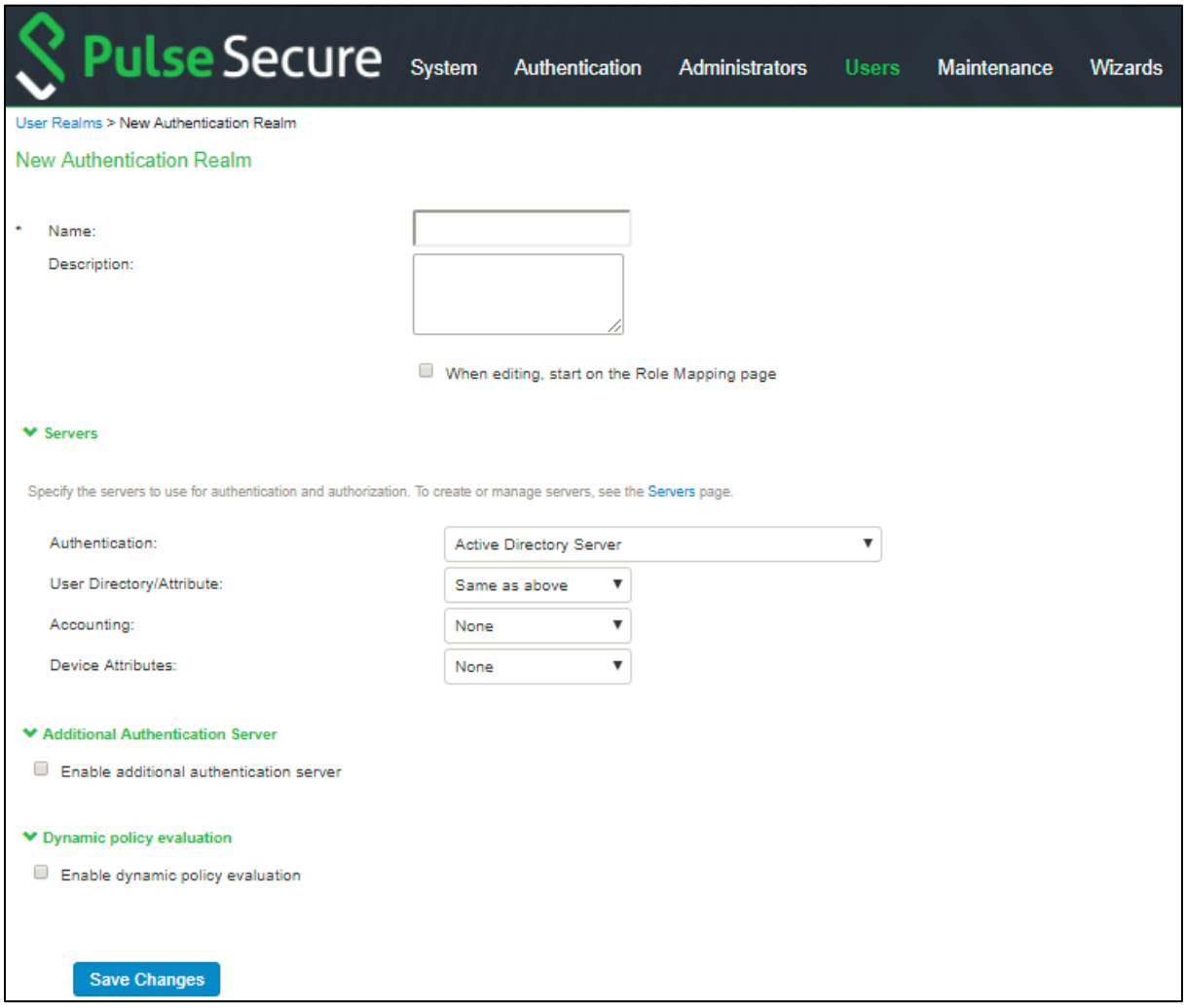
Role Creation

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**.

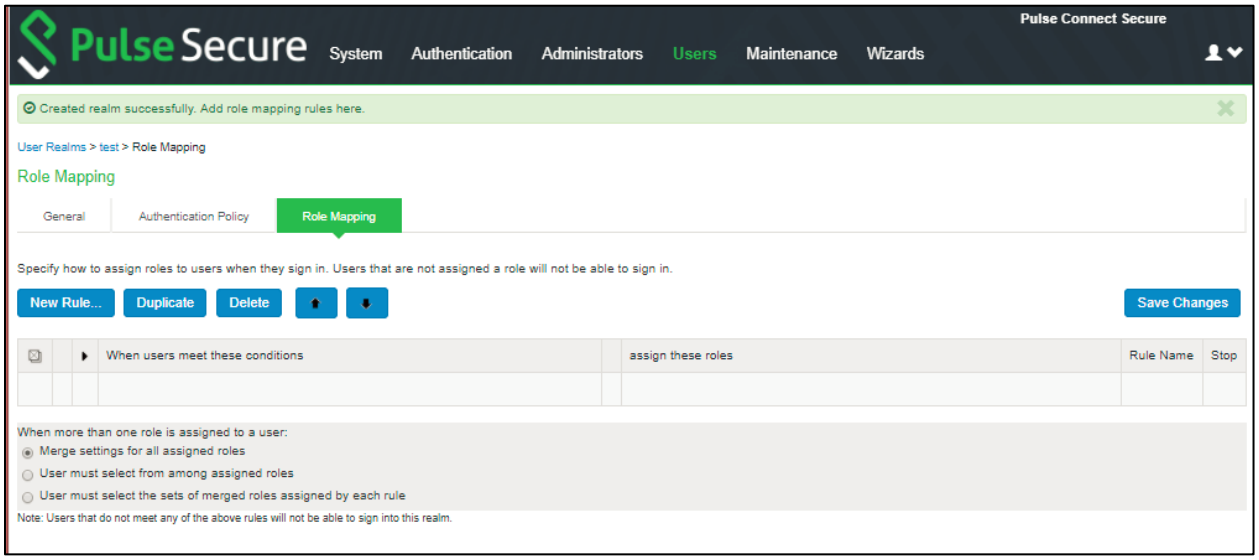


New User Realm Creation

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**.

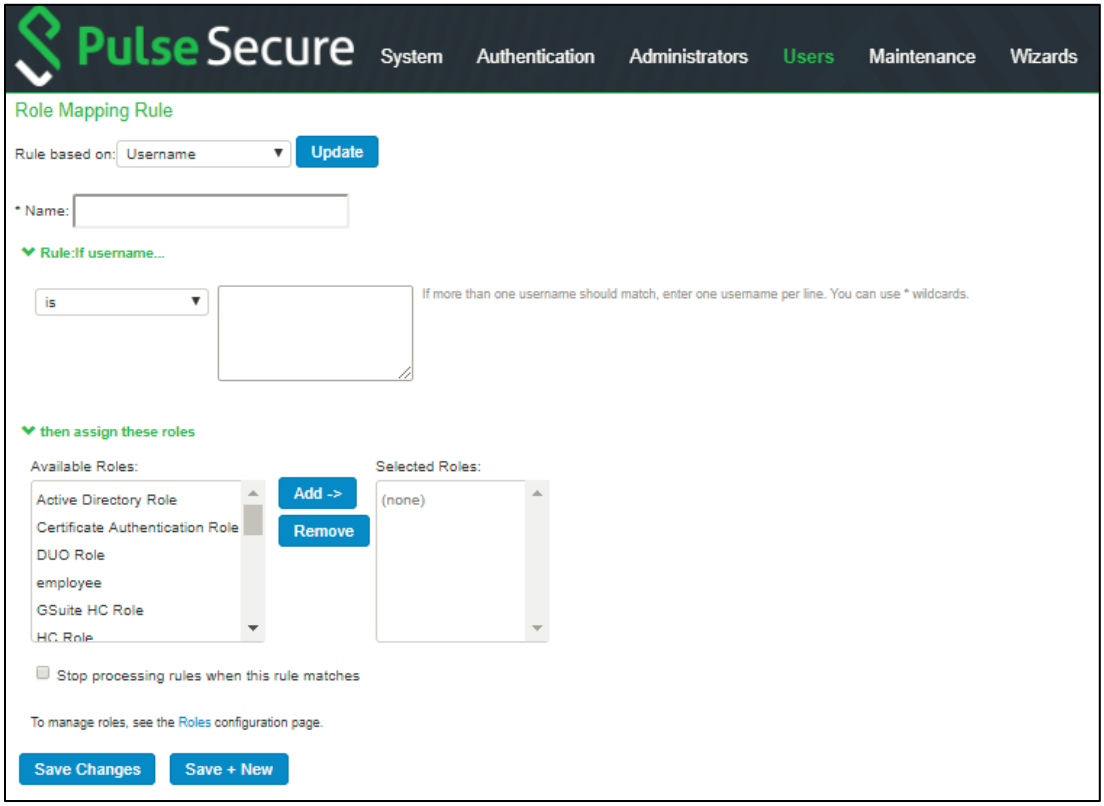


5. In the Role Mapping screen, click **New Rule**.



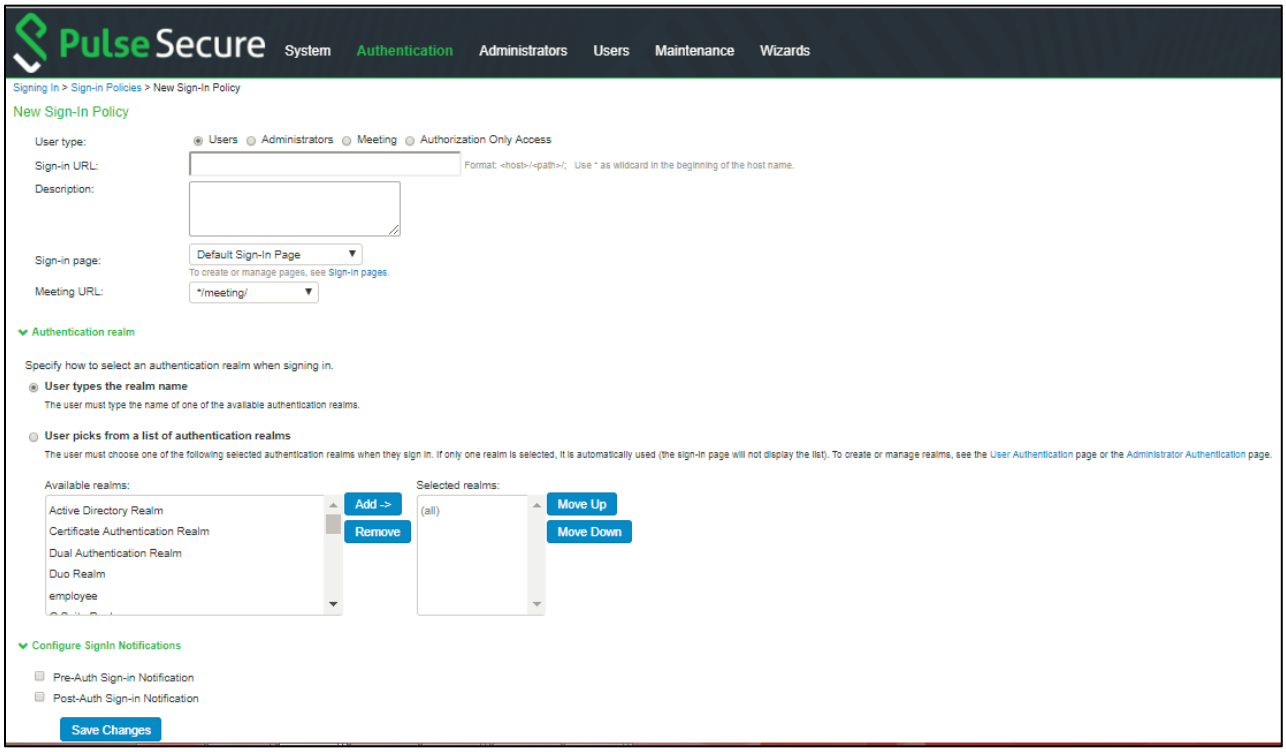
6. Enter **Name**.
7. Under **Rule: If username,** select **is** and type "*" without the quotes in the text box.

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



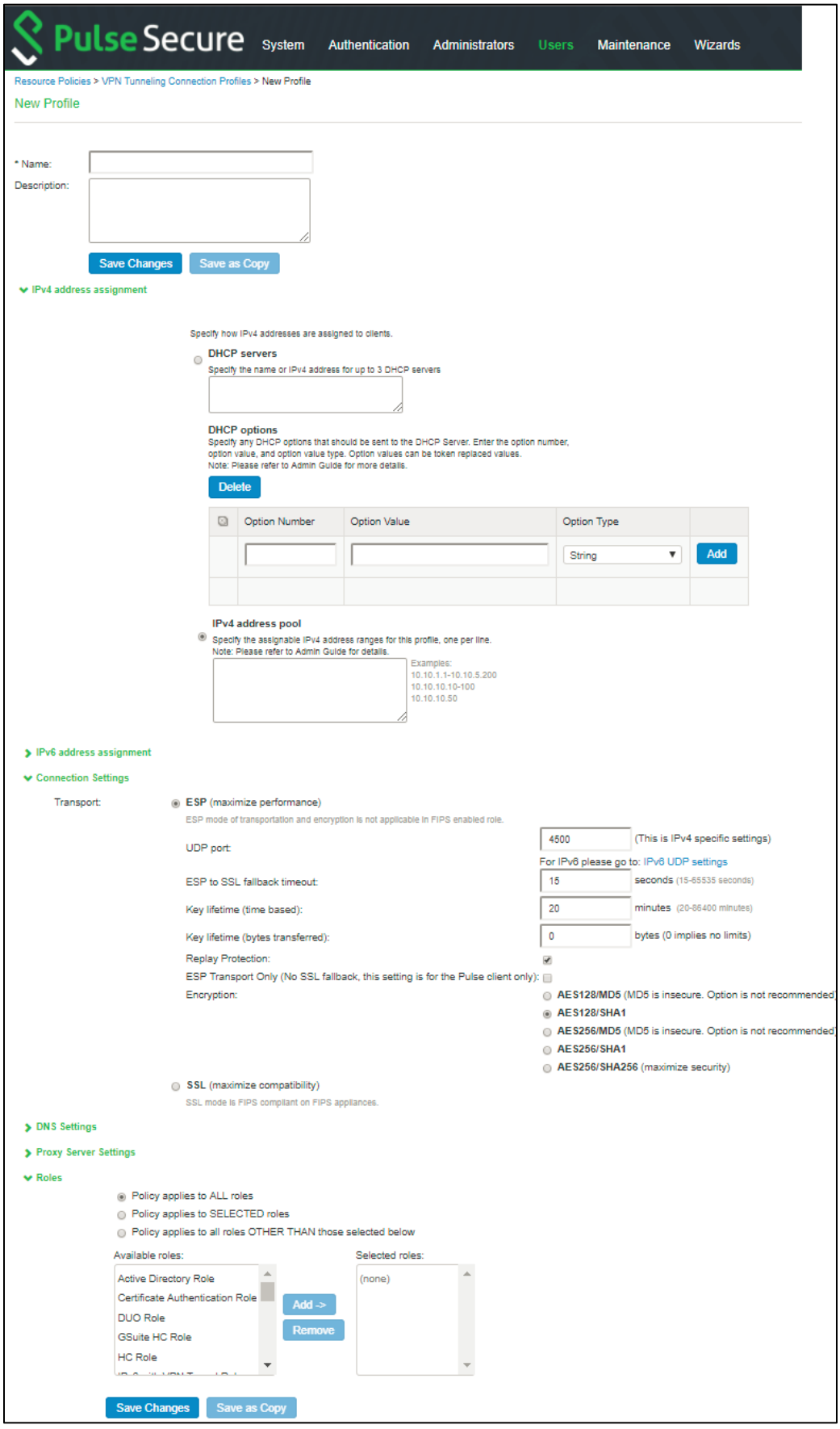
New Sign-In Policy Creation

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.**



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.**



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.