Pulse Secure®

Microsoft Azure Active Directory as SAML IdP with Pulse Connect Secure

Deployment Guide

Release	9.0R3
Document Revision	2.0
Published Date	February 2019

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

https://www.pulsesecure.net

Microsoft Azure Active Directory as SAML IdP with Pulse Connect Secure - Deployment Guide

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

END USER LICENSE AGREEMENT

Revision History

Revision and Date	Added/Updated /Removed	Remarks
2.0, February 2019	Updated	Updated the document with the latest MS Azure navigation
1.0, May 2018	Initial release	

Table of Contents

List of Figures

Introduction

This document describes how to set up Pulse Connect Secure for SP-initiated SAML authentication using the Microsoft Azure Active Directory as the SAML IdP. It also describes the user experience with Web browser and Pulse Secure Client access methods.

Prerequisites

Ensure you have the following:

- Administrative access to the Azure Management Portal
  - Azure subscription that includes Active Directory
- Pulse Connect Secure appliance running 8.2R1 or later

Configurations

The set up includes the following process steps:

- Microsoft Azure Active Directory Configuration
- Pulse Connect Secure Configuration

Microsoft Azure Active Directory Configuration

This section covers the configurations required on Microsoft Azure AD.
Microsoft Azure AD configurations include:

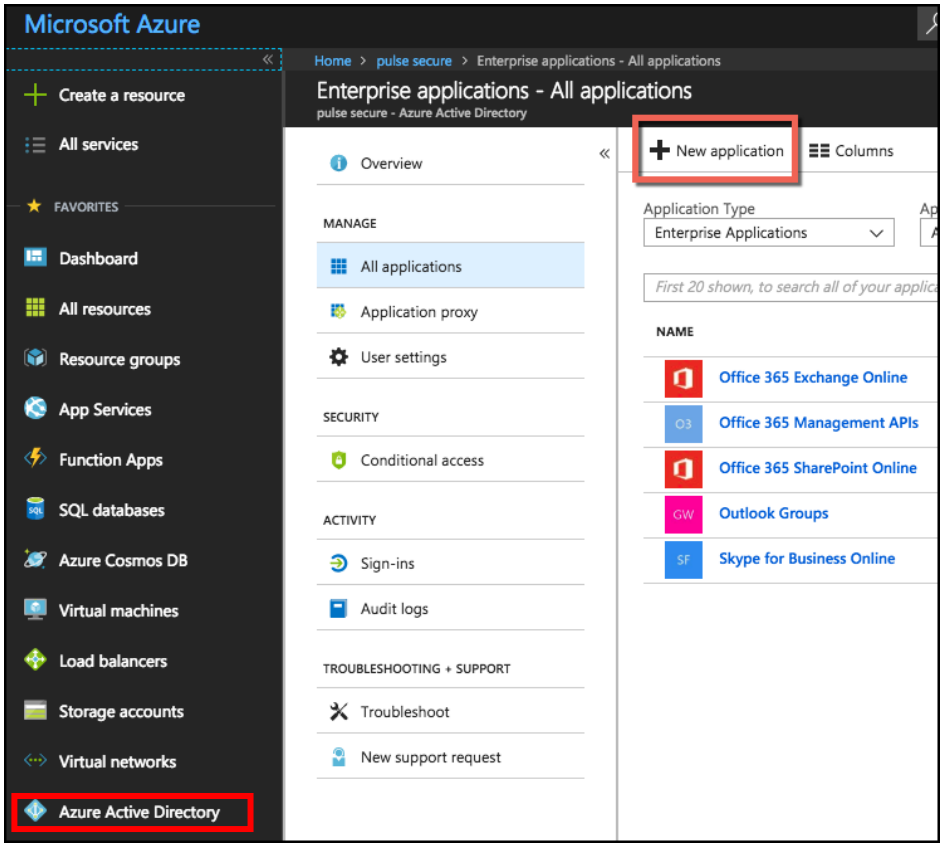
- Setting Up PCS as Enterprise Application
- Configuring Single Sign-on Settings
- Configuring PCS as Service Provider
- Assigning User to Application

Setting Up PCS as Enterprise Application

Perform the following steps:

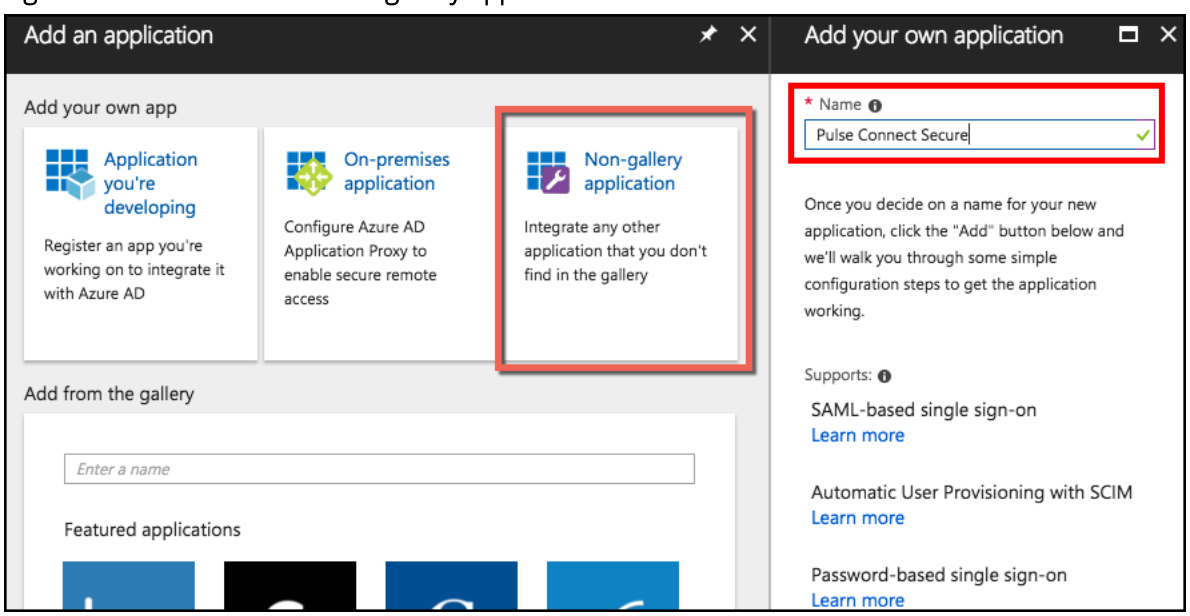
1. Log into the Azure Management Portal.
2. On the left pane, click **Azure Active Directory**.
3. Select your active directory from the active directory list.
4. Select **Enterprise Applications**.
5. Click on **New Application**.

Figure 1: Azure AD - Enterprise applications



6. Select **Non-gallery application**.
7. Provide a name for the application and click **Add**.

Figure 2: Azure AD - Select Non-gallery application

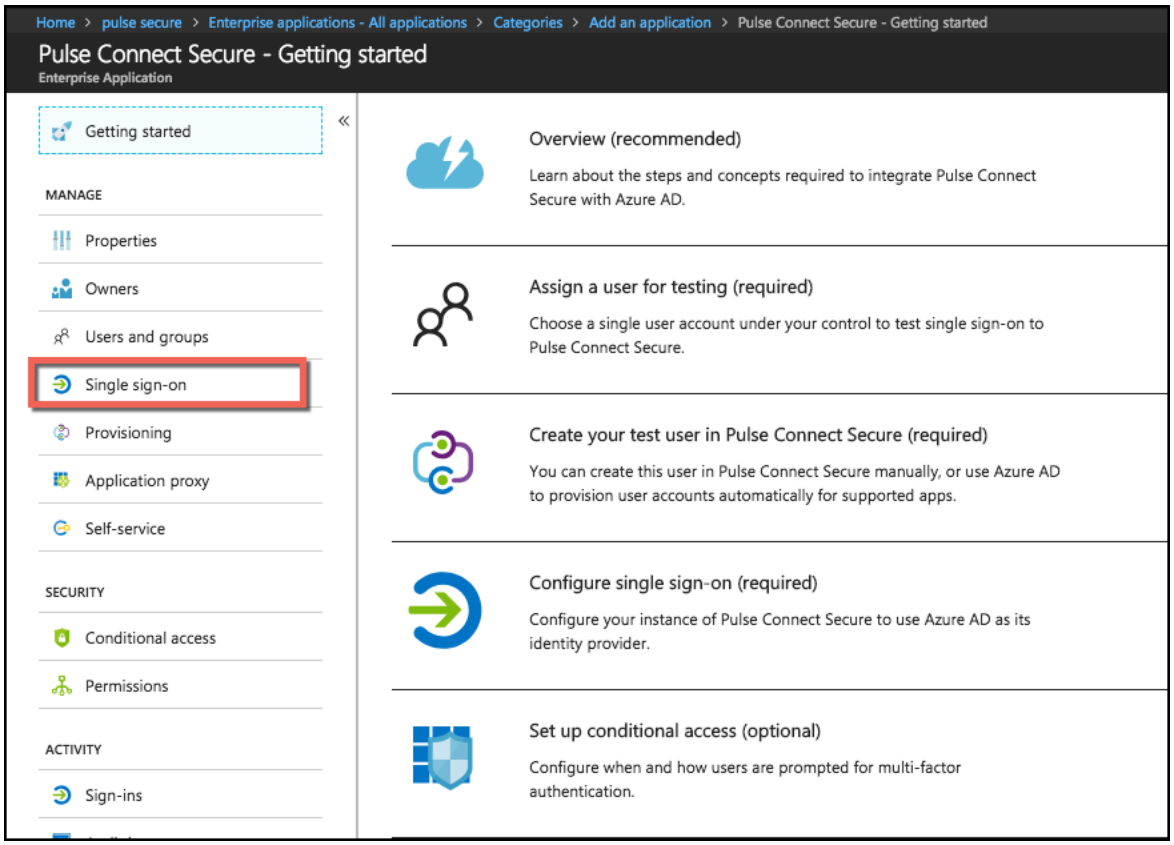


Configuring Single Sign-on Settings

After successfully configuring the enterprise application, the Getting Started page is displayed. Perform the following steps:

1. In the Getting Started page, select **Single sign-on**.

Figure 3: Azure AD - Single Sign-on settings

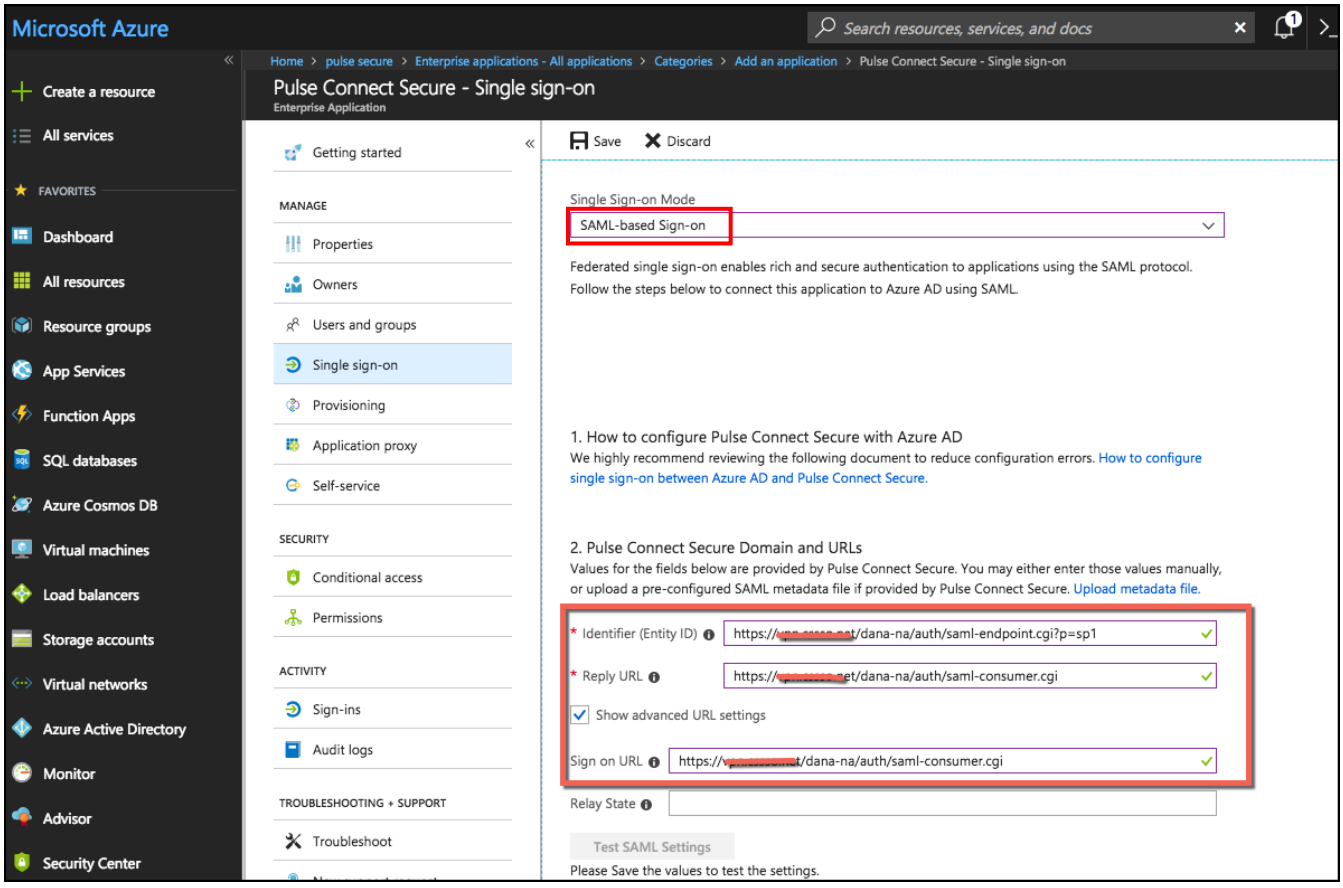


2. Select **Single sign-on Mode** as *SAML based Sign-on*.
3. The Entity ID of Pulse Connect Secure is: **https://[FQDN of PCS]/dana-na/auth/saml-endpoint.cgi?p=sp1**

NOTE: SP1 in the above Entity Id indicates that this is the first SAML Service Provider. If there are any existing SPs, then this number changes. Please check PCS configurations for exact number.

4. Reply URL of Pulse Connect Secure is **https://[FQDN of PCS]/dana-na/auth/saml-consumer.cgi**
5. Select **Show advance URL settings**.
6. Configure Sign on URL as **https://[FQDN of PCS]/dana-na/auth/saml-consumer.cgi**

Figure 4: Azure AD - Pulse Connect Secure settings

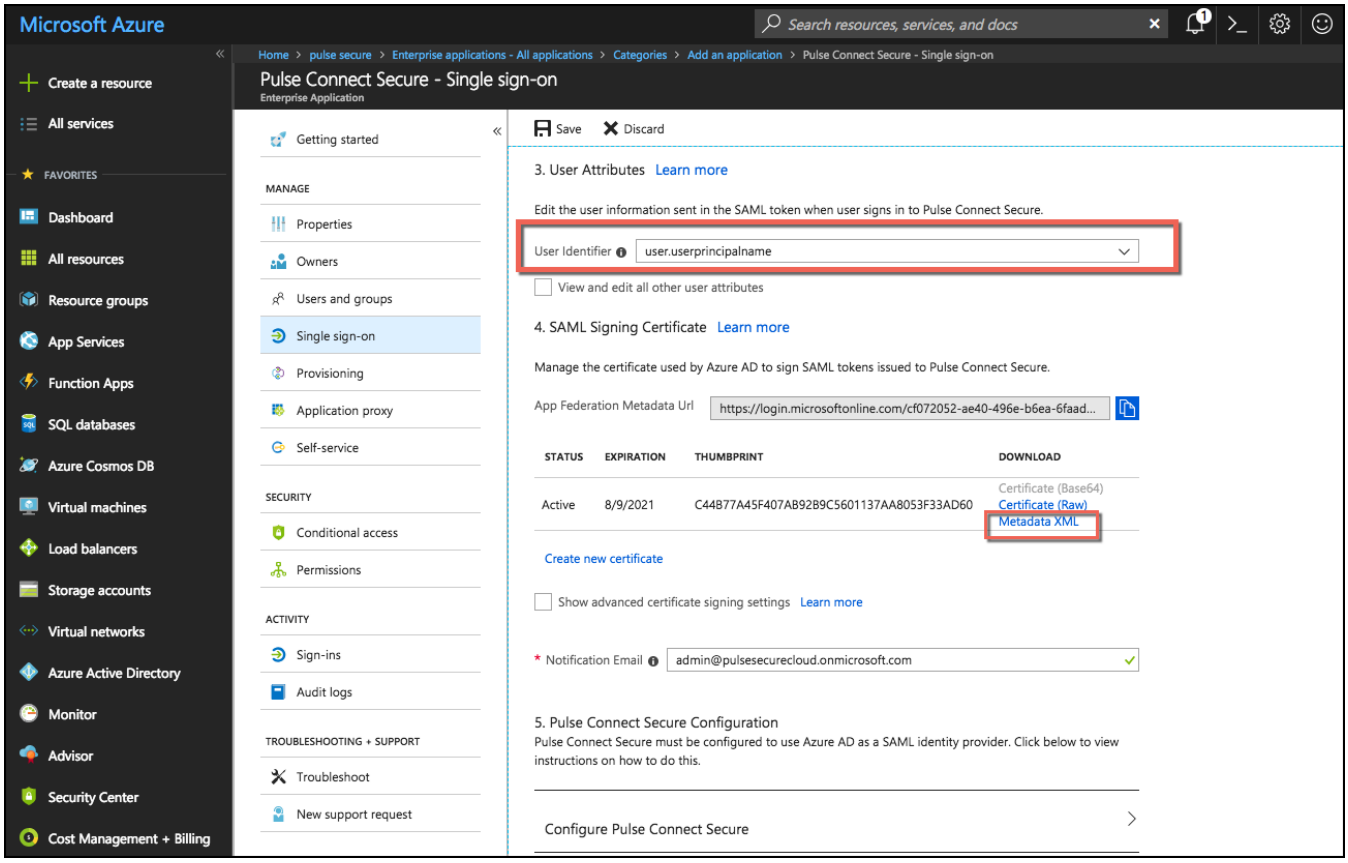


7. Select **User Identifier** from the drop-down list.

NOTE: User Identifier value is sent as Subject Name in SAML response. Please choose appropriate one of your choice.

8. Click **Metadata XML** to download Azure AD IdP metadata. This will be uploaded to Pulse Connect Secure to retrieve Azure AD SAML IdP configurations.

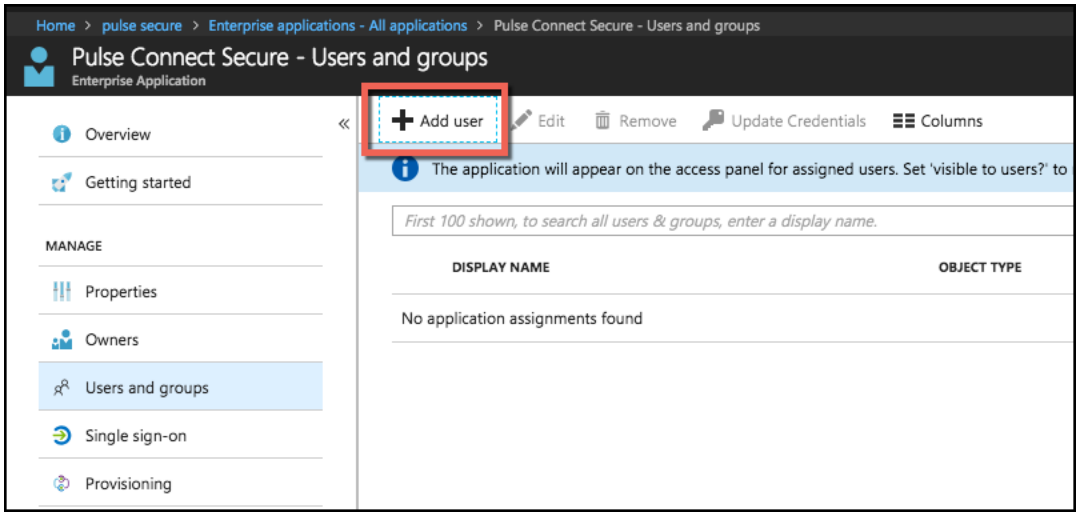
Figure 5: Azure AD - User attributes



Assigning User to Application

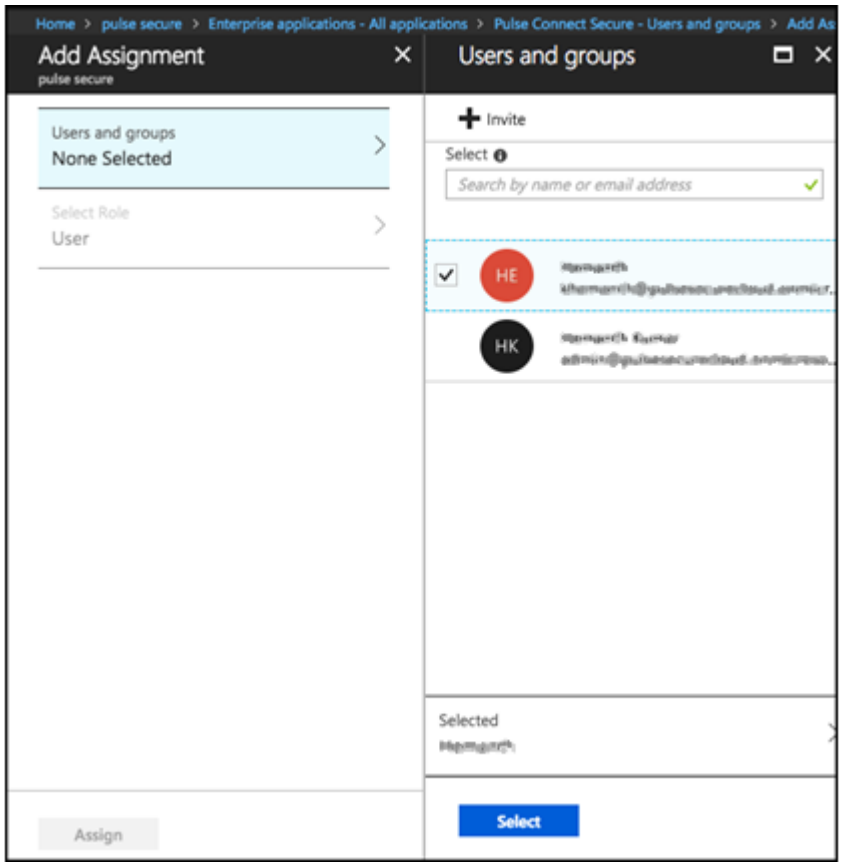
1. On the left pane, select **Users and groups**.
2. Click **Add user**.

Figure 6: Azure AD - Assign user to application



3. In the Add Assignment pane, click **Users and groups**.
4. Select the user who needs access to PCS.
5. Click **Assign**.

Figure 7: Azure AD - Select user



Pulse Connect Secure Configuration

This section covers the SAML configurations required to configure PCS as SAML SP. The other basic configurations like creating Realms and Roles are not covered.

Pulse Connect Secure configuration includes:

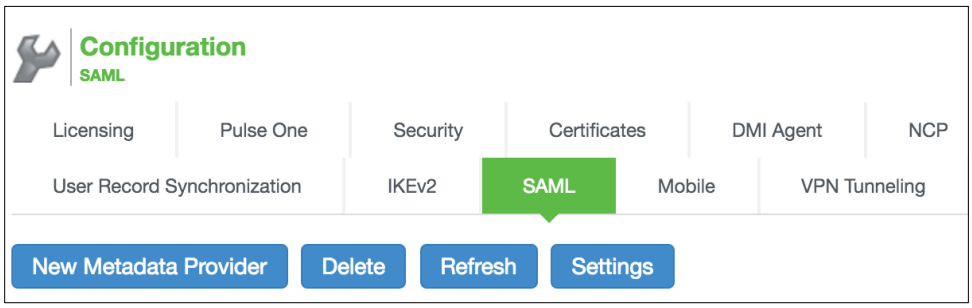
- Configuring Azure Active Directory as SAML Metadata Provider
- Configuring SAML Authentication Server
- Assigning to respective Realms and Roles

Configuring Azure Active Directory as SAML Metadata Provider

Perform the following steps:

1. Log into the Pulse Connect Secure admin console.
2. Navigate to **System > Configuration > SAML**.
3. Click **New Metadata Provider**.

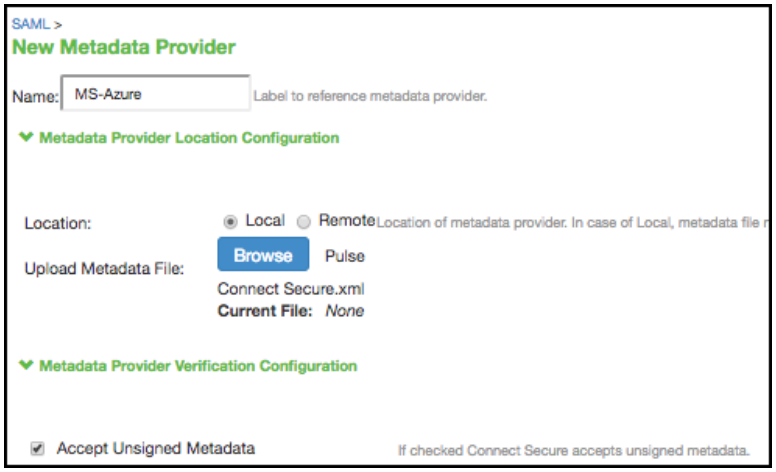
Figure 8: PCS: SAML Configuration



4. Provide a name for the new metadata provider.
5. Select **Location** as *Local*.
6. Upload Azure AD metadata file by clicking **Browse** and selecting the file.

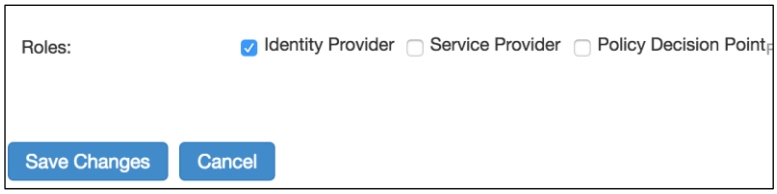
NOTE: Azure AD metadata is the XML file that should be downloaded from Azure portal. For details, see the 'Microsoft Azure AD Configurations' section above.

Figure 9: PCS: Azure AD as SAML IdP in PCS



7. Select **Accept Unsigned Metadata**.
8. Select **Roles** as *Identity Provider*.
9. Click **Save Changes**.

Figure 10: PCS: Select Identity Provider role

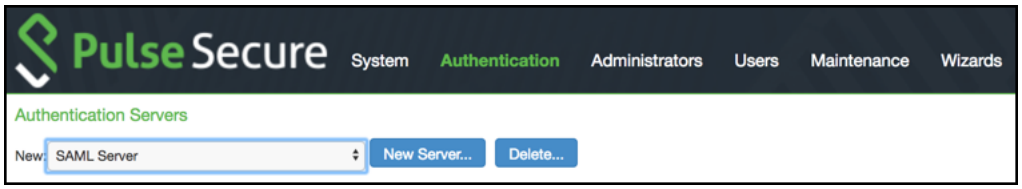


Configuring SAML Authentication Server

To create a SAML authentication server:

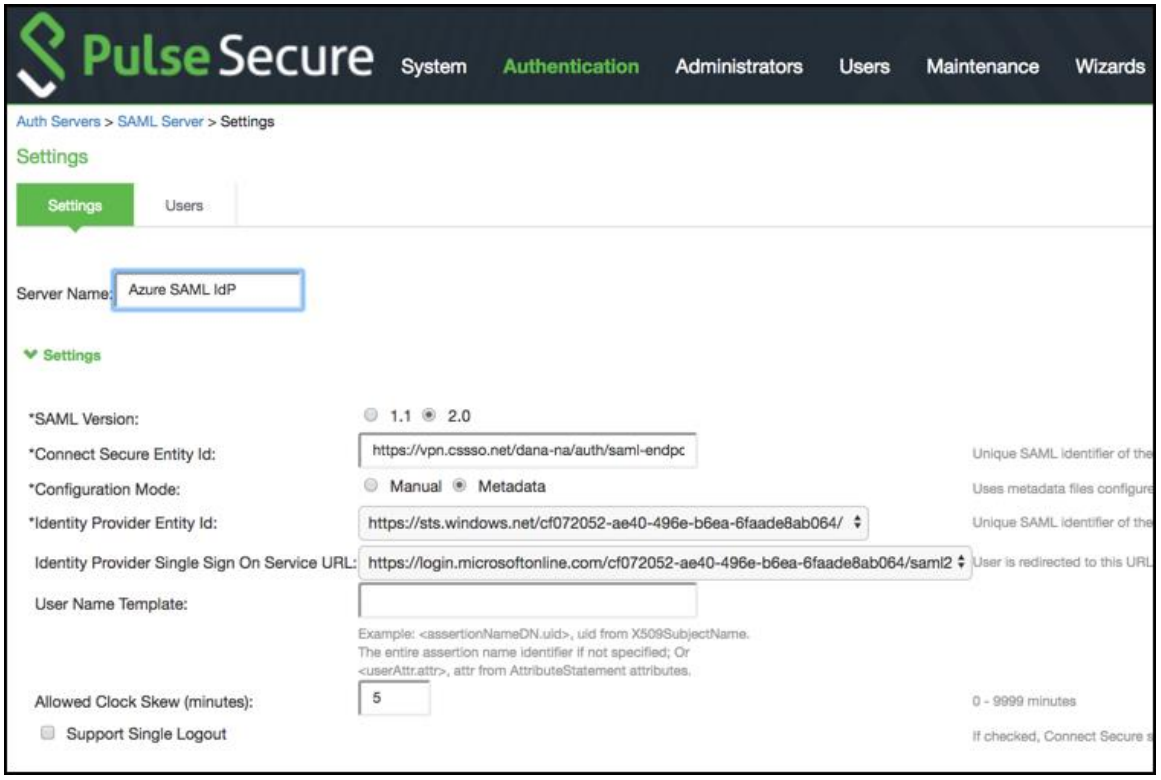
1. Navigate to **Authentication > Auth Servers**.
2. Select **New: SAML Server** and click **New Server**.

Figure 11: PCS: Authentication server selection



3. Provide **Server Name**.
4. Select **SAML Version** as *2.0,* and **Configuration Mode** as *Metadata*.
5. Select Azure AD Entity Id from the **Identity Provider Entity Id** drop-down list.

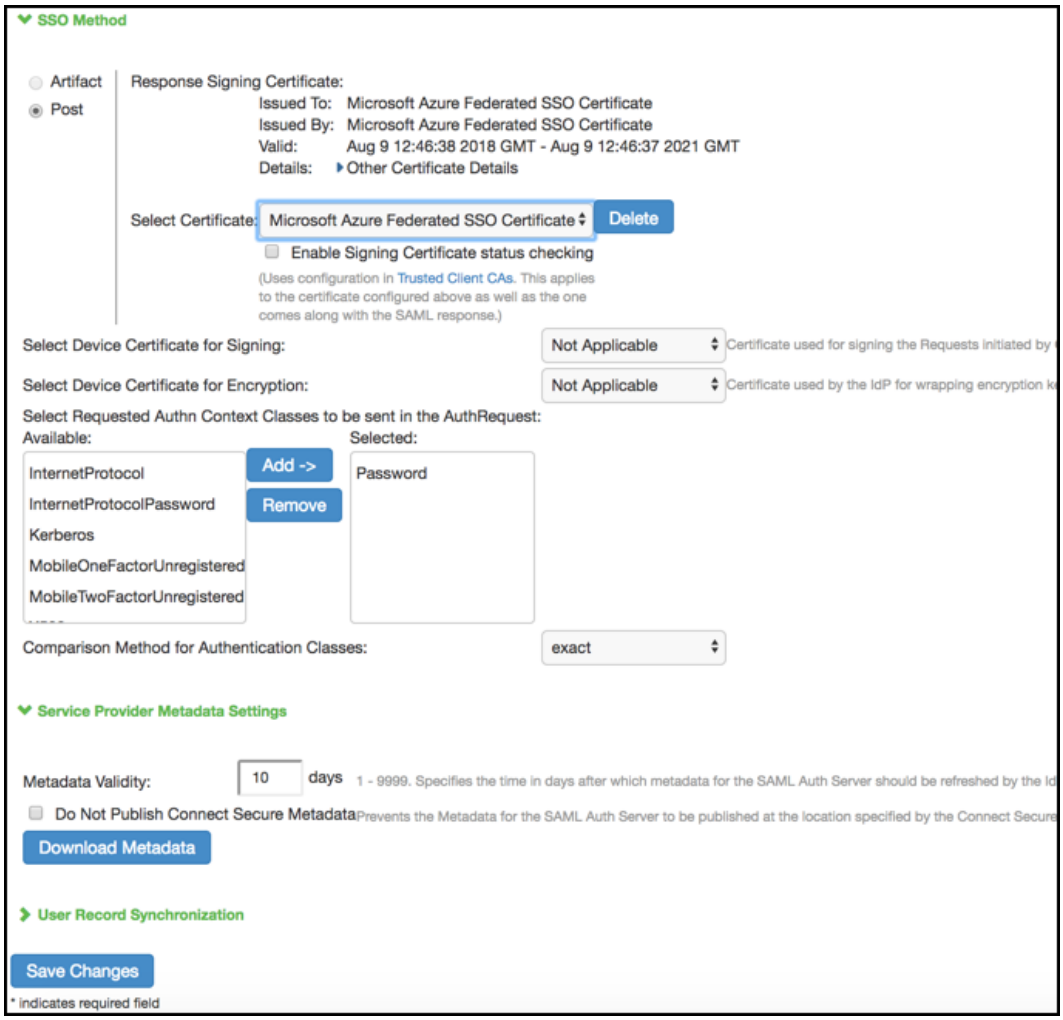
Figure 12: PCS: SAML Server settings



NOTE: Azure AD Metadata automatically sets various parameters for the SAML authentication server.

6. Single Logout is an optional setting. If this option is selected, it prompts for a new authentication after logout. If this option is not selected and you have not closed the browser, you can reconnect without authentication.
7. Select **Requested Authn Context Class** as *Password,* and **Comparison Method** as *exact*.
8. Set the **Metadata Validity** in terms of number of days.
9. Click **Save Changes**.

Figure 13: PCS: SSO Method settings



End-User Flow

Access through Browser (SP Initiated SSO)

1. Open web browser and access Pulse Connect Secure URL (Example: https://vpn.pulsesecure.net)

   It automatically redirects to Microsoft login page.
2. Provide Email Id.
3. When prompted for password, provide password.
4. Click Sign In.

   After successful authentication, user gets redirected to Pulse Connect Secure portal giving access to corporate resources.

Troubleshooting

For any issues with Pulse Connect Secure, submit a request with Pulse Secure support team and provide following PCS logs:

- Navigate to System > Log/Monitoring. Click Save All Logs and save the logs.
- Provide server debug logs with event codes “saml, auth, soap, dsdash, cloudsecure” at level 50.
- Provide Policy tracing for the specific user session with proper realm.

References

Microsoft Azure documentation: https://docs.microsoft.com/en-us/azure/

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.