`

Pulse Secure®
Acquired by Ivanti

Microsoft Azure Active Directory as SAML IdP with Pulse Connect Secure

Deployment Guide

Release	9.1R10
Document Revision	3.0
Published Date	February 2021

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

https://www.pulsesecure.net

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.

Products made or sold by Pulse Secure or components thereof might be covered by one or more of the following patents that are owned by or licensed to Pulse Secure: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

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

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 https://www.pulsesecure.net/support/EULA. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Revision History

Revision and Date	Added/Updated /Removed	Remarks
3.0, February 2021	Updated	Updated the document with the latest MS Azure navigation
2.0, February 2019	Updated	Updated the document with the latest MS Azure navigation
1.0, May 2018	Initial release	

Table of Contents

Revision History....3
Introduction....6
Prerequisites....6
Configurations....6
Microsoft Azure Active Directory Configuration....6
    Setting Up PCS as Enterprise Application....6
    Configuring Single Sign-on Settings....9
    Assigning User to Application....11
Pulse Connect Secure Configuration....13
    Configuring Azure Active Directory as SAML Metadata Provider....13
    Configuring SAML Authentication Server....15
End-User Flow....17
    Access through Browser (SP Initiated SSO)....17
Troubleshooting....17
References....18
Requesting Technical Support....18

List of Figures

Figure 1: Azure Services - Enterprise applications 6
Figure 2: Azure AD - Enterprise applications 7
Figure 3: Azure AD - Select Pulse Secure Application 7
Figure 4: Azure AD – Create Pulse Secure Application 8
Figure 5: Azure AD - Single Sign-on settings 9
Figure 6: Single Sign-on method 9
Figure 6: Azure AD - Pulse Connect Secure settings 10
Figure 7: Azure AD - User attributes 11
Figure 8: Azure AD - Assign user to application 11
Figure 9: Azure AD - Add user 12
Figure 10: PCS: SAML Configuration 13
Figure 11: PCS: Azure AD as SAML IdP in PCS 14
Figure 12: PCS: Select Identity Provider role 14
Figure 13: PCS: Authentication server selection 15
Figure 14: PCS: SAML Server settings 15
Figure 15: PCS: SSO Method settings 16

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:

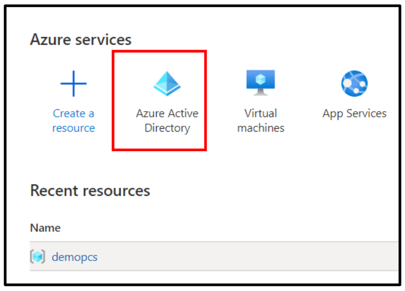
- Setting Up PCS as Enterprise Application
- Configuring Single Sign-on Settings
- Assigning User to Application

Setting Up PCS as Enterprise Application

Perform the following steps:

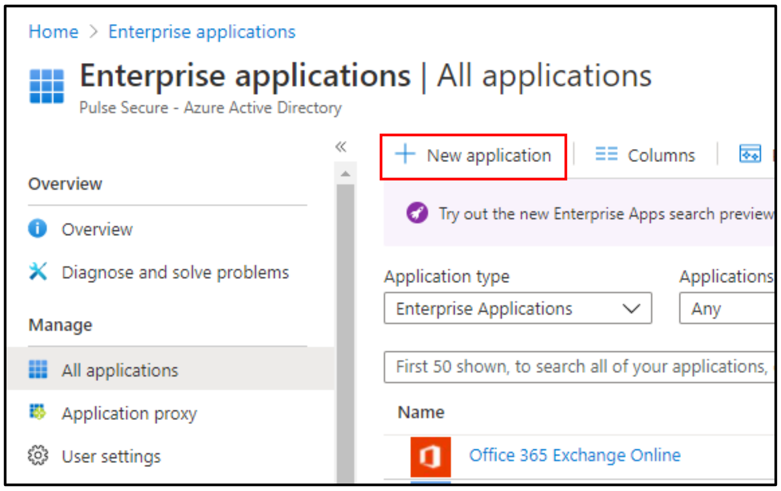
1. Log into the [Azure Management Portal].
2. On the Azure Services page, select **Azure Active Directory**.

Figure 1: Azure Services - Enterprise applications



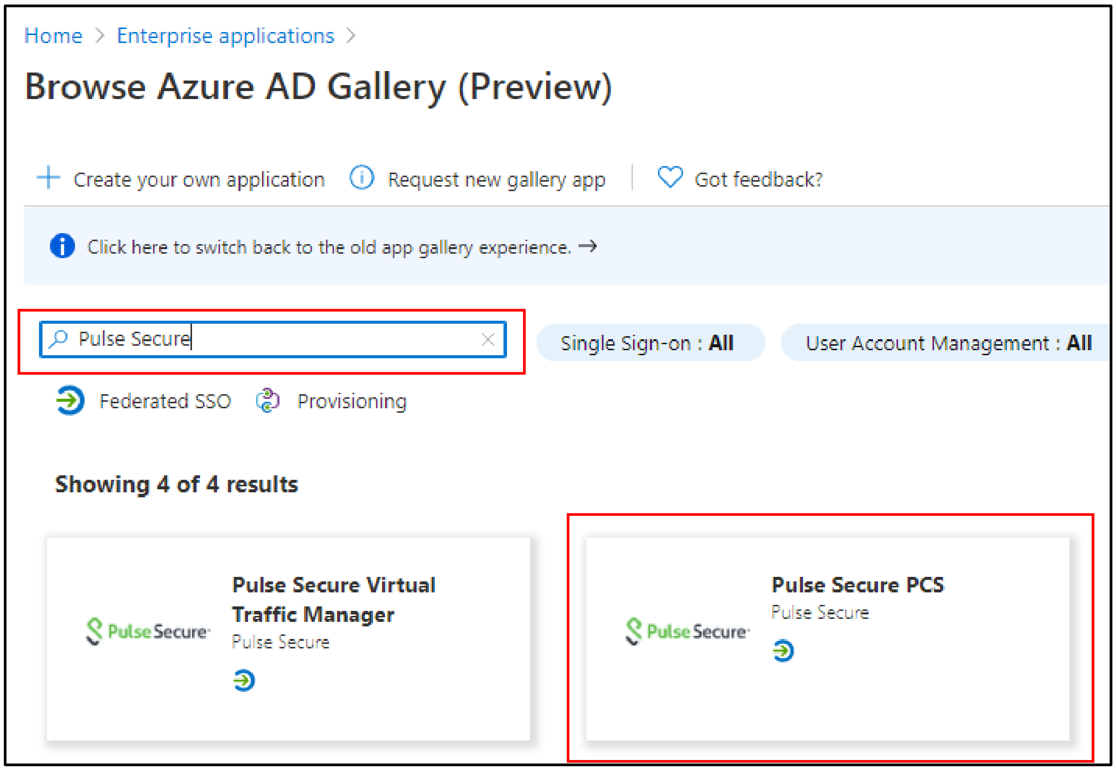
3. On the left pane, select **Enterprise applications**.
4. In the Enterprise applications page, click **New application**.

Figure 2: Azure AD - Enterprise applications


Home > Enterprise applications
Enterprise applications | All applications
Pulse Secure - Azure Active Directory
New application
Columns
Try out the new Enterprise Apps search preview
Overview
Overview
Diagnose and solve problems
Manage
All applications
Application proxy
User settings
Application type
Enterprise Applications
Applications
Any
First 50 shown, to search all of your applications,
Name
Office 365 Exchange Online

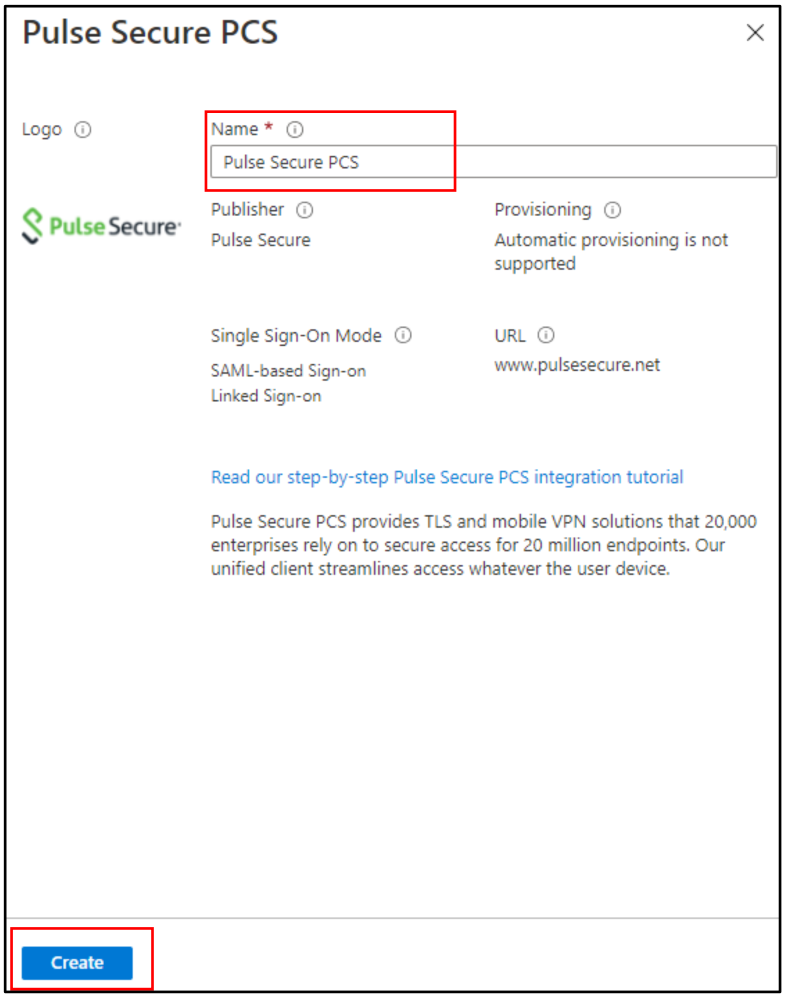
5. In the Browse Azure AD Gallery page, search with keyword **Pulse Secure**, and then select **Pulse Secure PCS** from the search result.

Figure 3: Azure AD - Select Pulse Secure Application


Home > Enterprise applications >
Browse Azure AD Gallery (Preview)
Create your own application
Request new gallery app
Got feedback?
Click here to switch back to the old app gallery experience. →
Pulse Secure
Single Sign-on : All
User Account Management : All
Federated SSO
Provisioning
Showing 4 of 4 results
Pulse Secure Virtual Traffic Manager
Pulse Secure
Pulse Secure PCS
Pulse Secure

6. In the window that is displayed, enter a unique name, and click **Create**.

Figure 4: Azure AD – Create Pulse Secure Application



Pulse Secure PCS

Logo ⓘ

Name * ⓘ

Pulse Secure PCS

Publisher ⓘ

Pulse Secure

Provisioning ⓘ

Automatic provisioning is not supported

Single Sign-On Mode ⓘ

SAML-based Sign-on
Linked Sign-on

URL ⓘ

www.pulsesecure.net

Read our step-by-step Pulse Secure PCS integration tutorial

Pulse Secure PCS provides TLS and mobile VPN solutions that 20,000 enterprises rely on to secure access for 20 million endpoints. Our unified client streamlines access whatever the user device.

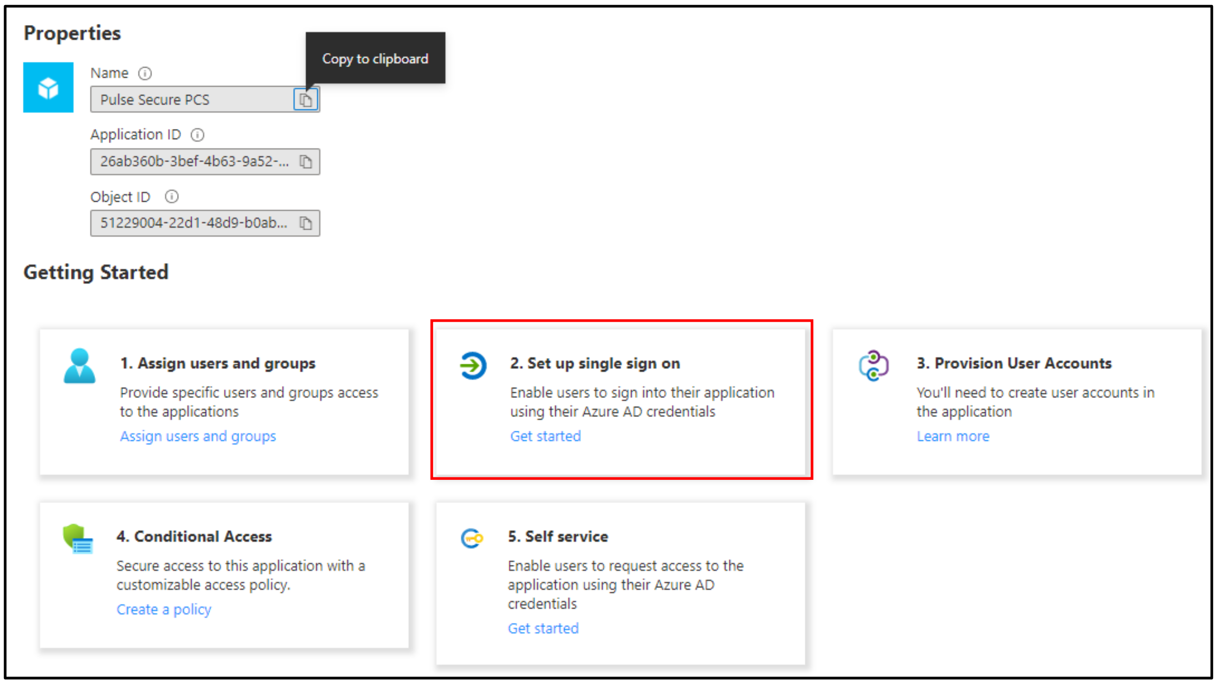
This completes setting up of enterprise application.

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 5: Azure AD - Single Sign-on settings



Properties

Name: Pulse Secure PCS

Application ID: 26ab360b-3bef-4b63-9a52-...

Object ID: 51229004-22d1-48d9-b0ab...

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started

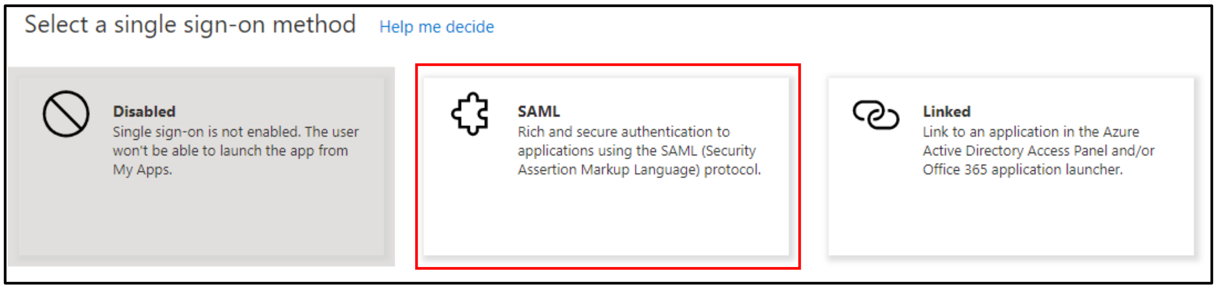
3. Provision User Accounts
You'll need to create user accounts in the application
Learn more

4. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

5. Self service
Enable users to request access to the application using their Azure AD credentials
Get started

2. Select **Single sign-on method** as **SAML**.

Figure 6: Single Sign-on method



Select a single sign-on method Help me decide

Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

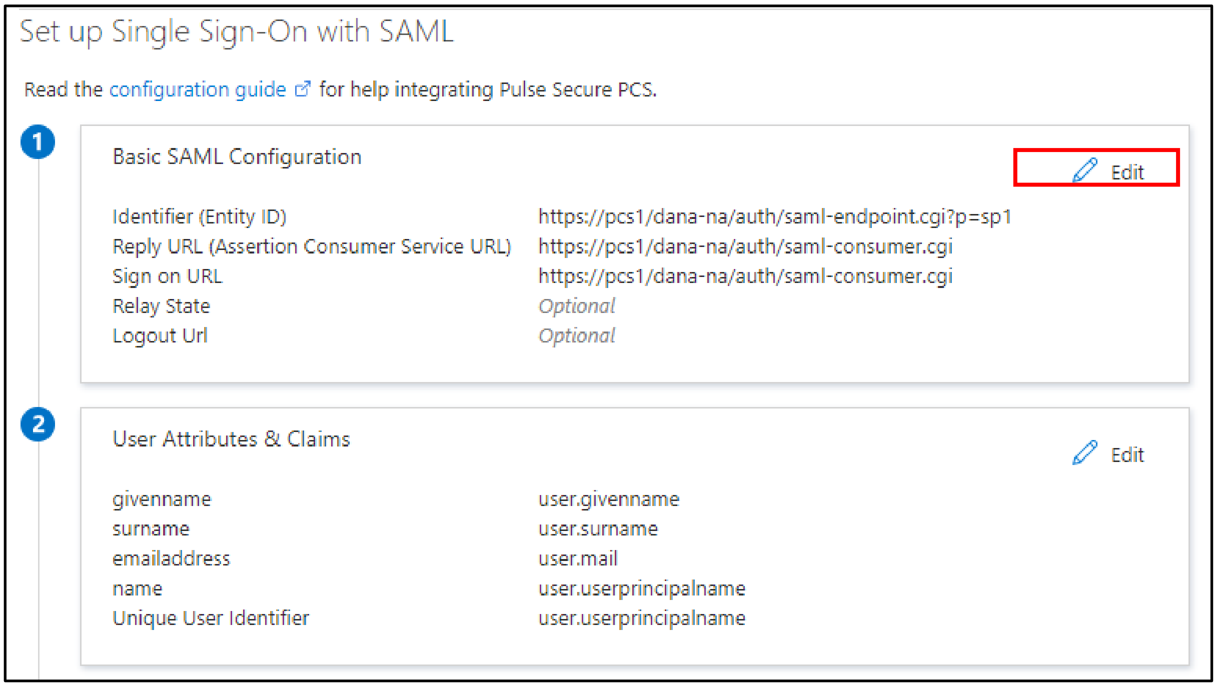
Linked
Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.

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. Configure Sign on URL as **https://[FQDN of PCS]/dana-na/auth/saml-consumer.cgi**

Figure 7: Azure AD - Pulse Connect Secure settings



Set up Single Sign-On with SAML

Read the configuration guide for help integrating Pulse Secure PCS.

1 Basic SAML Configuration

Identifier (Entity ID)	https://pcs1/dana-na/auth/saml-endpoint.cgi?p=sp1
Reply URL (Assertion Consumer Service URL)	https://pcs1/dana-na/auth/saml-consumer.cgi
Sign on URL	https://pcs1/dana-na/auth/saml-consumer.cgi
Relay State	*Optional*
Logout Url	*Optional*

2 User Attributes & Claims

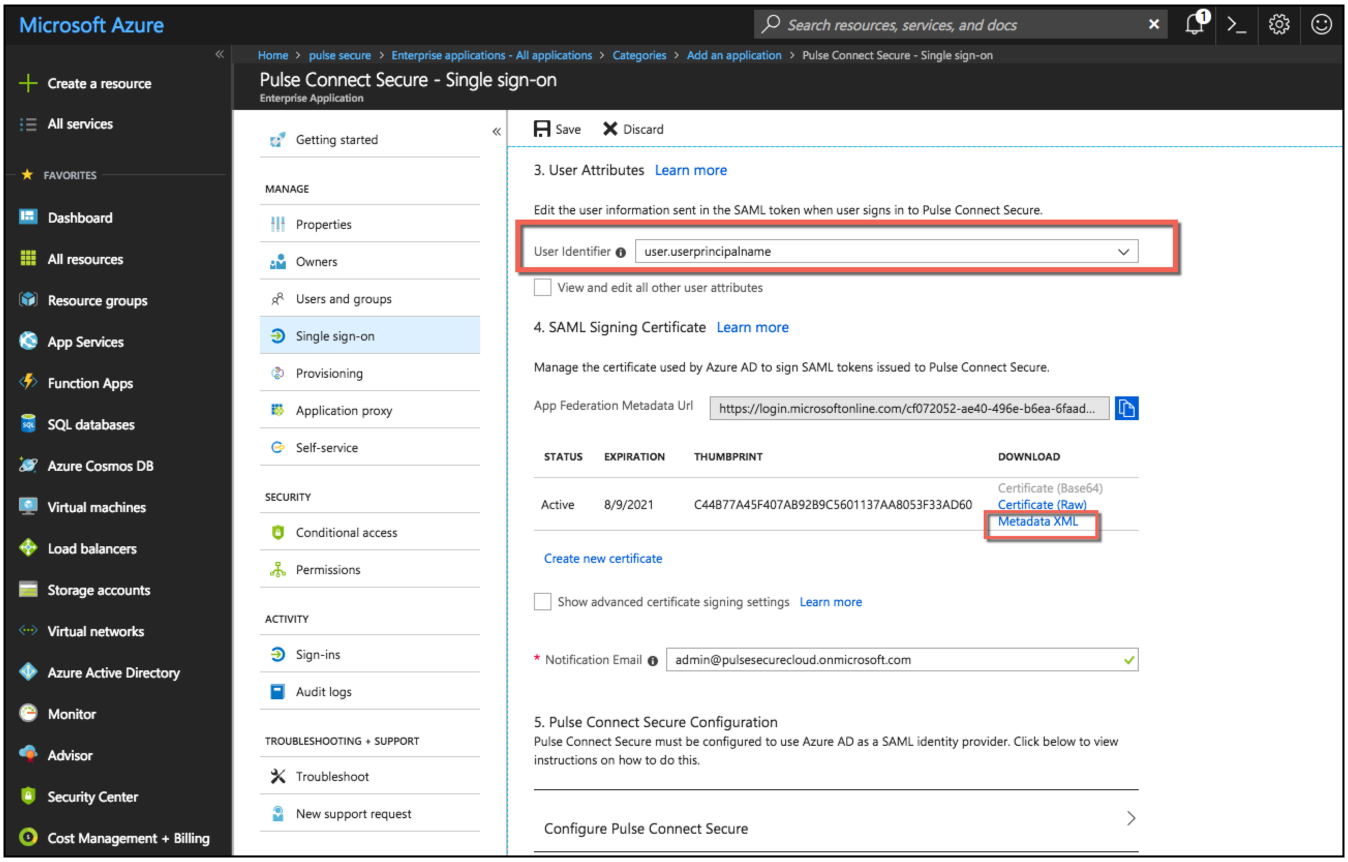
givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

6. 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.

7. 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 8: Azure AD - User attributes



3. User Attributes Learn more

Edit the user information sent in the SAML token when user signs in to Pulse Connect Secure.

User Identifier: user.userprincipalname

□ View and edit all other user attributes

4. SAML Signing Certificate Learn more

Manage the certificate used by Azure AD to sign SAML tokens issued to Pulse Connect Secure.

App Federation Metadata Url: https://login.microsoftonline.com/cf072052-ae40-496e-b6ea-6faad...

STATUS	EXPIRATION	THUMBPRINT	DOWNLOAD
Active	8/9/2021	C44B77A45F407AB92B9C5601137AA8053F33AD60	Certificate (Base64) Certificate (Raw) Metadata XML

Create new certificate

□ Show advanced certificate signing settings Learn more

* Notification Email: admin@pulsesecurecloud.onmicrosoft.com

5. Pulse Connect Secure Configuration

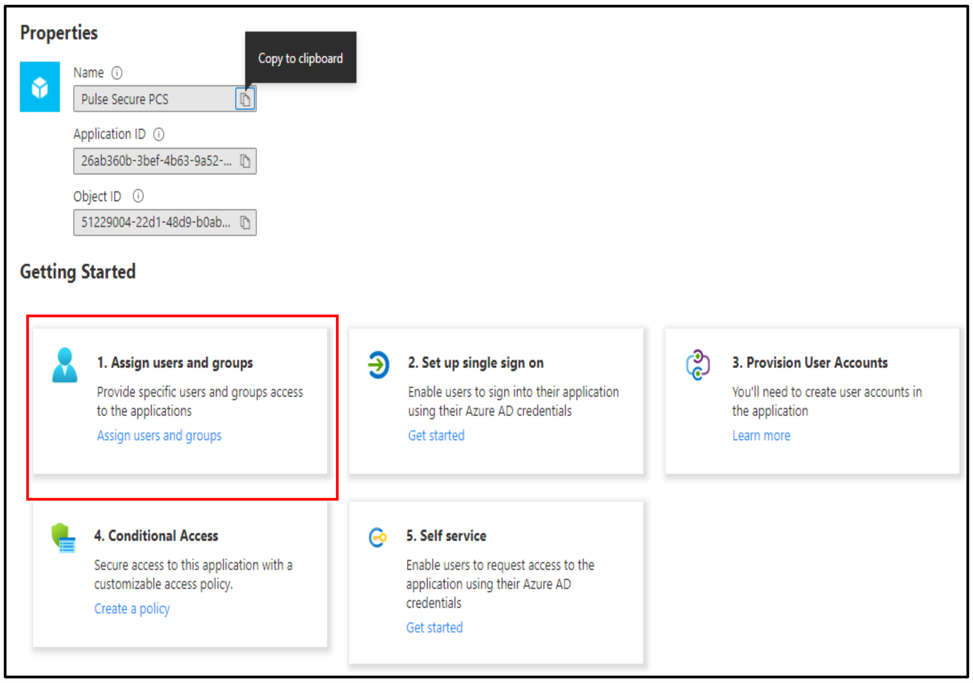
Pulse Connect Secure must be configured to use Azure AD as a SAML identity provider. Click below to view instructions on how to do this.

Configure Pulse Connect Secure

Assigning User to Application

1. In the Getting Starting page, select **Assign users and groups**.

Figure 9: Azure AD - Assign user to application



Properties

Name: Pulse Secure PCS

Application ID: 26ab360b-3bef-4b63-9a52-...

Object ID: 51229004-22d1-48d9-b0ab...

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started

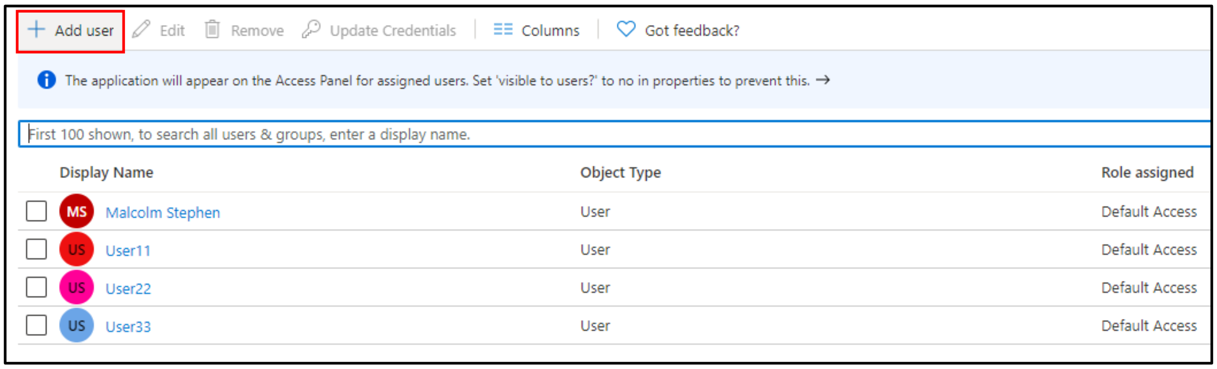
3. Provision User Accounts
You'll need to create user accounts in the application
Learn more

4. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

5. Self service
Enable users to request access to the application using their Azure AD credentials
Get started

2. Select the user who needs access to PCS.
3. Click Add User.

Figure 10: Azure AD - Add user

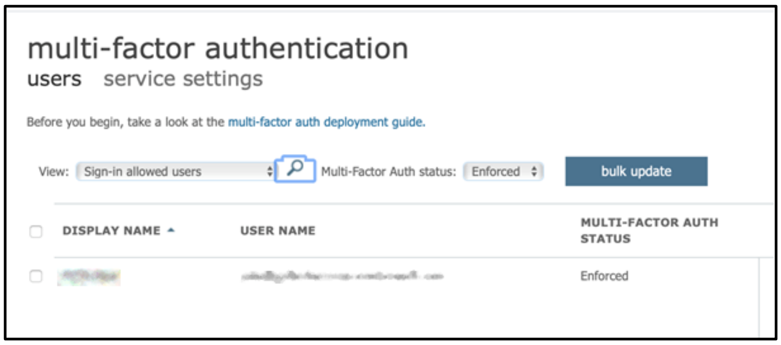


The application will appear on the Access Panel for assigned users. Set 'visible to users?' to no in properties to prevent this. →

First 100 shown, to search all users & groups, enter a display name.

	Display Name	Object Type	Role assigned
□	MS Malcolm Stephen	User	Default Access
□	US User11	User	Default Access
□	US User22	User	Default Access
□	US User33	User	Default Access

4. Microsoft MFA is then set on the user in Azure AD.



multi-factor authentication

Before you begin, take a look at the multi-factor auth deployment guide.

View: Sign-in allowed users

Multi-Factor Auth status: Enforced

□	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
□	[redacted]	[redacted]	Enforced

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:

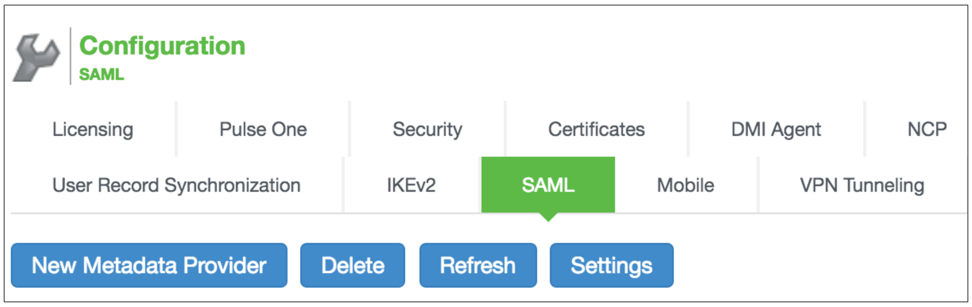
- Configuring Azure Active Directory as SAML Metadata Provider
- Configuring SAML Authentication Server

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.

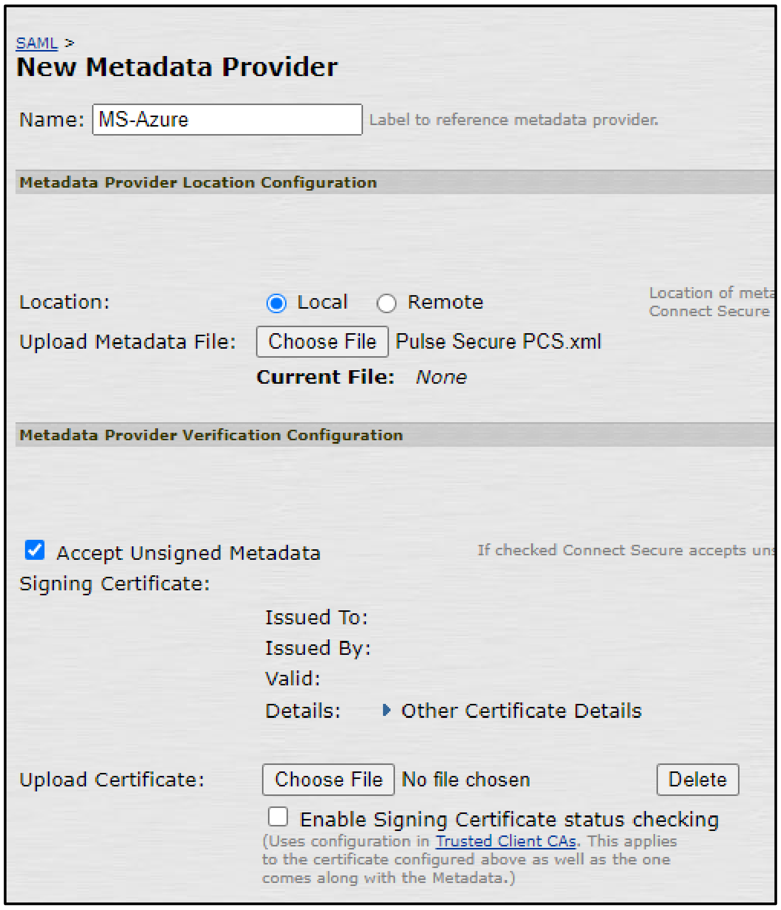
Figure 11: PCS: SAML Configuration



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 12: PCS: Azure AD as SAML IdP in PCS



SAML >

New Metadata Provider

Name: MS-Azure Label to reference metadata provider.

Metadata Provider Location Configuration

Location: ● Local ○ Remote Location of meta Connect Secure

Upload Metadata File: Choose File Pulse Secure PCS.xml

Current File: *None*

Metadata Provider Verification Configuration

☑ Accept Unsigned Metadata If checked Connect Secure accepts un

Signing Certificate:

Issued To:

Issued By:

Valid:

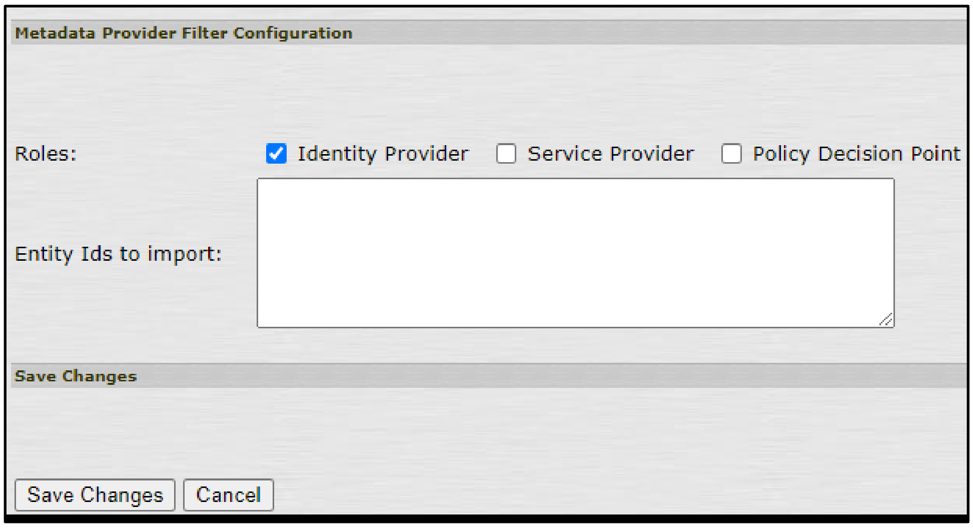
Details: ▸ Other Certificate Details

Upload Certificate: Choose File No file chosen 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 Metadata.)

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

Figure 13: PCS: Select Identity Provider role



Metadata Provider Filter Configuration

Roles: ☑ Identity Provider □ Service Provider □ Policy Decision Point

Entity Ids to import:

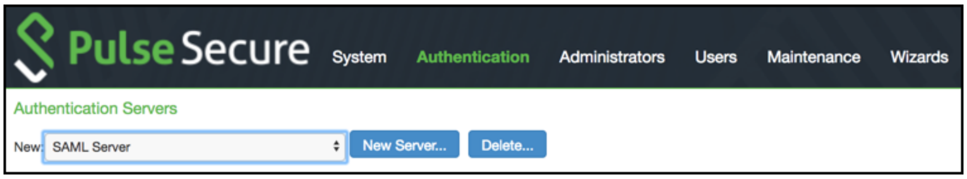
Save Changes

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 14: PCS: Authentication server selection

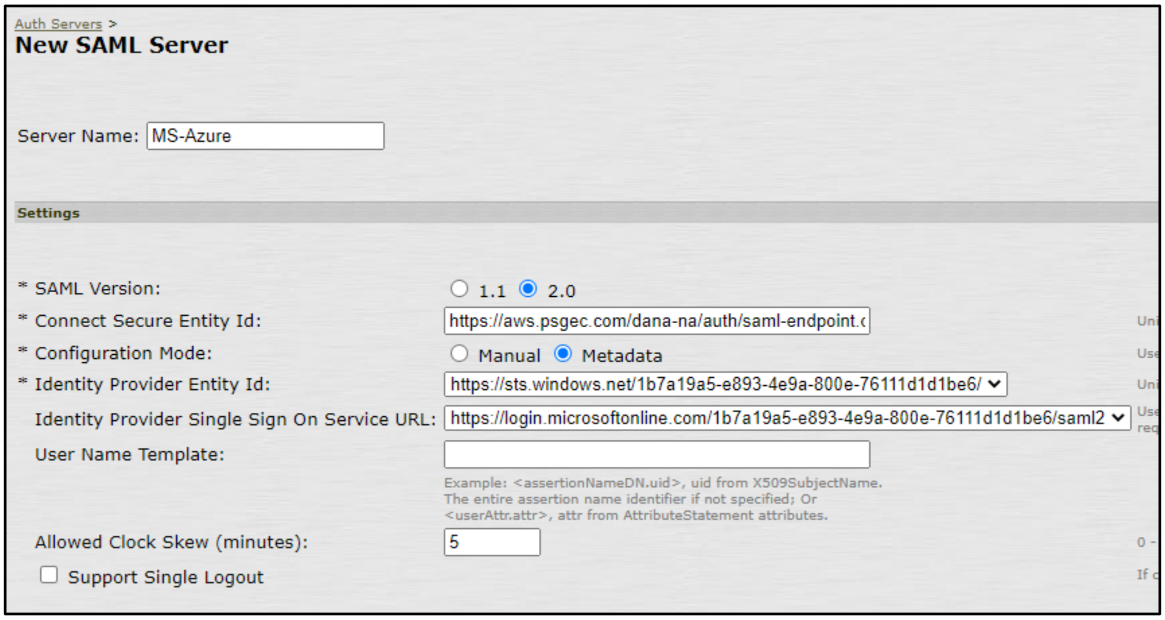


Authentication Servers

New: SAML Server

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 15: PCS: SAML Server settings



New SAML Server

Server Name: MS-Azure

Settings

* SAML Version: ○ 1.1 ● 2.0

* Connect Secure Entity Id: https://aws.psgec.com/dana-na/auth/saml-endpoint.c

* Configuration Mode: ○ Manual ● Metadata

* Identity Provider Entity Id: https://sts.windows.net/1b7a19a5-e893-4e9a-800e-76111d1d1be6/

Identity Provider Single Sign On Service URL: https://login.microsoftonline.com/1b7a19a5-e893-4e9a-800e-76111d1d1be6/saml2

User Name Template:

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

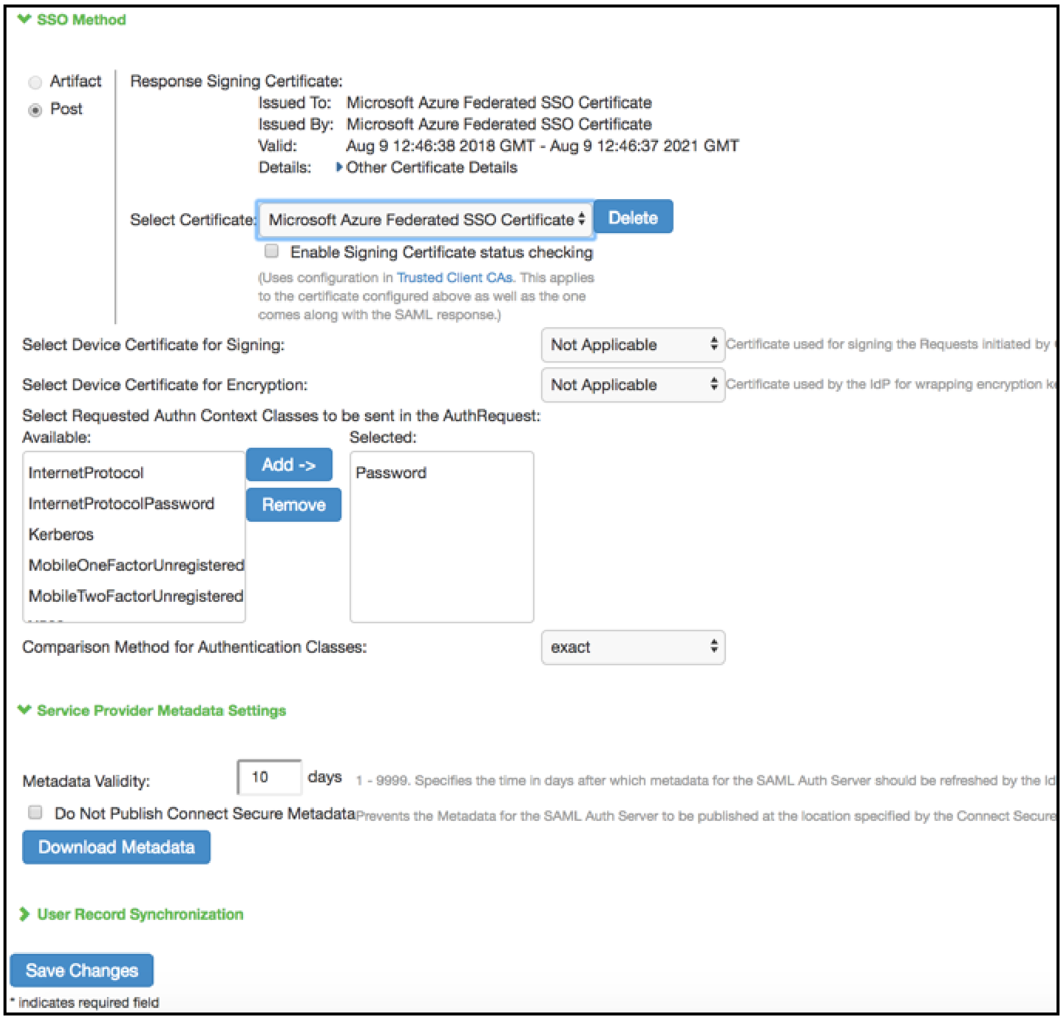
Allowed Clock Skew (minutes): 5

□ Support Single Logout

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 16: PCS: SSO Method settings



SSO Method

○ Artifact
● Post

Response Signing Certificate:
Issued To: Microsoft Azure Federated SSO Certificate
Issued By: Microsoft Azure Federated SSO Certificate
Valid: Aug 9 12:46:38 2018 GMT - Aug 9 12:46:37 2021 GMT
Details: Other Certificate Details

Select Certificate: Microsoft Azure Federated SSO Certificate

□ 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: Not Applicable — Certificate used for signing the Requests initiated by

Select Device Certificate for Encryption: Not Applicable — Certificate used by the IdP for wrapping encryption k

Select Requested Authn Context Classes to be sent in the AuthRequest:

Available:
InternetProtocol
InternetProtocolPassword
Kerberos
MobileOneFactorUnregistered
MobileTwoFactorUnregistered

Selected:
Password

Comparison Method for Authentication Classes: exact

Service Provider Metadata Settings

Metadata Validity: 10 days 1 - 9999. Specifies the time in days after which metadata for the SAML Auth Server should be refreshed by the Id

□ 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

* indicates required field

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.