Pulse Secure®

Cloud Secure Integration with ADFS

Deployment Guide

Document Revisions	2.0
Published Date	DECEMBER 2018

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

http://www.pulsesecure.net

Cloud Secure Integration with ADFS 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").By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

Introduction

About this guide

This document outlines the Cloud Secure integration with Microsoft's Active Directory Federation Services (ADFS). The guide explains the configuration required to setup Cloud Secure as a third-party Identity Provider (IdP) with ADFS. It is assumed that Office 365 is already configured as an IdP in ADFS.

To configure Office 365 to authenticate directly with Cloud Secure, refer to Cloud Secure Microsoft Office 365 guide which explains the configuration and benefits of using Cloud Secure as standalone IdP.

Overview

Cloud Secure provides secure access to anyone, anytime on a hybrid IT environment where enterprise companies are combining the best of the cloud with their own localized data centers.

Cloud Secure uses Security Assertion Markup Language (SAML) for exchange of authentication between client devices (Windows, MacOS, iOS, Android), Service Providers (Cloud applications like Office 365, Salesforce etc.) and Identity Providers (Pulse Connect Secure) to provide Single-Sign on access seamlessly to applications. In addition, Cloud Secure provides a greater level of flexibility with integration to many third-party IdP's like PingOne, OKTA, and Active Directory Federation Services (ADFS) for seamless migration of existing customers.

Cloud Secure ADFS Integration

Pulse Secure's Cloud Secure solution is capable of providing authentication as well as secure single sign-on to Office 365 services as a standalone Identity Provider. Most of the companies who are using Office 365 have also implemented Active Directory Federation Services (ADFS) for authentication.

Note: In many cases, it would not be feasible for a company that has already deployed ADFS as their Identity Provider to change their Office 365 configuration.

The deployment discussed in the guide explores an alternative approach called IdP chaining, where Cloud Secure (PCS) acts as IdP for ADFS and handles all the authentication requests. This helps the customer to get the benefits of Cloud Secure such as compliance checks, secure single sign-on through VPN tunneling without making major changes to the existing setup. Pulse Connect Secure (PCS) is used as Identity Provider in Cloud Secure solution.

Deployment Scenarios

ADFS allows Pulse Connect Secure (PCS) to be configured as Third-Party Identity Provider and redirects all the SAML Authentication requests from Service Providers (SP) to PCS and vice-versa.
In this deployment scenario,

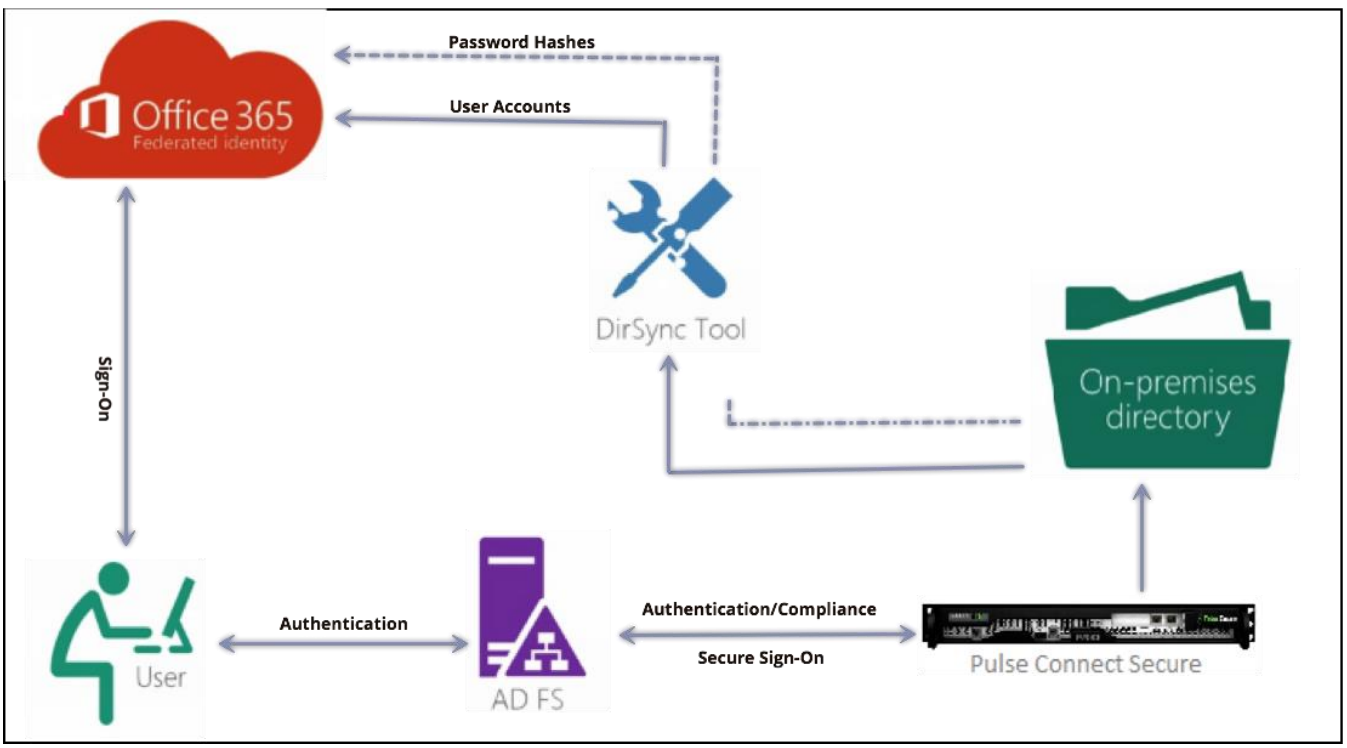
- ADFS is configured as Service Provider (SP) in PCS
- PCS is configured as claims provider in ADFS
- ADFS is configured as Identity Provider in SP

Cloud Secure integration with ADFS supports both SP initiated and IdP initiated SSO.

Office 365 access through applications (SP Initiated SSO)

When a user tries to access cloud service, the SAML enabled Service Provider generates SAML request and redirects it to ADFS. ADFS in turn redirects the incoming SAML authentication requests to PCS. PCS authenticates the user, and generates SAML AuthNResponse after compliance posture assessments. ADFS relays the response to Service provider thus providing access to the cloud resource

Figure 1 Deployment Diagram: Cloud Secure ADFS Integration – SP Initiated



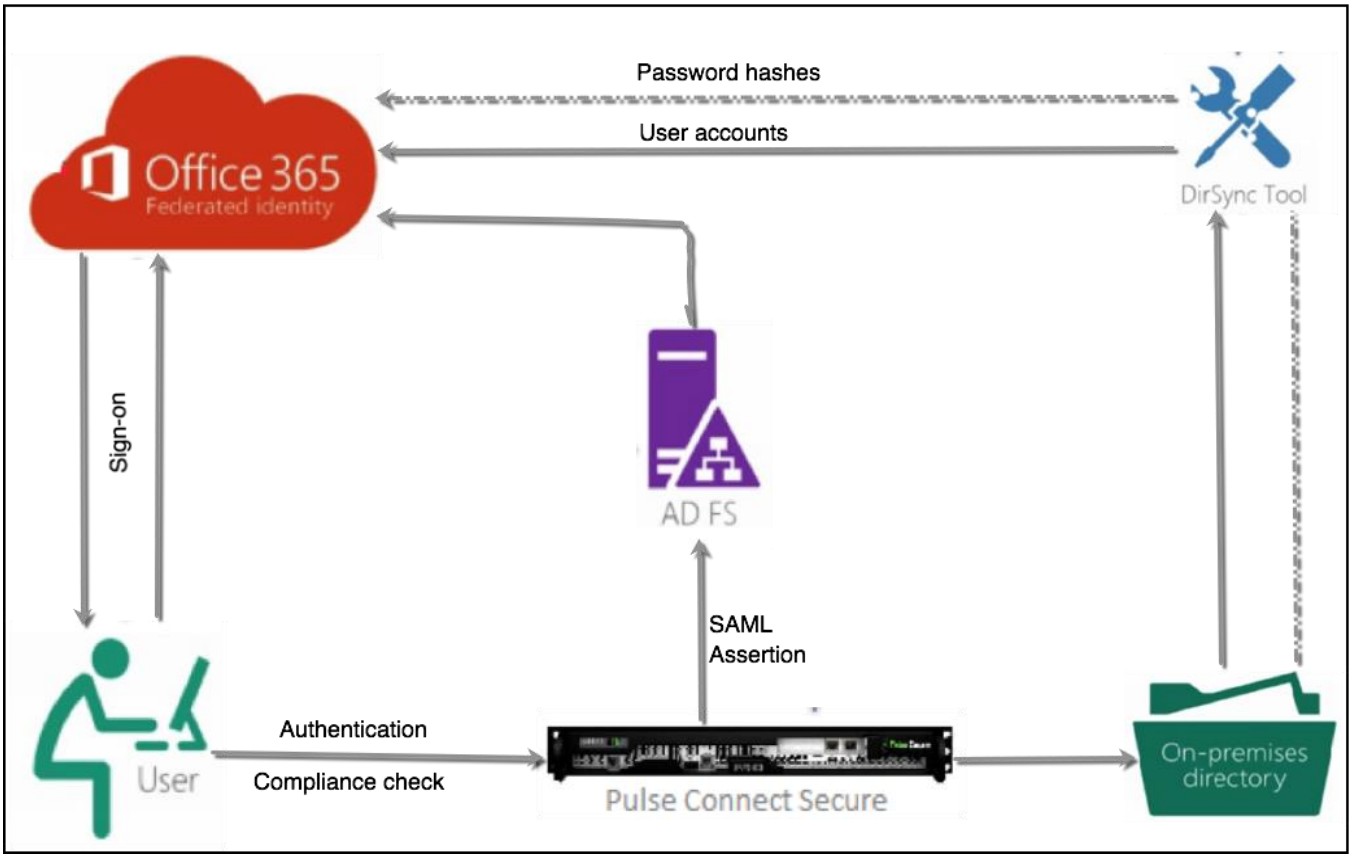
Note: If the client has an existing VPN connection to PCS, then the same session will be reused and provides seamless SSO without asking for credentials

MobileIron and AirWatch Third-party MDM servers can also be used in this solution to manage devices and to evaluate compliance posture of the mobile devices

Office 365 access through bookmark (IdP Initiated SSO)

In IdP Initiated Single Sign-on, user first logs into PCS through browser. After authentication and compliance posture assessments, PCS shows up the browser page with all the configured bookmarks. When the user access the Office 365 bookmark, PCS generates the SAML assertion and relays it to ADFS. ADFS again relays the Assertion to Office 365 and provides seamless access to cloud resource

Figure 2 Deployment Diagram: Cloud Secure ADFS Integration – IdP Initiated



Note: Cloud Secure ADFS integration solution works well with all Service Providers (like Salesforce, Zendesk etc.,), provided the SPs should be configured as Relying Party Trusts in ADFS

Pre-requisites

Prerequisites for this solution include:

- Identity Management Provider: Active Directory Federation Services (ADFS)
- Service Provider (Office 365): Office 365 Subscription. Office 365 Service Provider should be configured as Relying Party Trust in ADFS and ADFS is configured as Identity Provider in Office365 SP
- Wildcard or SAN Certificates: Wildcard or Subject Alternative Name (SAN) Certificates are required. SAN certificate should include the fqdn of PCS as well as ADFS.
- AD/LDAP Server: AD/LDAP with directory synchronization enabled
- Clients: iOS Device/ Android Device/ Windows/ MAC OS X Desktops
- (Optional) MDM Servers: Pulse Workspace Server/ MobileIron/ AirWatch servers are used for Mobile Device Management and Mobile Compliance posture assessments

Limitations

- Email Access through Native Email Client in iOS and GMAIL in Android are yet to be validated

Supported Platforms

- Browsers (Chrome, Safari, Firefox, Internet Explorer)
- Microsoft Outlook 2016 on desktops and mobiles
- Microsoft Outlook 2013 with a registry update
- Microsoft applications (Word, PowerPoint, Excel) on desktops and mobiles

End-User Flow

Sign-in experience for end user is different based on his location and the device used to access Office 365 services.

Access through Outlook client (SP Initiated SSO)

Cloud Secure requires Microsoft Office 2013 or 2016 client for providing SSO access to emails through modern authentication. In Office 2016 client, Microsoft has added support for modern authentication (for doing web browser SSO) and is enabled by default. Earlier versions of outlook client support only ECP profile for SAML exchanges.

Follow below steps to enable modern authentication in Office 2013 clients on Windows platform:

1. Update Office 2013 client to obtain the update that includes the new Azure Active Directory Authentication Libraries (ADAL) based authentication features.
2. Set the following registry keys.

Registry Key	Type	Value
HKCU\SOFTWARE\Microsoft\Office\15.0\Common\Identity\EnableADAL	REG_DWORD	1
HKCU\SOFTWARE\Microsoft\Office\15.0\Common\Identity\Version	REG_DWORD	1

Note: End-Users are usually not recommended to change the registry settings

Below steps need to be performed once for setting up Outlook client to access emails:

1. Add email account in Outlook client by navigating to File > Add Account (in Windows) or Tools > Accounts (in MAC). Provide only the name and email address (without password) and click Next. In latest version of Outlook client, provide only Email address
2. Outlook client starts searching for server settings and once the details are obtained, new browser windows is opened and gets redirected to PCS login page.
3. Provide user credentials and 'Sign In' for authenticating with PCS.
4. After successful authentication with PCS, SAML SSO is triggered and email account gets added to Outlook.

Access through browser (SP Initiated SSO)

1. Open web browser and access Microsoft login URL "https://login.microsoftonline.com/"
2. Provide Email address and press tab. It automatically redirects to PCS login page
3. Provide credentials in the user login page to authentication to PCS
4. After successful authentication, user gets redirected to ADFS, ADFS in turn redirects to Microsoft Office 365 portal site giving access to Office365 services

Note: If the client has an existing VPN connection to PCS, then the same session will be reused and provides seamless SSO without asking for credentials

Access through PCS bookmark (IdP Initiated SSO)

1. Open web browser and access PCS external URL (Ex: https://sso.pulsesecure.net)
2. Provide credentials in the user login page to authenticate to PCS
3. Once authenticated, click on Office 365 Web Bookmark in the homepage
4. Single Sign-On will happen and user gets redirected to ADFS, ADFS in turn redirects to Microsoft Office 365 portal site giving access to Office 365 services

Configurations

This section covers the configurations required on ADFS and PCS for Cloud Secure integration with ADFS.

Active Directory Federations Services configurations include:

- Downloading Metadata from PCS and upload it in ADFS
- Adding Cloud Secure(PCS) as Claims Provider Trust in ADFS
- Adding Claim rules to process the SAML authentication requests
- Enabling RelayState for Idp initiated single sign-on

Pulse Connect Secure configurations include:

- Enabling and configuring SAML in PCS
- Adding ADFS metadata
- Configuring ADFS as Service Provider in PCS
- Configuring bookmark for Idp initiated single sign-on

ADFS Configurations

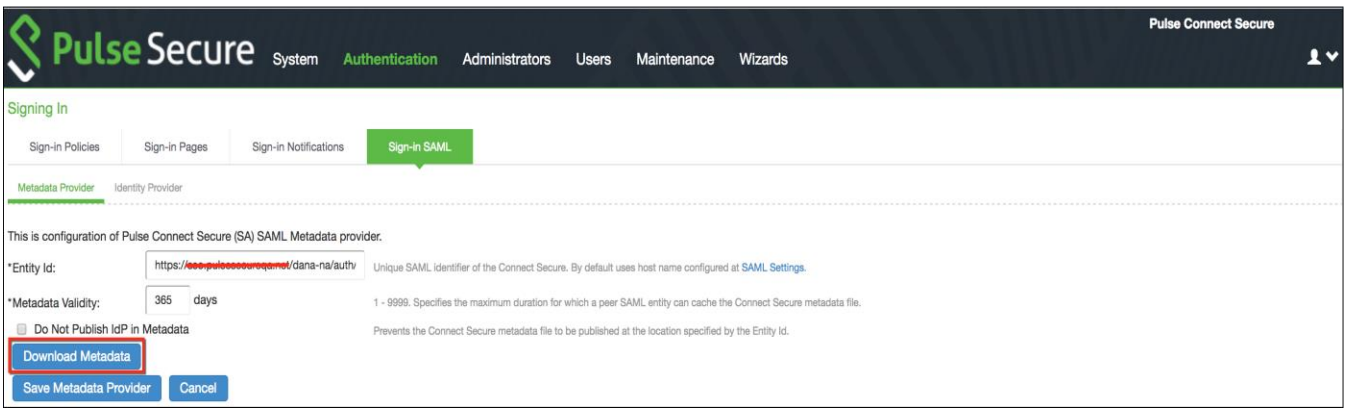
Before configuring PCS as Claims Provider Trust in ADFS, download metadata from PCS and upload it in ADFS.

Download PCS metadata

To download PCS SAML metadata:

1. Login to PCS admin console.
2. Go to Authentication > Signing In > Sign-in SAML > Metadata Provider
3. Click Download Metadata and save the file

Figure 3 Download Metadata

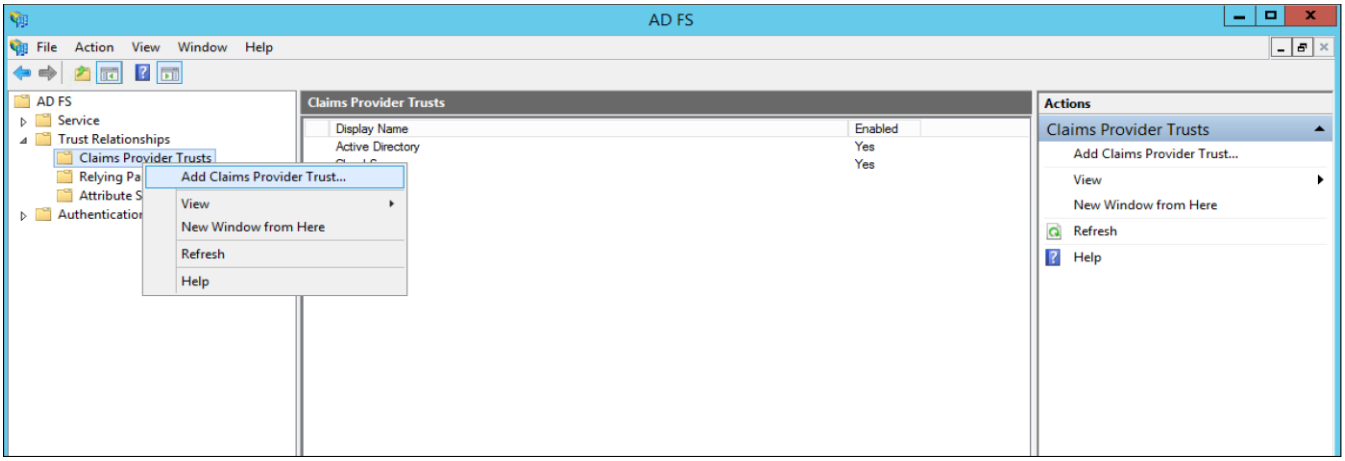


Note: The Metadata should be downloaded only after finishing the basic SAML configurations in PCS

Adding Cloud Secure (PCS) as Claims Provider trust

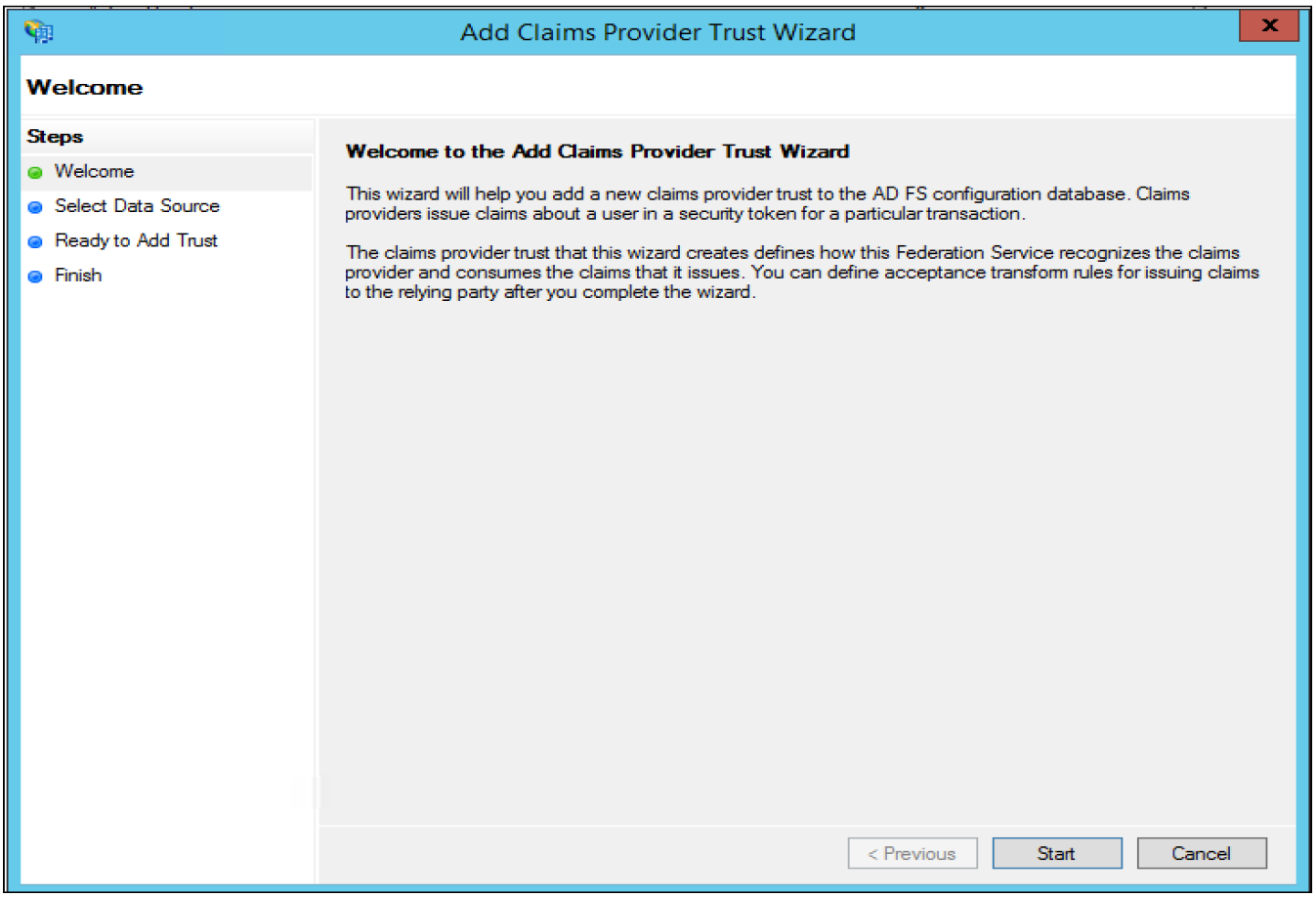
1. Login to AD Server where ADFS services are enabled
2. Open ADFS management snap-in
3. Right Click on "**Claims Provider Trusts"** and Select "**Add Claims Provider Trust**"

Figure 4 ADFS:Claims Provider Trust



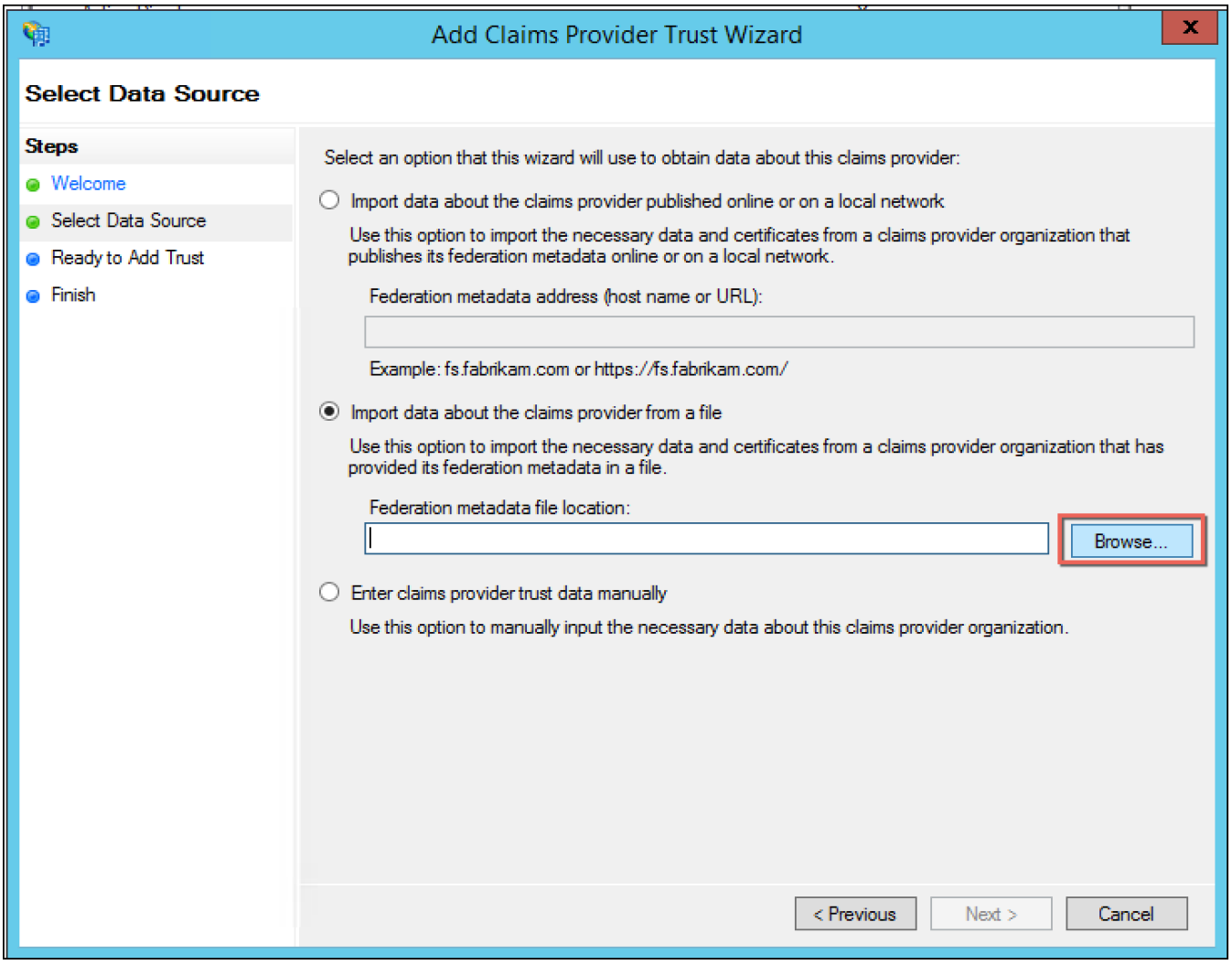
4. Click **Start**

Figure 5 ADFS Claims Provider Trust Wizard: Welcome



5. Click Browse and select **PCS Metadata file** (As mentioned in "Download PCS metadata" section)

Figure 6 ADFS Claims Provider Trust Wizard: Metadata Upload



6. Provide the claims provider **display name**
7. Select **Next**

Figure 7 ADFS Claims Provider Trust Wizard: Claims Provider Name

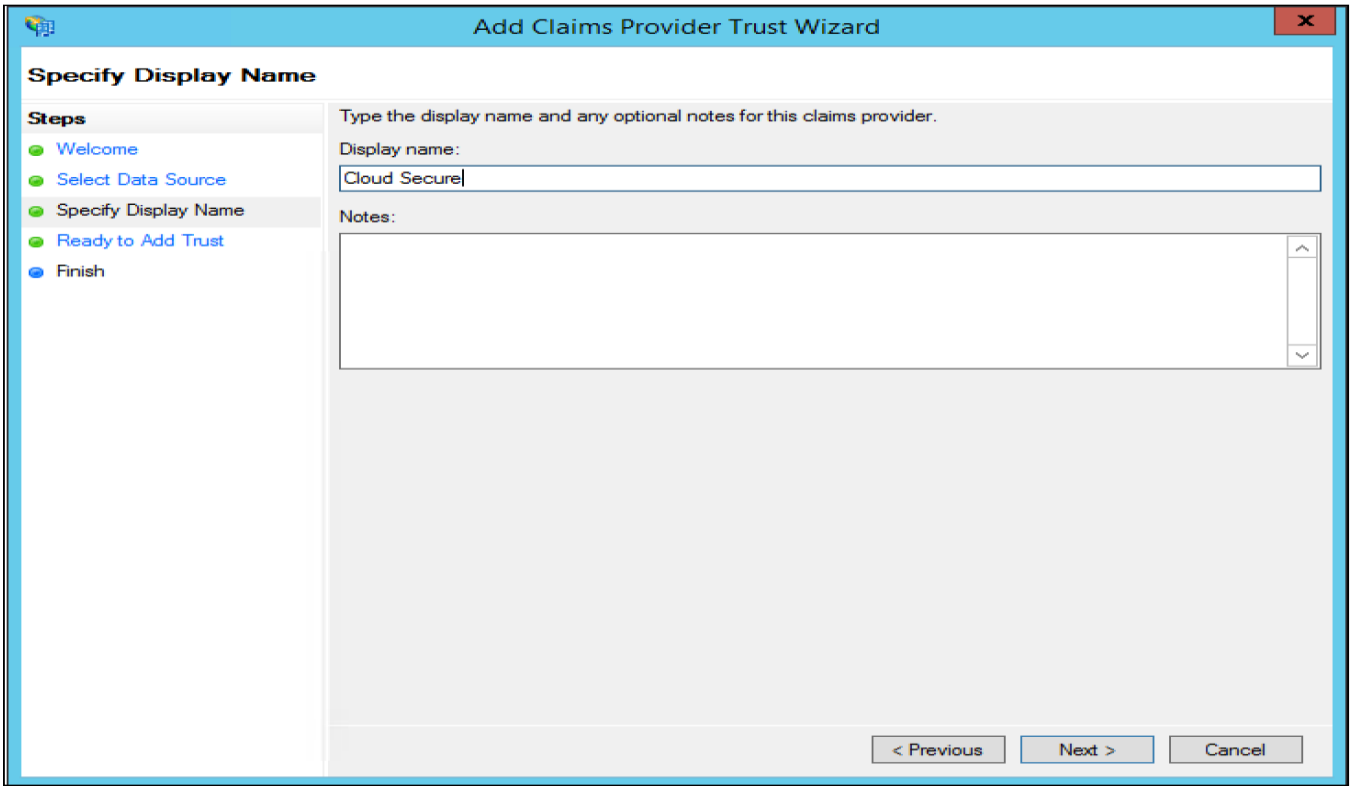
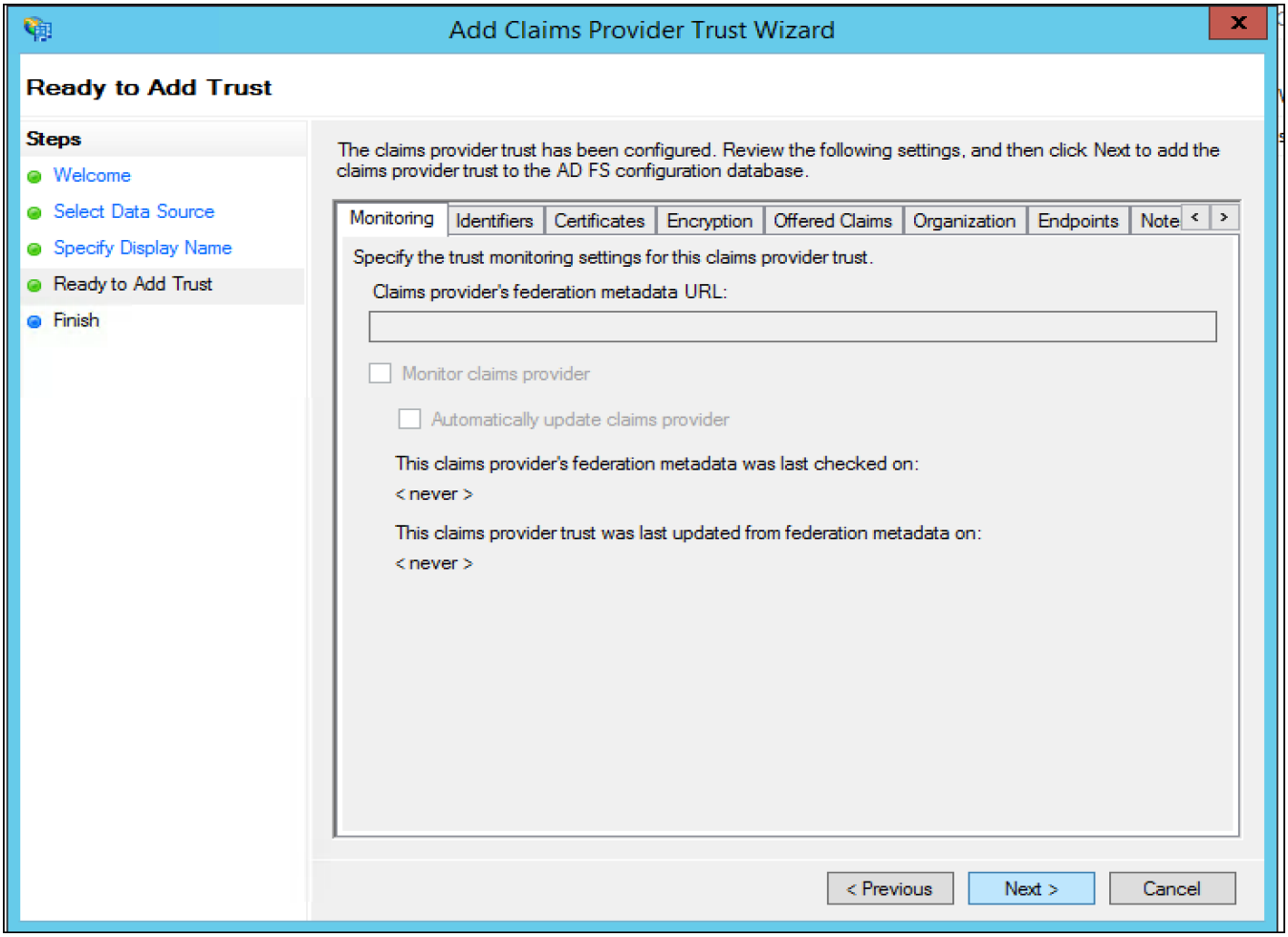
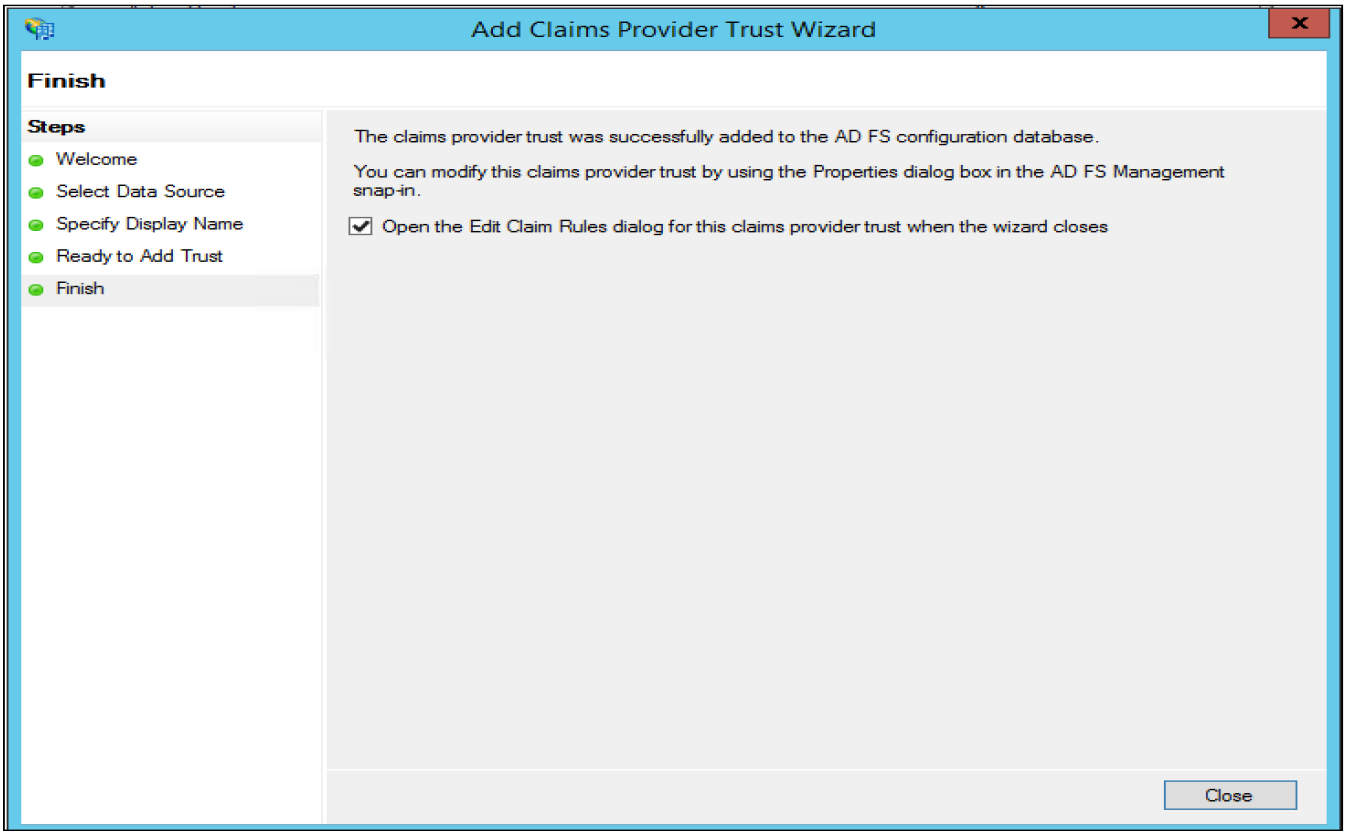


Figure 8 ADFS Claims Provider Trust Wizard: Review



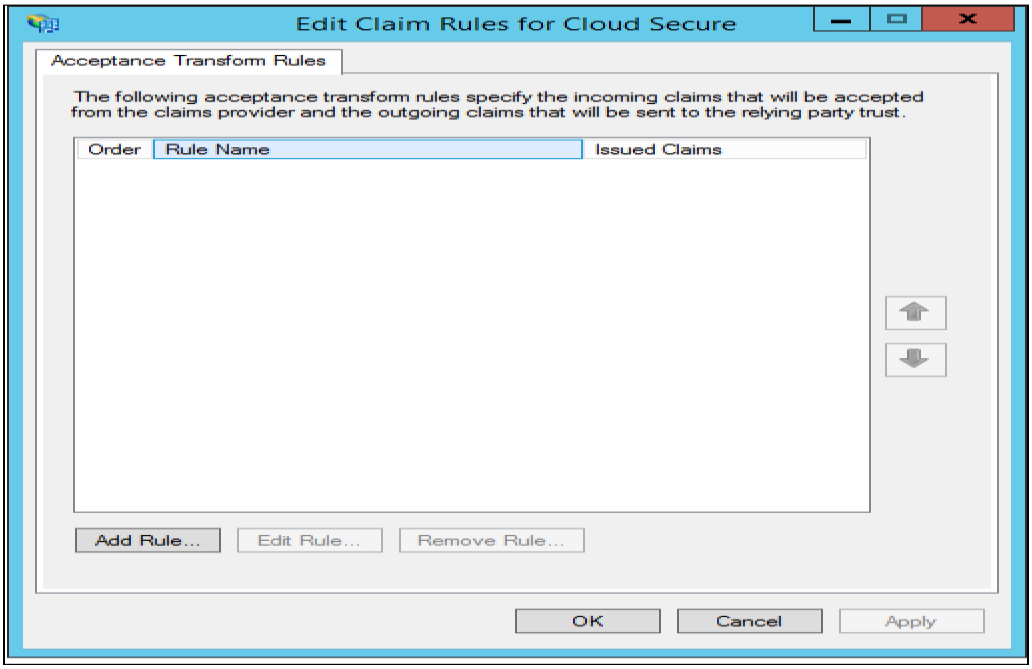
8. Click **Close**

Figure 9 ADFS Claims Provider Trust Wizard: Finish



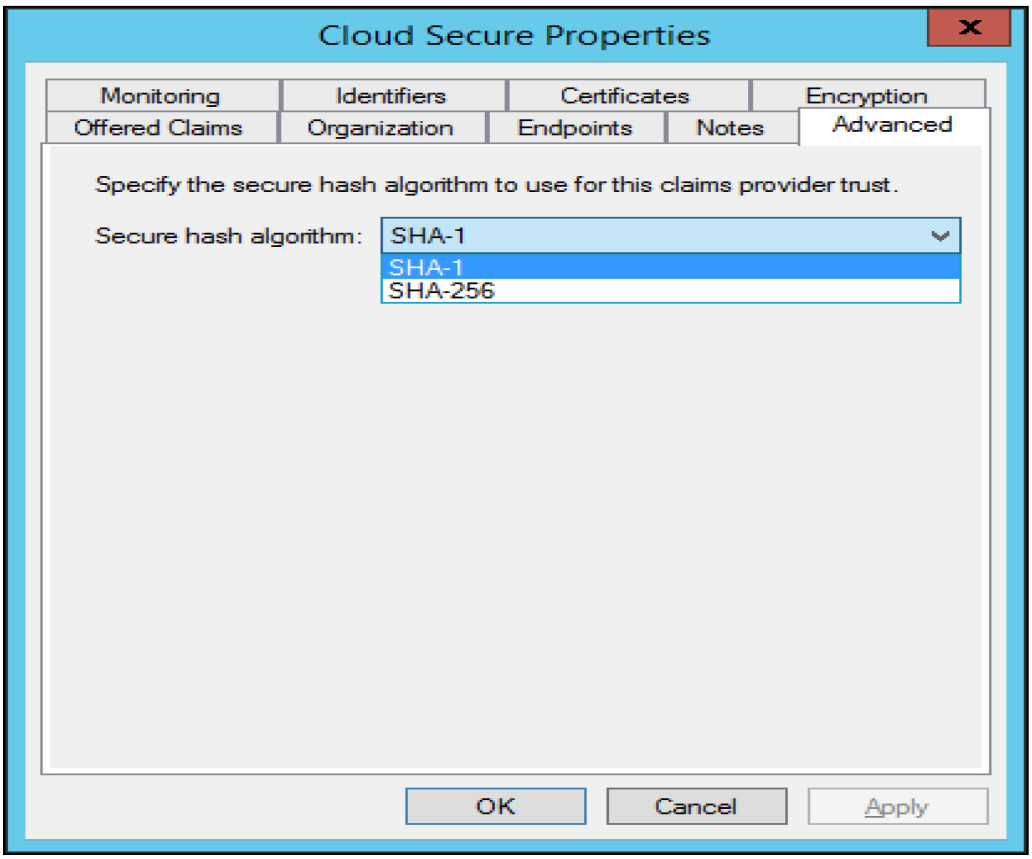
9. **ADFS claim rules page** is displayed, Do not add any rule. Click **OK**.

Figure 10 ADFS Claim Rules



10. ADFS sets **SHA-256** as default Secure hash algorithm, change it to **SHA-1.** To change Secure hash algorithm:
    a. Go to "**Claims Provider Trusts**". Right click on **Cloud Secure** (Claims provider added above).
    b. Select **"Properties"** and click **"Advanced"** tab.
    c. Select "**SHA-1**" Secure hash algorithm from the drop-down list.

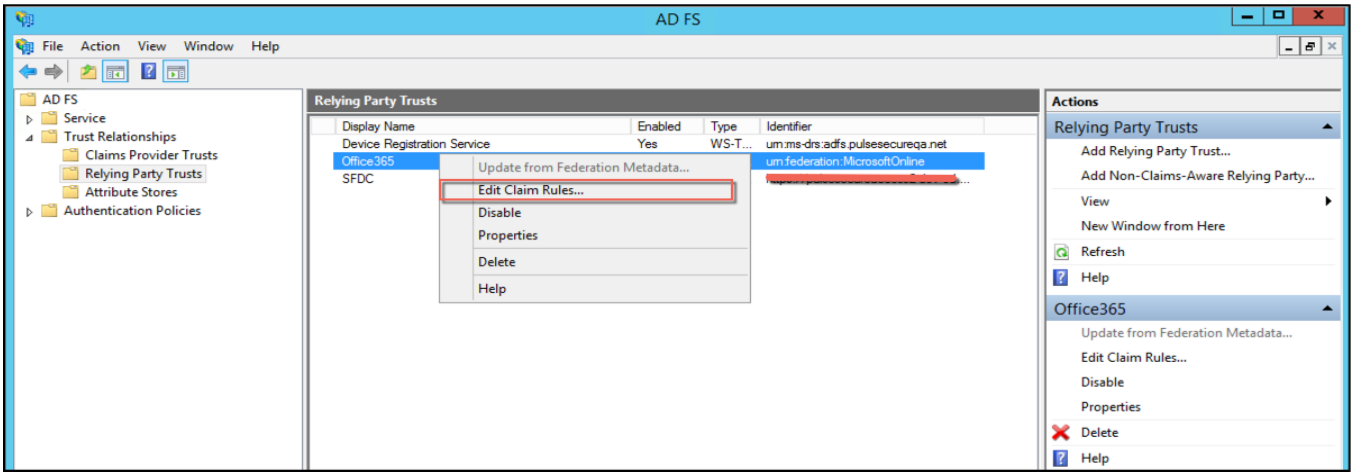
Figure 11 ADFS: Secure Hash Algorithm



Adding Claim Rules

1. Select "**Relying Party Trusts**". Right Click on "**Office365"** and click "**Edit Claim Rules"**
2. Select "**Issuance Transform Rules"** tab and click "**Add Rule"**

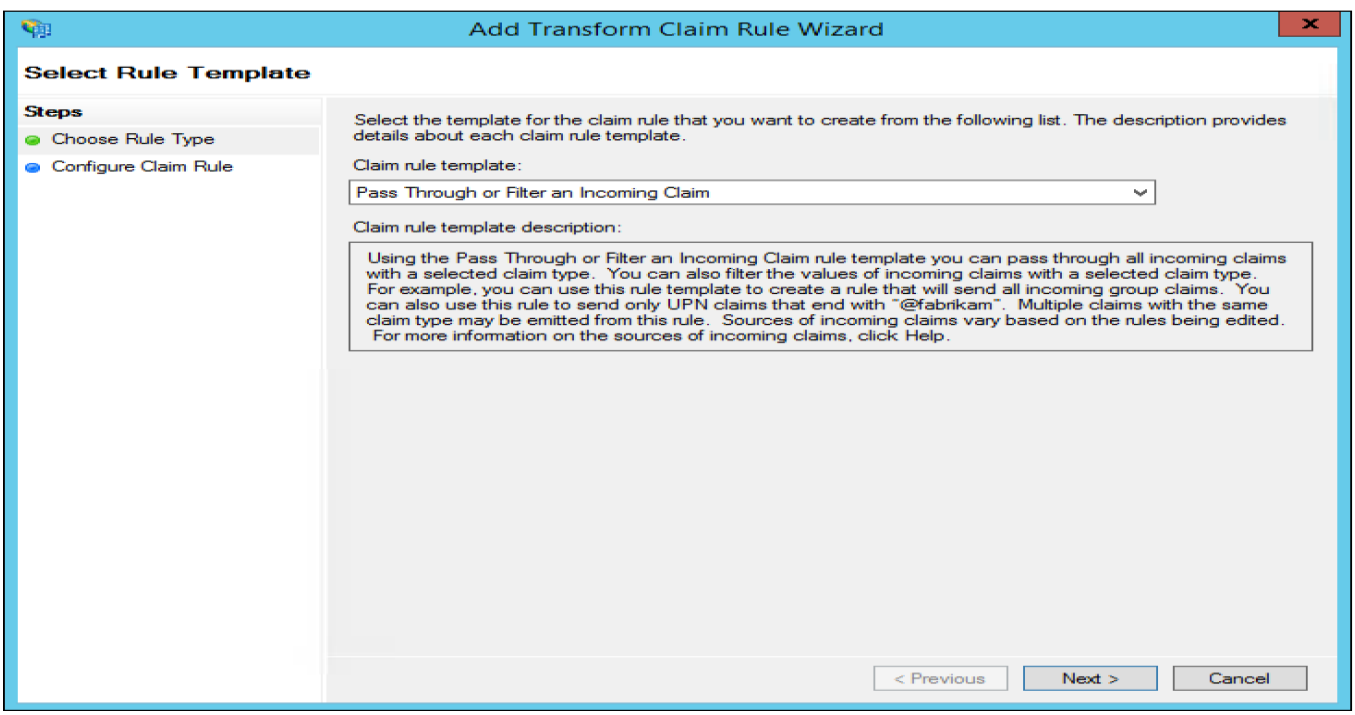
Figure 12 ADFS: Office365 Relying Party Trust



Note: Office365 federates the authentication to ADFS and this happens only when it is configured as "Relying Party Trusts" in ADFS and ADFS is configured as IdP in Office365

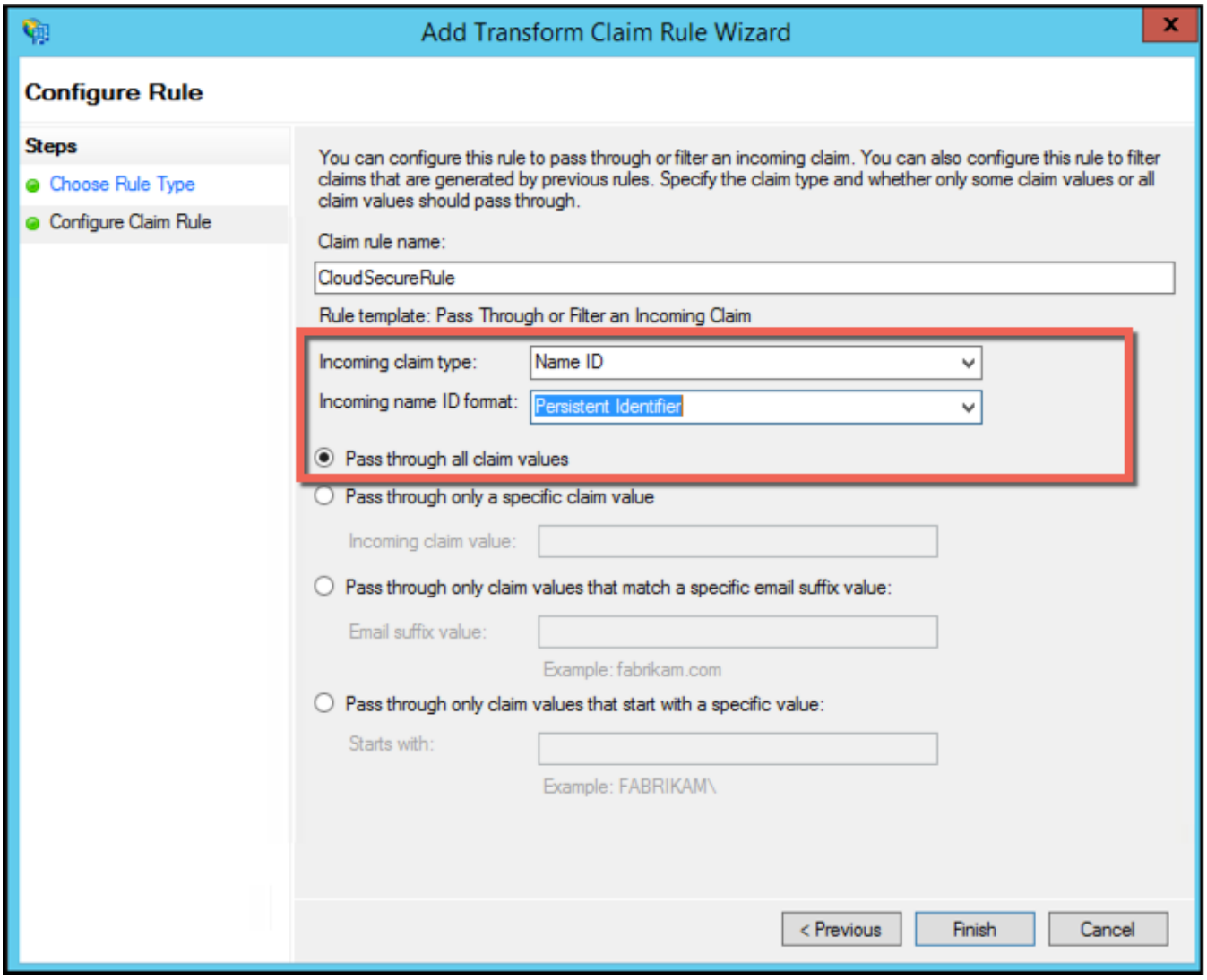
3. Select "**Pass Through or Filter an Incoming Claim**" as Claim rule template.
4. Click "**Next"**

Figure 13 ADFS:Claim Rules Wizard



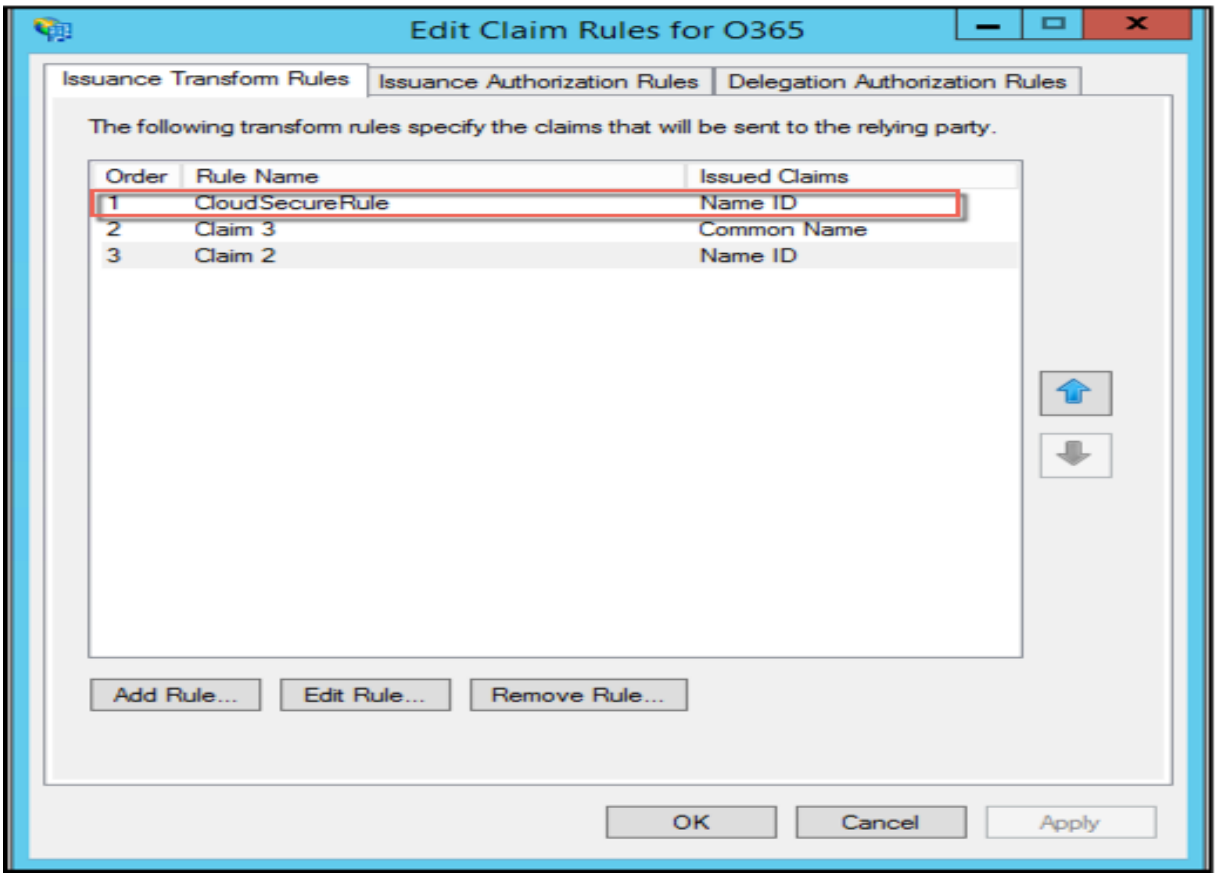
5. Provide **"Claim rule name"**
6. Select Incoming Claim type as **"Name ID"** and Incoming name ID format as **"Persistent Identifier"**
7. Select **"Pass through all claim values"**
8. Click **Finish**

Figure 14 ADFS: Claim Rules Wizard: Transform Claim Rule



9. Click on "**Up arrow**" on right side of the screen and move "**CloudSecureRule**" above the existing rules
10. Select **"OK"**

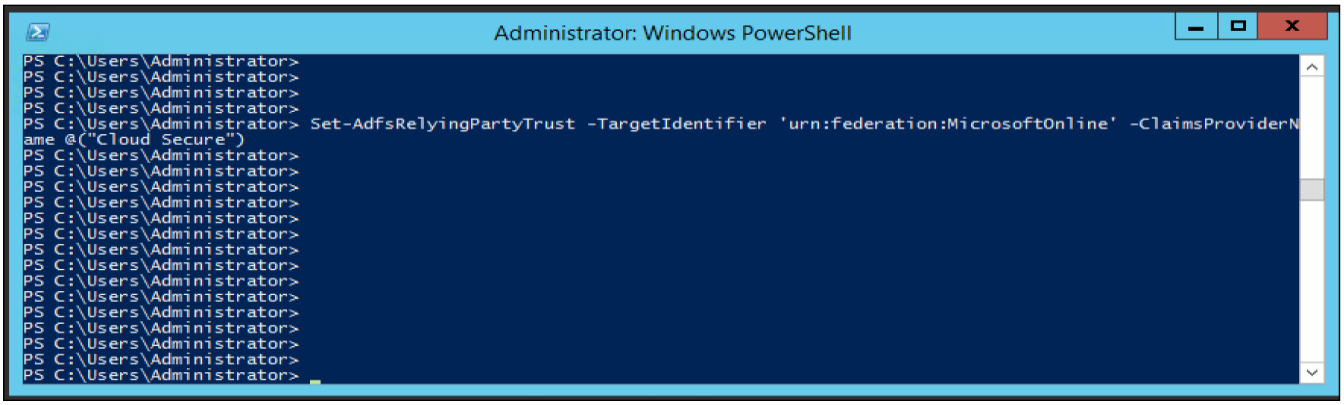
Figure 15 ADFS: Claim Rules Wizard: Transform Claim Rule



11. With all the above configurations, Cloud Secure(PCS) is successfully added as "**Claims Provider**" in ADFS. When the user access Office365 services then a login page prompts up asking user to select either "**ADFS**" or "**Cloud Secure**" for authentication.
12. Select "**Cloud Secure**" to get Secure Single Sign-on experience with existing VPN connection.
13. To avoid the additional selection page and use only Cloud Secure for Office 365 authentication federation, Launch "**Windows PowerShell"** and give the following command:

    - Set-AdfsRelyingPartyTrust -TargetIdentifier 'urn:federation:MicrosoftOnline' –ClaimsProviderName @("Cloud Secure")

Figure 16 ADFS Claim Rules Wizard:Transform Claim Rule

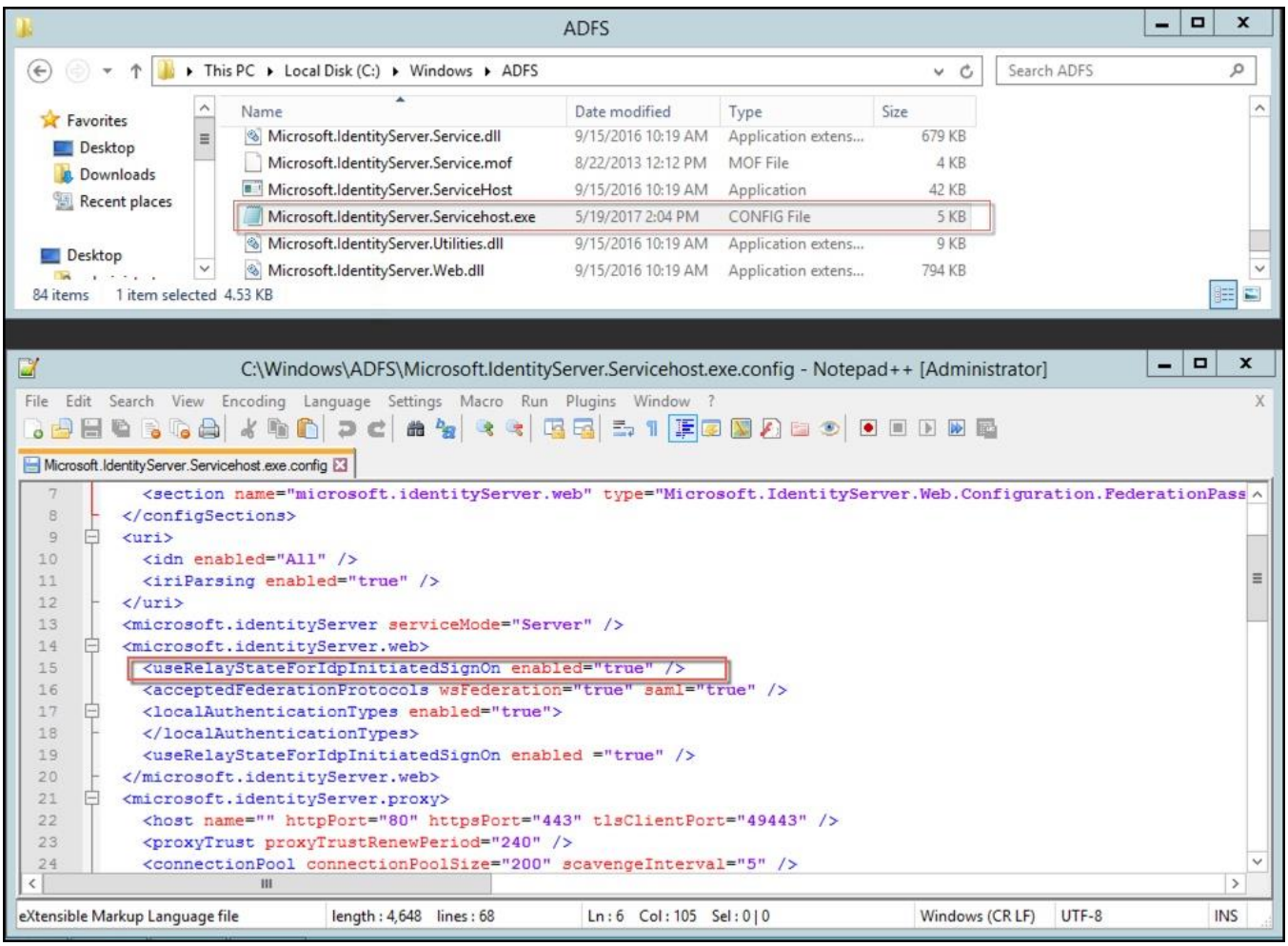


Enable Relay State for Idp Initiated Single Sign-on

In IdP initiated scenario, PCS triggers SAML assertion to ADFS when the user clicks on ADFS bookmark. However, user is not redirected to Office 365 portal, as ADFS is not aware of where the user should be redirected further. Below configuration settings enables ADFS service to relay the SAML assertion from ADFS to target cloud service

1. Go to C:\Windows\ADFS
2. Open the file Microsoft.IdentityServer.Servicehost.exe.config
3. Insert <useRelayStateForIdpInitiatedSignOn enabled="true" /> under the section <microsoft.identityServer.web>

Figure 17 ADFS Relay State configuration



Pulse Connect Secure Configuration

This section outlines the configurations for enabling PCS as SAML Identity Provider and configuring ADFS as Service Provider in PCS.

Basic Role, Realm and VPN configurations are not covered in this guide.
For basic configurations details, refer **Configuring Pulse Connect Secure - Basic Configurations (Mandatory)**

Pulse Connect Secure configurations include:

- Enabling and configuring SAML in PCS.
- Adding ADFS metadata.
- Configuring ADFS as Service Provider.

Download/Upload ADFS metadata

After configuring and enabling Cloud Secure in ADFS, it gives metadata file. This file should be uploaded in Pulse Connect Secure.
Download the AD FS server metadata file by navigating to this URL.
https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml

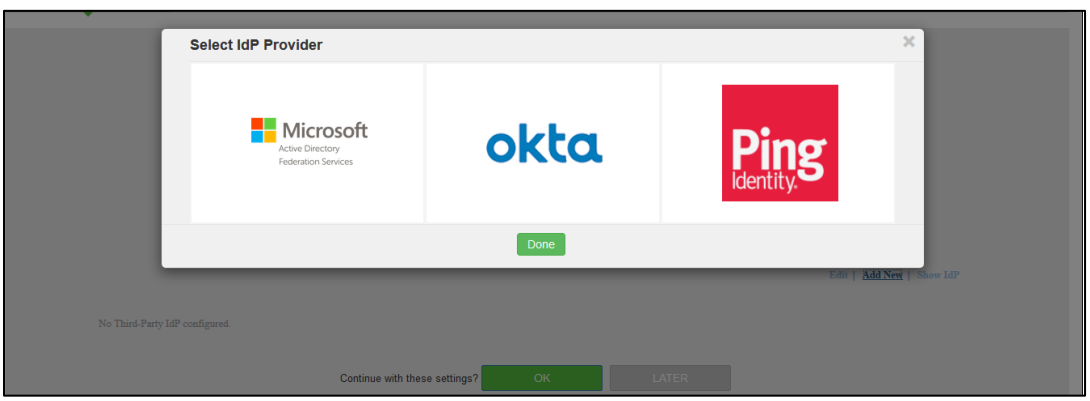
Configure ADFS as Service Provider

SAML allows cloud services to delegate user authentication to IdP. The IdP can also delegate the authentication to another IdP, which is called IdP federation.

To add ADFS as third-party IdP provider:

1. Click **Add New** and select the **Third-party IdP** as Microsoft ADFS

   Figure: UX: Third-Party IdP



2. Click **Done**
3. Under User Identity, select the Subject Name format
4. Enter the Subject Name
5. Click **Browse** and upload the metadata file.
6. Enter the relay state.
7. Set the signature algorithm to **Sha-1** or **Sha-256**.
8. Select the desired roles.

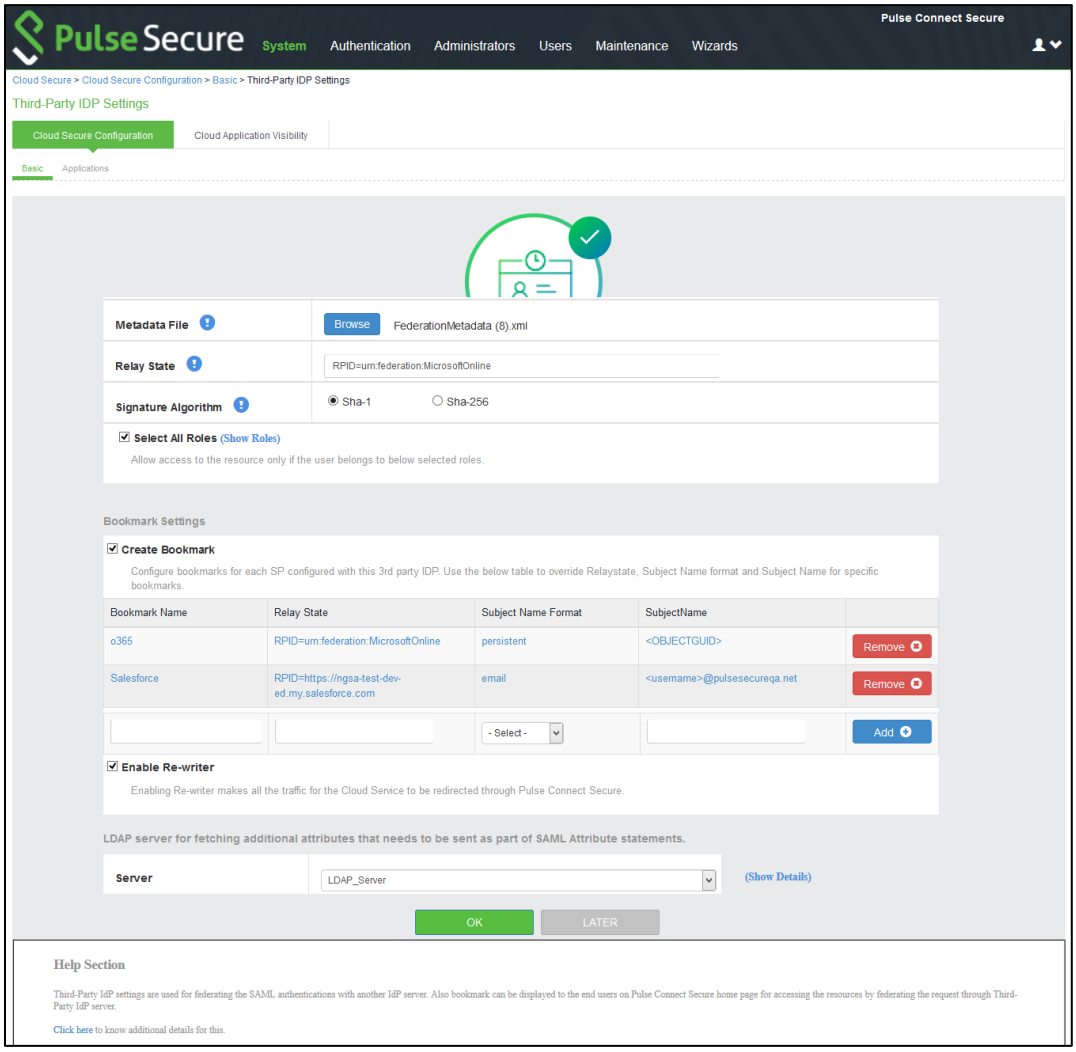
9. Under **Bookmark settings**, enable the checkbox for **Create Bookmark** to configure bookmarks for each SP configured with the third-party IDP.

   You can configure multiple bookmarks for each SP configured with the Microsoft Active Directory Federation Service (ADFS) server.

   a. Enter the bookmark name.
   b. Enter the relay state.
   c. Enter the subject name format.
   d. Enter the subject name.
   e. Click Add.

10. Enable the checkbox **Enable Re-writer** to redirect all the Cloud Secure traffic through PCS.
11. Configure the LDAP server for fetching the additional details.
12. Click **OK**.

Figure: UX: Third-Party IdP- ADFS Settings



Note: Click **Show IdP** to view the details of the configured Third-Party IdP servers.

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

ADFS deployment and configuration: https://technet.microsoft.com/en-us/library/gg188612.aspx

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**.