Adobe Sign

Enabling SAML Single Sign-On with Microsoft Active Directory Federation Services Reference Guide
# Table of Contents

Overview ................................................................................................................................................................... 3
- Installing the Active Directory Domain Service ........................................................................................................ 3
- Installing the Active Directory Federation Service ..................................................................................................... 3
- Adding Adobe Sign as a relying party ......................................................................................................................... 12
- Adding the Certificate from Adobe Sign .................................................................................................................. 25
- Adobe Sign specific settings ........................................................................................................................................... 25
- Certificate Creation ............................................................................................................................................................ 26
Overview

This document describes the process for setting up Single Sign On for Adobe Sign using Microsoft Active
Directory Federation Service. Before proceeding, please review the Adobe Sign Single Sign On Using SAML
Guide, which describes the SAML set up process and provides detailed information on the SAML Settings in
Adobe Sign.

The process of setting up SAML SSO includes the following:

- Installing the Active Directory Domain Service
- Installing the Active Directory Federation Service
- Creating a Test User
- Adding Adobe Sign as a relying party

Installing the Active Directory Domain Service

Before configuring SAML for MSAD, you must install the Active Directory Domain Service if it is not already
installed. You must have system administrator privileges in Windows Server to install Active Directory Domain
Services.

Installing the Active Directory Federation Service

1. If required, launch the Server Manager, then click Dashboard.
2. In the Dashboard, click **Add roles and features**. The Add Roles and Features Wizard displays.

3. In the *Select installation type* dialog, select **Rule-based or Feature-based Installation** then click **Next**.

4. In the *Select destination server* dialog of the wizard, leave the *Select a server from the server pool* option enabled, select a *Server Pool*, then click **Next**.
5. In the Select server roles dialog, select **Active Directory Federation Services**, then click **Next**.
6. In the Confirm installation selections dialog of the wizard, accept all the defaults by clicking **Install**.
7. On the post install options, select **Create the first federation server in a federation server farm**.
8. On the Welcome page, leave the options as is and click **Next**.
9. In the **Connect to Active Directory Domain Services** dialog of the wizard, select the **Administrator** account if not by default, then click **Next**.
10. In the Specify Service Properties dialog, import the pfx file that you created using the steps defined in the Certificate Creation section, enter a **Federation Service Display Name**, then click **Next**.
11. In the Specify Service Account dialog, select **Use an existing domain user account or group Managed Service Account**. Use Administrator as the service account and provide your administrator password, then click **Next**.
12. In the Specify Configuration Database dialog, select **Create a database on this server using Windows Internal Database**, then click **Next**.

13. In the Review Options dialog, click **Next**.
14. In the Prerequisite Checks dialog, once the prerequisite check is done, click Configure.

15. In the Results dialog, ignore the warning and click Close.
Adding Adobe Sign as a relying party

1. From the Apps menu, launch **AD Federation Service Management**.

2. In the AD FS console, select **Authentication Policies** then Edit.
3. In the Edit Global Authentication Policy dialog, under both Extranet and Intranet, enable Forms Authentication.


5. In the Select Data Source dialog of the wizard, enable the Enter Data about the relying party manually option, then click Next.
6. In the Specify Display Name dialog, enter a **Display Name**, then click **Next**.
7. In the Choose Profile dialog, enable the **AD FS profile** option, then click **Next**.

8. In the **Configure Certification** dialog there is no certificate to configure, so click **Next**.
9. In the Configure URL dialog, select **Enable support for the SAML 2.0 WebSSO protocol** and enter the **Assertion Consumer URL** from Adobe Sign, then click **Next**. (See the Single Sign On with SAML Guide for more information about the Assertion Consume URL.)
10. In the Configure Identifiers dialog, enter http://echosign.com for Relying party trust Identifier and click Add, then click Next.

11. In the next screen, leave the defaults as-is, and click Next.
12. In the Choose Issuance Authorization Rules dialog, confirm that the **Permit all users to access the relying party** option is enabled.

13. In the Ready to Add Trust dialog, click **Next**.

15. In the Edit Claim Rules dialog, click Add Rule.

The Add Transform Claim Rule Wizard displays.
16. In the Select Rule Template dialog of the wizard, select **Send LDAP Attributes as Claims** from the **Claim rule template** drop-down.
17. In the Configure Rule dialog, select the options shown in the dialog and click **Finish**. Adobe Sign only supports the email address as the unique identifier. You need to select **E-Mail Addresses** as the LDAP Attribute and **E-Mail Address** as the Outgoing Claim.

18. When the Select Rule Template dialog of the wizard redisplayes, select **Send Claims Using a Custom Rule** from the Claim rule template drop-down, then click **Next**.
19. In the Configure Rule dialog, enter the following:
   o **Name of rule**—Enter **EmailToNameId**
   o **Custom rule description**—enter the following:

```c
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
    => issue(Type =
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer
    = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
    c.ValueType,
    at"] = "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress",
    Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spn
    mequalifier"] = "";
```

20. Click **Finish**. The *Add Transform Claim Rule Wizard* closes.

21. Back in the *Edit Claim Rules for Adobe Sign* dialog, click the *Issuance Authorization Rules* tab and *Delegation Authorization rules* tab and ensure that the **Permit Access to All Users** is enabled for both as shown below. If not, add a rule, so that **Permit Access To All Users** is enabled.
22. Click OK to accept all changes can close the Edit Claims Rules for Adobe Sign dialog.

Adding the Certificate from Adobe Sign

1. In the AD FS console, under Trust Relationships, select the Adobe Sign Relying Party click Properties.
2. Once launched, select Authentication Policies and then Edit.

3. Select the Signature tab.
4. Click Add and add the SP certificate file you downloaded from Adobe Sign. (See the Single Sign On with SAML Guide for more information about the SP certificate.)
5. Select the Advanced tab and change the Secure Hash Algorithm to SHA-1.
6. Select the Endpoints tab and add the Single Logout (SLO) URL from Adobe Sign. (See the Single Sign On with SAML Guide for more information about the Single Logout (SLO) URL).
7. Disable Claims Encryption – Open power shell on the ADFS server and type

   Set-ADFSRelyingPartyTrust -TargetName "Adobe Sign" -EncryptClaims $false

Adobe Sign specific settings

• The account should have SAMLAVAILABLE=true
• Host Name
• SAML Mode
• ACCOUNT_USER_ADD_EMAIL_DOMAINS setting to be for example dev.com
• Select the token signing certificate in ADFS and export it as a cer file (do not export private key) and add it to the account admins SAML Settings page in Adobe Sign.
Open this certificate file in notepad, and Adobe Sign Admin copy its contents into the *IdP Certificate* field in SAML Settings.

Now you should be able to test.

**Certificate Creation**

1. On Windows, install openssl. On Mac, openssl is present.
2. Launch a command prompt and type
   ```bash
   openssl req -x509 -newkey rsa:2048 -keyout <yourkeyName>.pem -out <yourkeyNameCer>.pem -days <#ofdays>
   ```
Enter the following:
Country code - US
State - California – San Jose
Enter some Organization and Organization unit
Common Name- This is the fully qualified name that is the same as your host system name example sjtest.es.com

3. Now create the pkcs12 key
   
```bash
pkcs12 -export -in <yourkeynameCer>.pem -inkey <yourkeyName>.pem -out my_pkcs12.pfx
```

4. Enter password when prompted

5. Click Import and select the my_pkcs12.pfx selected above and enter password that you provided at pkcs12 export time when prompted