PebblePad AD FS Authentication Guide

Overview

In this guide we will instruct you on how to set up your AD FS 2.0 as an Identity Provider (IdP) to be used with PebblePad via Shibboleth 2 as a Service Provider (SP).

1. Create test user (optional)
2. Add PebblePad Shibboleth as a Relying Party using metadata.
3. Edit the claim rules used by AD FS for Shibboleth security tokens.
4. Provide AD FS metadata to PebblePad Shibboleth.

"This guide provides step-by-step instructions for configuring a basic identity federation deployment between Active Directory Federation Services 2.0 (AD FS 2.0) and Shibboleth by using the Security Assertion Mark-up Language (SAML) 2.0 protocol with the SAML 2.0 HTTP POST binding."

UK Test PebblePad Shibboleth server is 54.215.168.29 (shibtest.pebblepad.com)

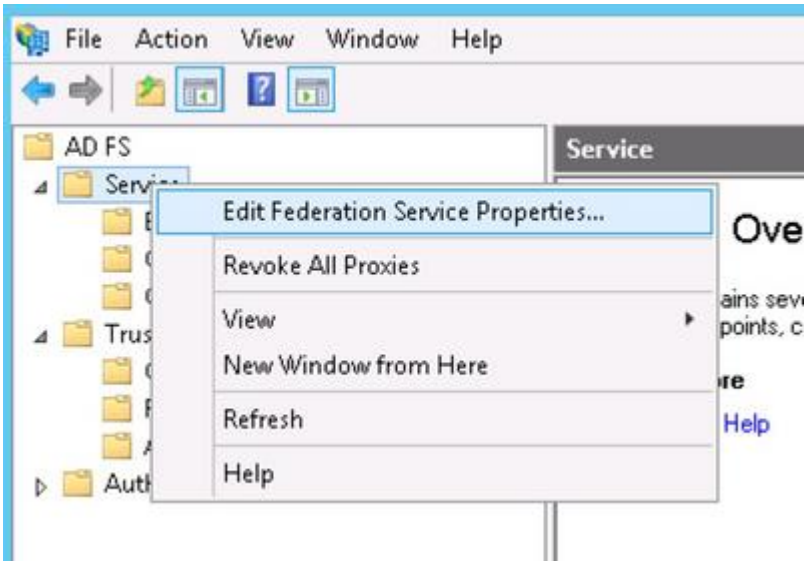
Our procedure is to set up an instance of PebblePad for testing using a test location and the test Shibboleth server accessing this location first before moving to production.

Once the integration has been confirmed working you will be provided with our production metadata and EntityID.

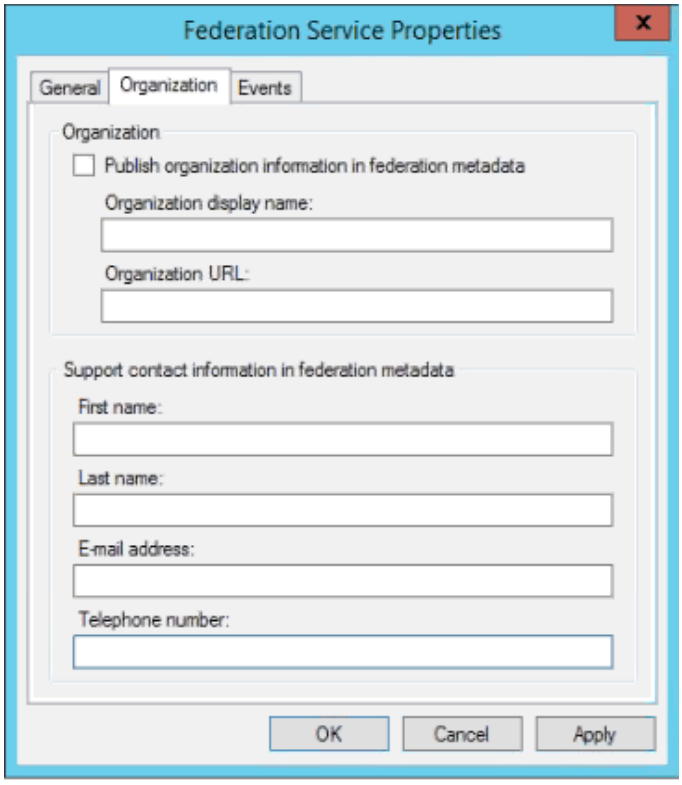
Known issues

Our Shibboleth Service Provider instance requires that a support contact be present in your AD-FS metadata.

1. Right click on the Service folder under AD FS and click Edit Federation Service Properties...



2. Complete the Support contact information in federation metadata section, as a minimum the E-mail address and Telephone number must be set.



3. Click OK to save.

Create test user (optional)

Next you will need to create an optional test user in Active Directory so that we can check the authentication route between Shibboleth and AD FS. If you have an existing account you are happy to provide us you can skip to the next step.

1. Click **Start**, click **Administrative Tools**, and then click **Active Directory Users and Computers**.

2. In the console tree, under your domain, right-click the **Users** folder. Click **New**, and then click **User**.

3. On the **New Object – User** page, type the following values, and then click **Next**.

Name	Value
First name	PebblePad
Last name	Test
Full name	Pebble Test
User logon name	pebbletest

4. Provide a password, clear the **User must change password at next logon** check box, and then click **Next**. (please let us know what this password is)

5. Click **Finish**.

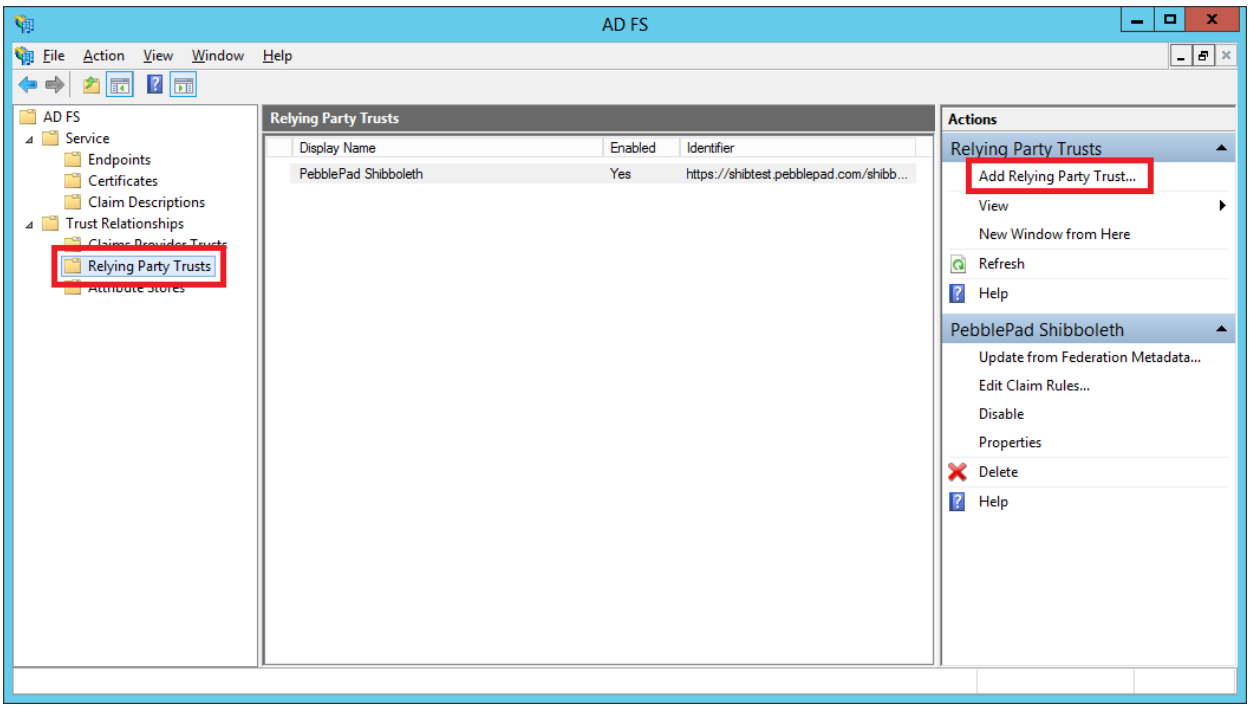
6. In the right pane of Active Directory Users and Computers, right-click the new user object, and then click **Properties**.

7. On the **General** tab, in the **E-mail** box, type the following value, and then click **OK**.

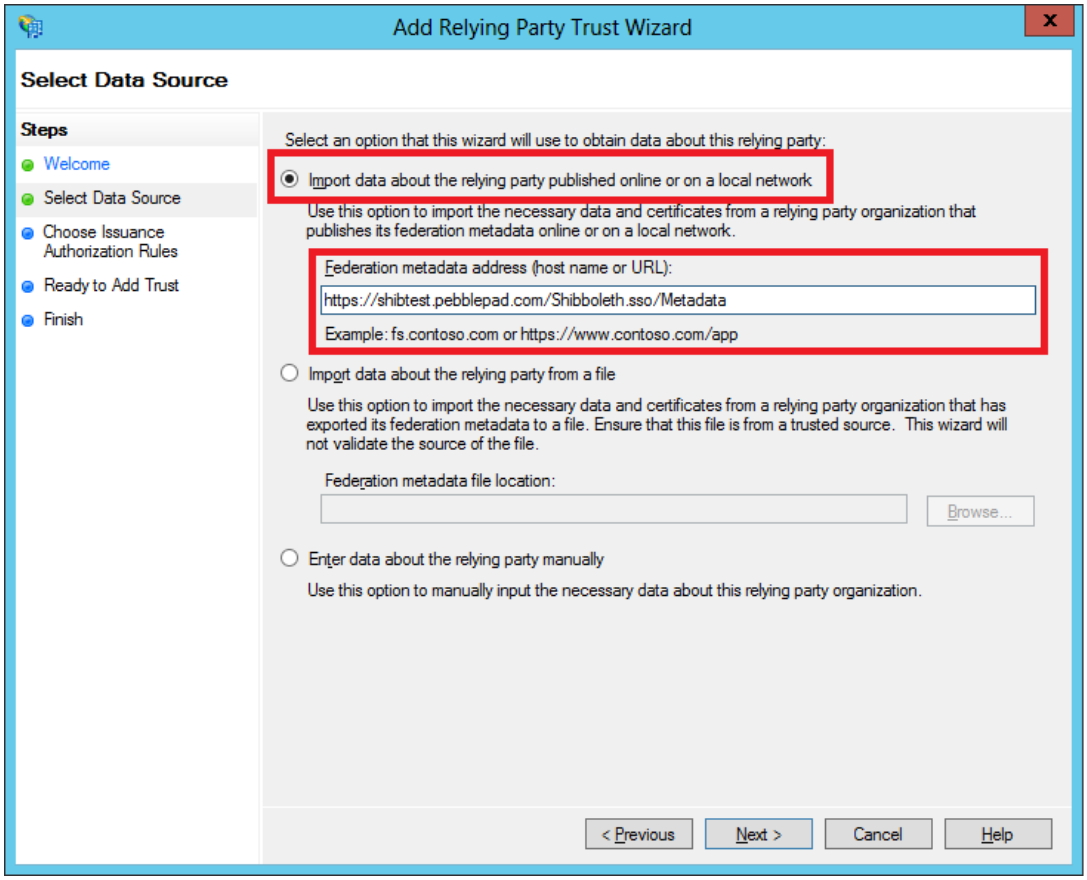
Name	Value
E-mail	support@pebblepad.com

AD FS Management

1. In AD FS 2.0, in the console tree, right-click the **Relying Party Trusts** folder, and then click **Add Relying Party Trust** to start the Add Relying Party Trust Wizard.

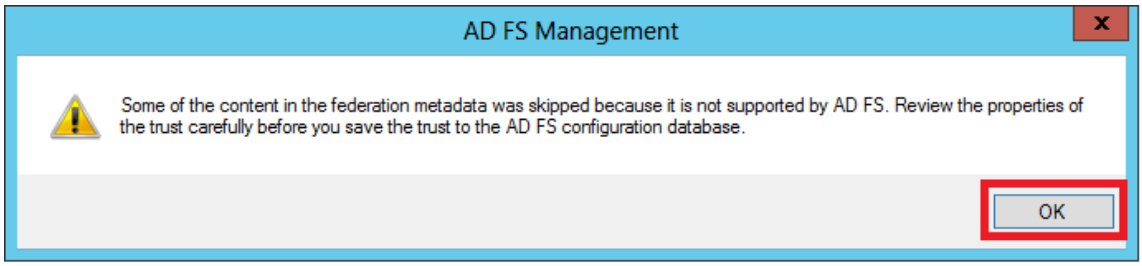


2. On the **Select Data Source** page, leave selected **Import data about the relying party published online or on a local network**.



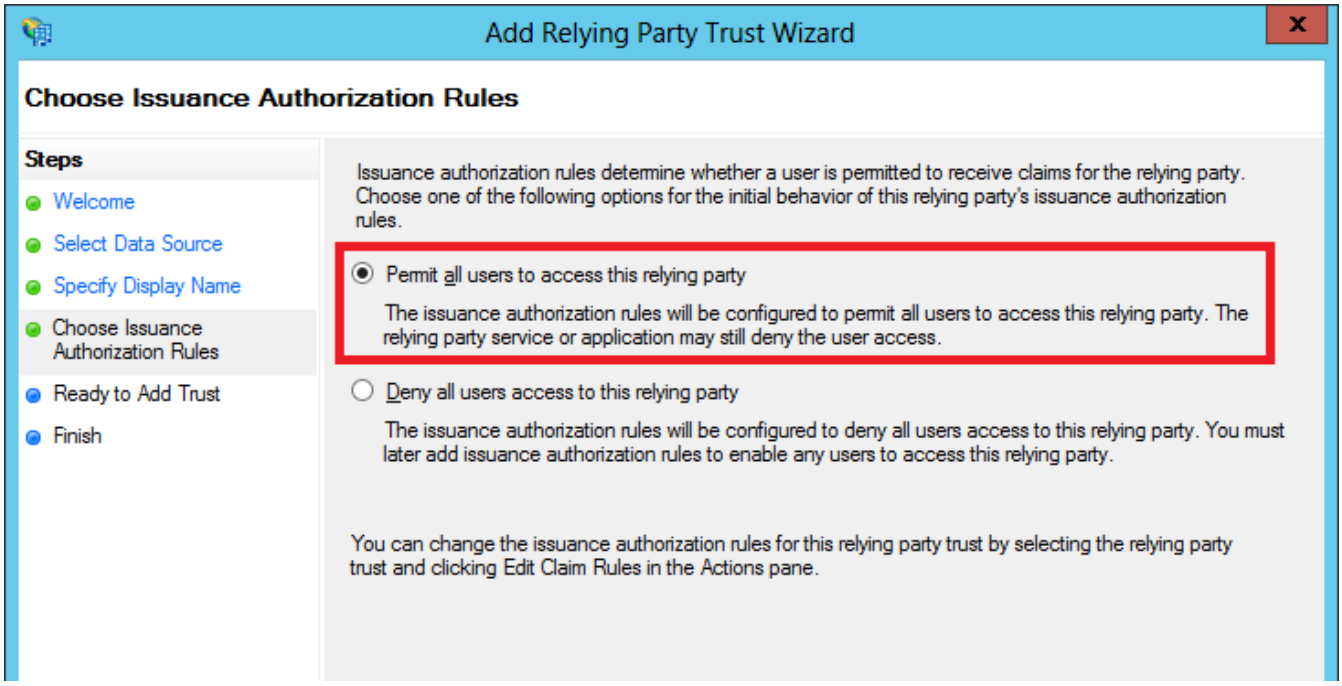
3. In the **Federation metadata address** field, type https://shibtest.pebblepad.com/public/metadata.xml, and then click **Next**.

4. Click **OK** to acknowledge the message "Some of the content in the federation metadata was skipped because it is not supported by AD FS 2.0."



5. In the **Specify Display Name** page, leave **shibtest.pebblepad.com**, and then click **Next**.

6. On the **Choose Issuance Authorization Rules** page, leave the default **Permit all users to access the relying party** selected, and then click **Next**.



7. Click **Next**, and then click **Close**.

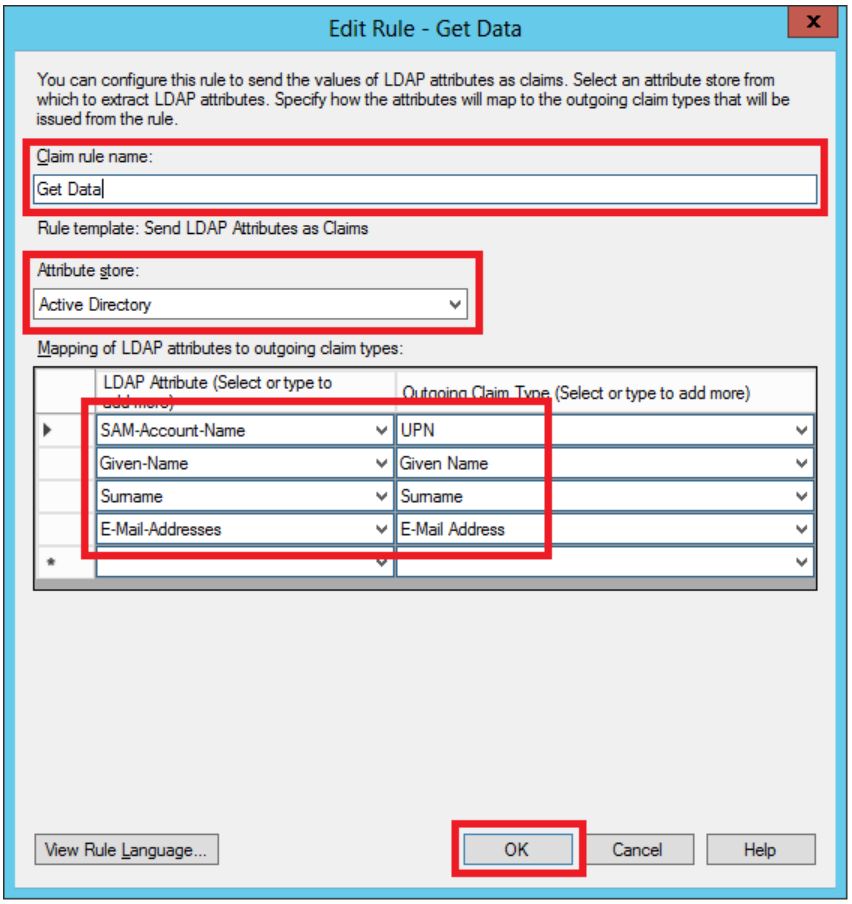
Claim rules

Get Data Transform Rule

1. The **Edit Claim Rules** dialog box should already be open. If not, In the AD FS 2.0 centre pane, under **Relying Party Trusts**, right-click **shibtest.pebblepad.com**, and then click **Edit Claim Rules**.
2. On the **Issuance Transform Rules** tab, click **Add Rule**.
3. On the **Select Rule Template** page, select **Send LDAP Attributes as Claims**, and then click **Next**.
4. On the **Configure Claim Rule** page, in the **Claim rule name** box, type **Get Data**.
5. In the **Attribute Store** list, select **Active Directory**.
6. In the **Mapping of LDAP attributes** section, create the following mappings.

LDAP Attribute	Outgoing Claim Type
SAM-Account-Name	UPN
Given-Name	Given Name
Surname	Surname
E-Mail-Addresses	E-Mail Address

7. Click **Finish**.



Transform UPN to eduPPN

1. On the **Issuance Transform Rules** tab, click **Add Rule**.
2. On the **Select Rule Template** page, select **Send Claims Using a Custom Rule**, and then click **Next**.
3. In the **Configure Rule** page, in the **Claim rule name** box, type **Transform UPN to eduPPN**.
4. In the **Custom Rule** window, type or copy and paste the following:

   c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/upn"]

   => issue(Type = "urn:oid:1.3.6.1.4.1.5923.1.1.1.6", Value = c.Value, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] = "urn:oasis:names:tc:SAML:2.0:attrname-format:uri");

   The object-identifier-style uniform resource name (URN) string urn:oid:1.3.6.1.4.1.5923.1.1.1.6 is the formal SAML 2.0 name for the eduPersonPrincipalName attribute—a name that the Shibboleth SP software understands by default.

5. Click **Finish**.

Transform E-Mail Address to mail

1. On the **Issuance Transform Rules** tab, click **Add Rule**.
2. On the **Select Rule Template** page, select **Send Claims Using a Custom Rule**, and then click **Next**.
3. In the **Configure Rule** page, in the **Claim rule name** box, type **Transform E-Mail Address to mail**.
4. In the **Custom Rule** window, type or copy and paste the following:

   c:[Type == "urn:oid:0.9.2342.19200300.100.1.3"]

   => issue(Type = c.Type, Value = c.Value, Issuer = c.Issuer, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] = "urn:oasis:names:tc:SAML:2.0:attrname-format:uri");

5. Click **Finish**.

Transform Given Name to givenName

1. On the **Issuance Transform Rules** tab, click **Add Rule**.
2. On the **Select Rule Template** page, select **Send Claims Using a Custom Rule**, and then click **Next**.
3. In the **Configure Rule** page, in the **Claim rule name** box, type **Transform Given Name to givenName**.
4. In the **Custom Rule** window, type or copy and paste the following:

   c:[Type == "urn:oid:2.5.4.42"]

   => issue(Type = c.Type, Value = c.Value, Issuer = c.Issuer, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] = "urn:oasis:names:tc:SAML:2.0:attrname-format:uri");

5. Click **Finish**.

Transform Surname to sn

1. On the **Issuance Transform Rules** tab, click **Add Rule**.
2. On the **Select Rule Template** page, select **Send Claims Using a Custom Rule**, and then click **Next**.
3. In the **Configure Rule** page, in the **Claim rule name** box, type **Transform Surname to sn**.
4. In the **Custom Rule** window, type or copy and paste the following:

   c:[Type == "urn:oid:2.5.4.4"]

   => issue(Type = c.Type, Value = c.Value, Issuer = c.Issuer, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] = "urn:oasis:names:tc:SAML:2.0:attrname-format:uri");

5. Click **Finish**.

Providing metadata

Once all the required steps have been completed please provide us with the link to your metadata file on your AD FS server, this will be located at:

https://*your-domain*/FederationMetadata/2007-06/FederationMetadata.xml.

We will then test to see if our Shibboleth server can see your AD FS server, access the claims and grant access through this method to our application.