OpenAir

SAML 2 Quick Start Guide

April 14, 2018

ORACLE NETSUITE

Table of Contents

OpenAir SAML 2 Quick Start Guide 1
Identity Provider Setup 1
Provider Integration Setup 1
OpenAir Account Configuration 8

OpenAir SAML 2 Quick Start Guide

Identity Provider Setup

This section details OpenAir Service Provider authentication attribute mapping.

Below are the relevant SAML assertion fields for exchanges. The mapping describes the relationship between SAML attributes to OpenAir login identifiers. These attributes must be included in all SAML assertions, unless otherwise marked as [Optional].

1. SAML *NameID*: OpenAir user nickname which represents the unique user nicknames defined in the OpenAir account.

   Note: If this field does not send the user's nickname as a persistent attribute, then the provider must follow Step 3 below.

2. SAML assertion string attribute *account_nickname*: OpenAir company name. This is the name of your OpenAir account.
3. [Optional] SAML assertion string attribute *user_nickname*: alternate OpenAir user nickname. If specified, the user_nickname takes precedence over NameID for identifying the user. Use of this attribute provides the IdP with an option to use a transient NameID for session management, while still providing the user nickname for OpenAir authentication.

Note: OpenAir does not support multiple identity providers. For example, customers cannot use both OKTA and Azure at the same time.

Provider Integration Setup

The steps below describe one-time setup requirements necessary before assertions can be exchanged between the IdP and OpenAir SP endpoints.

1. The Identity Provider should provide OpenAir with a copy of their service metadata, or a URL at which we can access it.
2. OpenAir SAML metadata is available for download at the following URLs:
   - Sandbox (test) — https://sandbox.openair.com/saml.pl?o=B
   - Production — https://www.openair.com/saml.pl?o=B
3. Integration testing should be performed in a sandbox server account. You should plan to provide an active SAML identity provider instance for our sandbox integration, for future support and troubleshooting.
4. The Identity Provider must support Redirect/POST SSO assertions as the default exchange method. All assertions must be signed. SAML assertion encryption is optional, but recommended.
5. Any Vendor-specific IdP custom configuration requirements should be accounted for.

The following are custom configuration requirements for known IdP products. All steps assume the IdP has created an SP profile via OpenAir SP metadata first.

- **PingFederate 6 or later**
  1. Manually choose POST as the primary exchange method (IdP to SP). Otherwise, the Artifact endpoint may be incorrectly used as the default.

2. In Single Log-Out (SLO) options, manually remove query string parameters such as "?o=Q" or "?o=S" from the URLs. This avoids malformed assertions, a known issue in PF 6.0 and 6.1.
3. Enable the following setting: SP configuration > Protocol Settings > Signature Policy > Always sign the SAML assertion.

- **Microsoft Active Directory Federation Services 2**
  1. In the SP configuration "Identifiers" tab, be sure to specify two identifiers representing the entityID, one with the "?o=B" query string and one without.
  2. In the SP configuration "Advanced" tab, specify "SHA-1" as the Secure hash algorithm.

  > **Note:** The ADFS 2 default, SHA-256, is not supported at this time.

- **Shibboleth 2**

  Shibboleth requires custom OpenAir authentication attribute mapping. These attributes should be used instead of those described in Identity Provider Setup.

  1. SAML assertion *NameID*: IdP-defined, transient session ID. This attribute is expected, but not used directly in OpenAir authentication.
  2. SAML assertion attribute *eduPersonEntitlement*: OpenAir domain and OpenAir company name. This should contain both the service provider domain, sub-domain, and company name. The format is:

     urn:mace: <*domain*>: <*server instance*>:account_nickname: <*account nickname*>

- **Okta**

  No special steps are needed.

- **OneLogin**

  No special steps are needed.

- **Symplified**
  1. Generic SAML plugin with SAML Metadata export extension (separate purchase)

     For example, if assertions for an account called "Sample Account" are sent to the OpenAir production site, the attribute value would be:

     urn:mace: *openair.com:production*:account_nickname: *SampleAccount*

     For non-production OpenAir servers, <*serverinstance*> must exactly match the sub-domain, as in the following example for sandbox.openair.com:

     urn:mace: *openair.com*:sandbox:account_nickname: *SampleAccount*
  2. SAML assertion attribute eduPersonPrincipalName: OpenAir user nickname

     The common format for this Shibboleth attribute is an email address, for example: user@someschool.edu

- **Microsoft AD FS 3.0**

  Follow these steps to set up Microsoft AD FS 3.0: SSO to OpenAir:

  1. Make sure that you have installed the following patches on your AD FS server:
     - Windows Server 2008 — **KB2896713**

       This patch fixes a problem which appeared in KB2843638, when error message MSIS0038 (SAML Message has wrong signature) would appear even for correct signatures.
     - Windows Server 2012 (R2) — **KB3003381**

       Again fixes the incorrect MSIS0038 error reported in AD FS 2.0 and AD FS 3.0
  2. Install AD FS 3.0 on Windows Server.

3. Download the AD FS Metadata XML from the following location:

   https://{your_federation_server_name}/federationmetadata/2007-06/federationmetadata.xml

4. In AD FS 3.0, open the Add Relying Party Trust Wizard. Click **Start**.

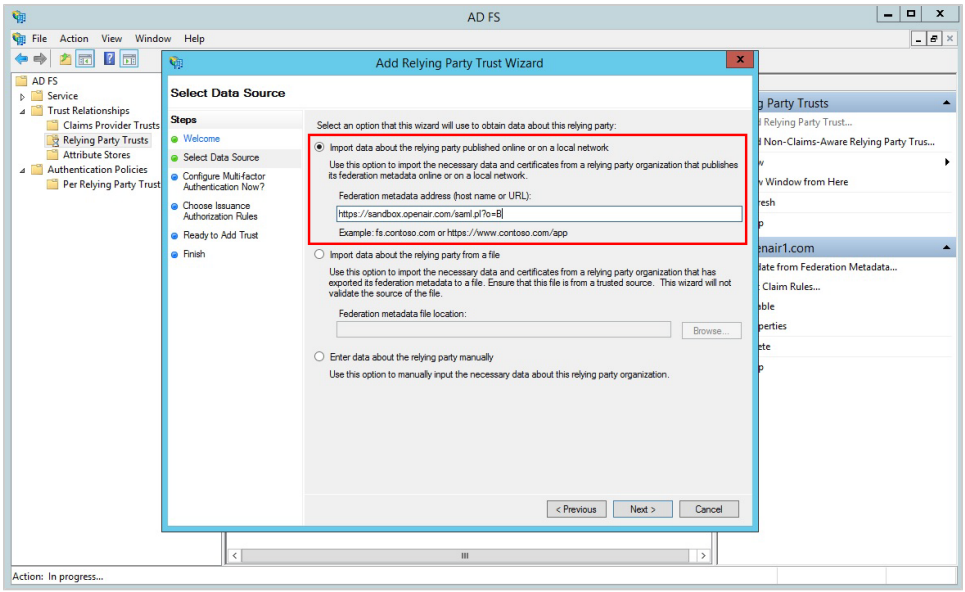
5. On the "Select Data Source" step, select "Import data about the relying party published online or on a local network," and enter one of the following in the "Federation metadata address (host name or URL)" field

   https://sandbox.openair.com/saml.pl?o=B (Sandbox metadata for testing)

   https://www.openair.com/saml.pl?o=B (Production metadata)

   > **Note:** This procedure uses the Sandbox metadata in its examples. To set up AD FS in Production, replace the references to the Sandbox URLs with the Production URLs.

   Click **Next**.



6. Click **OK** when the following warning appears:

   "AD FS Management: Some of the content in the federation metadata was skipped because it is not supported by AD FS. Review the properties of the trust carefully before you save the trust to the AD FS configuration database."

7. On the "Specify Display Name" step, enter a name for the Relying Party Trust in the "Display name" field. Click **Next**.

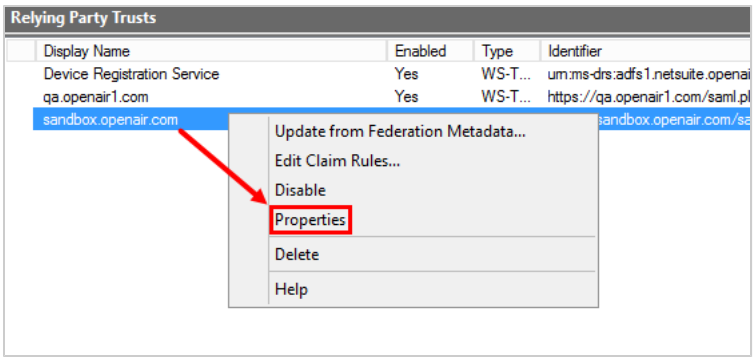
8. On the "Configure Multi-factor Authentication Now?" step, select "I do not want to configure multi-factor authentication settings for this relying party trust at this time." Click **Next**.

9. On the "Choose Issuance Authorization Rules" step, select the option permitted by your company's policies or preferences. Click **Next**.

10. Click **Next** on the "Ready to Add Trust" step.

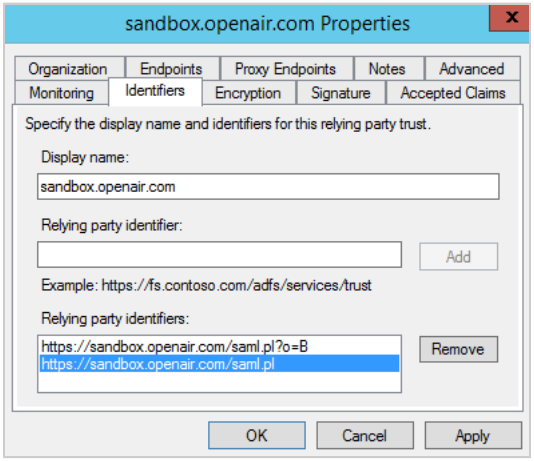
11. On the "Finish" step, clear the "Open the Edit Claim Rules dialog..." option and click **Close** on the "Finish" step.

12. Go to the "Relying Party Trusts" menu in AD FS, right-click the Relying Party Trust name you entered in step 7, and click "Properties".



13. Click the "Monitoring" tab and clear the "Monitor relying party" option. Click **Apply**.
14. In the "Encryption" tab, click **Remove** and click **Yes** in the confirmation message.
15. In the "Signature" tab, confirm that a certificate still appears in the list.
16. In the "Identifiers" tab, confirm that the **https://sandbox.openair.com/saml.pl?o=B** link appears, enter the following into the "Relying party identifier" field, and click **Add**:

    https://sandbox.openair.com/saml.pl

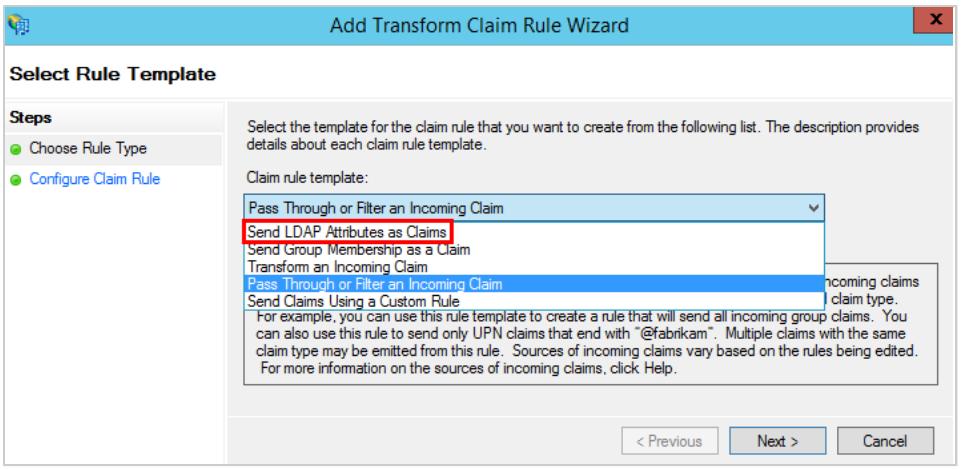


17. Click **OK** to close the Properties.

You will now need to create claim rules for your account's Company ID and nameID/User Name. The following steps set up examples of these Claim Rules. Please note that your company's specific claim rules may appear differently depending on what you use for nameID or companyID. See Identity Provider Setup for more details.

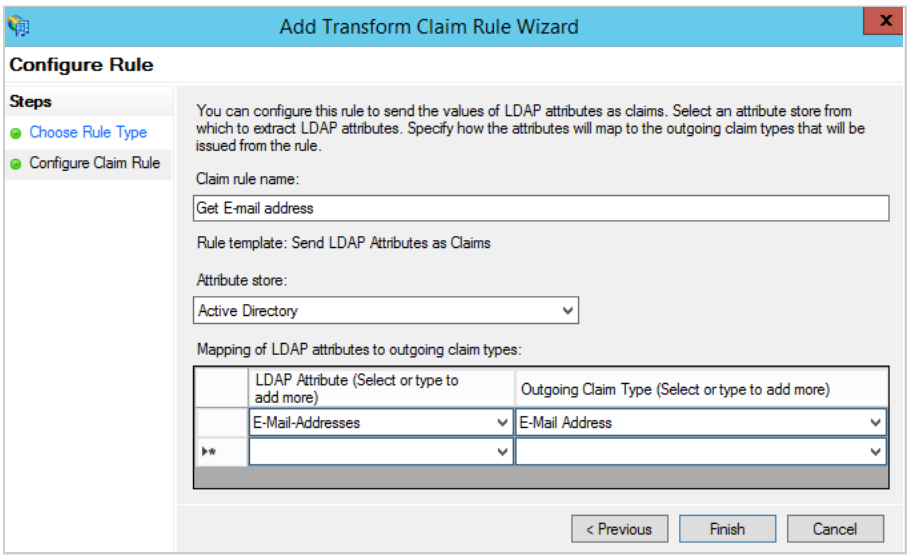
Set Up a Claim Rule Using E-mail Address as NameID

1. Go to the "Relying Party Trusts" menu in AD FS and right click the OpenAir Relying Party Trust. Click **Edit Claim Rules....**
2. Click **Add rule...**
3. In the "Choose Rule Type" step, select "Send LDAP Attributes as Claims" for the "Claim rule template". Click **Next**.



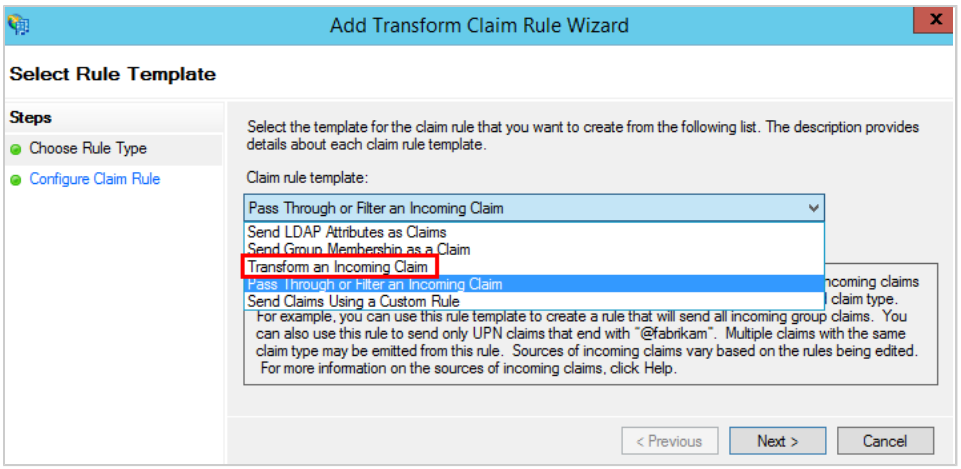
4. In the "Configure Claim Rule" step:
   - Enter a name for the rule in the "Claim rule name" field.
   - Select "Active Directory" from the "Attribute store" dropdown list.
   - Select "E-Mail-Addresses" in the "LDAP Attribute" list.
   - Select "E-Mail Address" in the Outgoing Claim Type" list.

   Click **Finish**.



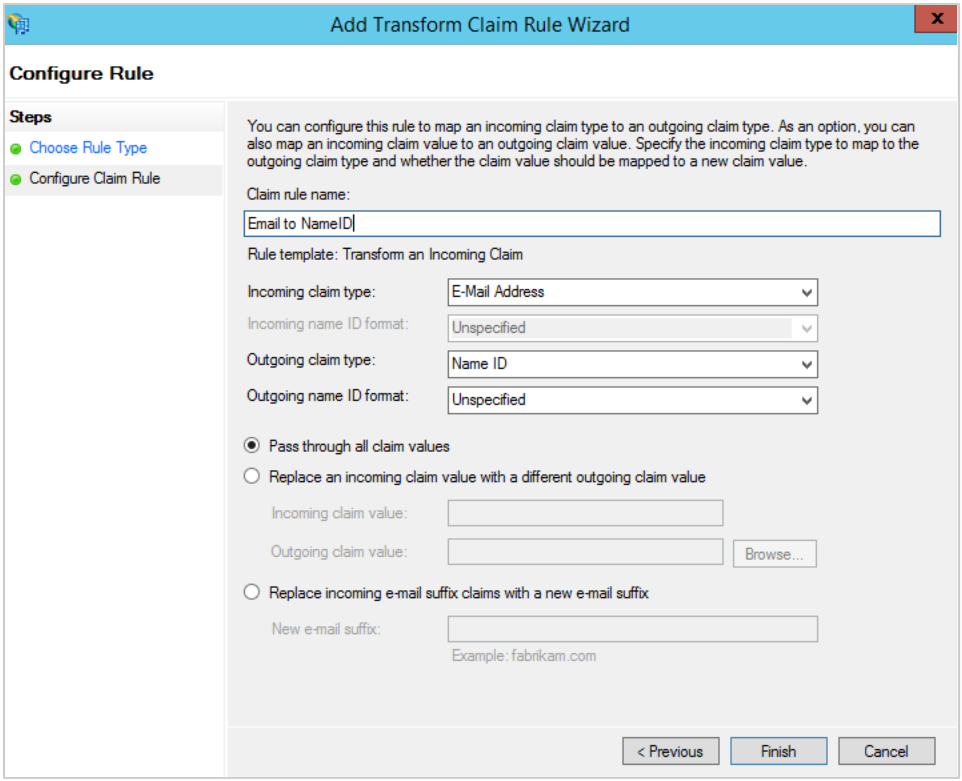
Set Up a Claim Rule to Transform an Incoming Claim

1. Go to the "Relying Party Trusts" menu in AD FS and right click the OpenAir Relying Party Trust. Click **Edit Claim Rules....**
2. Click **Add rule...**
3. In the "Choose Rule Type" step, select "Transform an Incoming Claim" for the "Claim rule template". Click **Next**.



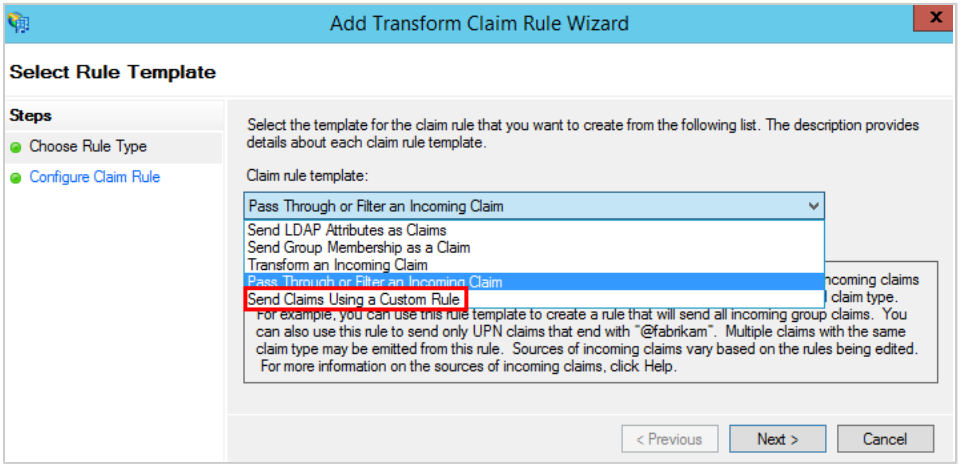
4. In the "Configure Claim Rule" step:
   - Enter a name for the rule in the "Claim rule name" field.
   - Select "E-Mail Address" in the "Incoming claim type" dropdown list.
   - Select "Name ID" in the "Outgoing claim type" dropdown list.
   - Select "Unspecified" in the "Outgoing name ID format" dropdown list.
   - Select "E-Mail Address" in the Outgoing Claim Type" list.
   - Select the "Pass through all claim values" radio button.

   Click **Finish**.



Set up a Claim Rule for a CompanyID

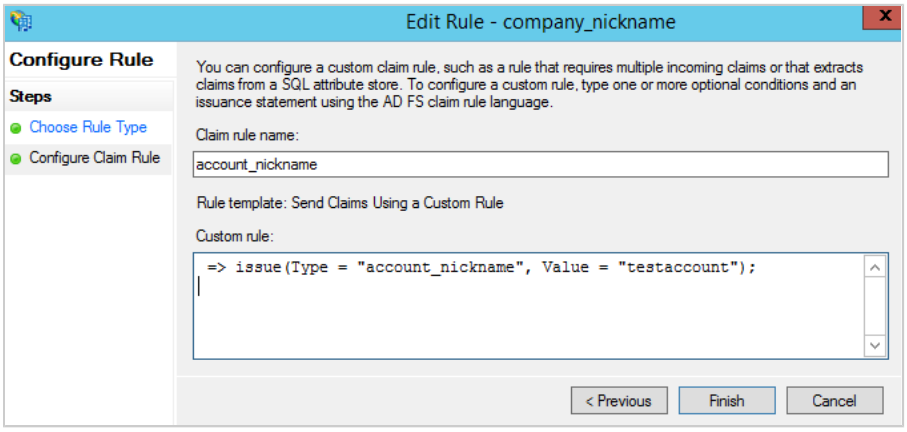
1. Go to the "Relying Party Trusts" menu in AD FS and right click the OpenAir Relying Party Trust. Click **Edit Claim Rules....**
2. Click **Add rule...**
3. In the "Choose Rule Type" step, select "Send Claims Using a Custom Rule". Click **Next**.



4. In the "Configure Claim Rule" step:
   - Enter a name for the rule in the "Claim rule name" field.
   - Enter **=> issue(Type = "account_nickname", Value = "testaccount");** in the "Custom rule" field.

> **Note:** You should replace "testaccount" in this example with your company's account nickname.

Click **Finish**.



18. Open a web browser and test your connection at the following address:

https://{your_federation_server_name}/adfs/ls/IdpInitiatedSignOn.aspx

OpenAir Account Configuration

OpenAir Customer Service or Professional Services can enable the SAML feature on request in your OpenAir account.

Once enabled, additional account settings for customizing your SAML user experience will be available at Administration > Integration: SAML Single Sign-On.