OpenAir
SAML 2 Quick Start Guide

April 13, 2019
Table of Contents

OpenAir SAML 2 Quick Start Guide ................................................................. 1
Identity Provider Setup ...................................................................................... 1
Provider Integration Setup ................................................................................... 1
OpenAir Account Configuration ....................................................................... 10
OpenAir Mobile Apps and SAML2 ................................................................. 12
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 ID 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 accountNickname**: OpenAir Company ID. This is the name of your OpenAir account.

3. [Optional] **SAML assertion string attribute userNickname**: alternate OpenAir User ID. If specified, the userNickname 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.

Custom configuration requirements for the following known IdP products are given in this section:

- PingFederate 6 or later
Provider Integration Setup

- Microsoft Active Directory Federation Services 2
- Shibboleth 2
- Okta
- OneLogin
- Symplified
- Microsoft AD FS 3.0
- Microsoft Azure AD

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 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.
Click Finish.

18. Open a web browser and test your connection at the following address:
https://{your_federation_server_name}/adfs/ls/IdpInitiatedSignOn.aspx

Microsoft Azure AD

**Important:** SAML SSO can be configured on Microsoft Azure AD Premium only.

The Free and Basic versions of Microsoft Azure AD only support pre-configured attributes in the SAML assertion. It is not possible to rename or add the custom attributes `user_nickname` and `account_nickname` required by OpenAir Service Provider when using MS Azure AD Free or MS Azure AD Basic.

1. Sign in to the Azure Portal using your Azure Active Directory administrator account.
2. Browse to Azure Active Directory > Enterprise Applications > New application > Non-gallery application. The Add your own application pane displays.
3. Enter a Name for the application (e.g., “OpenAir Sandbox” or “OpenAir Production”) and click Add. The Application Overview screen displays.
4. Click **Single sign-on** on the left hand side pane, and select **SAML**. The SAML-based sign-on configuration screen displays.

5. Enter **Basic SAML Configuration** settings:
   - **Identifier (Entity ID)** — Enter one of the following:
     - https://sandbox.openair.com/saml.pl?o=B (Sandbox metadata for testing)
     - https://www.openair.com/saml.pl?o=B (Production metadata)
   - **Reply URL (Assertion Consumer Service URL)** — Enter one of the following:
     - https://sandbox.openair.com/saml.pl?o=P (Sandbox — for testing)
     - https://www.openair.com/saml.pl?o=P (Production)
   - Leave the optional fields **Sign on URL** and **Relay State** blank.

![Basic SAML Configuration](image)

6. Add the **User Attributes & Claims** `user_nickname` and `account_nickname`:
   a. Click **Add new claim**.
   b. Enter the **Name** `user_nickname`.
   c. From the **Source attribute** dropdown, select the source attribute containing the OpenAir User ID.
   d. Click **Save**. The attribute `user_nickname` is now listed in the table.
   e. Repeat steps a-d for the `account_nickname` attribute. You may select the source attribute containing the OpenAir Company ID from the dropdown or type the OpenAir Company ID as a constant.
   f. Delete all other attributes & claims that can be deleted.
7. Review the SAML Signing Certificate, download the Metadata XML file or make a note of the App Federation Metadata Url. OpenAir Customer Service or Professional Services will need this to enable the SAML feature or change the SAML settings on your account.

8. Review Setup Your Application Name and make a note of the Azure AD Identifier. You will need to provide this to OpenAir Customer Service or Professional Services.

9. Click Users and groups on the left hand side pane and assign users and group to this SAML application. Azure AD will not issue a token allowing a user to sign into the application unless Azure AD has granted access to the user. Users may be granted access directly, or through a group membership. To assign a user or group to your application, click the Assign Users button. Select the user or group you wish to assign, and click the Assign button.

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.
- **Account Overview:**
  - IdP Entity ID — This is set by OpenAir Customer Service or Professional Services when enabling the SAML feature. The Entity ID is part of the SAML service metadata Identity Provider should provide in order to enable the SAML feature.
  - SP Entity ID — This is OpenAir Service Provider Entity ID. Click the link to fetch the SAML metadata for OpenAir Service Provider.

- **Security Settings:**
  - Affiliate ID — If a SAML Affiliation is assigned at the Identity Provider, enter the affiliation ID included in the Identity Provider assertions. This is not required if the Affiliation ID is the same as the IdP Entity ID.

- **Protocol Settings**
  - Enable SP SSO:
    - If unchecked, Identity Provider initiated Single Sign-On (IdP-initiated SSO) is used.
    - If checked, Service Provider initiated Single Sign-On (SP-initiated SSO) is used.

- **Miscellaneous Settings:**
  - SP-initiated SSO alternate login URL — Enter the URL for the Single Sign-On page users need to be redirected to when attempting to login on the OpenAir default login page. This is also the page users will be redirected to, if there is no user interaction within a set period.
- **SP-initiated SSO alternate login text** — Enter any message to be displayed on the OpenAir default login page.

**OpenAir Mobile Apps and SAML2**

OpenAir Mobile Apps, including OpenAir Mobile for iPhone and OpenAir Mobile for Android, support SAML Single Sign-On. Both Service Provider initiated Single Sign-On (SP-initiated SSO) and Identity Provider initiated Single Sign-On (IdP-initiated SSO) are supported.