



SAML Single Sign-On



2024.1

July 24, 2024



Copyright © 2013, 2024, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

If this document is in public or private pre-General Availability status:

This documentation is in pre-General Availability status and is intended for demonstration and preliminary use only. It may not be specific to the hardware on which you are using the software. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to this documentation and will not be responsible for any loss, costs, or damages incurred due to the use of this documentation.

If this document is in private pre-General Availability status:

The information contained in this document is for informational sharing purposes only and should be considered in your capacity as a customer advisory board member or pursuant to your pre-General Availability trial agreement only. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described in this document may change and remains at the sole discretion of Oracle.

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle Master Agreement, Oracle License and Services Agreement, Oracle PartnerNetwork Agreement, Oracle distribution agreement, or other license agreement which has been executed by you and Oracle and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Sample Code

Oracle may provide sample code in SuiteAnswers, the Help Center, User Guides, or elsewhere through help links. All such sample code is provided "as is" and "as available", for use only with an authorized NetSuite Service account, and is made available as a SuiteCloud Technology subject to the SuiteCloud Terms of Service at www.netsuite.com/tos, where the term "Service" shall mean the OpenAir Service.

Oracle may modify or remove sample code at any time without notice.

No Excessive Use of the Service

As the Service is a multi-tenant service offering on shared databases, Customer may not use the Service in excess of limits or thresholds that Oracle considers commercially reasonable for the Service. If Oracle reasonably concludes that a Customer's use is excessive and/or will cause immediate or ongoing performance issues for one or more of Oracle's other customers, Oracle may slow down or throttle Customer's excess use until such time that Customer's use stays within reasonable limits. If Customer's particular usage pattern requires a higher limit or threshold, then the Customer should procure a subscription to the Service that accommodates a higher limit and/or threshold that more effectively aligns with the Customer's actual usage pattern.

Table of Contents

OpenAir SAML Single Sign-On Overview	1
SAML Single Sign-On	1
SAML Deployment Best Practice Guidelines	2
Deploying SAML Single Sign-On on Your OpenAir Account	2
OpenAir Mobile Apps and SAML Single Sign-On	3
Configuring the Identity Provider for the SAML Integration	4
OpenAir SAML Metadata	5
SAML Assertion Attributes	5
Updating the OpenAir SAML Signing and Encryption Certificates in the Identity Provider Configuration	6
Configuring Microsoft AD FS 3.0 for the SAML Integration	8
Configuring Microsoft Entra ID for the SAML Integration	14
Configuring the SAML Integration in OpenAir	18
Adding a New Identity Provider Profile	18
Deleting an Identity Provider Profile	19
Changing Profile Details or Upload the Metadata for an Identity Provider	19
Viewing Audit Trail Information for Identity Provider Profiles	21
Testing the SAML Integration	22
Enabling Employees to Sign In Using SAML Single Sign-On	23
Creating a Support Case	25

OpenAir SAML Single Sign-On Overview

The OpenAir SAML Single Sign-On (SSO) feature lets you use an external identity provider service to manage user access to your OpenAir account.

For more information about the SAML SSO feature, including a brief review of key terminology, feature requirements and limitations, see [SAML Single Sign-On](#).

For best practice guidelines to ensure the seamless deployment of SAML SSO on your account, see [SAML Deployment Best Practice Guidelines](#).

For an overview of steps required to set up and deploy SAML SSO on your OpenAir account, see [Deploying SAML Single Sign-On on Your OpenAir Account](#).

OpenAir Mobile supports OpenAir single sign-on. See [OpenAir Mobile Apps and SAML Single Sign-On](#).

SAML Single Sign-On

Security Assertion Markup Language (SAML) is an OASIS open standard that supports secure communication of user authentication, entitlement and attribute information between different enterprise applications. It provides a method of secure integration with existing, on-site authentication infrastructures without exposing these services to direct public access, and enables federation of user identity across any number of additional services. SAML enables single sign-on (SSO), a scheme that allows users to sign in to one application — the identity provider — and automatically have access to separate applications — the service providers — without having to sign in to each of these other applications separately.

- The **identity provider (IdP)** validates the identity of the user and makes an SAML assertion to authorize access to a service provider. As a user, the IdP service is often a sign-in page where you enter your SSO sign-in details, or a dashboard you can use to access different enterprise applications.
- The **service provider (SP)** consumes the SAML assertion and grants the user access to the application.
- The **SAML assertion** uses a XML-based standard to send security information that applications working across security domain boundaries can trust.
- The SP and IdP use the **metadata** provided during configuration to establish a circle of trust.

The OpenAir SAML SSO feature uses the SAML version 2.0 specifications. For information about the SAML standard, refer to the [OASIS website](#).



Important: IdP services must support SAML 2.0 and allow custom assertions to be used with the OpenAir SAML SSO feature.

The OpenAir SAML SSO feature supports:


- IdP-initiated SSO — Typically, the user goes to the IdP service, signs in, and clicks a link or a button on the IdP page to access OpenAir. The IdP service redirects the user to OpenAir with a SAML assertion.
- SP-initiated SSO — Typically, the user goes to the OpenAir sign-in page for SSO users, enters the company ID and user ID. OpenAir redirects the user to the IdP service with an SAML request. The IdP prompts the user to enter a password, validates the identity of the user and redirects the user to OpenAir with an SAML assertion.
- Integration with multiple identity providers.

OpenAir account administrators control who can use SAML SSO to access OpenAir.

SAML Deployment Best Practice Guidelines


This section provides best practice guidelines for deploying SAML single sign-on (SSO) on your OpenAir account.

- For an initial SAML deployment:
 - Test the SAML deployment on a sandbox account. Make sure it works as expected before you deploy SAML to your production account.
 - When you deploy SAML to your production account, only enable a small group of OpenAir users to sign in using SAML SSO. Make sure it works as expected before you enable all users to login using SAML SSO.
- When changing over to a new identity provider (IdP):
 - Test the new IdP configuration on a sandbox account. Make sure it works as expected before you change the IdP configuration on your production account. To discuss procuring a sandbox account for this purpose, contact your OpenAir account manager.
- Always have at least one account administrator who can sign in to OpenAir using password authentication. This will ensure an account administrator will be able to access your account in case there is an unexpected problem with SAML. If you enable a user to login using SAML SSO, this user can no longer use the default password authentication method to access OpenAir.
- OpenAir SAML certificates on sandbox and production environments have a finite lifetime. OpenAir rotates SAML certificates that are about to expire. When OpenAir rotates the SAML certificates, you must update the SAML signing and encryption certificates for the OpenAir service provider profile in your identity provider product. See [Updating the OpenAir SAML Signing and Encryption Certificates in the Identity Provider Configuration](#).

 **Note:** Before OpenAir rotates the SAML certificates, you will receive a proactive feature change notification (PFCN) with information about the dates when new certificates will become available and previous certificates are due to expire.

Deploying SAML Single Sign-On on Your OpenAir Account

This section gives an overview of steps required to set up and deploy SAML single sign-on (SSO) on your OpenAir account.

 **Important:** Make sure you review the best practice guidelines before deploying SAML SSO on your OpenAir account or changing over to a new identity provider (IdP) — See [SAML Deployment Best Practice Guidelines](#).

To deploy SAML SSO on your OpenAir account

1. **Configure the identity provider (IdP) for the SAML integration** — Import the OpenAir service provider metadata XML file and configure the attributes required in the SAML assertion by the OpenAir service provider. See [Configuring the Identity Provider for the SAML Integration](#)
2. **Configure the SAML Integration in OpenAir** — Go to Administration > Global Settings > Account > Integration: SAML Single Sign-On and modify the settings are required. See [Configuring the SAML Integration in OpenAir](#).
3. **Test the SAML integration** — See [Testing the SAML Integration](#).

4. **Enable employees to sign in using SAML single sign-on** — Create the `saml_auth` custom field associated with the Employee entity form and check the corresponding box on the employee demographic form for SAML SSO users. See [Enabling Employees to Sign In Using SAML Single Sign-On](#).

Contact OpenAir Customer Support if you have any questions or encounter any difficulties when deploying SAML SSO on your OpenAir account. See [Creating a Support Case](#).


OpenAir Mobile Apps and SAML Single Sign-On

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.

For information about setting up OpenAir Mobile to sign in using SAML single sign-on, see  [OpenAir Mobile 3 User Guide](#).

Configuring the Identity Provider for the SAML Integration

This section describes the information you need to configure your identity provider (IdP) product for the SAML integration.

 **Important:** Note the following requirements:


- IdP services must support SAML 2.0. In particular IdP services must support Redirect/POST bindings, and POST responses containing the SAML authentication assertion must be digitally signed.
- IdP services must allow custom assertions.
- SAML assertion encryption is optional, but should be used.
- Make sure you review the best practice guidelines before deploying SAML SSO on your OpenAir account or changing over to a new identity provider (IdP) — See [SAML Deployment Best Practice Guidelines](#).

The following IdP configuration steps are required before SAML authentication assertions can be exchanged between the IdP and the OpenAir service provider (SP). Specific IdP products may require custom configuration — refer to the IdP product documentation for details.

1. **Import the OpenAir service provider (SP) metadata** — See [OpenAir SAML Metadata](#).
2. **Configure the assertion attributes required by the OpenAir SP** — Either of the attribute NameID or user_nickname must be included in the SAML assertion. See [SAML Assertion Attributes](#).
3. **Download the IdP metadata XML file** — You will need to upload the IdP metadata XML file when configuring OpenAir to work with the IdP service, or when you need to update the metadata (after a new security certificate for your IdP service, for example).

OpenAir SAML certificates on sandbox and production environments have a finite lifetime. OpenAir rotates SAML certificates that are about to expire. When OpenAir rotates the SAML certificates you must update the SAML signing and encryption certificates for the OpenAir service provider profile in your identity provider product. See [Updating the OpenAir SAML Signing and Encryption Certificates in the Identity Provider Configuration](#).

This guide includes steps to set up the following identity provider products with OpenAir SAML SSO.

 **Important:** The third party product setup steps are given for illustration purposes only. OpenAir does not support specific identity provider products or product versions. Refer to the product documentation for your identity provider for detailed and updated instructions. For additional questions about setting up your identity provider, please contact the Support services for your identity provider product.

- [Configuring Microsoft AD FS 3.0 for the SAML Integration](#)
- [Configuring Microsoft Entra ID for the SAML Integration](#)


OpenAir SAML Metadata

The first step in configuring the identity provider (IdP) service for the SAML integration is to create a service provider (SP) profile for OpenAir.

OpenAir generates a unique SAML **Entity ID** (metadata URL) and **Assertion Consumer Service URL** for each identity provider profile you create. To find the correct **Entity ID** and **Assertion Consumer Service URL** to use in the SP profile for OpenAir, go to Administration > Global Settings > Account > Integration: SAML Single Sign-On and do one of the following:

- Click the name of the identity provider profile, if a profile exists for the identity provider.
- Add a profile for the identity provider, if a profile does not already exist. See [Adding a New Identity Provider Profile](#).

The Identity provider profile form appears and shows the **Entity ID** (metadata URL) and **Assertion Consumer Service URL** under the Service Provider section.

 **Service Provider**


Entity ID
<https://auth.openair.com/sso/metadata/> (URL, http://localhost:3000)

Assertion Consumer Service (ACS) URL
<https://auth.openair.com/sso/acs/> (URL, http://localhost:3000)

SAML Assertion Attributes

After you have created a service provider (SP) profile for OpenAir and imported the OpenAir SAML metadata into your IdP service, you need to ensure that SAML assertions contain the required attributes with the appropriate OpenAir sign-in identifiers.

This following table lists both required and optional assertion attributes and the OpenAir sign-in identifiers they map to.

Attribute	Required / Optional	Description
NameID	Required	<p>OpenAir User ID — The unique user identifier (Employee ID on the employee demographic form in OpenAir).</p> <div style="border: 1px solid #ffc107; padding: 5px; margin-top: 10px;"> <p> Important: Depending on your IdP configuration, you may not be able to map NameID to the source attribute containing the OpenAir User ID. For example, the IdP service may use NameID as a transient identifier for session management. If this is the case:</p> <ul style="list-style-type: none"> ■ The assertion must contain both NameID and user_nickname attributes. ■ Use user_nickname to send the OpenAir User ID in the SAML assertion. </div>
user_nickname	Optional	If specified, user_nickname takes precedence over NameID for identifying the user. You can use user_nickname to send the OpenAir User ID in the SAML assertion if NameID cannot be used.

Note: The attribute `account_nickname` is no longer required. The OpenAir SAML endpoint is unique to your OpenAir account and to each IdP profile.

Updating the OpenAir SAML Signing and Encryption Certificates in the Identity Provider Configuration

SAML signing and encryption certificates provide additional security when using SAML single sign-on (SSO) authentication to access OpenAir. SAML signing and encryption uses public keys, or certificates, to verify data sent between the OpenAir service provider (SP) and the identity provider (IdP). The IdP uses the signing certificate to verify the signature sent by the OpenAir SP during the authentication request. The IdP uses the encryption certificate to conceal the content in the return response (assertion) to the OpenAir SP.

OpenAir SAML certificates on sandbox and production environments have a finite lifetime. OpenAir rotates SAML certificates that are about to expire.

When OpenAir rotates the SAML certificates, you must retrieve SAML certificate information from your OpenAir account, save it in the correct format and import it in to your identity provider product on the service provider profile you created for this OpenAir account.

Important: Do not download the SSL certificate from your browser header. SAML certificates are distinct from SSL (TLS) certificates. SSL certificates apply to the browser you use to access OpenAir and they are configured and maintained by the server.

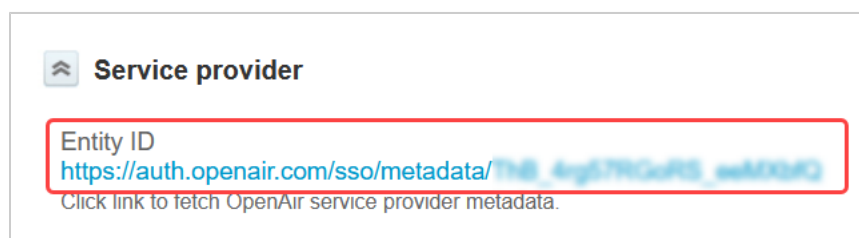
Before OpenAir rotates the SAML certificates, you will receive a proactive feature change notification (PFCN) with information about the dates when new certificates will become available and previous certificates are due to expire.

To update the OpenAir SAML signing and encryption certificates in your identity provider configuration:

1. In OpenAir, go to Administration > Account> Integration: SAML Single Sign-On > [Select the active identity provider profile].

The identity provider profile form opens.

2. Click the link under **Entity ID**.



The OpenAir SAML metadata associated with the identity provider profile appears.

3. Right-click anywhere on the page and select **View Page Source** from the context menu.

The page source appears.

```

1 <md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://auth.openair.com/sso/metadata/166.483790401_wwwopenair">
2 <md:SPSSODescriptor AuthnRequestsSigned="1" WantAssertionsSigned="1" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
3 <md:KeyDescriptor use="signing">
4 <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
5 <ds:X509Data>
6 <ds:X509Certificate>
7 -----BEGIN CERTIFICATE-----
8 MIIEAjCCAgICgAwwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAA
9 QgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQ
10 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
11 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
12 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
13 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
14 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
15 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
16 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
17 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
18 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
19 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
20 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
21 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
22 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
23 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
24 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
25 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
26 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
27 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
28 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
29 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
30 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
31 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
32 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
33 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
34 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
35 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
36 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
37 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
38 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
39 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
40 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
41 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
42 AAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgEAAQAAQgIwAgE
43 -----END CERTIFICATE-----
44 </ds:X509Certificate>
45 </ds:X509Data>
46 </ds:KeyInfo>
47 </md:KeyDescriptor>

```

4. Copy the text between the <ds:X509Certificate> and </ds:X509Certificate> tags.
Make sure that you select the entire certificate text and only the certificate text before you copy it to your clipboard. Do not select any of the characters in the <ds:X509Certificate> and </ds:X509Certificate> tags.

5. Paste the content of the clipboard into a text editor.
6. Insert the following certificate header on a separate line at the top.

```

1 | -----BEGIN CERTIFICATE-----

```

7. Insert the following certificate footer on a separate line at the bottom.

```

1 | -----END CERTIFICATE-----

```

8. Save the file. Use the file extension .pem or .crt depending on the file extension required by the identity provider product for SAML certificates.

```

1  -----BEGIN CERTIFICATE-----
2  MIIEvDCCBgkqhkiG9w0BCQsBAQswCgYIKoZIeHjVGA1BgEEAQYwRjEwLwYw
3  RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
4  RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
5  RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
6  RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
7  RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
8  RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
9  RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
10 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
11 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
12 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
13 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
14 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
15 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
16 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
17 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
18 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
19 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
20 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
21 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
22 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
23 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
24 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
25 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
26 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
27 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
28 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
29 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
30 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
31 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
32 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
33 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
34 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
35 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
36 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
37 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
38 RjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYwRjEwLwYw
39  -----END CERTIFICATE-----

```

9. In your identity provider product, go to the service provider profile you set up for your OpenAir account and import the PEM or CRT SAML certificate file for OpenAir under both the Signing certificate and Encryption certificate sections.

Configuring Microsoft AD FS 3.0 for the SAML Integration

This section provides the steps to set up Microsoft Active Directory Federation Service (AD FS) 3.0 to provide single sign-on (SSO) access to OpenAir using the OpenAir SAML SSO feature.

**Important: The following configuration steps are given for illustration purposes only.**

OpenAir does not support specific identity provider products or product versions. The following steps may not reflect the latest identity provider product version. Refer to Microsoft product documentation for detailed and updated instructions about Microsoft ADFS. For additional questions about setting up Microsoft ADFS, please contact Microsoft Support.

To Configure Microsoft AD FS 3.0 for the SAML Integration:

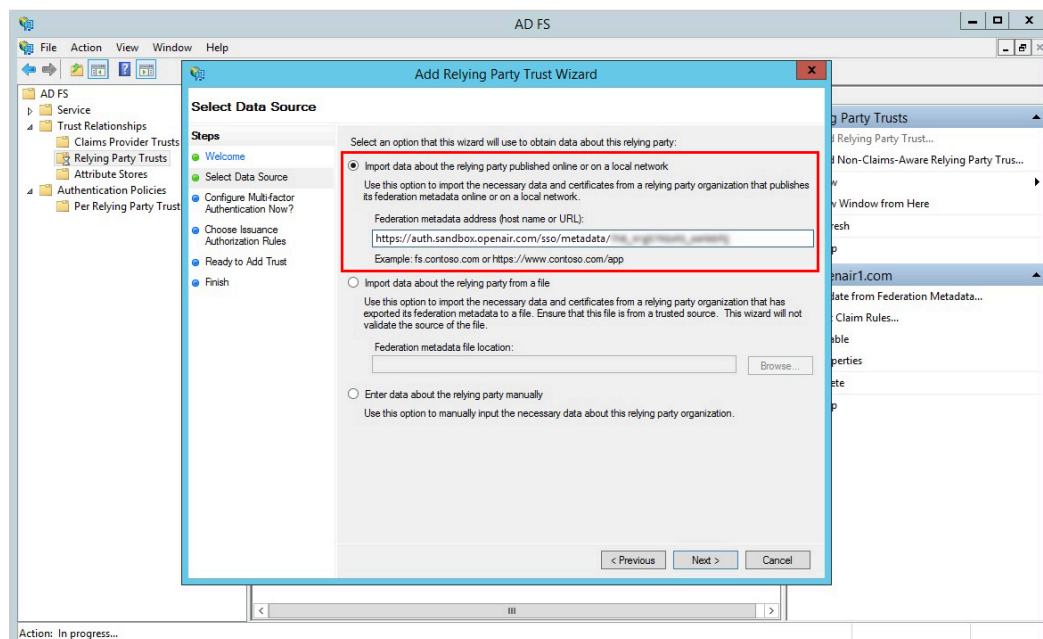
1. Make sure that you have installed the following patch on your AD FS server:
 - Windows Server 2012 (R2) — **KB3003381**

This patch 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 file 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 the **Federation metadata address (host name or URL)**:
 - https://auth.sandbox.openair.com/sso/metadata/<unique_ref_generated_by_OpenAir>, if testing the SAML deployment on a sandbox OpenAir account.
 - https://auth.openair.com/sso/metadata/<unique_ref_generated_by_OpenAir>, if deploying SAML SSO on a production OpenAir account.



Note: Examples in this help topic use a sample metadata URL generated for a sandbox account. To set up AD FS SSO with your production or sandbox account, replace the URL with the unique **Entity ID** generated by OpenAir on the identity provider profile you created for Microsoft AD FS 3.0 on your OpenAir account. See [OpenAir SAML Metadata](#).

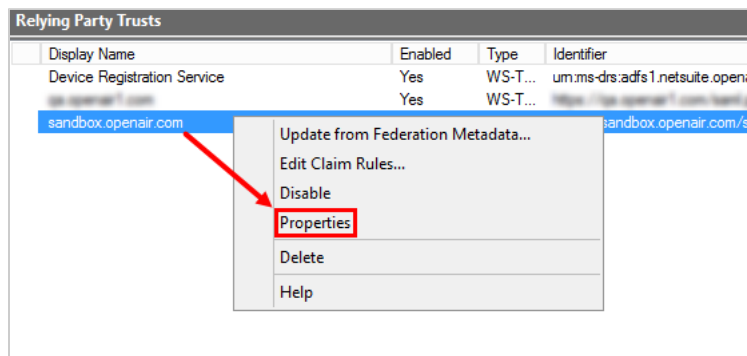
Click **Next**.



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.”

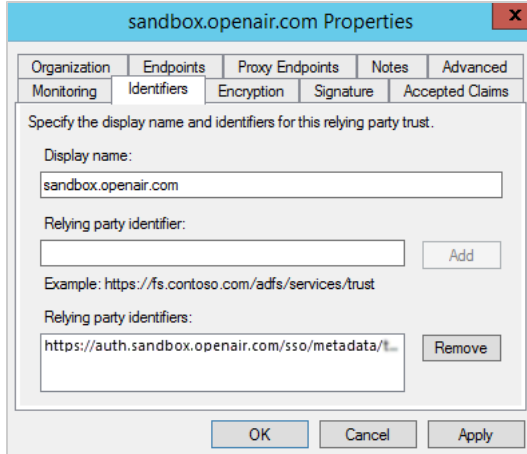
Click **OK**

6. On the “Specify Display Name” step, enter a **Display name** for the Relying Party Trust, and click **Next**.
7. 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**, and click **Next**.
8. On the “Choose Issuance Authorization Rules” step, select the option permitted by your company’s policies or preferences then click **Next**.
9. On the “Ready to Add Trust” step, click **Next**.
10. On the “Finish” step, clear the **Open the Edit Claim Rules dialog...** box, and click **Close**.
11. In AD FS, go to Relying Party Trusts, right-click the display name you entered for the OpenAir SAML endpoint, and click **Properties**.



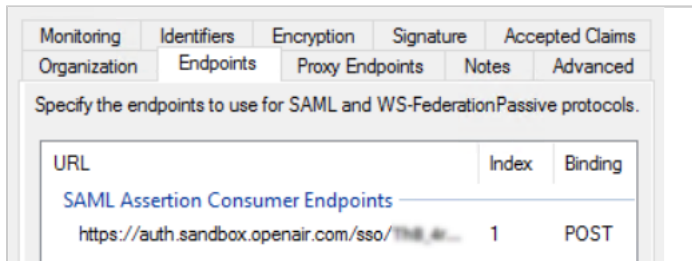
12. On the Monitoring tab, clear the **Monitor relying party** box, and click **Apply**.
13. On the Encryption tab, click **Remove**, then click **Yes** to confirm.
14. On the Signature tab, verify that a certificate still appears in the list.
15. On the Identifiers tab, verify that **Relying party identifiers** includes the relevant OpenAir metadata URL:
 - https://auth.sandbox.openair.com/sso/metadata/<unique_ref_generated_by_OpenAir>, if testing the SAML deployment on a sandbox OpenAir account.
 - https://auth.openair.com/sso/metadata/<unique_ref_generated_by_OpenAir>, if deploying SAML SSO on a production OpenAir account.

Note: Examples in this help topic use a sample metadata URL generated for a sandbox account. To set up AD FS SSO with your production or sandbox account, replace the URL with the unique **Entity ID** generated by OpenAir on the identity provider profile you created for Microsoft AD FS 3.0 on your OpenAir account. See [OpenAir SAML Metadata](#).



16. On the Endpoints tab, verify that the list of **SAML Assertion Consumer Endpoints** includes the relevant OpenAir SAML endpoint:
 - URL: `https://auth.sandbox.openair.com/sso/acs/<unique_ref_generated_by_OpenAir>` — Index: 1 — Binding: POST, if testing the SAML deployment on a sandbox OpenAir account.
 - URL: `https://auth.openair.com/sso/acs/<unique_ref_generated_by_OpenAir>` — Index: 1 — Binding: POST, if deploying SAML SSO on a production OpenAir account.

Note: Examples in this help topic use a sample Assertion Consumer Service URL generated for a sandbox account. To set up AD FS SSO with your production or sandbox account, replace the URLs with the unique **Assertion Consumer Service URL** generated by OpenAir on the identity provider profile you created for Microsoft AD FS 3.0 on your OpenAir account. See [OpenAir SAML Metadata](#).



17. Click **OK**.
18. Set up claim rules to ensure that SAML assertions contain the required attributes with the appropriate OpenAir sign-in identifiers. See [Creating Claim Rules to Send OpenAir Sign-In Identifiers as SAML Assertion Attributes](#).
19. To test your connection, open a web browser and go to the following web address:
`https://<your_federation_server_name>/adfs/ls/IdpInitiatedSignOn.aspx`

Creating Claim Rules to Send OpenAir Sign-In Identifiers as SAML Assertion Attributes

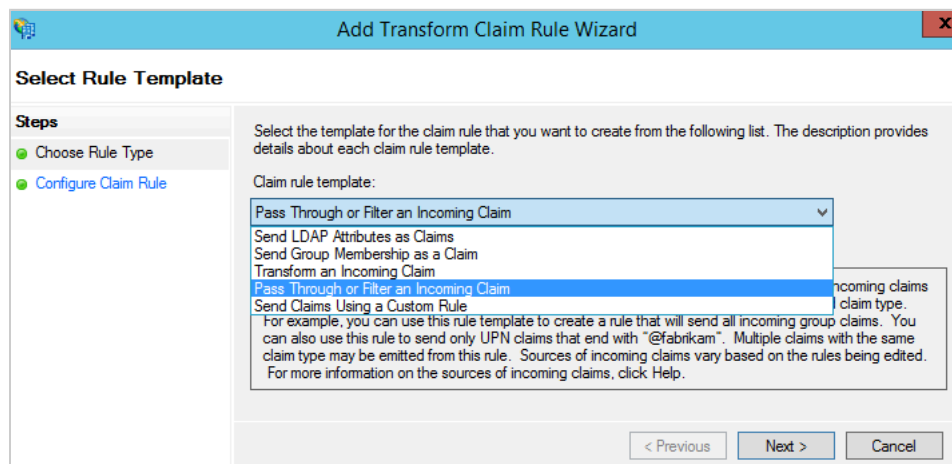
The type and configuration of claim rules you use depend on the values used to populate the SAML assertion attributes (or outgoing claim type), as well as any convention used for the OpenAir User ID in your company. This guide provides steps for the following examples:

- **NameID**— If the OpenAir User ID is the same as the user's Active Directory email address, create two rules and map it to the NameID assertion attribute. See [Mapping the Active Directory Email Address to the NameID Assertion Attribute](#).
- The attribute `account_nickname` is no longer required. The OpenAir SAML endpoint is unique to your OpenAir account and to each identity provider profile.

For general guidelines about SAML assertion attributes expected by OpenAir, see [SAML Assertion Attributes](#).

To create a claim rule:

1. In AD FS, go to Relying Party Trusts, right-click the display name you entered for the OpenAir SAML endpoint, and click **Edit Claim Rules...**
2. Click **Add rule...**. The Add transform claim rule wizard appears.
3. Choose Rule Type page — Select the appropriate **Claim rule template**, and click **Next**.



- To use values from attributes in Lightweight Directory Access Protocol (LDAP) attribute store and associate a claim type with each of the LDAP attributes, use **Send LDAP Attributes as Claims**.
 - To use a value from an incoming claim type and map it to a different claim type or map its claim value to a new claim value in the outgoing assertion, use **Transform an Incoming Claim**. For example, you can use this template to use the value from the E-mail Address from an incoming claim type and map it to the Name ID outgoing claim type, if this is what you use as OpenAir User ID.
 - To use more advanced options and write a custom rule in AD FS claim rule language, use **Send Claims Using a Custom Rule**.
4. Configure Claim Rule page — Enter a **Claim rule name**, and other claim rule configuration settings. These settings depend on the chosen claim rule template.

5. Click **Finish**.

Mapping the Active Directory Email Address to the NameID Assertion Attribute

If the OpenAir User ID is the same as the user's Active Directory email address, you can create two rules to get the email address and map it to the NameID assertion attribute.

To map the AD email address to the NameID assertion attribute:

1. Create a claim rule using the **Send LDAP Attributes as Claims** template and use the following steps on the Configure Claim Rule page. See [Creating Claim Rules to Send OpenAir Sign-In Identifiers as SAML Assertion Attributes](#).
 - a. Click the **Attribute store** dropdown, and select **Active Directory**.
 - b. Click the cell under **LDAP Attribute**, and select **E-Mail-Addresses**.
 - c. Click the cell under **Outgoing Claim Type**, and select **Name ID**.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:
Get E-mail address

Rule template: Send LDAP Attributes as Claims

Attribute store:
Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
	E-Mail-Addresses	E-Mail Address
▶*		

< Previous Finish Cancel

2. Create a claim rule using the **Transform an Incoming Claim** template and use the following steps on the Configure Claim Rule page. See [Creating Claim Rules to Send OpenAir Sign-In Identifiers as SAML Assertion Attributes](#).
 - a. Click the **Incoming claim type** dropdown, and select **E-Mail Address**.
 - b. Click the **Outgoing claim type** dropdown, and select **Name ID**.
 - c. Click the **Outgoing name ID format** dropdown, and select **Unspecified**.
 - d. Select **Pass through all claim values**.

Configuring Microsoft Entra ID for the SAML Integration

This section provides the steps to set up Microsoft Entra ID, formerly known as Microsoft Azure AD, to provide single sign-on (SSO) access to OpenAir using the OpenAir SAML SSO feature.



Important: The following configuration steps are given for illustration purposes only.

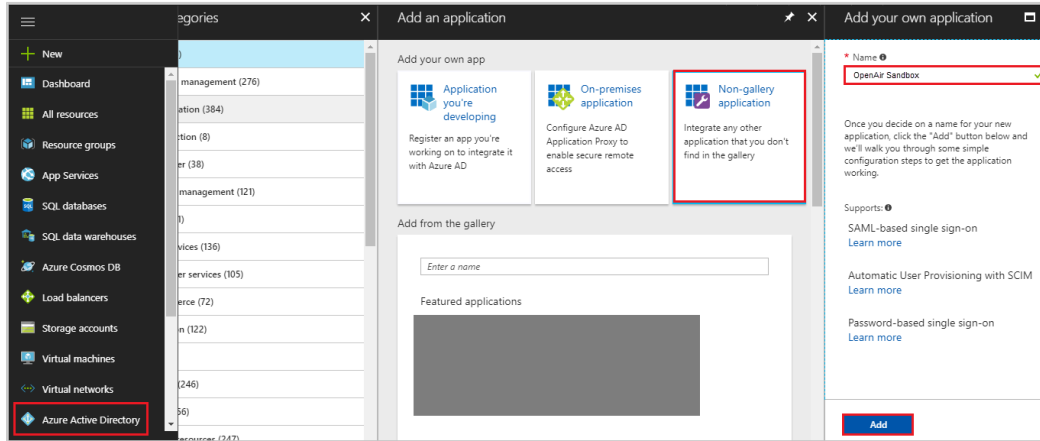
OpenAir does not support specific identity provider products or product versions. The following steps do not reflect the latest identity provider product version and still refer to the product name at the time these steps were written and tested. The Refer to Microsoft product documentation for detailed and updated instructions about Microsoft Entra ID. For additional questions about setting up Microsoft Entra ID, please contact Microsoft Support.

Microsoft Azure AD Premium is required. The Free and Basic versions of Microsoft Azure AD only support preconfigured attributes in the SAML assertion and do not let you define the custom attribute `user_nickname` required by the OpenAir service provider.

To configure Microsoft Azure AD for the SAML integration

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 (“OpenAir Sandbox” or “OpenAir Production”, for example) 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 the Entity ID generated by OpenAir on the identity provider profile you created for Microsoft Azure on your OpenAir account.
 - `https://auth.sandbox.openair.com/sso/metadata/<unique_ref_generated_by_OpenAir>` (Sandbox account)
 - `https://auth.openair.com/sso/metadata/<unique_ref_generated_by_OpenAir>` (Production account)
 - **Reply URL (Assertion Consumer Service URL)** — Enter the Assertion Consumer Service URL generated by OpenAir on the identity provider profile you created for Microsoft Azure on your OpenAir account.
 - `https://auth.sandbox.openair.com/sso/acs/<unique_ref_generated_by_OpenAir>` (Sandbox account)
 - `https://auth.openair.com/sso/acs/<unique_ref_generated_by_OpenAir>` (Production account)

Note: Examples in this help topic use sample Entity ID and Assertion Consumer Service URL generated for a sandbox account. To set up Microsoft Azure with your production or sandbox account, replace the URLs with the unique **Entity ID** and **Assertion Consumer Service URL** generated by OpenAir on the identity provider profile you created for Microsoft Azure on your OpenAir account. See [OpenAir SAML Metadata](#).

- Leave the optional fields **Sign on URL** and **Relay State** blank.

Basic SAML Configuration

Save

Values for the fields below are provided by OpenAir Production. You may either enter those values manually, or upload a pre-configured SAML metadata file if provided by OpenAir Production. [Upload metadata file.](#)

Select a file

* Identifier (Entity ID)

* Reply URL (Assertion Consumer Service URL)

^ Set additional URLs

Sign on URL

Relay State

6. Add the **User Attributes & Claims** user_nickname:
 1. Click **Add new claim**.
 2. Enter the **Name** user_nickname.
 3. From the **Source attribute** dropdown, select the source attribute containing the OpenAir User ID.
 4. Click **Save**. The attribute user_nickname is now listed in the table.
 5. Delete all other attributes & claims that can be deleted.

User Attributes & Claims

+ Add new claim

Name identifier value: **user.userprincipalname**

CLAIM NAME	VALUE
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/...	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/...	...

Manage user claims

* Name

Namespace

Source Attribute Transformation

* Source attribute

7. Review the **SAML Signing Certificate** and download the **Metadata XML** file. OpenAir Customer Service or OpenAir Professional Services will need the **Metadata XML** file to enable the SAML feature or change the SAML settings on your account.
8. 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 in to 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 want to assign, and click the **Assign** button.

Configuring the SAML Integration in OpenAir

The SAML integration administration page becomes available after the feature is enabled. To view or change the SAML integration settings for your OpenAir account, go to Administration > Global Settings > Account > Integration: SAML Single Sign-On.

You can configure the OpenAir SAML Single Sign-On feature to work with multiple identity providers. The list on the SAML integration administration page lets you manage the profile and upload the metadata for each identity provider.

The OpenAir SAML Single Sign-On feature lets you:

- Configure the OpenAir SAML Single Sign-On feature to work with multiple identity providers.

Important: Multiple identity provider support is currently available only for identity provider initiated single sign-on.

- Review configured identity providers from a list view. To view the list of identity provider profiles for your OpenAir account, go to Administration > Global Settings > Account > Integration: SAML Single Sign-On.
- Add identity provider profiles. See [Adding a New Identity Provider Profile](#).
- Delete identity provider profiles. See [Deleting an Identity Provider Profile](#).
- Change identity provider profiles:
 - Set or change the profile details and upload the SAML metadata file for each identity provider as and when required.
 - Set any identity providers as active. Only active identity providers can be used for service provider or identity provider initiated single sign-on.
 - Select one default identity provider. If the default identity provider is configured to be used with service provider initiated single sign-on request, it will serve as the identity provider when using the OpenAir sign-in page for single sign-on users.

See [Changing Profile Details or Upload the Metadata for an Identity Provider](#).

- View audit trail information for all identity provider profiles. See [Viewing Audit Trail Information for Identity Provider Profiles](#).

Integration: SAML Single Sign-On		All		Untitled*	Download	More
Identity Provider name	Active	Default	Notes	Updated	SAML Identity Provider meta-data	Service Provider initiated SSO
Google	✓		Expires on Dec 01, 2022	09/08/22 07:14 AM	selfservice1_30880.xml	✓
Legacy profile	✓	✓	Expires on Nov 01, 2022	09/08/22 07:14 AM		✓
OKTA	✓		Expires on Jan 01, 2022	09/08/22 07:15 AM	selfservice1_10880_single_line...	✓

Adding a New Identity Provider Profile

You can add new identity provider profiles and configure the OpenAir SAML Single Sign-On feature to work with multiple identity providers.

To add a new identity provider profile:

1. Go to Administration > Global Settings > Account > Integration: SAML Single Sign-On.
2. Click the Create button then New Identity provider.
The Identity provider profile form appears.
3. Enter an **Identity provider name** and all other profile details. Upload the metadata for the identity provider. For more information about the profile details on the form, see [Changing Profile Details](#) or [Upload the Metadata for an Identity Provider](#).

Deleting an Identity Provider Profile

You can delete obsolete identity provider profiles at any time.



Important: The identity provider profile marked as **Default**

To delete an identity provider profile:

1. Go to Administration > Global Settings > Account > Integration: SAML Single Sign-On.
2. Click the name of the identity provider profile you want to delete.
The Identity provider profile form appears.
3. Click **Delete**.
4. Click **OK** to confirm

Changing Profile Details or Upload the Metadata for an Identity Provider

You can change the profile details and upload the metadata for each identity provider on the SAML single sign-on integration administration page at any time.

To change profile details or upload the metadata for an identity provider:

1. Go to Administration > Global Settings > Account > Integration: SAML Single Sign-On.
2. Click the name of the identity provider profile.
3. Change all profile details and upload the metadata for the identity provider as required. The form includes the following information:
 - **Identity provider name** — (Required) Enter a name for the identity provider profile.
 - **SAML identity provider metadata** — To upload or change the metadata for the identity provider, click **Choose** and select the SAML metadata file from your computer. The selected document will be uploaded when you save the form. The file must be a valid XML document to be uploaded and must be a valid SAML 2.0 metadata file for SAML SSO to work.
 - **Active identity provider** — Check the box to mark the identity provider profile as active. Only active identity providers can be used for service provider or identity provider initiated single sign-on.
 - **Default identity provider** — Check the box to mark the identity provider profile as the new default profile. There can only be one default profile at any one time. If none of the existing profiles are marked as default, the legacy profile is the default profile.
 - **Notes** — Enter any relevant notes for the identity provider profile.

- **Service Provider | Entity ID** — (Read only) This is generated automatically by OpenAir. This is OpenAir service provider Entity ID. Click the link to fetch the SAML metadata for OpenAir service provider. You will need this information when configuring the identity provider service for the integration.
- **Service Provider | Assertion consumer service (ACS) URL** — (Read only) This is generated automatically by OpenAir. You will need this information when configuring the identity provider service for the integration.
- **Protocol Settings | Enable service provider initiated SSO** — Check this box to enable this identity provider profile to be used for service provider initiated single sign-on (SP-initiated SSO). The identity provider profile must also be set as the default profile to be used for service provider initiated SSO.

⚠ Important: An identity provider profile can only be used for service provider initiated single sign-on if both the following conditions are met:

- The identity provider profile is the default identity provider profile.
- The **Enable service provider initiated SSO** box is checked.

The OpenAir sign-in page for single sign-on users cannot be used to sign in to OpenAir otherwise.

- **Protocol Settings | Enable Service Provider Initiated SSO ForceAuthn** — Check this box to include the ForceAuthn flag in service provider initiated requests. ForceAuthn is an optional SAML feature that acts as a signal to the identity provider to require some form of user interaction when handling the request, overriding the usual implicit assumption that it is acceptable to reuse authentication state from an earlier request. The effect depends on the identity provider service and configuration.

The screenshot shows a configuration page for an identity provider profile. On the left is a sidebar with three tabs: 'General' (selected), 'Service Provider', and 'Protocol settings'. The main content area has a top bar with 'Cancel', 'Delete', and 'Save' buttons. Below this are three sections:

- General:**
 - Identity Provider name *:
 - SAML Identity Provider meta-data: No file chosen
 - Active Identity Provider
 - Default Identity Provider
Defaults to oldest provider if no other is set. Only one can be set at a time
 - Notes:
- Service Provider:**
 - Entity ID: <https://auth.openair.com/sso/metadata/>
 - Assertion Consumer Service (ACS) URL: <https://auth.openair.com/sso/acs/>
- Protocol settings:**
 - Enable Service Provider initiated SSO
Enable OpenAir Service Provider initiated Single Sign-On (SSO)
 - Enable Service Provider initiated SSO ForceAuthn
Send ForceAuthn flag in SP-initiated SSO requests. Effect depends on IdP vendor and configuration

Viewing Audit Trail Information for Identity Provider Profiles


Account administrators can view audit trail information directly on the identity provider profile form. The audit information appears in a popup window. The audit log is in a plain text format displaying the user who made the change, what was changed, the date the change was made, and what the value was changed to.

Note: The audit trail information includes an `oa_uid` field. This is the internal ID of the user who made the change in the OpenAir Identification Authentication Service, and is different from the internal ID of the user in OpenAir.

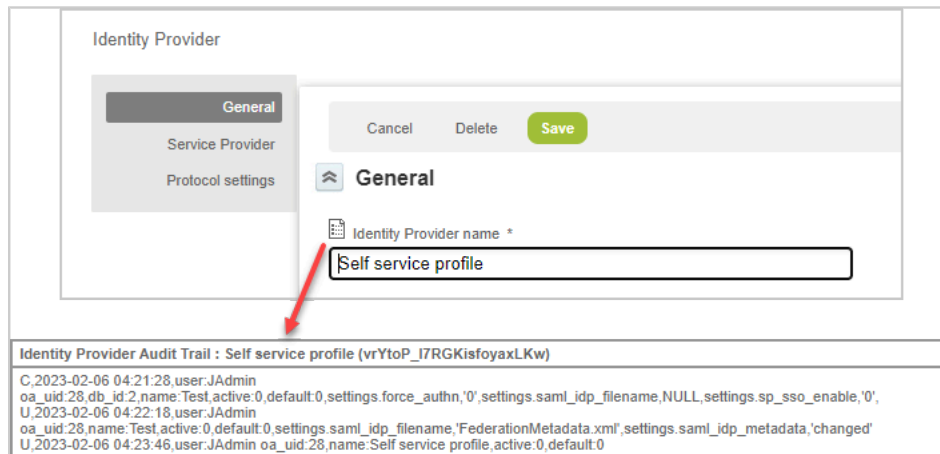
Important: The audit trail information is available on the identity profile form only if the Quick Audit Trail for Global Settings feature is enabled for your account. To enable this feature, contact OpenAir Customer Support.

For more information about the Quick Audit Trail for Global Settings feature, see [Optional Features](#) and [Security](#).

To view audit trail information for an identity provider profile:

1. Go to Administration > Global Settings > Account > Integration: SAML Single Sign-On.
2. Click the name of the identity provider profile.
3. Click the audit trail icon  next to the **Identity provider name** field.

A popup window appears showing the audit trail information.



The screenshot shows the 'Identity Provider' configuration form. The 'General' tab is selected, and the 'Identity Provider name' field contains 'Self service profile'. A red arrow points to the audit trail icon next to the field. Below the form, the audit trail information is displayed in a popup window.

Identity Provider Audit Trail : Self service profile (vrYtoP_I7RGKisfoyaXlKw)


```
C,2023-02-06 04:21:28,user:JAdmin
oa_uid:28,db_id:2,name:Test,active:0,default:0,settings.force_authn,'0',settings.saml_idp_filename,NULL,settings.sp_sso_enable,'0',
U,2023-02-06 04:22:18,user:JAdmin
oa_uid:28,name:Test,active:0,default:0,settings.saml_idp_filename,'FederationMetadata.xml',settings.saml_idp_metadata,'changed'
U,2023-02-06 04:23:46,user:JAdmin oa_uid:28,name:Self service profile,active:0,default:0
```

Testing the SAML Integration

After you enable the SAML Single Sign-On (SSO) feature for your OpenAir account and you configure at least one identity provider (IdP) service, create an identity provider profile in OpenAir, and upload the identity provider metadata, use the following steps to test the SAML integration.

To test the SAML integration:

1. Go to Administration > Global Settings > Account > Integration: SAML Single Sign-On.
2. Click the name of the identity provider profile you want to test.
3. Click the Tips menu, then click the following links:
 - **Test <IdP_profile_name> SP-initiated SSO** — Click this link to test the service provider initiated SSO

 **Note:** This link only shows if the **Active identity provider**, **Default identity provider**, and **Enable service provider initiated SSO** boxes are all checked.

- **Test <IdP_profile_name> IdP-initiated SSO** — Click this link to test the identity provider initiated SSO. A window appears. Enter the **URL for IdP-initiated SSO** and click **Test IdP SSO**.

 **Note:** This link only shows if the **Active identity provider** box is checked.

Enabling Employees to Sign In Using SAML Single Sign-On

After the SAML Single Sign-On (SSO) feature is enabled for your OpenAir account and you have configured the identity provider (IdP) service and OpenAir, you can enable your users to login using SAML Single Sign-on (SSO). To do so, you need to add a setting on the employee demographic form using a custom field.

To enable employees to sign in using SAML single sign-on:

1. In OpenAir, go to Administration > Global settings > Custom fields.
2. Click the Create button and select New Custom field. The New Custom field form appears.
3. Select 'Employee' from the **Add a custom field to** dropdown list and 'Checkbox' from the **Type of field to add** dropdown list. Click **Continue**.
4. Enter the **Field name** `saml_auth`, check the **Active** box, enter the **Display name** SAML Authentication. Enter a **Description** and **Hint** if required. Click **Save**.

Global Settings Custom fields

Cancel Save


For: Employee, Checkbox field

Field name*
saml_auth Active
Required, no spaces allowed

Description
SAML Authentication
Description of this custom field

Display name*
SAML Authentication
You must enter a title to display on forms

Hint
Check to enable SAML SSO and disable the default password authentication
Hint text will display on forms

 **Important:** The **Field name** must be set to `saml_auth`.

5. Go to Administration > Global Settings > Users > Employees > [Select an Employee]. The Employee Demographic form should now include the **SAML Authentication** box.
6. To enable SAML Authentication for an employee, check the **SAML Authentication** box on the employee demographic form.




Important: After you have enabled SAML Authentication for an employee, this employee will no longer be able to use the standard password authentication method to access OpenAir. Make sure you keep the SAML Authentication disabled for at least one administrator account for troubleshooting purposes.

SAML authentication is mutually exclusive with two-factor authentication (2FA). Saving the form returns an error if both the **Two-factor authentication required** and **SAML Authentication** [sam1_auth] boxes are checked. For more information about 2FA, see the help topic [Two-Factor Authentication](#).



Tip: You can use the bulk employee change wizard to copy the value of the sam1_auth field to other user records on your OpenAir Account.

See  [Administrator Guide](#) under Home > Home > Wizards > Making Changes to Multiple Employee Records at the Same Time.

Creating a Support Case

If you are experiencing difficulties with OpenAir or would like to enable an optional feature, go to SuiteAnswers through your OpenAir account and create a support case.

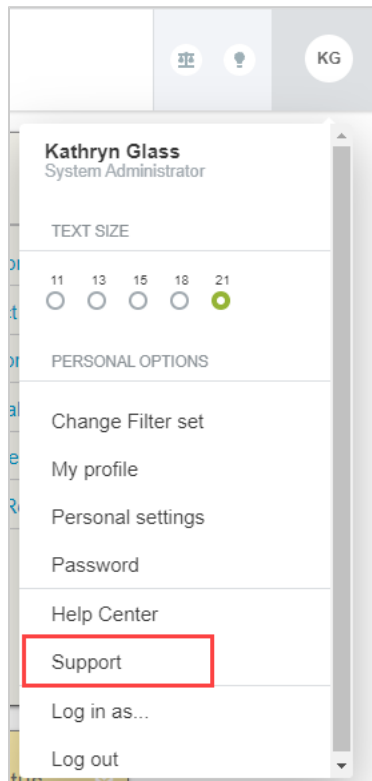
Our support staff and engineers will work with you to find a solution to your problem.

Important: Be sure to review the [Support Usage Best Practice Guidelines](#), [Case Severity Definitions](#) and [Case Resolution Overview](#) before you submit a support case or call the Support team.

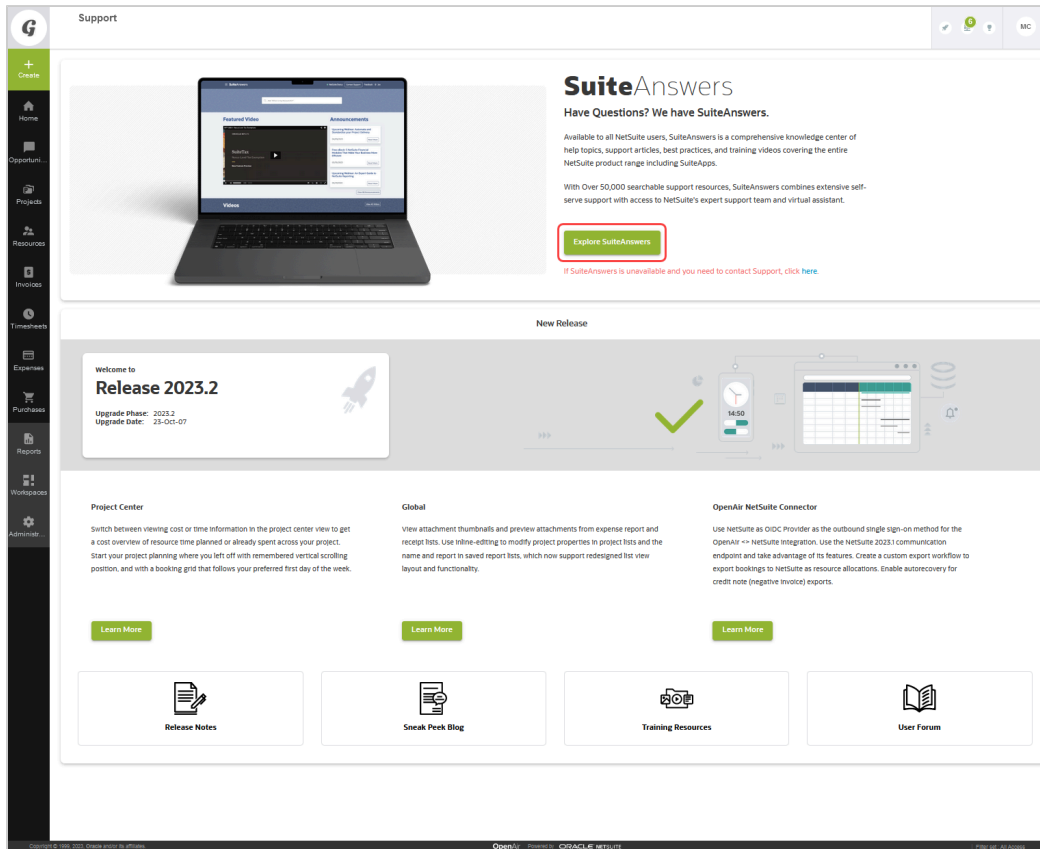
As a part of the support case creation process you will be presented with existing answers that may solve your problem. Take a moment to view the available answers before proceeding to create a support case.

To create a support case:

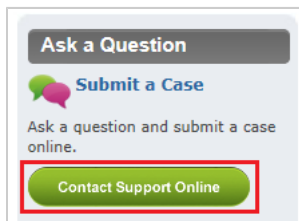
1. Sign in to your OpenAir account and select **Support** from the User Center menu.



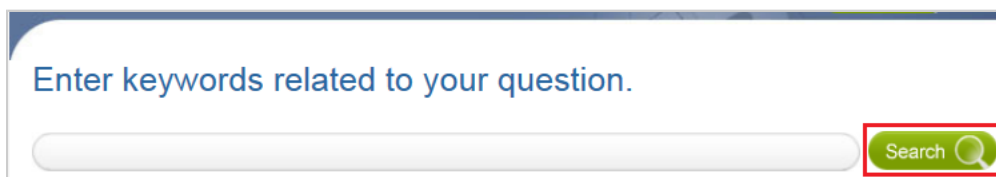
2. Click **Go to SuiteAnswers**.



3. On the OpenAir SuiteAnswers website, click **Contact Support Online**.



4. Enter keywords corresponding to the question or problem you want to resolve and click **Search**.



Note: If you do not have a question but need a feature enabled, for example, click **Search**.

5. Oftentimes, the answer to your question will be displayed. If you still want to create a support case, click **Continue to Create Case**.

Enter keywords related to your question.

We found the following answers that may help with your question. Click any answer to read it in a new window.

6. Fill out the **Create Case** form and then click **Submit**. You will receive an email confirmation with your support case reference (OpenAir Customer Care #).

Important: Review the **Case severity** definitions and always use the appropriate case severity when submitting a case. See the help topic [Case Severity Definitions](#).

Using the appropriate case severity helps OpenAir Customer Support prioritize between cases. Otherwise, OpenAir Customer Support need to evaluate the true urgency of each case, which slows down the response time to all cases.

Create Case

What would you like to do? *

Case Severity *

You can expand this section to review the description of each Case Severity. If you need to change the Case Severity, please provide specific details regarding the nature of the severity. +

Subject *

Question *

Product Area *

Feature

Attach Document

Email *

Phone (Optional)

Note: An asterisk * indicates a required field.