

Alibaba Cloud

Resource Access Management SSO Management

Document Version: 20220628

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).
5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.
6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions






Style	Description	Example
 Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
 Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
 Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: If the weight is set to 0, the server no longer receives new requests.
 Note	A note indicates supplemental instructions, best practices, tips, and other content.	 Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click Settings > Network > Set network type .
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click OK .
Courier font	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1.SSO overview	06
2.Scenarios of SSO	09
3.User-based SSO	10
3.1. Overview of user-based SSO	10
3.2. Configure the SAML settings of Alibaba Cloud for user-ba...	11
3.3. Configure Alibaba Cloud as a trusted SP for user-based S...	12
3.4. SAML response for user-based SSO	13
3.5. Implement user-based SSO from AD FS	17
3.6. Implement user-based SSO by using Okta	23
3.7. Implement user-based SSO by using Azure AD	27
4.Role-based SSO	32
4.1. Role-based SSO by using SAML	32
4.1.1. Overview	32
4.1.2. SAML IdP	34
4.1.2.1. Create a SAML IdP	34
4.1.2.2. View the basic information about a SAML IdP	34
4.1.2.3. Modify the basic information about a SAML IdP	35
4.1.2.4. Delete a SAML IdP	35
4.1.3. Configure the SAML settings of Alibaba Cloud for role-...	35
4.1.4. Configure Alibaba Cloud as a trusted SP for role-based...	36
4.1.5. SAML response for role-based SSO	37
4.1.6. Implement role-based SSO from AD FS	41
4.1.7. Implement role-based SSO from Okta	49
4.1.8. Implement role-based SSO from Azure AD	56
4.1.9. Implement role-based SSO from OneLogin to Alibaba C...	61
4.2. Role-based SSO by using OIDC	65

4.2.1. Overview of OIDC-based SSO	65
4.2.2. Manage an OIDC IdP	66
4.2.3. Implement OIDC-based SSO from Okta	68

1.SSO overview

Alibaba Cloud supports Security Assertion Markup Language (SAML) 2.0-based and OpenID Connect (OIDC)-based single sign-on (SSO). This feature is also known as identity federation. This topic introduces the terms that are related to SSO, and describes how to implement SSO between an enterprise identity management system and Alibaba Cloud.

Terms

Term	Description
identity provider (IdP)	<p>A RAM entity that provides identity management services. IdPs are classified into the following types:</p> <ul style="list-style-type: none">• IdPs that use the on-premises architecture, such as Microsoft Active Directory Federation Service (AD FS) and Shibboleth• IdPs that use the cloud-based architecture, such as Azure AD, Google G Suite, Okta, and OneLogin
service provider (SP)	<p>An application that uses the identity management feature of an IdP to provide users with specific services. An SP uses the user information that is provided by an IdP. In specific identity systems, such as OIDC, that are not based on the SAML protocol, SP is known as the relying party of an IdP.</p>
SAML 2.0	<p>A protocol that is designed for enterprise-level user identity authentication. SAML 2.0 is used for communication between an SP and an IdP. SAML 2.0 is a standard that enterprises use to implement enterprise-level SSO.</p>
SAML assertion	<p>A core element that is defined in the SAML protocol. This element describes the authentication request and response. For example, the SAML assertion for an authentication response can contain user attributes.</p>
trust	<p>A mutual trust relationship between an SP and an IdP. In most cases, the trust relationship is established by using public and private keys. An SP can obtain the SAML metadata of a trusted IdP. The metadata includes a public key. The SP uses the public key to verify the integrity of the SAML assertion that is issued by the IdP.</p>
OIDC	<p>An authentication protocol that is developed based on Open Authorization (OAuth) 2.0. For more information, see OIDC and OAuth 2.0. OAuth is an authorization protocol. OIDC adds an identity layer to extend OAuth. This way, OIDC can use OAuth for authorization. OIDC also allows clients to verify the identities of users and use an HTTP RESTful API to obtain basic information about the users.</p>
OIDC token	<p>An identity token that is issued by OIDC to an application. An OIDC token is an identity token that indicates a logon user. An OIDC token can be used to obtain the basic information about a logon user.</p>

Term	Description
client ID	An ID that is generated for an application when you register the application in an external IdP. When you apply for an OIDC token from an external IdP, you must use a client ID. The client ID is specified in the <code>aud</code> field of the OIDC token that is issued. When you create an OIDC IdP, you must configure the client ID. If you want to use the OIDC token to obtain an STS token, Alibaba Cloud checks whether the client ID that is included in the <code>aud</code> field is the same as the client ID that you configured in the OIDC IdP. You can assume a RAM role only when the client IDs are the same.
fingerprint	The fingerprint that is generated based on the HTTPS certificate of an external IdP. You can use a fingerprint to prevent the URL of the issuer from being hijacked or tampered with. Alibaba Cloud calculates the fingerprint. We recommend that you calculate the fingerprint on your computer. For example, you can use OpenSSL to calculate the fingerprint. Then, you can compare the calculation result with the calculation result provided by Alibaba Cloud. For more information about OpenSSL, visit the official website of OpenSSL . If the calculation results are different, the URL of the issuer may have been attacked. Make sure that you enter a valid fingerprint.
URL of an issuer	The URL of an issuer that is provided by an external IdP. The URL is indicated by the <code>iss</code> field in an OIDC token. The URL of the issuer must start with https and be in the valid URL format. The URL cannot contain query parameters that follow a question mark (<code>?</code>) or logon information that is identified by at signs (<code>@</code>). The URL cannot be a fragment URL that contains number signs (<code>#</code>).
STS token	A temporary identity credential that is provided by Alibaba Cloud Security Token Service (STS). STS allows you to manage temporary credentials for your Alibaba Cloud resources. You can configure a validity period and specify access permissions for an STS token. For more information about STS, see What is STS?

SSO methods

Alibaba Cloud provides the following SSO methods:

- User-based SSO

The RAM user identity that you can use to log on to the Alibaba Cloud Management Console is determined based on an SAML assertion. After you log on to the Alibaba Cloud Management Console, you can access Alibaba Cloud resources as a RAM user. For more information, see [Overview of user-based SSO](#).

- Role-based SSO


Alibaba Cloud supports SAML 2.0-based SSO and OIDC-based SSO.

- SAML 2.0-based SSO: The RAM role that you can use to log on to the Alibaba Cloud Management Console is determined based on a SAML assertion. After you log on to the Alibaba Cloud Management Console, you can use the RAM role specified in the SAML assertion to access Alibaba Cloud resources. For more information, see [Overview](#).

- **OIDC-based SSO:** You can use an OIDC token that is issued by an IdP to call an Alibaba Cloud operation to assume a specific RAM role and use the OIDC token to obtain an STS token. Then, you can use the STS token to access Alibaba Cloud resources. For more information, see [Overview of OIDC-based SSO](#).

Comparison between role-based SSO and user-based SSO

SSO method	SP-initiated SSO	IdP-initiated SSO	Logon by using logon names and passwords of RAM users	Association of multiple Alibaba Cloud accounts with a single IdP	Multiple IdPs
User-based SSO	Supported	Supported	Not supported	Not supported	Not supported
Role-based SSO	Not supported	Supported	Supported	Supported	Supported

 **Note** For more information about the differences between the two SSO methods, see [Scenarios of SSO](#).

2.Scenarios of SSO

This topic describes the scenarios of two single sign-on (SSO) methods that are supported by Alibaba Cloud: role-based SSO and user-based SSO. You can select an SSO method based on your business requirements.

Role-based SSO

Role-based SSO applies to the following scenarios:

- You do not want to create or manage users on Alibaba Cloud. Then, you can reduce costs and eliminate the need to synchronize users.
- You want to implement SSO to Alibaba Cloud and manage some users on Alibaba Cloud. The users managed on Alibaba Cloud can be used to test new features of Alibaba Cloud and log on to Alibaba Cloud if your network or identity provider (IdP) encounters exceptions.
- You want to manage the permissions on Alibaba Cloud based on the user groups in your local IdP or a specific user attribute. Then, you can manage user permissions by grouping users in your local IdP or changing the attribute of a user.
- You have multiple Alibaba Cloud accounts and only one IdP. You want to implement SSO to multiple Alibaba Cloud accounts by configuring your IdP only once.
- You have multiple IdPs and only one Alibaba Cloud account. You want to implement SSO from multiple IdPs to one Alibaba Cloud account by configuring IdPs in the Alibaba Cloud account.
- You want to implement SSO by using the console or by calling API operations.

User-based SSO

User-based SSO applies to the following scenarios:

- You want to initiate logon from Alibaba Cloud, not from your IdP.
- Some of your Alibaba Cloud services cannot be accessed by roles (that is, through STS). For more information, see [Services that work with STS](#).
- Your IdP does not support complex configuration of attributes.
- You want to simplify IdP configuration.

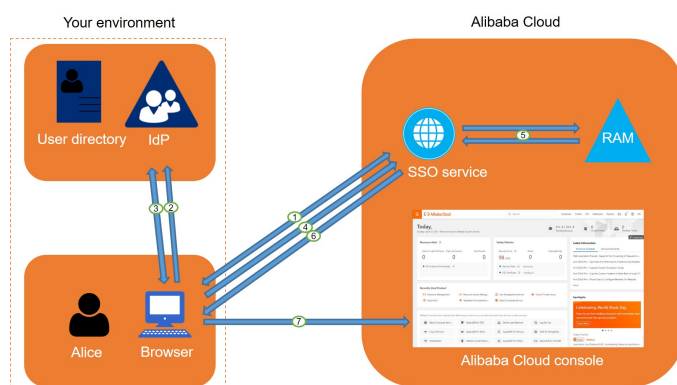
3. User-based SSO

3.1. Overview of user-based SSO

If Alibaba Cloud and the identity management system of an enterprise work together to implement user-based single sign-on (SSO), Alibaba Cloud is the service provider (SP) and the enterprise is the identity provider (IdP). User-based SSO allows an employee of the enterprise to access Alibaba Cloud resources as a Resource Access Management (RAM) user.

Process

After an administrator configures user-based SSO, the employee Alice can log on to the Alibaba Cloud Management Console. The following list describes the process.



1. Alice uses a browser to log on to the Alibaba Cloud Management Console. Then, the Alibaba Cloud Management Console returns a Security Assertion Markup Language (SAML) authentication request to the browser.
2. The browser forwards the SAML authentication request to the IdP.
3. Alice is prompted to log on to the IdP portal. After Alice logs on to the IdP portal, the IdP returns a SAML response to the browser.
4. The browser forwards the SAML response to the SSO service.
5. The SSO service verifies the digital signature in the SAML response based on the SAML mutual trust configuration to check the authenticity of the SAML assertion. Then, the SSO service maps the value of the `NameID` element in the SAML assertion to the RAM user.
6. The SSO service returns the URL of the Alibaba Cloud Management Console to the browser.
7. The browser redirects Alice to the Alibaba Cloud Management Console.

Note In Step 1, Alice initiates the logon from the Alibaba Cloud Management Console. This is optional. Instead, Alice can click the Alibaba Cloud logon URL in the IdP portal to send a SAML authentication request to the IdP.

Configure user-based SSO

Before you implement user-based SSO, you must establish trust between Alibaba Cloud and your IdP.

1. To make sure that your IdP is trusted by Alibaba Cloud, you must configure the IdP in the Alibaba Cloud Management Console.

For more information, see [Configure the SAML settings of Alibaba Cloud for user-based SSO](#).

2. To make sure that Alibaba Cloud is trusted by your IdP, you must configure Alibaba Cloud as a trusted SAML SP and configure SAML assertions in your IdP.

For more information, see [Configure Alibaba Cloud as a trusted SP for user-based SSO](#).

3. After the IdP and Alibaba Cloud SAML settings are configured, you must create RAM users that correspond to the users in the IdP by using SDKs, CLIs, or the RAM console.

For more information, see [Create a RAM user](#).

Examples

The following list provides examples of how to implement user-based SSO to Alibaba Cloud from common enterprise IdPs, such as Active Directory Federation Services (AD FS), Okta, and Azure AD:

- [Implement user-based SSO from AD FS](#)
- [Implement user-based SSO by using Okta](#)
- [Implement user-based SSO by using Azure AD](#)

3.2. Configure the SAML settings of Alibaba Cloud for user-based SSO


This topic describes how to configure metadata for user-based single sign-on (SSO) based on SAML 2.0, and establish trust between an identity provider (IdP) and Alibaba Cloud (service provider).

Context

You can specify the default domain name, a domain alias, or an auxiliary domain name to simplify the configuration of SAML-based SSO. For more information about how to specify the default domain name or domain alias for an Alibaba Cloud account, see [View and modify the default domain name](#) and [Create and verify a domain alias](#).


Procedure

1. Log on to the [RAM console](#) by using an Alibaba Cloud account.
2. In the left-side navigation pane, click **SSO**.
3. On the **SSO** page, click the **User-based SSO** tab. In the **SSO Settings** section, you can view the basic information of user-based SSO.
4. Click **Modify**. In the **SSO Settings** pane, set the following parameters:
 - **SSO Status**: Select **Enabled** to enable SSO or **Disabled** to disable SSO.

 **Note** This setting applies only to RAM users of your Alibaba Cloud account and does not affect the Alibaba Cloud account.


- The **Disabled** option is selected by default. If SSO is disabled, SSO settings do not take effect and RAM users can use their passwords to log on to the console.
- If you select the **Enabled** option, RAM users cannot use passwords to log on to the console. Instead, the RAM users must log on to an IdP service for identity authentication. If SSO is disabled at a later time, password-based logon is automatically re-enabled.

- **Metadata File:** Click **Upload** to upload the metadata file that is provided by your IdP.

 **Note** In most cases, the metadata file is provided in the XML format. The file contains the logon URL and X.509 public key certificate that is used to verify the validity of the SAML assertions issued by the IdP.

- **Auxiliary Domain:** Optional. Turn on or off this switch based on your business requirements.
 - If you turn on this switch, you can specify an auxiliary domain name and use it as the suffix of the `NameID` element in SAML assertions.
 - If you turn off this switch, you can use only the default domain name or domain alias of your Alibaba Cloud account as the suffix of the `NameID` element in SAML assertions.

For more information about the values of the `NameID` element, see [SAML response for user-based SSO](#).

 **Note** If you specify both a domain alias and an auxiliary domain name, only the domain alias or the default domain name can be used as the suffix of the `NameID` element.

5. Click **OK**.

What's next

You can create RAM users that correspond to the users of your IdP by using one of the following methods:

- Log on to the RAM console, and create RAM users in the console. For more information, see [Create a RAM user](#).
- Use a RAM SDK to write a program or use the Alibaba Cloud command line interface (CLI) to create RAM users. For more information, see [CreateUser](#).


3.3. Configure Alibaba Cloud as a trusted SP for user-based SSO

This topic describes how to configure Alibaba Cloud as a trusted SAML service provider (SP) of your identity provider (IdP) for user-based single sign-on (SSO).

Procedure

1. Obtain the SAML SP metadata URL from the Resource Access Management (RAM) console.
 - i. Log on to the [RAM console](#) by using your Alibaba Cloud account.
 - ii. In the left-side navigation pane, click **SSO**.
 - iii. On the SSO page, click the **User-based SSO** tab.
 - iv. In the **SSO Settings** section, copy the value of the **SAML Service Provider Metadata URL** parameter.
2. Create a SAML SP in your IdP and configure Alibaba Cloud as the relying party by using one of the following methods:
 - Use the SAML SP metadata URL of Alibaba Cloud that you copied in Step 1.

- If your IdP does not support the URL-based configuration of the relying party, download the metadata file from the URL that you copied in Step and upload the metadata file.
- If your IdP does not allow you to upload the metadata file, configure the following parameters:
 - **Entity ID** : the value of the `entityID` attribute in the `md:EntityDescriptor` element of the metadata file.
 - **ACS URL** : the value of the `Location` attribute in the `md:AssertionConsumerService` element of the metadata file.
 - **RelayState** : This parameter is optional. If your IdP requires the `RelayState` parameter, set the value of the parameter to a URL. Users will be redirected to the URL after SSO succeeds. If you do not configure this parameter, users are redirected to the homepage of the Alibaba Cloud Management Console after SSO succeeds.

 **Note** For security purposes, you must enter a URL that points to an Alibaba website for the `RelayState` parameter. For example, the domain name in the URL can be `*.aliyun.com`, `*.hichina.com`, `*.yunos.com`, `*.taobao.com`, `*.tmall.com`, `*.alibabacloud.com`, or `*.alipay.com`.

What's next

After you configure Alibaba Cloud as a trusted SAML SP, you must configure SAML assertions for your IdP. For more information, see [SAML response for user-based SSO](#).

3.4. SAML response for user-based SSO

This topic describes the syntax of a Security Assertion Markup Language (SAML) response for user-based single sign-on (SSO). This topic also describes the elements of a SAML assertion in a SAML response.

Background information

During SAML 2.0-based SSO, after the identity of a user is verified, the identity provider (IdP) generates an authentication response and sends this response to Alibaba Cloud by using a browser or a program. This response contains a SAML assertion that complies with the specifications of the HTTP POST binding in SAML 2.0. Alibaba Cloud uses the SAML assertion to determine the logon status and identity of the user. Therefore, the SAML assertion must contain the elements that are required by Alibaba Cloud. If the SAML assertion does not contain the required elements, SSO fails.

SAML response

Make sure that each SAML response that is sent by your IdP to Alibaba Cloud contains the following elements. Otherwise, SSO fails.

```
<saml2p:Response>
  <saml2:Issuer>...</saml2:Issuer>
  <saml2p:Status>
    ...
  </saml2p:Status>
  <saml2:Assertion>
    <saml2:Issuer>...</saml2:Issuer>
    <ds:Signature>
      ...
    </ds:Signature>
    <saml2:Subject>
      <saml2:NameID>${NameID}</saml2:NameID>
      <saml2:SubjectConfirmation>
        ...
      </saml2:SubjectConfirmation>
    </saml2:Subject>
    <saml2:Conditions>
      <saml2:AudienceRestriction>
        <saml2:Audience>${Audience}</saml2:Audience>
      </saml2:AudienceRestriction>
    </saml2:Conditions>
    <saml2:AuthnStatement>
      ...
    </saml2:AuthnStatement>
  </saml2:Assertion>
</saml2p:Response>
```

Elements in a SAML assertion

- Common elements in SAML 2.0

Element	Description
Issuer	The value of the <code>Issuer</code> element must match <code>EntityID</code> in the metadata file that you upload for the IdP in the Alibaba Cloud Management Console.
Signature	The SAML assertion must be signed. The <code>Signature</code> element must contain information such as the signature value and signature algorithm. The signature is used to confirm that the signed SAML assertion is not modified after the signature is generated.

Element	Description
Subject	<p>The <code>Subject</code> element must contain the following sub-elements:</p> <ul style="list-style-type: none"> Only one <code>NameID</code> sub-element. The sub-element is used to identify a RAM user within your Alibaba Cloud account. For more information, see the description and example of <code>NameID</code> in this topic. Only one <code>SubjectConfirmation</code> sub-element that contains a <code>SubjectConfirmationData</code> sub-element. The <code>SubjectConfirmationData</code> sub-element must contain the following attributes: <ul style="list-style-type: none"> <code>NotOnOrAfter</code>: the validity period of a SAML assertion. <code>Recipient</code>: the recipient of the SAML assertion. Alibaba Cloud checks the recipient of the SAML assertion based on the value of this attribute. Therefore, you must set this attribute to <code>https://signin-intl.aliyun.com/saml/SSO</code>. <p>The following script provides an example of the <code>Subject</code> element:</p> <pre><Subject> <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">Alice@example.onaliyun.com</NameID> <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"> <SubjectConfirmationData NotOnOrAfter="2019-01-01T00:01:00.000Z" Recipient="https://signin-intl.aliyun.com/saml/SSO"/> </SubjectConfirmation> </Subject></pre>

Element	Description
Conditions	<p>The <code>Conditions</code> element must contain an <code>AudienceRestriction</code> sub-element. The <code>AudienceRestriction</code> sub-element can contain one or more <code>Audience</code> sub-elements. The value of an <code>Audience</code> sub-element must be <code>https://signin-intl.aliyun.com/\${accountId}/saml/SSO</code>. <code>\${accountId}</code> specifies the ID of the Alibaba Cloud account.</p> <p>The following script provides an example of the <code>Conditions</code> element:</p> <pre><Conditions> <AudienceRestriction> <Audience>https://signin- intl.aliyun.com/\${accountId}/saml/SSO</Audience> </AudienceRestriction> </Conditions></pre>


• NameID element

Alibaba Cloud uses a User Principal Name (UPN) to locate a RAM user. Therefore, the SAML assertion that is generated by your IdP must contain the UPN of the RAM user. To implement user-based SSO, Alibaba Cloud resolves the `NameID` element in the SAML assertion and maps this element to the UPN of the corresponding RAM user.


When you configure the SAML assertion that is issued by your IdP, you must map the UPN of the RAM user to the `NameID` element in the SAML assertion.

The value of the `NameID` element must include one of the following suffixes:

- The **domain alias** of your Alibaba Cloud account: `<username>@<domain_alias>`. `<username>` specifies the username of a RAM user. `<domain_alias>` specifies the domain alias. For more information, see [Create and verify a domain alias](#).
- The **auxiliary domain name**: `<username>@<auxiliary_domain>`. `<username>` specifies the username of the RAM user. `<auxiliary_domain>` specifies the auxiliary domain name. For information about how to configure an auxiliary domain name, see [Configure the SAML settings of Alibaba Cloud for user-based SSO](#).

 **Note** If you configure both a domain alias and an auxiliary domain name, the value of the `NameID` element is suffixed with the domain alias.

- The **default domain name** of your Alibaba Cloud account: `<username>@<default_domain>`. `<username>` specifies the username of a RAM user. `<default_domain>` specifies the default domain name. For more information, see [View and modify the default domain name](#).

 **Note** You can use the default domain name of your Alibaba Cloud account as the suffix of the `NameID` element even if you have configured a domain alias or an auxiliary domain name.

• NameID example

In this example, a RAM user that is named `Alice` is created for your Alibaba Cloud account and the default domain name of your Alibaba Cloud account is `example.onaliyun.com`.

- If you set the domain alias of your Alibaba Cloud account to `example.com`, the value of the `NameID` element in a SAML assertion is `Alice@example.onaliyun.com` or `Alice@example.com`.
- If you have set the auxiliary domain name to `example.net` and no domain aliases are configured, the value of the `NameID` element in a SAML assertion is `Alice@example.onaliyun.com` or `Alice@example.net`.
- If you set the domain alias of your Alibaba Cloud account to `example.com` and the auxiliary domain name to `example.net`, the value of the `NameID` element in a SAML assertion is `Alice@example.onaliyun.com` or `Alice@example.com`. The auxiliary domain name cannot be used.


3.5. Implement user-based SSO from AD FS

This topic provides an example on how to implement user-based single sign-on (SSO) from Active Directory Federation Services (AD FS) to Alibaba Cloud. The example describes the end-to-end SSO process from a cloud identity provider (IdP) to Alibaba Cloud. This topic uses AD FS deployed on an Elastic Compute Service (ECS) instance that runs Windows Server 2012 R2 as an example.

Preparations

Before you configure SSO, perform the following operations:

1. Deploy the following servers on the ECS instance that runs Windows Server 2012 R2:
 - DNS server: resolves and sends identity authentication requests to the correct Federation Service.
 - Active Directory Domain Service (AD DS): creates, queries, and modifies objects such as domain users and domain devices.
 - AD FS: configures the relying party for SSO and performs SSO authentication for the configured relying party.

 **Notice** The configuration of Microsoft Active Directory (AD) described in this topic is for reference only and helps you understand the configuration procedure of SSO logon to Alibaba Cloud. Alibaba Cloud does not provide consultation services for the configuration of Microsoft AD.

2. Prepare the following data:
 - The default domain name of the Alibaba Cloud account: `secloud.onaliyun.com`.
 - The username of the RAM user that belongs to the Alibaba Cloud account: `alice`. The User Principal Name (UPN) of the RAM user is `alice@secloud.onaliyun.com`.
 - The name of the AD FS service that has been registered in Microsoft AD: `adfs.secloud.club`.
 - The domain name of Microsoft AD: `secloud.club`. The NetBIOS name is `secloud`.
 - The UPN of the RAM user `alice` in Microsoft AD: `alice@secloud.club`. The RAM user can also use `secloud\alice` to log on from the Microsoft AD domain.

Step 1: Configure AD FS as a trusted SAML IdP in RAM

1. Enter the following URL in the address bar of your browser: `https://adfs.seclcloud.club/FederationMetadata/2007-06/FederationMetadata.xml`.
2. Download the metadata file in the XML format to your computer.
3. Log on to the RAM console and use the metadata file for SSO configuration.

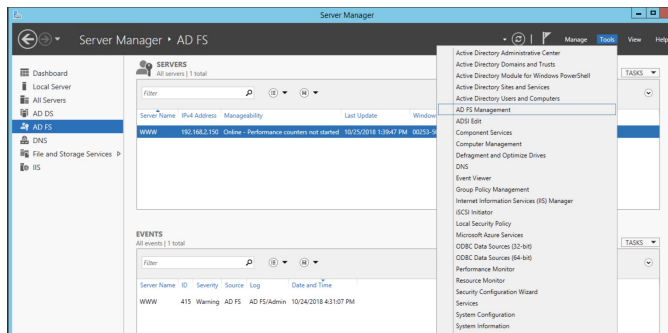
For more information, see [Configure the SAML settings of Alibaba Cloud for user-based SSO](#).

Note If the size of the metadata file exceeds the upper limit, you can delete all content in `<fed:ClaimTypesRequested>` and `<fed:ClaimTypesOffered>`.

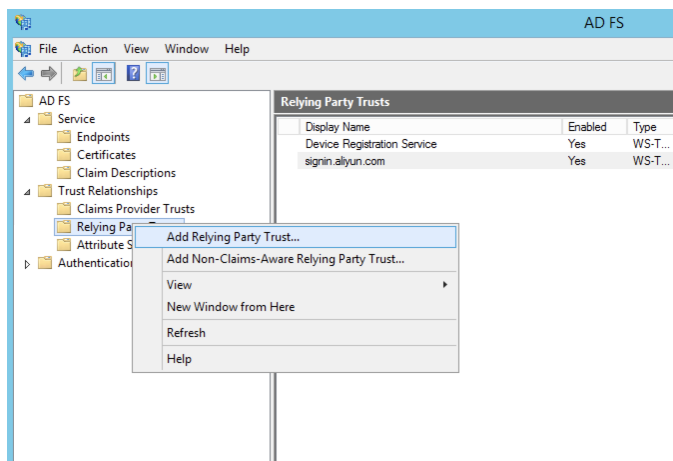
Step 2: Configure Alibaba Cloud as a trusted SAML SP in AD FS

In AD FS, the SAML service provider (SP) is called the **relying party**. To configure Alibaba Cloud as a trusted SP, perform the following steps:

1. In the top navigation bar of **Server Manager**, choose **Tools > AD FS Management**.

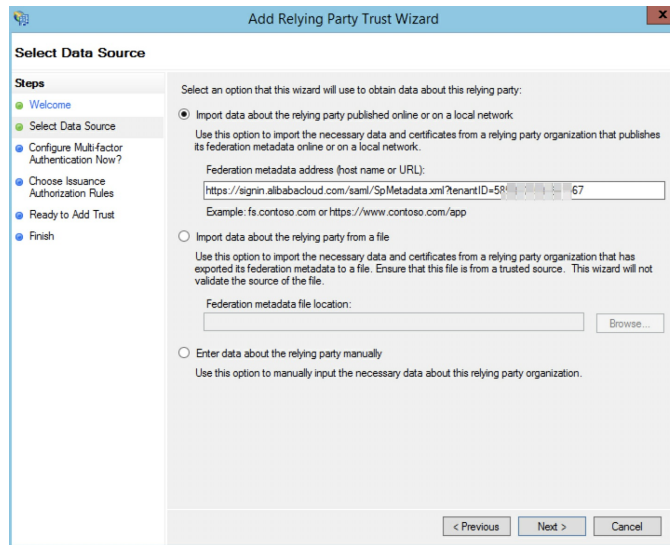


2. Right-click **Relying Parties** and select **Add Relying Party Trust**.



3. Configure the SAML metadata of Alibaba Cloud for the relying party.

To view the URL of the SAML metadata, log on to the [RAM console](#). In the left-side navigation pane, click **SSO**. On the page that appears, click **User-based SSO**. You can view the URL in the **SSO Settings** section. You can directly enter the metadata URL when you configure the relying party in AD FS.



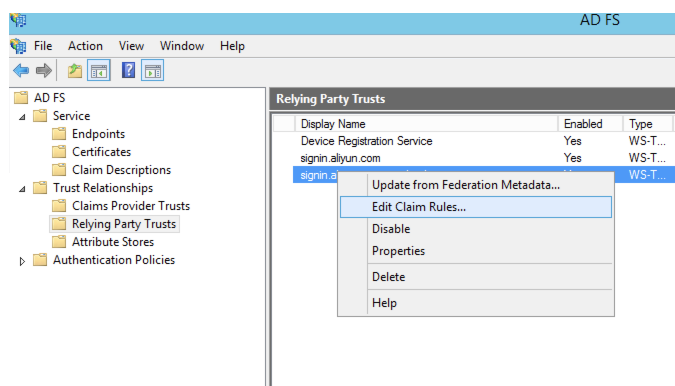
After the relying party is configured, Alibaba Cloud sends a request to the AD FS service whose name is `adfs.secloud.club`. The request is sent to authenticate RAM users that belong to the Alibaba Cloud account whose default domain name is `secloud.onaliyun.com`. After AD FS receives the request, it authenticates the RAM users and sends a response to Alibaba Cloud.

Step 3: Configure SAML assertion attributes for the Alibaba Cloud SP

We recommend that you set the value of the `NameID` field in the SAML assertion to the UPN of the RAM user. This way, Alibaba Cloud can locate the correct RAM user based on the SAML response.

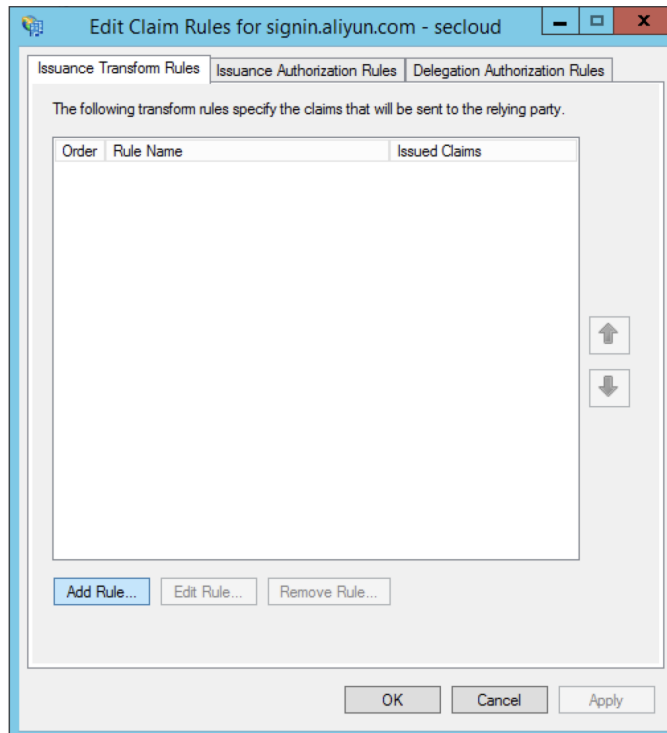
You must set the UPN in Microsoft AD to the value of `NameID` in the SAML assertion.

1. Right-click the display name of the relying party and select **Edit Claim Rules**.

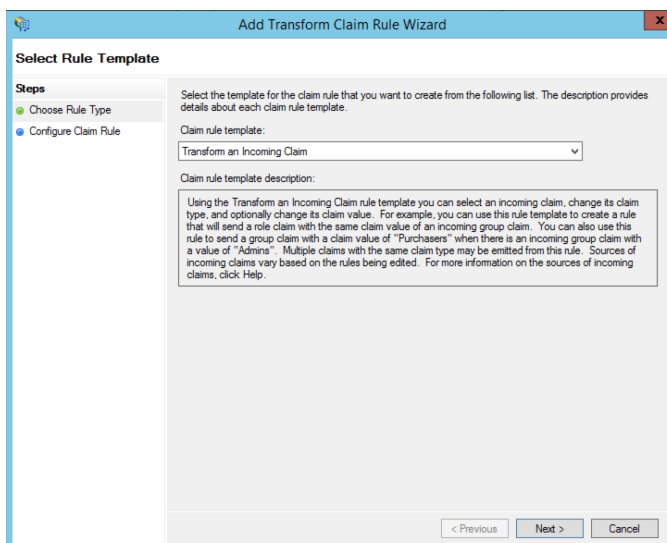


2. Click **Issuance Transform Rules** to add a rule.

Note Issuance transform rules indicate how to transform a known user attribute and issue it as an attribute in the SAML assertion. You must issue the UPN of a user in Microsoft AD as a `NameID`. In this case, a new rule is required.



- From the **Claim rule template** drop-down list, select **Transform an Incoming Claim**.



- Select **Edit Rule**.

Note In this example, the domain name of the UPN in the Alibaba Cloud account is `seccloud.onaliyun.com`, and the domain name of the UPN in Microsoft AD is `seccloud.club`. If you map the UPN in Microsoft AD to the `NameID`, the user cannot be identified by Alibaba Cloud.

To solve this problem, use one of the following methods:

- i. Method 1: Set the domain name of Microsoft AD to the **domain alias** that is configured in RAM.

If the domain name `secloud.club` of Microsoft AD is registered in a DNS on the Internet, you can change `secloud.club` to the **domain alias** that is configured in RAM. For information about how to configure a domain alias, see [Create and verify a domain alias](#).

After the settings are complete, map the UPN to the `NameID` in the **Edit Rule** dialog box.

Edit Rule

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Rule template: Transform an Incoming Claim

Incoming claim type:

Incoming name ID format:

Outgoing claim type:

Outgoing name ID format:

☒ Pass through all claim values

☐ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value:

☐ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

ii. Method 2: Transform the domain name in AD FS.

If the domain name `secloud.club` is an internal domain name of an enterprise, the domain ownership of the enterprise cannot be verified by Alibaba Cloud. RAM can use only the default domain name `secloud.onaliyun.com`.

In this case, you must change the domain name suffix `secloud.club` of the UPN to `secloud.onaliyun.com` in the SAML assertion that is issued by AD FS to Alibaba Cloud.

Edit Rule

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Rule template: Transform an Incoming Claim

Incoming claim type:

Incoming name ID format:

Outgoing claim type:

Outgoing name ID format:

☐ Pass through all claim values

☐ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value:

☒ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

- iii. Method 3: Specify the domain name of Microsoft AD as the auxiliary domain name for user-based SSO.

If the domain name `secloud.club` is an internal domain name of an enterprise, the domain ownership of the enterprise cannot be verified by Alibaba Cloud. In this case, you can specify `secloud.club` as the auxiliary domain name without the need to transform the domain name. For information about how to specify an auxiliary domain name, see [Configure the SAML settings of Alibaba Cloud for user-based SSO](#).

After the settings are complete, map the UPN to the `NameID` in the **Edit Rule** dialog box.

Edit Rule

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Rule template: Transform an Incoming Claim

Incoming claim type:

Incoming name ID format:

Outgoing claim type:

Outgoing name ID format:

☒ Pass through all claim values

☐ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value:

☐ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

3.6. Implement user-based SSO by using Okta

This topic provides an example on how to implement user-based single sign-on (SSO) between Okta and Alibaba Cloud. The example describes the end-to-end SSO process between a cloud identity provider (IdP) and Alibaba Cloud.

Step 1: Download the Security Assertion Markup Language (SAML) SP metadata file of Alibaba Cloud

1. Log on to the [RAM console](#) by using your Alibaba Cloud account.
2. In the left-side navigation pane, click **SSO**.
3. On the **SSO** page, click the **User-based SSO** tab.
4. In the **Setup SSO** section, copy the value of **SAML Service Provider Metadata URL**.
5. Open a new tab in your browser and paste the URL in the address bar. On the page that appears, right-click the page and select **Save As** to download the SAML service provider (SP) metadata file in the XML format to your computer.

Note The XML file contains the information that is required to configure Alibaba Cloud as a SAML SP. Record the value of `entityID` in the `EntityDescriptor` element and the value of `Location` in the `AssertionConsumerService` element for subsequent use.

Step 2: Create an application that supports SAML 2.0-based SSO in Okta

1. Log on to the [Okta portal](#).
2. In the upper-right corner of the Okta portal, click the account name and select **Your Org** from the drop-down list.
3. In the left-side navigation pane, choose **Applications > Applications**.
4. On the **Applications** page, click **Create App Integration**.
5. In the **Create a new app integration** dialog box, select **SAML 2.0** and click **Next**.
6. In the General Settings step of the page that appears, enter AliyunSSODemo in the App name field and click **Next**.
7. In the Configure SAML step, configure the parameters and click **Next**.

GENERAL

Single sign on URL ?

☒ Use this for Recipient URL and Destination URL

☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ?

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

Application username ?

- o In the **Single sign on URL** field, enter the value of `Location` that you obtained in **Step 1: Download the Security Assertion Markup Language (SAML) SP metadata file of Alibaba Cloud**.
- o In the **Audience URI** field, enter the value of `entityID` that you obtained in **Step 1: Download the Security Assertion Markup Language (SAML) SP metadata file of Alibaba Cloud**.
- o In the **Default RelayState** field, enter a URL. Then, the system redirects you to the URL after login.

Note For security purposes, you must enter a URL that points to an Alibaba website in the **Default RelayState** field. For example, you can enter a URL that contains the following domain names: `*.aliyun.com`, `*.hichina.com`, `*.yunos.com`, `*.taobao.com`, `*.tmall.com`, `*.alibabacloud.com`, or `*.alipay.com`. If you leave this parameter empty, you are redirected to the homepage of the Alibaba Cloud Management Console.


- Select **Persistent** for **Name ID format**.
 - Select **Email** for **Application username**.
8. On the **Feedback** page, select a type for the application and click **Finish**.

Step 3: Download the SAML IdP metadata file of Okta


1. On the **Applications** page, click **AliyunSSODemo**. On the page that appears, click the **Sign On** tab.
2. In the **Settings** section of the **Sign On** tab, click **Identity Provider metadata**. On the page that appears, right-click the page and click **Save As** to download the metadata file to your computer.

Step 4: Enable user-based SSO in the Alibaba Cloud Management Console

1. In the left-side navigation pane of the RAM console, click **SSO**.
2. On the **SSO** page, click the **User-based SSO** tab.
3. Click **Edit** to the right of **Setup SSO**.
4. In the **SSO Status** section of the **SSO Settings** panel, click **Enabled**.

 **Note** User-based SSO takes effect on all RAM users in your Alibaba Cloud account. If you enable this feature, all RAM users in your Alibaba Cloud account must log on to the Alibaba Cloud Management Console by using SSO. If you use a RAM user, set the SSO Status parameter to Disabled in this step. Before you enable user-based SSO, you must complete the SSO settings for the RAM user. Otherwise, you cannot log on as the RAM user. To avoid this issue, you can also use your Alibaba Cloud account to configure user-based SSO.

5. In the **Metadata File** section, click **Upload** to upload the IdP metadata file obtained in [Step 3: Download the SAML IdP metadata file of Okta](#).
6. Select **Enabled** for **Auxiliary Domain**. In the field that appears, enter the domain name of the email address that you use as the Okta username.

 **Note** If the usernames that belong to your Okta account are suffixed with different domain names, only the users whose usernames are suffixed with the specified domain name can log on to the Alibaba Cloud Management Console.

7. Click **OK**.


Step 5: Create a user and assign the application to the user in Okta

1. In the left-side navigation pane, choose **Directory > People**.
2. On the page that appears, click **Add Person**.
3. In the **Add Person** dialog box, enter **u2@example.com** in the **Primary email** field, configure other parameters, and then click **Save**.
4. In the user list, find **u2@example.com** and click **Activate** in the **Status** column. In the dialog box that appears, activate **u2@example.com** as prompted.
5. In the left-side navigation pane, choose **Applications > Applications**.
6. Click the application name **AliyunSSODemo**. On the **Assignments** tab, choose **Assign > Assign to People**.

7. In the dialog box that appears, click **Assign** next to the u2@example.com user.
8. In the dialog box that appears, click **Save and Go Back**.
9. Click **Done**.

Step 6: Create a RAM user in the Alibaba Cloud Management Console

1. In the left-side navigation pane of the RAM console, choose **Identities > Users**.
2. On the **Users** page, click **Create User**.
3. On the **Create User** page, configure the **Logon Name** and **Display Name** parameters.

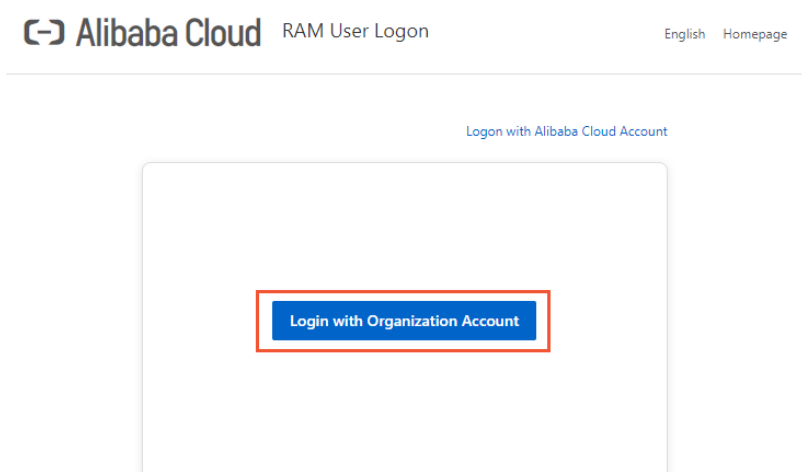
 **Note** The logon name and Okta username must have the same prefix. In this example, the prefix of the logon name must be u2.

4. In the **Access Mode** section, select **Console Access** and configure the parameters.
5. Click **OK**.

Verify the user-based SSO configurations

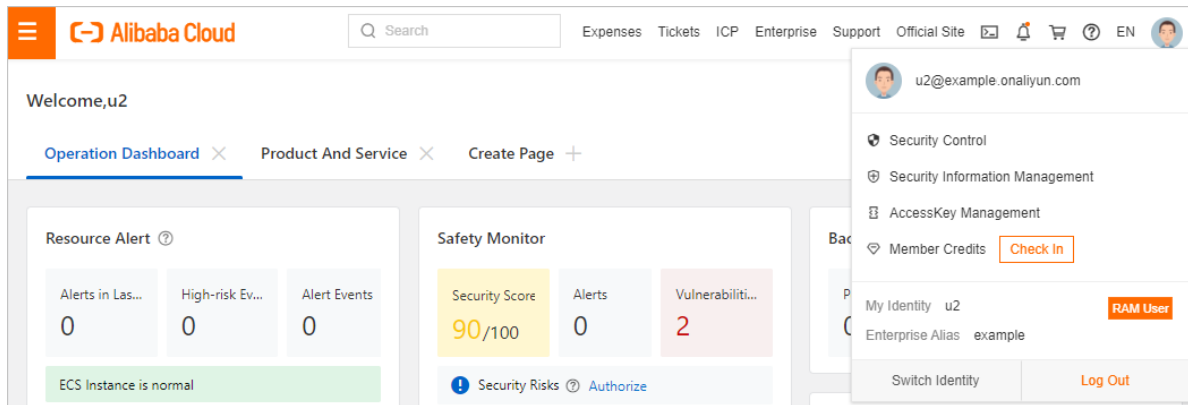
After you configure SSO, you can initiate SSO logon from both Alibaba Cloud and Okta.

- Logon from Alibaba Cloud
 - i. Log on to the **RAM console** by using your Alibaba Cloud account. On the **Overview** page, copy the logon URL of a RAM user.
 - ii. Move the pointer over the profile picture in the upper-right corner of the page and click **Log Out**. Then, paste the logon URL into the address bar of your browser and press Enter. You can also access the URL on a new tab.
 - iii. On the page that appears, click **Logon with Organization Account**. The system redirects you to the logon page of Okta.



- iv. On the logon page of Okta, enter the username (u2@example.com) and password, and click **Login**.

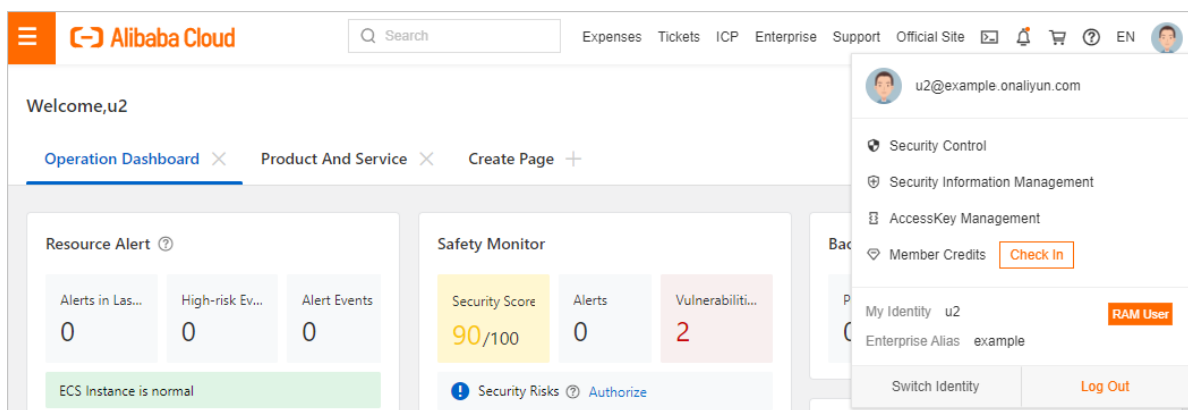
After the logon succeeds, you are redirected to the page that is specified by **Default RelayState**. If **Default RelayState** is invalid or not specified, you are redirected to the homepage of the Alibaba Cloud Management Console. If the page shown in the following figure appears, the user-based SSO configurations are successful.



- Logon from Okt a

Log on to the [Okt a portal](#) as an Okt a user. On the page that appears, click the **AliyunSSODemo** application.

After the logon succeeds, you are redirected to the page that is specified by **Default RelaySt ate**. If **Default RelaySt ate** is invalid or not specified, you are redirected to the homepage of the Alibaba Cloud Management Console. If the page shown in the following figure appears, the user-based SSO configurations are successful.



3.7. Implement user-based SSO by using Azure AD

This topic provides an example on how to implement user-based single sign-on (SSO) between Azure Active Directory (Azure AD) and Alibaba Cloud. The example describes the end-to-end SSO process between a cloud identity provider (IdP) and Alibaba Cloud.


Context

Before you start, you must create an Alibaba Cloud account and an Azure AD tenant. An administrator and an organization user u2 are added to the Azure AD tenant. The administrator is assigned the global administrative rights. You want the organization user u2 to access Alibaba Cloud as a Resource Access Management (RAM) user.


You must log on to the Azure portal as the administrator that is assigned the global administrative rights and perform the following steps in this example. For more information about how to create and authorize users in Azure AD, see [Azure AD documentation](#).

Step 1: Download the SAML SP metadata file of Alibaba Cloud

1. Log on to the [RAM console](#) by using your Alibaba Cloud account.
2. In the left-side navigation pane, click **SSO**.
3. On the **SSO** page, click the **User-based SSO** tab.
4. In the **Setup SSO** section, copy the value of **SAML Service Provider Metadata URL**.
5. Open a new tab in your browser and paste the URL in the address bar. On the page that appears, right-click the page and select **Save As** to download the SAML service provider (SP) metadata file in the XML format to your computer.


 **Note** The XML file contains the information that is required to configure Alibaba Cloud as a SAML SP. Record the values of the `entityID` and `Location` parameters for subsequent use.

Step 2: Create an application in Azure AD


1. Log on to the [Azure portal](#) as the administrator.
2. In the upper-left corner of the homepage, click the  icon.
3. In the left-side navigation pane, choose **Azure Active Directory > Enterprise applications > All applications**.
4. On the page that appears, click **New application**.
5. On the **Browse Azure AD Gallery** page, click **Create your own application**.
6. In the **Create your own application** panel, enter a name for your application. For example, you can enter `AliyunSSODemo`. Then, select **Integrate any other application you don't find in the gallery** and click **Create**.

Step 3: Configure SAML in Azure AD

1. On the `AliyunSSODemo` page, click **Single sign-on** in the left-side navigation pane.
2. In the **Select a single sign-on method** section of the page that appears, click **SAML**.
3. On the **Set up Single Sign-On with SAML** page, perform the following steps:
 - i. In the upper-left corner of the page, click **Upload metadata file**, select your metadata file, and then click **Add**.


 **Note** In this example, the XML file that you downloaded in [Step 1: Download the SAML SP metadata file of Alibaba Cloud](#) is uploaded.

- ii. In the **Basic SAML Configuration** panel, configure the following parameters and click **Save**.
 - **Identifier (Entity ID)**: Set this parameter to the value of `entityID` that is read from the preceding metadata file.
 - **Reply URL (Assertion Consumer Service URL)**: By default, this parameter is set to the value of the `Location` parameter that is read from the preceding metadata file.
 - **Relay State**: Enter the URL of the Alibaba Cloud service page to which an Azure AD user is redirected after the user logs on to Azure AD by using SSO.

 **Note** For security purposes, you must enter a URL that points to an Alibaba website for the **Relay State** parameter. For example, the domain name in the URL can be *.aliyun.com, *.hichina.com, *.yunos.com, *.taobao.com, *.tmall.com, *.alibabacloud.com, or *.alipay.com. If this parameter is empty, you are redirected to the homepage of the Alibaba Cloud Management Console after logon.

- iii. In the **SAML Signing Certificate** section, click **Download** in the **Federation Metadata XML** field to download the related XML file.

Step 4: Assign a user to the application in Azure AD

1. In the upper-left corner of the AAD homepage, click the  icon.
2. In the left-side navigation pane, choose **Azure Active Directory > Enterprise applications > All applications**.
3. In the **Name** column, click **AliyunSSODemo**.
4. In the left-side navigation pane, click **Users and groups**.
5. On the page that appears, click **Add user/group**.
6. On the Add Assignment page, click **Users**. In the Users panel, select **u2** and click **Select**.
7. Click **Assign**.

Step 5: Create a RAM user in the Alibaba Cloud Management Console

1. In the left-side navigation pane of the RAM console, choose **Identities > Users**.
2. On the **Users** page, click **Create User**.
3. On the **Create User** page, specify **Logon Name** and **Display Name** in the **User Account Information** section.

The logon name and Azure AD username must have the same prefix. In this example, the prefix of the logon name must be **u2**.
4. In the **Access Mode** section, select **Console Access** or **OpenAPI Access**.
5. Click **OK**.

Step 6: Enable user-based SSO in the Alibaba Cloud Management Console

1. In the left-side navigation pane, click **SSO**.
2. On the **SSO** page, click the **User-based SSO** tab.
3. Click **Edit** to the right of **SSO Settings**.

4. In the **SSO Status** section of the **SSO Settings** panel, click **Enabled**.

Note User-based SSO takes effect on all RAM users in your Alibaba Cloud account. If you enable this feature, all RAM users in your Alibaba Cloud account must log on to the Alibaba Cloud Management Console by using SSO. If you are using a RAM user, set the SSO Status parameter to Disabled in this step. You must complete the SSO settings for the RAM user before you enable user-based SSO. Otherwise, logon based on the RAM user will fail. To avoid this issue, you can also use the Alibaba Cloud account to configure user-based SSO.

5. In the **Metadata File** section, click **Upload** to upload the IdP metadata file obtained in [Step 3: Configure SAML in Azure AD](#).

6. Select **Enabled** for **Auxiliary Domain**. In the field that appears, enter the domain name of the email address that you use as the Azure AD username.

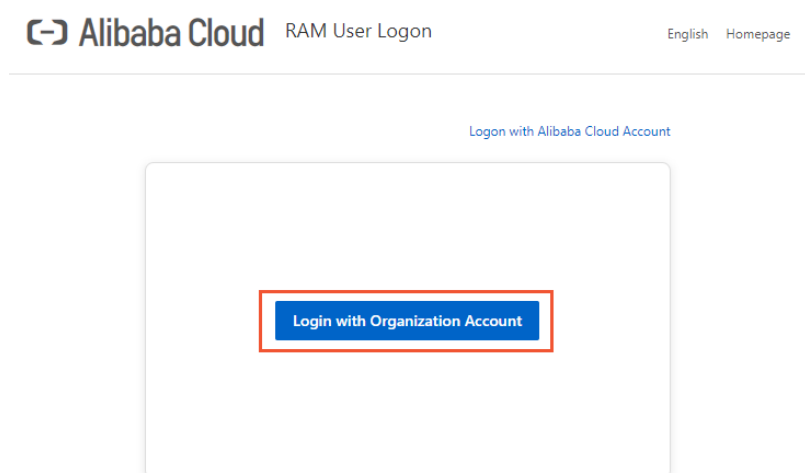
In this example, the domain name is test.onmicrosoft.com because the username of the Azure AD user u2 is u2@test.onmicrosoft.com.

7. Click **OK**.

Verify the user-based SSO configurations

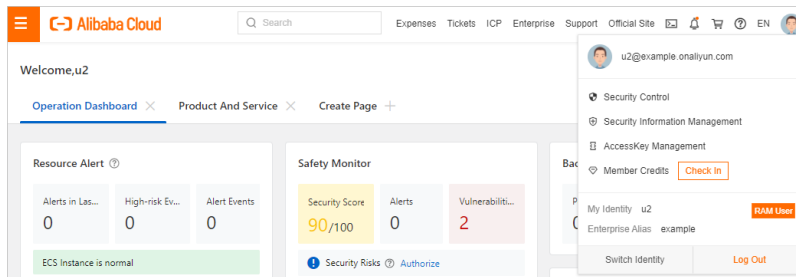
After you configure SSO, you can initiate SSO logon from both Alibaba Cloud and Azure AD.


- Logon from Alibaba Cloud
 - i. Log on to the [RAM console](#) by using your Alibaba Cloud account. On the **Overview** page, copy the logon URL of a RAM user.
 - ii. Move the pointer over the profile picture in the upper-right corner of the page and click **Log Out**. Then, paste the logon URL into the address bar of your browser and press Enter. You can also access the URL on a new tab.
 - iii. On the page that appears, click **Logon with Organization Account**. You are redirected to the logon page of Azure AD.



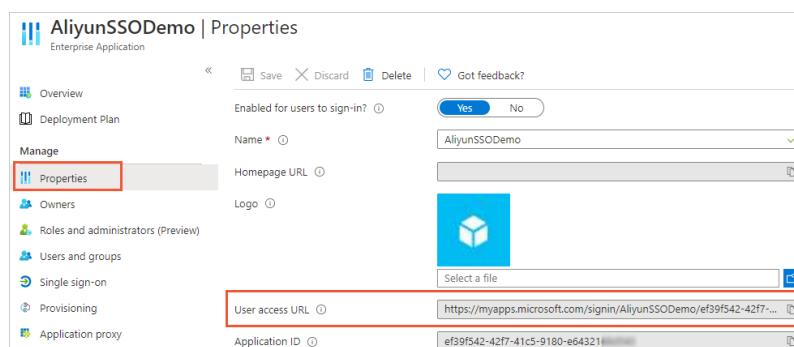
- iv. Log on by using the Azure AD user u2.

After the logon succeeds, you are redirected to the page that is specified by **Relay State**. If **Relay State** is invalid or not specified, you are redirected to the homepage of the Alibaba Cloud Management Console.



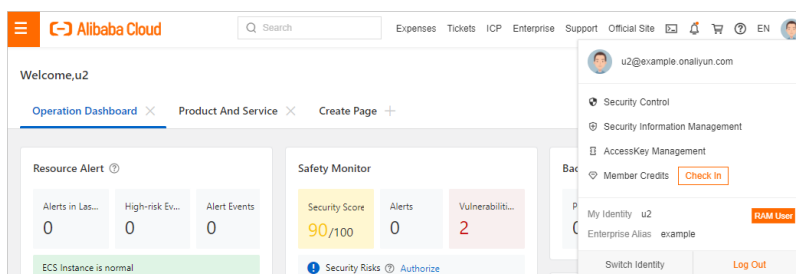
- Logon from Azure AD
 - i. Obtain the user access URL.
 - a. Log on to the [Azure portal](#) as the administrator.
 - b. In the upper-left corner of the homepage, click the  icon.
 - c. In the left-side navigation pane, choose **Azure Active Directory > Enterprise applications > All applications**.
 - d. Click **AliyunSSODemo**.
 - e. In the left-side navigation pane, click **Properties** and obtain the user access URL.

You can enter the user access URL in the address bar of your browser to access the application.



- ii. Enter the user access URL in the address bar of your browser and enter the username and password of u2 for the logon. You can obtain the URL from the administrator.

After the logon succeeds, you are redirected to the page that is specified by the **Relay State** parameter. If **Relay State** is invalid or not specified, you are redirected to the homepage of the Alibaba Cloud Management Console.



4. Role-based SSO

4.1. Role-based SSO by using SAML

4.1.1. Overview

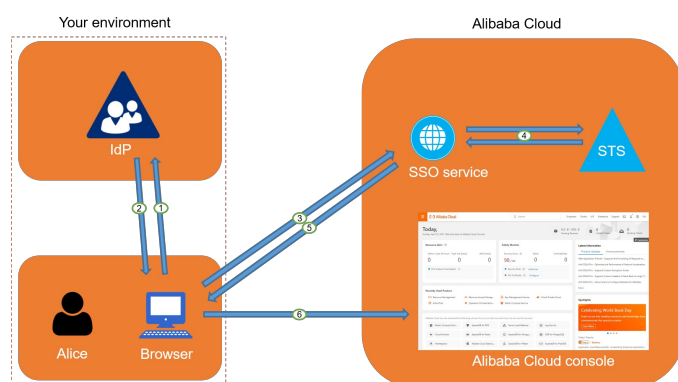
If Alibaba Cloud and the identity management system of an enterprise work together to implement role-based single sign-on (SSO), Alibaba Cloud is the service provider (SP) and the identity management system is the identity provider (IdP). Role-based SSO allows the enterprise to manage users in the local IdP without the need to synchronize users from the IdP to Alibaba Cloud. In addition, employees of the enterprise can access Alibaba Cloud by using a specific RAM role.

Process

Role-based SSO allows employees of the enterprise to access Alibaba Cloud by logging on to the Alibaba Cloud Management Console or by using a program.

- **Access Alibaba Cloud by logging on to the Alibaba Cloud Management Console**

The following figure shows how Alice, an employee, accesses Alibaba Cloud by logging on to the Alibaba Cloud Management Console after an administrator configures role-based SSO.



The following list describes the process:

- Alice opens the logon page of the IdP on a browser and selects Alibaba Cloud as the required service.

In this example, the IdP is Microsoft Active Directory Federation Services (AD FS). Therefore, the logon URL is `https://ADFSServiceName/adfs/ls/IdpInitiatedSignOn.aspx`.

Note Some IdPs require users to log on before users can select the SSO application that represents Alibaba Cloud.

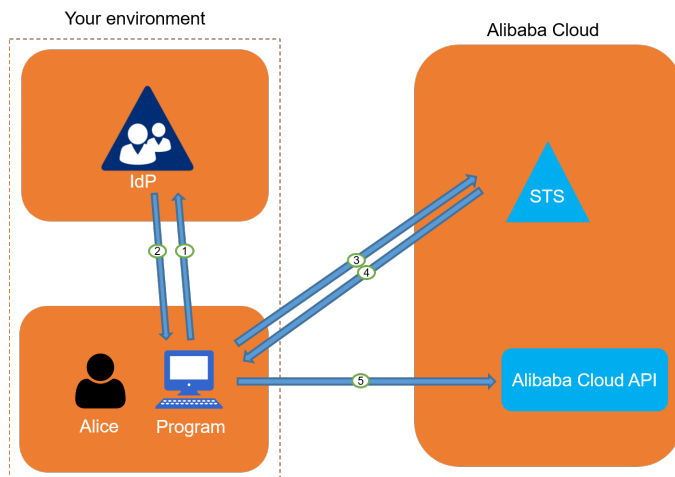
- The IdP generates a Security Assertion Markup Language (SAML) response and returns the response to the browser.
- The browser redirects Alice to the SSO service page and forwards the SAML response to the SSO service.
- The SSO service uses the SAML response to request an STS token from the Alibaba Cloud STS service. Then, the SSO service generates a URL that Alice can use to log on to the Alibaba Cloud Management Console by using the STS token.

Note If the SAML response contains attributes that map to multiple RAM roles, Alice is prompted to first select a role.

- v. The SSO service returns the URL to the browser.
- vi. The browser redirects Alice to the URL, and Alice logs on to the Alibaba Cloud Management Console as the specified role.

• Access Alibaba Cloud by using a program

The following figure shows how Alice accesses Alibaba Cloud by using a program.



The following list describes the process:

- i. Alice initiates a login request to the IdP by using a program.
- ii. The IdP generates a SAML response that contains the SAML assertion and returns the SAML response to the program.
- iii. The program calls the [AssumeRoleWithSAML](#) operation of the Alibaba Cloud STS service and forwards the following information:
The Alibaba Cloud Resource Name (ARN) of the IdP, the ARN of the role to be assumed, and the SAML assertion that is obtained from the IdP
- iv. The STS service verifies the SAML assertion and returns an STS token to the program.
- v. The program calls Alibaba Cloud API operations by using the STS token.

Configure role-based SSO

Before you can implement role-based SSO, you must establish trust between Alibaba Cloud and your IdP.

1. Configure the IdP in the Alibaba Cloud Management Console to ensure that your IdP is trusted by Alibaba Cloud.

For more information, see [Configure the SAML settings of Alibaba Cloud for role-based SSO](#).

2. Use a program or log on to the RAM console to create RAM roles for role-based SSO and grant permissions to the RAM roles.

For more information, see [Create a RAM role for a trusted IdP](#).

3. Configure Alibaba Cloud as a trusted SAML SP and configure SAML assertions in your IdP to ensure

that Alibaba Cloud is trusted by your IdP.

For more information, see [Configure Alibaba Cloud as a trusted SP for role-based SSO](#).

Examples

The following list provides examples on how to implement role-based SSO to Alibaba Cloud from common enterprise IdPs, such as AD FS, Okta, Azure AD, and OneLogin:

- [Implement role-based SSO from AD FS](#)
- [Implement role-based SSO from Okta](#)
- [Implement role-based SSO from Azure AD](#)
- [Implement role-based SSO from OneLogin to Alibaba Cloud](#)

4.1.2. SAML IdP

4.1.2.1. Create a SAML IdP

This topic describes how to create a Security Assertion Markup Language (SAML) identity provider (IdP). Before you implement role-based single sign-on (SSO), you must create a SAML IdP.

Prerequisites

The metadata file of your IdP is obtained. The metadata file is in the XML format. The metadata file contains the logon URLs, the public key that is used to verify SAML assertions, and the assertion format.

Procedure

1. Log on to the [RAM console](#) by using your Alibaba Cloud account.
2. In the left-side navigation pane, click **SSO**.
3. On the **Role-based SSO** tab, click the **SAML** tab and click **Create IdP**.
4. On the **Create IdP** page, configure **IdP Name** and **Note**.
5. In the **Metadata File** section, click **Upload** to upload the metadata file that is obtained from your IdP.
6. Click **OK**.

What's next

On the page that appears, click **Create RAM Role** to create RAM roles based on your business requirements. For more information, see [Create a RAM role for a trusted IdP](#).

4.1.2.2. View the basic information about a SAML IdP

This topic describes how to view the basic information about a Security Assertion Markup Language (SAML) identity provider (IdP), such as the name, type, description, and Alibaba Cloud Resource Name (ARN) of the IdP, the time when the IdP was created, and the time when the information about the IdP was updated.

Procedure

1. Log on to the [RAM console](#) by using your Alibaba Cloud account.

2. In the left-side navigation pane, click **SSO**.
3. On the **Role-based SSO** tab, click the **SAML** tab and click the IdP whose basic information you want to view.
4. In the **Details** section, view the basic information about the IdP, such as **IdP Name**, **IdP Type**, **Created At**, **Updated At**, **ARN**, and **Remarks**.

4.1.2.3. Modify the basic information about a SAML IdP

This topic describes how to modify the basic information about a Security Assertion Markup Language (SAML) identity provider (IdP). You can modify only the IdP description and metadata file.

Procedure

1. Log on to the **RAM console** by using your Alibaba Cloud account.
2. In the left-side navigation pane, click **SSO**.
3. On the **Role-based SSO** tab, click the **SAML** tab and click the IdP whose basic information you want to modify.
4. To modify the IdP description, click **Edit** to the right of **Remarks**.
5. To upload another metadata file, click **Replace Metadata**.

4.1.2.4. Delete a SAML IdP

If you no longer need a Security Assertion Markup Language (SAML) identity provider (IdP), you can delete the SAML IdP. This topic describes how to delete a SAML IdP. After you delete a SAML IdP, role-based single sign-on (SSO) cannot be implemented between your business system and Resource Access Management (RAM).

Procedure

1. Log on to the **RAM console** by using your Alibaba Cloud account.
2. In the left-side navigation pane, click **SSO**.
3. On the **Role-based SSO** tab, click the **SSO** tab. Then, find the SAML IdP that you want to delete and click **Delete** in the **Actions** column.
4. In the **Delete** message, click **OK**.

4.1.3. Configure the SAML settings of Alibaba Cloud for role-based SSO

This topic describes how to configure metadata for role-based single sign-on (SSO) to make sure that your identity provider (IdP) is trusted by Alibaba Cloud (service provider).

Prerequisites

The metadata file of your IdP is obtained. The metadata file is in the XML format. The metadata file contains the logon URLs, the public key that is used to verify SAML assertions, and the assertion format.

Procedure

1. Log on to the [RAM console](#) by using your Alibaba Cloud account.
2. In the left-side navigation pane, click **SSO**.
3. On the **Role-based SSO** tab, click the **SAML** tab and click **Create IdP**.
4. On the **Create IdP** page, configure **IdP Name** and **Note**.
5. In the **Metadata File** section, click **Upload** to upload the metadata file that is obtained from your IdP.
6. Click **OK**.

What's next


On the page that appears, click **Create RAM Role** to create RAM roles based on your business requirements. For more information, see [Create a RAM role for a trusted IdP](#).

4.1.4. Configure Alibaba Cloud as a trusted SP for role-based SSO

This topic describes how to configure Alibaba Cloud as a trusted Security Assertion Markup Language (SAML) service provider (SP) of your identity provider (IdP) for role-based single sign-on (SSO).

Procedure

1. Obtain the SAML SP metadata URL of Alibaba Cloud in the Resource Access Management (RAM) console.
The SAML SP metadata URL is `https://signin.alibabacloud.com/saml-role/sp-metadata.xml`.
2. Create a SAML SP in your IdP and configure Alibaba Cloud as the relying party by using one of the following methods:
 - Use the SAML SP metadata URL of Alibaba Cloud that you copied in the Step .
 - If your IdP does not support the URL-based configuration of the relying party, download the metadata file from the URL that you copied in Step and upload the metadata file.
 - If your IdP does not allow you to upload the metadata file, configure the following parameters:
 - **Entity ID** : `urn:alibaba:cloudcomputing:international`
 - **ACS URL** : `https://signin.alibabacloud.com/saml-role/sso`
 - **RelayState** : This parameter is optional. If your IdP requires the **RelayState** parameter, set the value of the parameter to a URL. Users will be redirected to the URL after SSO succeeds. If you do not configure this parameter, users are redirected to the homepage of the Alibaba Cloud Management Console after SSO succeeds.

 **Note** For security purposes, you must enter a URL that points to an Alibaba website for the **RelayState** parameter. For example, the domain name in the URL can be `*.aliyun.com`, `*.hichina.com`, `*.yunos.com`, `*.taobao.com`, `*.tmall.com`, `*.alibabacloud.com`, or `*.alipay.com`.

What's next

After you configure Alibaba Cloud as a trusted SAML SP, you must configure SAML assertions for your IdP. For more information, see [SAML response for role-based SSO](#).

4.1.5. SAML response for role-based SSO

This topic describes the syntax of a SAML response for role-based single sign-on (SSO). This topic also describes the elements of a SAML assertion in a SAML response.

Background information

During SAML 2.0-based SSO, after the identity of a user is verified, the identity provider (IdP) generates an authentication response and sends this response to Alibaba Cloud by using a browser or a program. This response contains a SAML assertion that complies with the specifications of HTTP POST binding in SAML 2.0. Alibaba Cloud uses the SAML assertion to determine the logon status and identity of the user. Therefore, the SAML assertion must contain the elements that are required by Alibaba Cloud. If the SAML assertion does not contain the required elements, SSO fails.

SAML response

Make sure that each SAML response that is sent by your IdP to Alibaba Cloud contains the following elements. Otherwise, SSO fails.

```

<saml2p:Response>
  <saml2:Issuer>...</saml2:Issuer>
  <saml2p:Status>
    ...
  </saml2p:Status>
  <saml2:Assertion>
    <saml2:Issuer>...</saml2:Issuer>
    <ds:Signature>
      ...
    </ds:Signature>
    <saml2:Subject>
      <saml2:NameID>${NameID}</saml2:NameID>
      <saml2:SubjectConfirmation>
        ...
      </saml2:SubjectConfirmation>
    </saml2:Subject>
    <saml2:Conditions>
      <saml2:AudienceRestriction>
        <saml2:Audience>${Audience}</saml2:Audience>
      </saml2:AudienceRestriction>
    </saml2:Conditions>
    <saml2:AuthnStatement>
      ...
    </saml2:AuthnStatement>
    <saml2:AttributeStatement>
      <saml2:Attribute Name="https://www.aliyun.com/SAML-Role/Attributes/RoleSessionName">
        ...
      </saml2:Attribute>
      <saml2:Attribute Name="https://www.aliyun.com/SAML-Role/Attributes/Role">
        ...
      </saml2:Attribute>
    </saml2:AttributeStatement>
  </saml2:Assertion>
</saml2p:Response>

```

Elements in a SAML assertion

- Common elements in SAML 2.0

Element	Description
Issuer	The value of the <code>Issuer</code> element must match the value of <code>EntityID</code> in the metadata file that you uploaded for the IdP in the Alibaba Cloud Management Console.
Signature	The SAML assertion must be signed. The <code>Signature</code> element must contain information such as the signature value and signature algorithm. The signature is used to confirm that the signed SAML assertion has not been modified after the signature was generated.

Element	Description
Subject	<p>The <code>Subject</code> element must contain the following sub-elements:</p> <ul style="list-style-type: none"> Only one <code>NameID</code> sub-element. You must specify the value of <code>NameID</code> based on SAML 2.0. However, Alibaba Cloud does not determine a logon identity based on the value of <code>NameID</code>. Only one <code>SubjectConfirmation</code> sub-element that contains a <code>SubjectConfirmationData</code> sub-element. The <code>SubjectConfirmationData</code> sub-element must contain the following attributes: <ul style="list-style-type: none"> <code>NotOnOrAfter</code>: the validity period of a SAML assertion. <code>Recipient</code>: the recipient of the SAML assertion. Alibaba Cloud checks whether it is the recipient of the SAML assertion based on the value of this attribute. Therefore, you must set this attribute to <code>https://signin.alibabacloud.com/saml-role/sso</code>. <p>The following script provides an example of the <code>Subject</code> element:</p> <pre><Subject> <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">administrator</NameID> <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"> <SubjectConfirmationData NotOnOrAfter="2019-01-01T00:01:00.000Z" Recipient="https://signin.alibabacloud.com/saml-role/sso"/> </SubjectConfirmation> </Subject></pre>
Conditions	<p>The <code>Conditions</code> element must contain an <code>AudienceRestriction</code> sub-element. The <code>AudienceRestriction</code> sub-element can contain one or more <code>Audience</code> sub-elements. The value of an <code>Audience</code> sub-element must be <code>urn:alibaba:cloudcomputing:international</code>.</p> <p>The following script provides an example of the <code>Conditions</code> element:</p> <pre><Conditions> <AudienceRestriction> <Audience>urn:alibaba:cloudcomputing:international</Audience> </AudienceRestriction> </Conditions></pre>

- Custom elements required by Alibaba Cloud


Alibaba Cloud requires that the `AttributeStatement` element in a SAML assertion contains the following `Attribute` sub-elements:

- o **Role attribute:** an `Attribute` element with the `Name` attribute set to `https://www.aliyun.com/SAML-Role/Attributes/Role`

This sub-element is required and contains one or more `AttributeValue` sub-elements.


`AttributeValue` lists the roles that can be assumed by a user in your IdP. The value of the `AttributeValue` sub-element is a comma-delimited pair of the Alibaba Cloud Resource Name (ARN) of the role and the ARN of the IdP. You can view the ARN of the role and the ARN of the IdP in the RAM console.

- To view the ARN of the role, go to the **Roles** page and click the name of the RAM role. On the page that appears, you can view the ARN of the role in the **Basic Information** section.
- To view the ARN of the IdP, go to the **SSO** page. On the **Role-based SSO** tab, click the name of the IdP. You can view the ARN of the IdP in the **IdP Information** section.

 **Note** If a role attribute contains multiple `AttributeValue` sub-elements, the user must select which role to assume when the user logs on to the Alibaba Cloud Management Console.

The following script provides an example of the `Role` attribute:

```
<Attribute Name="https://www.aliyun.com/SAML-Role/Attributes/Role">
  <AttributeValue>acs:ram::$account_id:role/role1,acs:ram::$account_id:saml-provider/pr
  ovider1</AttributeValue>
  <AttributeValue>acs:ram::$account_id:role/role2,acs:ram::$account_id:saml-provider/pr
  ovider1</AttributeValue>
</Attribute>
```

 **Note** The value of `$account_id` is the ID of the Alibaba Cloud account that defines the RAM role and IdP.

- o **Role attribute:** an `Attribute` element with the `Name` attribute set to `https://www.aliyun.com/SAML-Role/Attributes/RoleSessionName`

This sub-element is required and contains only one `AttributeValue` sub-element that specifies the user information to be displayed in the RAM console and ActionTrail logs. If you want multiple users to assume the same role, specify different values of the `RoleSessionName` attribute for the users. Each value uniquely identifies a user. For example, you can set the value to an employee ID or email address.

The value in the `AttributeValue` sub-element must be 2 to 64 characters in length, and can contain only letters, digits, and the following special characters: `- _ .@ =`

The following script provides an example of the `RoleSessionName` attribute:

```
<Attribute Name="https://www.aliyun.com/SAML-Role/Attributes/RoleSessionName">
  <AttributeValue>user_id</AttributeValue>
</Attribute>
```


- **SessionDuration attribute:** an `Attribute` sub-element with the `Name` attribute set to `https://www.aliyun.com/SAML-Role/Attributes/SessionDuration`

This element is optional and contains only one `AttributeValue` sub-element that specifies the maximum duration of each session. The value of this sub-element is an integer, in seconds. The value cannot exceed the maximum session duration that is specified for the Role attribute. The minimum value is 900 seconds.

The following script provides an example of the `SessionDuration` attribute:

```
<Attribute Name="https://www.aliyun.com/SAML-Role/Attributes/SessionDuration">
  <AttributeValue>1800</AttributeValue>
</Attribute>
```

- **Maximum role session duration**

If you use the console to assume a role, the maximum session duration for the role is the value of the `SessionDuration` attribute that is specified in a SAML assertion. If the `SessionNotOnOrAfter` attribute of the `AuthnStatement` element is also specified, the maximum session duration is the smaller value between `SessionDuration` and `SessionNotOnOrAfter`. If neither `SessionDuration` nor `SessionNotOnOrAfter` is specified, the maximum session duration is the smaller value between the **Maximum Session Duration** parameter of the role and the **Logon Session Valid For** parameter. For more information, see [Configure security policies for RAM users](#) and [Specify the maximum session duration for a RAM role](#).

If you have specified the `DurationSeconds` parameter when you call the [AssumeRoleWithSAML](#) operation and defined the `SessionNotOnOrAfter` attribute in the `AuthnStatement` element, the maximum session duration is the smaller value between `SessionDuration` and `SessionNotOnOrAfter`. If neither `SessionDuration` nor `SessionNotOnOrAfter` is specified, the maximum session duration is 3,600 seconds by default.

4.1.6. Implement role-based SSO from AD FS

This topic provides an example on how to implement role-based single sign-on (SSO) from Active Directory Federation Services (AD FS) to Alibaba Cloud. The example includes the steps that are required to configure role-based SSO on both an identity provider (IdP) and Alibaba Cloud. In the following example, AD FS is deployed on an Elastic Compute Service (ECS) instance that runs Windows Server 2012 R2.

Context

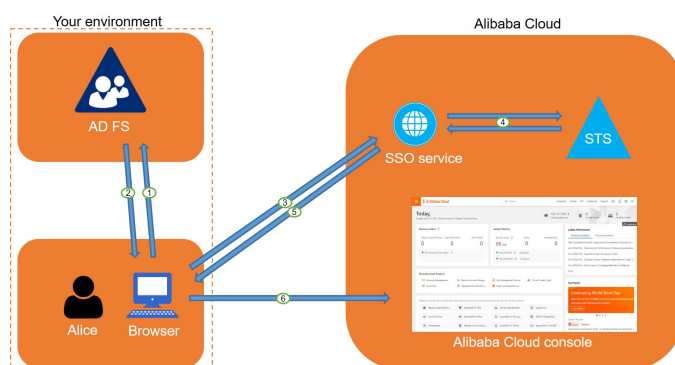
An enterprise uses Active Directory (AD) to manage users and AD FS to configure enterprise applications such as Alibaba Cloud. After role-based SSO is configured, an AD administrator can control user access to the resources of Alibaba Cloud accounts by user group. In this example, the enterprise has Alibaba Cloud accounts, Account 1 and Account 2, and AD user groups, Aliyun-<account-id>-ADFS-Admin and Aliyun-<account-id>-ADFS-Reader. A user named Alice belongs to these groups. The enterprise wants to implement role-based SSO from AD FS to Account 1 and Account 2.

? Note

- <account-id> indicates the ID of Account 1 or Account 2. Therefore, the user Alice belongs to four user groups. The group whose name contains Admin has the Admin permission on Account 1 or Account 2. The group whose name contains Reader has the Reader permission on Account 1 or Account 2.
- The configuration of Microsoft AD described in this topic is for reference only and helps you understand the configuration procedure of SSO to Alibaba Cloud. Alibaba Cloud does not provide consultation services for the configuration of Microsoft AD.

Process

The following figure shows the process of role-based SSO.



After an AD administrator completes the configurations of role-based SSO, the user Alice can log on to the Alibaba Cloud Management Console based on the process shown in the figure. For more information, see [Overview](#).

The process shows that users can be authenticated without the need to provide Alibaba Cloud usernames or passwords during login.

Step 1: Configure AD FS as a trusted Security Assertion Markup Language (SAML) IdP in Alibaba Cloud

1. Log on to the Alibaba Cloud RAM console. Create an IdP named ADFS and upload a metadata file. You can obtain the metadata file of AD FS from `https://<ADFS-server>/federationmetadata/2007-06/federationmetadata.xml`.

? Note <ADFS-server> indicates the domain name or IP address of your AD FS server.

For more information, see [Configure the SAML settings of Alibaba Cloud for role-based SSO](#).

? Note If the size of the metadata file exceeds the upper limit, you can delete all content in `<fed:ClaimTypesRequested>` and `<fed:ClaimTypesOffered>`.

2. Create two RAM roles named ADFS-Admin and ADFS-Reader for Account 1. When you create the RAM roles, select IdP as the type of trusted entity and ADFS as the trusted IdP. Then, attach the `AdministratorAccess` policy to the ADFS-Admin role and the `ReadOnlyAccess` policy to the ADFS-Reader role. A

For more information, see [Create a RAM role for a trusted IdP](#).

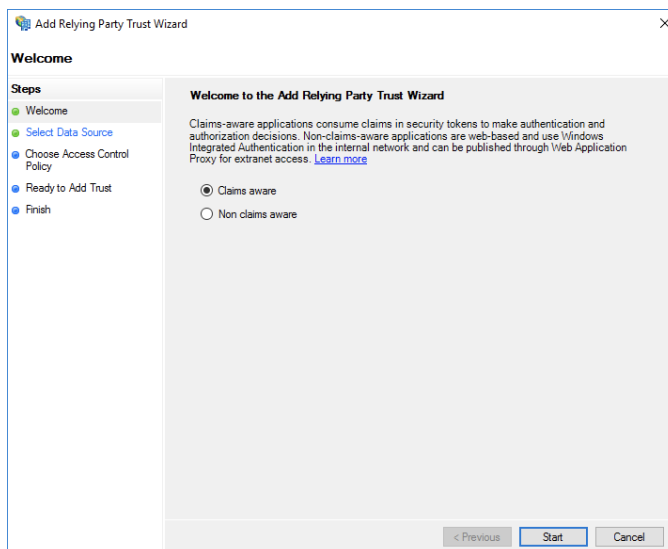
3. Repeat the preceding steps to create the same IdP and two RAM roles for Account 2. Then, attach the `AdministratorAccess` policy to the ADFS-Admin role and the `ReadOnlyAccess` policy to the ADFS-Reader role.

Note After you complete the configurations, Account 1 and Account 2 trust the information about user identities and roles. The information is included in Security Assertions Markup Language (SAML) requests sent from your AD FS server.

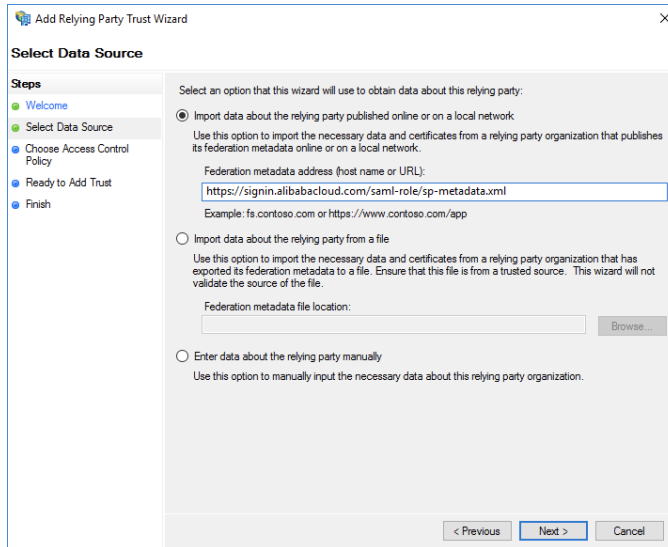
Step 2: Configure Alibaba Cloud as a trusted SAML SP in AD FS

In AD FS, a SAML service provider (SP) is a **relying party**. To configure Alibaba Cloud as a trusted SAML SP in AD FS, perform the following steps:

1. In the top navigation bar of **Server Manager**, choose **Tools > AD FS Management**.
2. Right-click **Relying Parties** and select **Add Relying Party Trust**.



3. Configure the SAML SP metadata file of Alibaba Cloud for the relying party. You can obtain the metadata file from the following URL: `https://signin.alibabacloud.com/saml-role/sp-metadata.xml`.



4. Complete the wizard as prompted.

Step 3: Configure SAML assertion attributes for the Alibaba Cloud SP

The SAML assertion that is issued by AD FS must contain the `NameID`, `Role`, and `RoleSessionName` attributes. AD FS provides these attributes by using issuance transform rules.

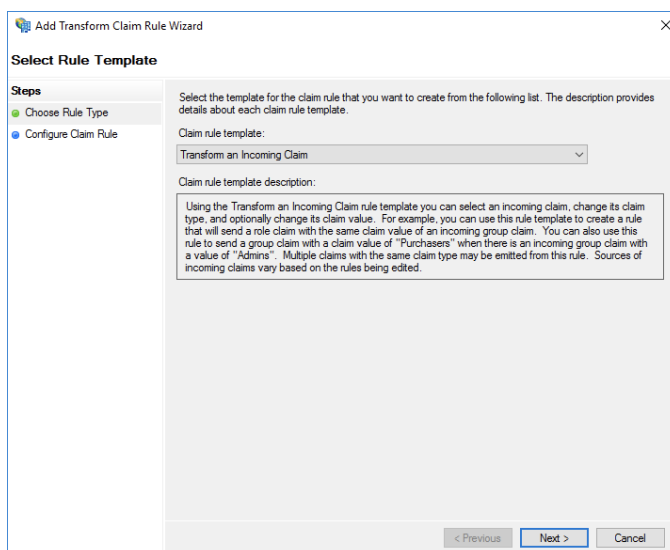
- `NameID`

Perform the following steps to set the `NameID` attribute in the SAML assertion to the Windows account name of a user in AD:

- Right-click the display name of the relying party and select **Edit Claim Issuance Policy**.
- Click **Issuance Transform Rules** to add a rule.

Note An issuance transform rule indicates how to transform a known user attribute and issue it as an attribute in the SAML assertion. If you want to issue the Windows account name of a user in AD as `NameID`, you must create an issuance transform rule.

- Set **Claim rule template to Transform an Incoming Claim**.



iv. Configure the following parameters and click **Finish**.

- Set **Claim rule name** to **NameID**.
- Set **Incoming claim type** to **Windows account name**.
- Set **Outgoing claim type** to **Name ID**.
- Set **Outgoing name ID format** to **Persistent Identifier**.
- Select **Pass through all claim values**.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule**

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Rule template: Transform an Incoming Claim

Incoming claim type:

Incoming name ID format:

Outgoing claim type:

Outgoing name ID format:

☒ Pass through all claim values

☐ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value:

☐ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

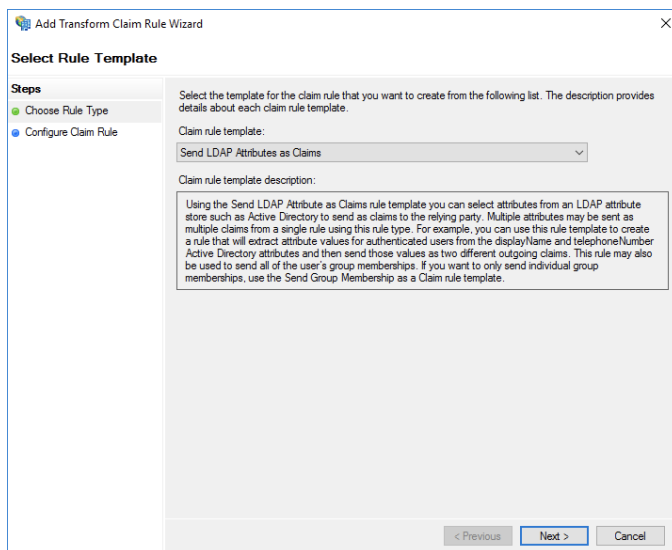
After you complete the configurations, AD FS sends the **NameID** attribute in the format required by Alibaba Cloud. The following code shows an example:

```
<NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">
  YourDomain\rolessouser
</NameID>
```

● RoleSessionName

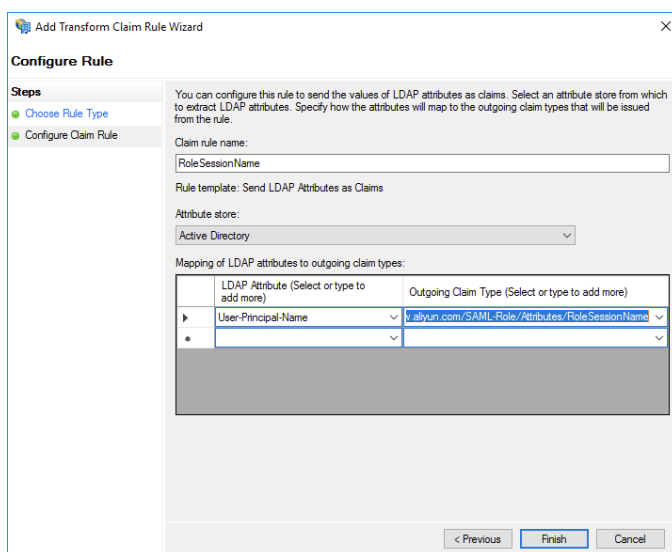
Perform the following steps to set the **RoleSessionName** attribute in the SAML assertion to the User Principal Name (UPN) of a user in AD:

- i. In the Issuance Transform Rules dialog box, click **Add Rule**.
- ii. Set **Claim rule template** to **Send LDAP Attributes as Claims**.



iii. Configure the following parameters and click **Finish**.

- Set **Claim rule name** to `RoleSessionName`.
- Set **Attribute store** to `Active Directory`.
- Select `User-Principal-Name` in the **LDAP Attribute** column. You can also use a different option, such as `Email`, based on your business requirements.
- Enter `https://www.aliyun.com/SAML-Role/Attributes/RoleSessionName` in the **Outgoing Claim Type** column.



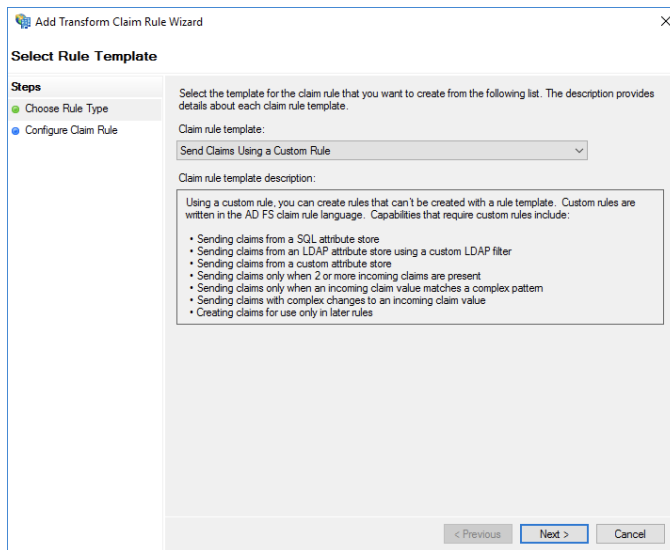
After you complete the configurations, AD FS sends the `RoleSessionName` attribute in the format required by Alibaba Cloud. The following code shows an example.

```
<Attribute Name="https://www.aliyun.com/SAML-Role/Attributes/RoleSessionName">
  <AttributeValue>rolessouser@example.com</AttributeValue>
</Attribute>
```

- **Role**

Perform the following steps to configure a custom attribute and set its value to the name of an Alibaba Cloud RAM role that is associated with the AD group of a user:

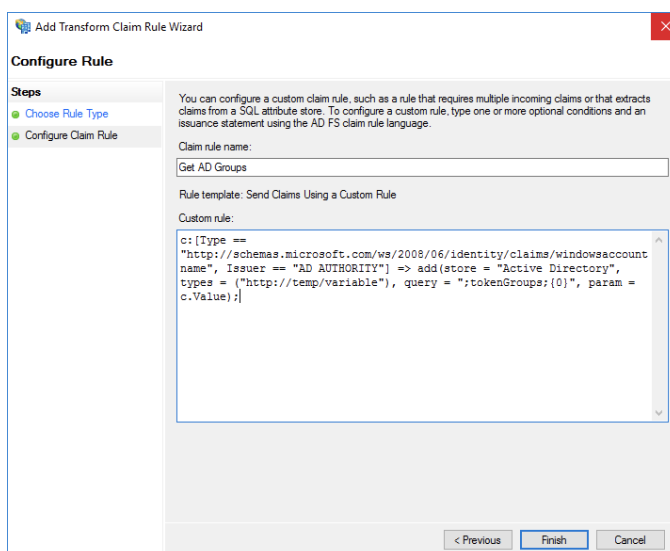
- i. In the Issuance Transform Rules dialog box, click **Add Rule**.
- ii. Set **Claim rule template** to **Send Claims Using a Custom Rule** and click **Next**.



- iii. Configure the following parameters and click **Finish**.

- Set **Claim rule name** to **Get AD Groups**.
- In the **Custom rule** field, enter the required information. Set this parameter based on the following example:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"] => add(store = "Active Directory", types = ("http://temp/variable"), query = ";tokenGroups;{0}", param = c.Value);
```



Note This rule is used to obtain the AD group to which the user belongs. The rule is saved in the *http://temp/variable* intermediate variable.

- iv. In the Issuance Transform Rules dialog box, click **Add Rule**.
- v. Repeat the preceding steps and click **Finish**.
- Set **Claim rule name** to **Role**.

- In the **Custom rule** field, enter the required information. Set this parameter based on the following example:

```
c:[Type == "http://temp/variable", Value =~ "(?i)^Aliyun-([\d]+)"] => issue(Type = "https://www.aliyun.com/SAML-Role/Attributes/Role", Value = RegexReplace(c.Value, "Aliyun-([\d]+)-(.+)", "acs:ram::$1:role/$2,acs:ram::$1:saml-provider/ADFS"));
```

Note If the user belongs to the Aliyun-<account-id>-ADFS-Admin or Aliyun-<account-id>-ADFS-Reader group, a SAML attribute is generated and mapped to the ADFS-Admin or ADFS-Reader role in Alibaba Cloud based on this rule.

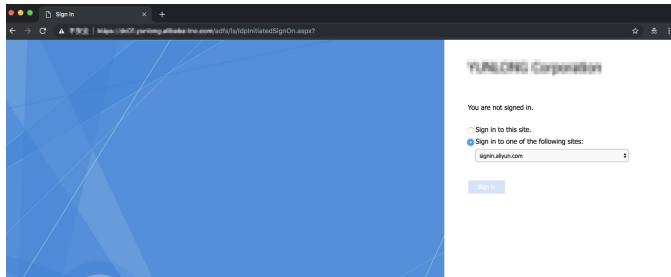
After you complete the configurations, your IdP returns the required part of a SAML assertion to Alibaba Cloud. The following code shows an example.

```
<Attribute Name="https://www.aliyun.com/SAML-Role/Attributes/Role">
  <AttributeValue>acs:ram::<account-id>:role/ADFS-Admin,acs:ram::<account-id>:saml-provider/ADFS</AttributeValue>
</Attribute>
```

Verify the user-based SSO configurations

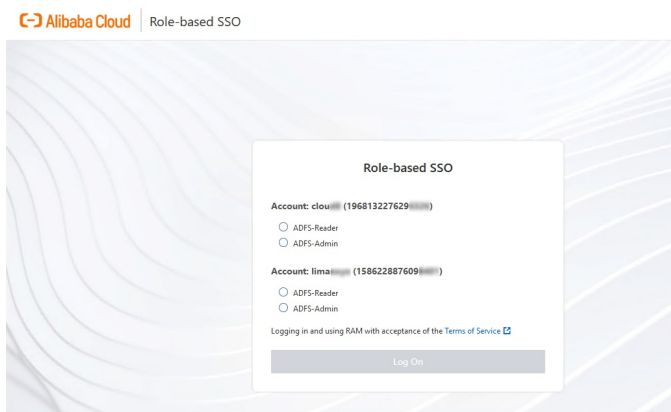
1. Log on to the AD FS portal for SSO at `https://<ADFS-server>/ads/ls/IdpInitiatedSignOn.aspx`. Select the Alibaba Cloud application and enter the username and password of your user.

Note <ADFS-server> indicates the domain name or IP address of your AD FS server. If the URL is unavailable, run the `Set-AdfsProperties -EnableIdpInitiatedSignonPage $True` command in PowerShell.



2. On the Role-based SSO page of Alibaba Cloud, select the RAM role that you want to use and click Sign In.

Note If your user belongs to only one AD group, the user corresponds to only one RAM role in Alibaba Cloud. In this case, you can log on to the Alibaba Cloud Management Console without the need to select a RAM role.

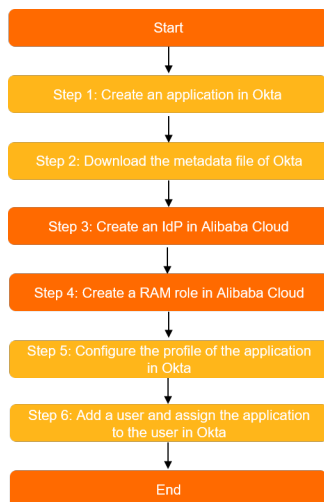


4.1.7. Implement role-based SSO from Okta

This topic provides an example on how to implement role-based single sign-on (SSO) from Okta to Alibaba Cloud. The example describes the end-to-end SSO process from a cloud identity provider (IdP) to Alibaba Cloud.

Procedure

In this example, an attribute named `approle` is added to the profile of an Okta application. The `approle` attribute is used to specify a Resource Access Management (RAM) role. The following figure shows the procedure to implement role-based SSO in Alibaba Cloud and Okta.



Step 1: Create an application that supports Security Assertion Markup Language (SAML) 2.0-based SSO in Okta

1. Log on to the [Okta portal](#).
2. In the upper-right corner of the Okta portal, click the account name and select **Your Org** from the drop-down list.
3. In the left-side navigation pane, choose **Applications > Applications**.
4. On the **Applications** page, click **Create App Integration**.
5. In the **Create a new app integration** dialog box, select **SAML 2.0** and click **Next**.
6. In the General Settings step, enter `role-sso-test` in the App name field and click **Next**.
7. In the Configure SAML step, configure the parameters and click **Next**.

GENERAL

Single sign on URL ?

☒ Use this for Recipient URL and Destination URL

☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ?

Default RelayState ?

If no value is set, a blank RelayState is sent


Name ID format ?

Application username ?

[Show Advanced Settings](#)

- In the **Single sign on URL** field, enter `https://signin.alibabacloud.com/saml-role/sso` .
- In the **Audience URI** field, enter `urn:alibaba:cloudcomputing:international` .

- In the **Default RelayState** field, enter a URL. A user is redirected to the URL after login.

 **Note** For security purposes, you must enter a URL that points to an Alibaba website in the **Default RelayState** field. For example, the domain name in the URL can be *.aliyun.com, *.hichina.com, *.yunos.com, *.taobao.com, *.tmall.com, *.alibabacloud.com, or *.alipay.com. If you leave this parameter empty, you are redirected to the homepage of the Alibaba Cloud Management Console after login.

- Select **EmailAddress** from the **Name ID format** drop-down list.
 - Select **Email** from the **Application username** drop-down list.
8. In the **Feedback** step, select an application type based on your business requirements and click **Finish**.

Step 2: Download the SAML IdP metadata file of Okta

1. On the Applications page, click role-sso-test. On the page that appears, click the **Sign On** tab.
2. In the **Settings** section of the Sign On tab, click **Identity Provider metadata**. On the page that appears, right-click the page and click **Save As** to download the metadata file.


Step 3: Create a SAML IdP in Alibaba Cloud

1. Log on to the **RAM console** by using your Alibaba Cloud account.
2. In the left-side navigation pane, click **SSO**.
3. On the **Role-based SSO** tab, click the **SAML** tab and click **Create IdP**.
4. On the **Create IdP** page, set **IdP Name** to okta-provider and configure **Description**.
5. In the **Metadata File** section, click **Upload** to upload the IdP metadata file that is obtained in [Step 2: Download the SAML IdP metadata file of Okta](#).
6. Click **OK**.
7. Click **Close**.

Step 4: Create a RAM role in Alibaba Cloud


1. In the left-side navigation pane of the RAM console, choose **Identities > Users**.
2. On the **Roles** page, click **Create Role**.
3. In the **Create Role** panel, select **IdP** for Select Trusted Entity and click **Next**.
4. Set **RAM Role Name** to admin and enter the description of the RAM role in the **Note** field.
5. Select **SAML** for the IdP Type parameter.
6. Select the IdP that you created in [Step 3: Create a SAML IdP in Alibaba Cloud](#), read the conditions, and then click **OK**.
7. Click **Close**.

Step 5: Configure the profile of the application in Okta

1. Add an attribute to the profile of the application.
 - i. In the left-side navigation pane, choose **Directory > Profile Editor**.
 - ii. Click the  **Profile** icon next to the profile.

iii. Click **Add Attribute**. In the Add Attribute dialog box, configure the attribute parameters.

- Select **string** from the **Data type** drop-down list.
- In the **Display name** field, enter `approle`. The name is displayed in the portal to represent the attribute.
- In the **Variable name** field, enter `approle`. The variable is used to specify the Alibaba Cloud RAM role. You must record the value of Variable name for subsequent use.
- In the **Description** field, enter a description for the attribute. This parameter is optional.
- Select **Define enumerated list of values** next to **Enum**.

 **Note** If you select **Define enumerated list of values**, only enumeration values of the attribute are valid. You can clear **Enum** to increase flexibility.

- In the **Attribute members** section, specify an enumeration value for the attribute. Each enumeration value must be the same as the name of a RAM role that you created in Alibaba Cloud. In this example, the values are `admin` and `reader`.
- In this example, you do not need to set **Attribute Length** because an enumeration value is configured for the attribute. If no enumeration values are configured for an attribute, set the attribute length.
- Select **Yes** next to **Attribute required**.
- Clear **User personal** next to **Scope**.

iv. Click **Save**.

2. Configure the attribute.

- i. In the left-side navigation pane, choose **Applications > Applications**.
- ii. On the Applications page, click the application name `role-sso-test`.
- iii. On the **General** tab, click **Edit** in the **SAML Settings** section.

- iv. In the **Attribute Statements (optional)** section of the **Configure SAML** page, configure two statements, as shown in the following figure.

Name	Name format (optional)	Value
1 <code>https://www.aliyun.com/S</code>	Unspecified	<code>user.email</code>
2 <code>https://www.aliyun.com/S</code>	Unspecified	<code>String.replace("acs:ram::<account_id>:role/\$approle,acs:ram::<account_id>:saml-provider/okta-provider", "\$approle", appuser.approle)</code>

■ **Attribute statement 1**

- Enter `https://www.aliyun.com/SAML-Role/Attributes/RoleSessionName` in the **Name** column.
- Select `user.email` from the **Value** drop-down list.

■ **Attribute statement 2**

- Enter `https://www.aliyun.com/SAML-Role/Attributes/Role` in the **Name** column.
- Select `String.replace("acs:ram::<account_id>:role/$approle,acs:ram::<account_id>:saml-provider/okta-provider", "$approle", appuser.approle)` from the **Value** drop-down list. Replace `$approle` with an enumeration value of `approle`. `approle` is the attribute that you added to the profile. `okta-provider` is the name of the IdP that you created in [Step 3: Create a SAML IdP in Alibaba Cloud](#). Replace `<account_id>` with the ID of your Alibaba Cloud account. Example: `String.replace("acs:ram::177242285274****:role/$approle,acs:ram::177242285274****:saml-provider/okta-provider", "$approle", appuser.approle)`.

Step 6: Create a user and assign the application to the user in Okta

1. Create a user.


- In the left-side navigation pane, choose **Directory > People**.
- On the page that appears, click **Add Person**.
- In the **Add Person** dialog box, enter the email address of the user in the **Primary email** field, configure other parameters, and then click **Save**. In this example, the email address is `test@example.com`.
- In the user list, find `test@example.com` and click **Activate** in the **Status** column. In the dialog box that appears, activate `test@example.com` as prompted.

2. Assign the application to the user.

You can use one of the following methods to assign the application.

- Assign the application to the user
 - In the left-side navigation pane, choose **Applications > Applications**.
 - Click the application name `role-sso-test`. On the **Assignments** tab, choose **Assign > Assign to People**.
 - In the dialog box that appears, click **Assign** next to the `test@example.com` user.
 - Select `admin` from the **approle** drop-down list.
 - Click **Save and Go Back**.

- f. Click **Done**.
- o Add the user to a group and assign the application to the group
 - a. In the left-side navigation pane, choose **Directory > Groups**. On the page that appears, click **Add Group** to create a group.
 - b. Click the name of the group. On the page that appears, click **Manage People** to add the user to the group.
 - c. In the left-side navigation pane, choose **Applications > Applications**.
 - d. Click the application name role-sso-test. On the **Assignments** tab, choose **Assign > Assign to Groups**.
 - e. Click **Assign** next to the group.
 - f. Select admin from the **approle** drop-down list.
 - g. Click **Save and Go Back**.
 - h. Click **Done**.

 **Note** If the user belongs to multiple groups, only one value of the approle attribute is used. The used attribute value is the value that is specified for the group to which the user is first added. If the user is added to or removed from groups, the value of the approle attribute changes. For more information, see [Okta Documentation](#).

Verify the role-based SSO configurations

1. In the left-side navigation pane, choose **Applications > Applications**.
2. On the Applications page, click the application name role-sso-test.
3. In the **App Embed Link** section of the **General** tab, copy the logon URL.

App Embed Link Edit

EMBED LINK

You can use the URL below to sign into role-sso-test from a portal or other location outside of Okta.

`https://example.okta.com/home/..._rolestest_1/0oafcbq3pjw5FoDG44.../aInfcci8IzNteJBB...`

APPLICATION LOGIN PAGE

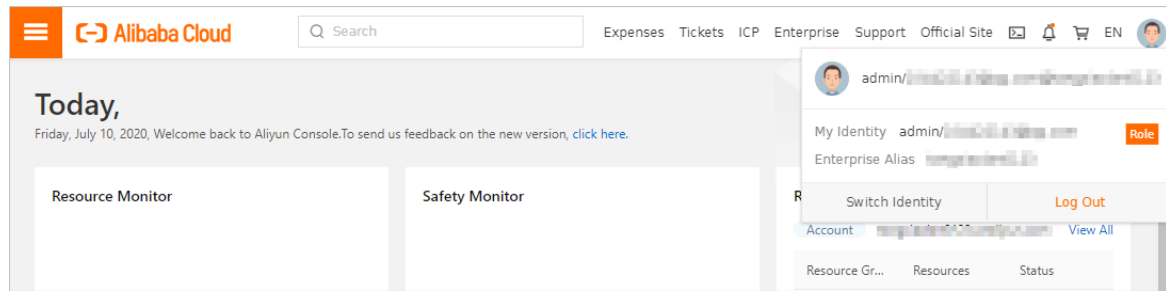
If someone who is not authenticated attempts to access this application, they will be redirected to a default login page or one that can be customized. An application level setting will override default URL settings and IdP routing rules for this app.

☒ Use the default organization login page.

☐ Use a custom login page for this application.

4. Open a new browser window, paste the logon URL in the address bar, and then press Enter. On the logon page, use test@example.com to log on.

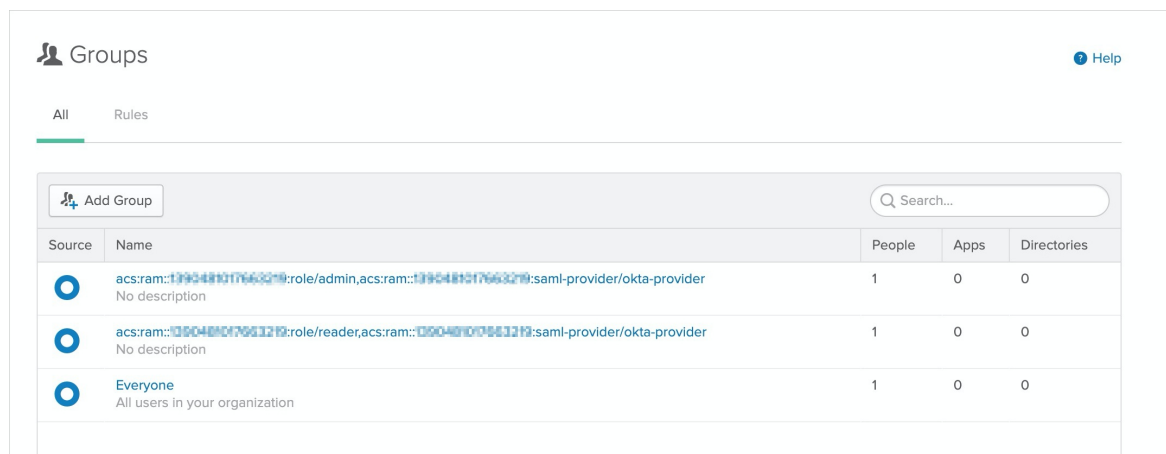
The logon is successful if the following page appears: the page to which the URL specified by the `Default RelayState` field points or the homepage of the Alibaba Cloud Management Console.



(Optional) Assign multiple roles to a user in Okta

If you want to assign multiple roles to a user in Okta, you must create multiple user groups in the required format and create a group attribute statement. To assign multiple roles to a user in Okta, perform the following steps:

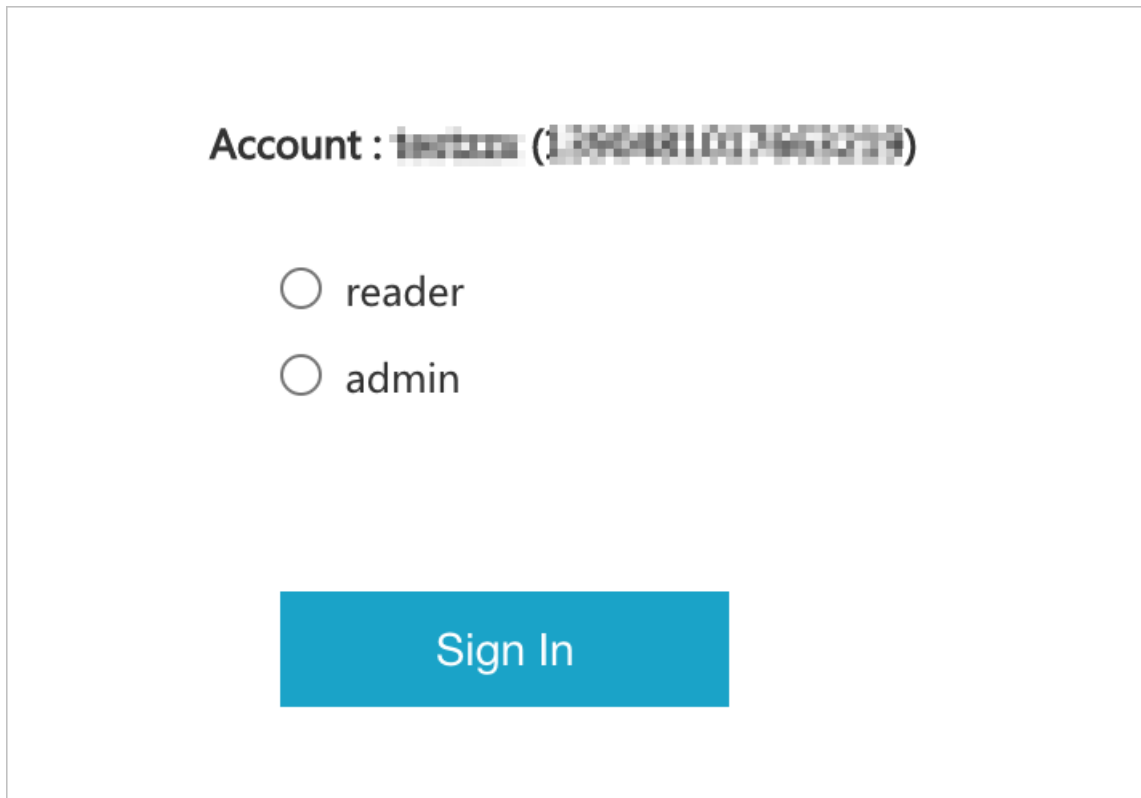
1. Create multiple groups. Each group name must follow the same format as a value of the role attribute in the SAML assertion. For example, you can set the name of a group to `acs:ram::177242285274****:role/admin,acs:ram::177242285274****:saml-provider/okta-provider`.



2. Add the test@example.com user to the groups.
3. Delete the attribute statements of RAM roles from the **SAML Settings** section of the application. Create a group attribute statement. Make sure that the filter condition can be used to filter all the group names. For example, you can set the filter to Start with acs:ram.

Name	Name format (optional)	Filter
https://www.aliyun.com/SAM	Unspecified	Starts with acs:ram
<input type="button" value="Add Another"/>		

4. After the configurations are complete, log on to the Alibaba Cloud Management Console as the test@example.com user. You are prompted to select a role to assume.



The screenshot shows a login form with the following elements:

- Account : **testuser (1390481017661274)**
- Two radio button options: **reader** and **admin**.
- A blue **Sign In** button.

For more information about how to use Okta, see [Okta Documentation](#).

4.1.8. Implement role-based SSO from Azure AD


This topic provides an example on how to implement role-based single sign-on (SSO) from Azure Active Directory (Azure AD) to Alibaba Cloud. The example includes the steps that are required to configure role-based SSO on both an identity provider (IdP) and Alibaba Cloud.

Context

Before you start, you must create an Alibaba Cloud account (Account 1) and an Azure AD tenant. An administrator and an organization user (u2) are added to the Azure AD tenant. The administrator is assigned the global administrative rights. You want to configure the required settings to enable the user u2 to access the resources of Account 1 by using role-based SSO.

To complete the configurations in Azure AD, you must log on to the Azure portal as an administrator that is assigned the global administrative rights. For more information about how to create and authorize users in Azure AD, see [Azure AD documentation](#).

Step 1: Create an application in Azure AD

1. Log on to the [Azure portal](#) as the administrator.
2. In the upper-left corner of the AAD homepage, click the  icon.
3. In the left-side navigation pane, choose **Azure Active Directory > Enterprise applications > All applications**.
4. On the page that appears, click **New application**.
5. Enter **Alibaba Cloud Service (Role-based SSO)** in the search box and click Alibaba Cloud Service

(Role-based SSO) in the search results.


6. In the panel that appears, enter a name for the application and click **Create**.

In this example, use the default application name `Alibaba Cloud Service (Role-based SSO)`. You can also enter a custom name for the application.


7. In the left-side navigation pane of the **Alibaba Cloud Service (Role-based SSO)** page, click **Properties**. Then, copy and save the value of **Object ID** for subsequent use.


Step 2: Configure SSO in Azure AD

1. In the left-side navigation pane of the **Alibaba Cloud Service (Role-based SSO)** page, click **Single sign-on**.
2. In the **Select a single sign-on method** section, click **SAML**.
3. In the **Set up Single Sign-On with SAML** section, configure SSO information.
 - i. In the upper-left corner, click **Upload metadata file**, select a file, and then click **Add**.

 **Note** You can obtain the metadata file from the following URL: `https://signin.alibabacloud.com/saml-role/sp-metadata.xml`.

- ii. In the **Basic SAML Configuration** panel, configure the following parameters and click **Save**.
 - **Identifier (Entity ID)**: Set this parameter to the value of `entityID` that is read from the preceding metadata file.
 - **Reply URL (Assertion Consumer Service URL)**: Set this parameter to the value of `Location` that is read from the preceding metadata file.
 - **Relay State**: Set this parameter to the URL of the page that is displayed after a user logs on to the Alibaba Cloud Management Console by using role-based SSO.


 **Note** For security purposes, you must enter a URL that points to an Alibaba website for **Relay State**. For example, the domain name in the URL can be `*.aliyun.com`, `*.hichina.com`, `*.yunos.com`, `*.taobao.com`, `*.tmall.com`, `*.alibabacloud.com`, or `*.alipay.com`. If you enter a URL that does not point to an Alibaba website, the configuration is invalid. If you leave this parameter empty, you are redirected to the homepage of the Alibaba Cloud Management Console.

- iii. In the **User Attributes & Claims** section, click the  icon.
- iv. Click **Add new claim**, configure the following parameters, and then click **Save**.
 - **Name**: Enter `Role`.
 - **Namespace**: Enter `https://www.aliyun.com/SAML-Role/Attributes`.
 - **Source**: Select **Attribute**.
 - **Source attribute**: Select `user.assignedroles` from the drop-down list.

- v. Repeat the previous step to add another claim.
 - **Name:** Enter `RoleSessionName` .
 - **Namespace:** Enter `https://www.aliyun.com/SAML-Role/Attributes` .
 - **Source:** Select **Attribute**.
 - **Source attribute:** Select `user.userprincipalname` from the drop-down list.
- vi. In the **SAML Signing Certificate** section, click **Download** on the right of **Federation Metadata XML** to download the IdP metadata file.

Step 3: Create an IdP in Alibaba Cloud


1. Log on to the [RAM console](#) by using Account 1.
2. In the left-side navigation pane, click **SSO**.
3. On the **Role-based SSO** tab, click the **SAML** tab and click **Create IdP**.
4. On the **Create IdP** page, set **IdP Name** to `AAD` and configure **Remarks**.
5. In the **Metadata File** section, click **Upload**.

 **Note** You must upload the federation metadata XML file that is downloaded in [Step 2: Configure SSO in Azure AD](#).

6. Click **OK**.
7. Click **Close**.

Step 4: Create a RAM role in Alibaba Cloud

1. In the left-side navigation pane of the RAM console, choose **Identities > Roles**.
2. On the **Roles** page, click **Create Role**.
3. In the **Create Role** panel, select **IdP** for Select Trusted Entity and click **Next**.
4. Set **RAM Role Name** to `AADrole` and set **Note**.
5. Select **SAML** for the IdP Type parameter.
6. Select `AAD` from the Select IdP drop-down list and click **OK**.

 **Note**


- You can grant permissions to the RAM role based on your business requirements. For more information, see [Grant permissions to a RAM role](#).
- After you create the IdP and the RAM role, save the Alibaba Cloud Resource Names (ARNs) of the IdP and the RAM role for subsequent use. For more information about how to obtain the ARN of a RAM role, see [View the basic information about a RAM role](#).

7. Click **Close**.


Step 5: Associate the RAM role with the Azure AD user


1. Create a role in Azure AD.
 - i. Log on to the [Azure portal](#) as the administrator.
 - ii. In the left-side navigation pane, choose **Azure Active Directory > App registrations**.

- iii. Click the **All applications** tab, and then click **Alibaba Cloud Service (Role-based SSO)**.
- iv. In the left-side navigation pane, click **App roles**.
- v. On the page that appears, click **Create app role**.
- vi. In the **Create app role** panel, configure the following parameters and click **Apply**.
 - **Display name**: In this example, enter `Admin`.
 - **Allowed member types**: In this example, select **Both (Users/Groups + Applications)**.
 - **Value**: Enter the ARN of the RAM role and the ARN of the IdP. Separate the ARNs with commas (,). In this example, enter `acs:ram::187125022722****:role/aadrole,acs:ram::187125022722****:saml-provider/AAD`.
 - **Description**: Enter a description.
 - Select **Do you want to enable this app role?**

 **Note** If you want to create multiple roles in Azure AD, repeat the preceding steps.

2. Assign roles to the user u2.
 - i. In the left-side navigation pane, choose **Azure Active Directory > Enterprise applications > All applications**.
 - ii. In the **Name** column, click **Alibaba Cloud Service (Role-based SSO)**.
 - iii. In the left-side navigation pane, click **Users and groups**.
 - iv. On the page that appears, click **Add user/group**.
 - v. On the page that appears, click **Users**. In the Users panel, select u2 and click **Select**.
 - vi. Click **Assign**.
 - vii. View the roles that are assigned to the user u2.

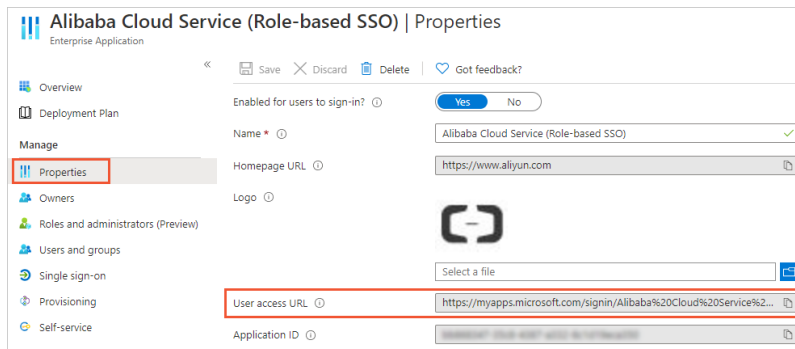
Display Name	Object Type	Role assigned
 u2	User	Admin

 **Note** After you select u2, the created role is assigned to the user u2. If multiple roles are created, you must assign the roles to the Azure AD user based on your business requirements.

Verify the configuration results

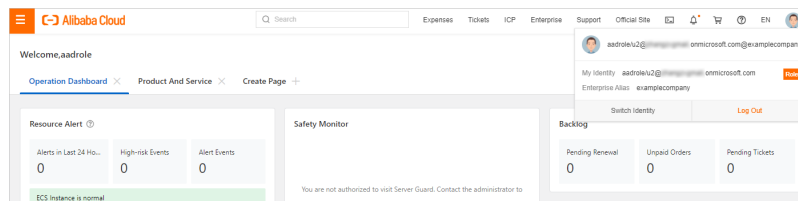
1. Obtain the user access URL.
 - i. Log on to the **Azure portal** as the administrator.
 - ii. In the left-side navigation pane, choose **Azure Active Directory > Enterprise applications > All applications**.
 - iii. In the **Name** column, click **Alibaba Cloud Service (Role-based SSO)**.

- iv. In the left-side navigation pane of the page that appears, click **Properties** and obtain the value of **User access URL**.



2. After you obtain the **user access URL** from the administrator, enter the URL in a browser and use the required username and password for login.

After the logon succeeds, you are redirected to the page that is specified by the **Relay State** parameter. If **Relay State** is invalid or not specified, you are redirected to the homepage of the Alibaba Cloud Management Console.



(Optional) Configure the role-based SSO between Azure AD and multiple Alibaba Cloud accounts

Assume that you have two Alibaba Cloud accounts, Account 1 and Account 2. If you want the user u2 to access the resources of both Account 1 and Account 2 by using role-based SSO after the user u2 logs on to Azure AD, perform the following operations:

- Create an application named `Alibaba Cloud Service (Role-based SSO)` in Azure AD.
For more information, see [Step 1: Create an application in Azure AD](#).
- Configure SSO in Azure AD.
For more information, see [Step 2: Configure SSO in Azure AD](#).
- Create IdPs in Alibaba Cloud.
You must create the `AAD` IdP for both Account 1 and Account 2.
For more information, see [Step 3: Create an IdP in Alibaba Cloud](#).
- Create RAM roles in Alibaba Cloud.
You must create RAM roles for both Account 1 and Account 2. In this example, create two RAM roles for Account 1 and one RAM role for Account 2.
 - Create the `adminaad` and `readaad` RAM roles for Account 1.
 - Create the `financeaad` RAM role for Account 2.
 For more information, see [Step 4: Create a RAM role in Alibaba Cloud](#).
- Associate the RAM roles with the user u2.

Create three roles in Azure AD and assign the roles to the user u2. The values of the roles are:

- o `acs:ram::<Account1_ID>:role/adminaad,acs:ram::<Account1_ID>:saml-provider/AAD`
- o `acs:ram::<Account1_ID>:role/readaad,acs:ram::<Account1_ID>:saml-provider/AAD`
- o `acs:ram::<Account2_ID>:role/financeaad,acs:ram::<Account2_ID>:saml-provider/AAD`

For more information, see [Step 5: Associate the RAM role with the Azure AD user](#).

6. Use the user u2 to access Alibaba Cloud by using role-based SSO.

You can log on to the Azure portal as the user u2 and click **Alibaba Cloud Service (Role-based SSO)** on the **My apps** page. Then, you must select the Alibaba Cloud account whose resources you want to access and its role as prompted in the Alibaba Cloud Management Console.

4.1.9. Implement role-based SSO from OneLogin to Alibaba Cloud

This topic provides an example on how to implement role-based single sign-on (SSO) from OneLogin to Alibaba Cloud. The example describes the end-to-end role-based SSO process from a cloud identity provider (IdP) to Alibaba Cloud.

Context

In this example, an enterprise has an Alibaba Cloud account, a OneLogin administrator account, and multiple OneLogin users. The enterprise wants the OneLogin users to use their OneLogin accounts to access Alibaba Cloud by using role-based SSO without the need to create RAM users in Alibaba Cloud.

For more information about OneLogin, see [OneLogin documentation](#).

Step 1: Create an application in OneLogin

1. Log on to [OneLogin](#) as an administrator.
2. In the left side of the profile picture, click **Administration** to go to the Administration page.
3. In the top navigation bar, choose **Applications > Applications**.
4. In the upper-right corner of the **Applications** page, click **Add App**.
5. On the **Find Applications** page, search for **SAML Test Connector (Advanced)**.
6. On the page that appears, click **SAML Test Connector (Advanced)**. On the **Add SAML Test Connector (Advanced)** page, configure the parameters and click **Save**.

In this example, set the **Display Name** parameter to `LoginToAliyun`. Use the default values for other parameters.

7. On the page that appears, move the pointer over **More Actions** in the upper-right corner and select **SAML Metadata** from the drop-down list. The IdP metadata file is downloaded. Save the file to your computer.

Step 2: Create an IdP in the Alibaba Cloud Management Console

1. Log on to the [RAM console](#) by using the Alibaba Cloud account.
2. In the left-side navigation pane, click **SSO**.
3. On the **Role-based SSO** tab, click the **SAML** tab and click **Create IdP**.
4. On the **Create IdP** page, set **IdP Name** to OneLogin and configure **Remarks**.

5. In the **Metadata File** section, click **Upload** to upload the IdP metadata file that is obtained from [Step 1: Create an application in OneLogin](#).
6. Click **OK**.
7. Click **Close**.

View the details of the created IdP and record the Alibaba Cloud Resource Name (ARN) of the IdP for subsequent use.

Step 3: Create a RAM role in the Alibaba Cloud Management Console

1. In the left-side navigation pane of the RAM console, choose **Identities > Roles**.
2. On the **Roles** page, click **Create Role**.
3. In the **Create Role** panel, select **IdP** for Select Trusted Entity and click **Next**.
4. In the Configure Role step, configure the **RAM Role Name** and **Note** parameters. For example, you can set the RAM Role Name parameter to Reader-OneLogin.
5. Select **SAML** for the IdP Type parameter.
6. Select OneLogin that you created in [Step 2: Create an IdP in the Alibaba Cloud Management Console](#) for the Select IdP parameter, read the conditions, and then click **OK**.
7. Click **Close**.

View the details of the created RAM role and record the ARN of the RAM role for subsequent use.


Step 4: Configure the application in OneLogin

1. Log on to [OneLogin](#) as an administrator.
2. Create a custom user attribute.
 - i. In the top navigation bar, choose **Users > Users**.
 - ii. On the **Users** page, move the pointer over **More Actions** in the upper-right corner and select **Custom user fields** from the drop-down list.
 - iii. In the upper-right corner of the **Custom User Fields** page, click **New User Field**.
 - iv. In the **New User Field** dialog box, configure the **Name** and **Short name** parameters and click **Save**.

In this example, set the **Name** parameter to `AliyunRoles for SSO` and the **Short name** parameter to `AliyunRoles`.
3. Configure the application.
 - i. In the top navigation bar, choose **Applications > Applications**.
 - ii. On the **Applications** page, click **LoginToAliyun** that you created in [Step 1: Create an application in OneLogin](#).
 - iii. In the left-side navigation pane of the page that appears, click **Configuration**.


iv. In the **Application details** section, configure the following parameters and click **Save**.

- **RelayState**: Enter a URL. You are redirected to the URL after login.


 **Note** For security purposes, you must enter a URL that points to an Alibaba website for the **RelayState** parameter. For example, the domain name in the URL can be *.aliyun.com, *.hichina.com, *.yunos.com, *.taobao.com, *.tmall.com, *.alibabacloud.com, or *.alipay.com. If you leave this parameter empty, you are redirected to the homepage of the Alibaba Cloud Management Console after login.

- **Audience (EntityID)**: Enter `urn:alibaba:cloudcomputing:international`.
- **Recipient**: Enter `https://signin.alibabacloud.com/saml-role/sso`.
- **ACS (Consumer) URL**: Enter `https://signin.alibabacloud.com/saml-role/sso`.


v. In the left-side navigation pane, click **Parameters**.

vi. Click the  icon to create the first custom application attribute.

- In the **New Field** dialog box, set the **Field name** parameter to `https://www.aliyun.com/SAML-Role/Attributes/Role`, select **Include in SAML assertion** and **Multi-value parameter**, and then click **Save**.
- In the **Edit Field https://www.aliyun.com/SAML-Role/Attributes/Role** dialog box, select **Aliyun Roles for SSO (Custom)** from the first drop-down list and **Semicolon Delimited input (Multi-value output)** from the second drop-down list in the **Default if no value selected** section. Then, click **Save**.

vii. Click the  icon again to create the second custom application attribute.


- In the **New Field** dialog box, set the **Field name** parameter to `https://www.aliyun.com/SAML-Role/Attributes/RoleSessionName`, select **Include in SAML assertion**, and then click **Save**.
- In the **Edit Field https://www.aliyun.com/SAML-Role/Attributes/RoleSessionName** dialog box, select **Email** from the drop-down list in the **Value** section and click **Save**.

 **Note** You can also select another value such as **Username** or **userPrincipalName** from the drop-down list in the **Value** section based on your business requirements.

viii. In the upper-right corner of the page, click **Save**.

Step 5: Create a user in OneLogin and assign the application to the user

1. Log on to **OneLogin** as an administrator.
2. In the top navigation bar, choose **Users > Users**.
3. Create a user.


 **Note** If you have a OneLogin user, skip this step.


- i. In the upper-right corner of the **Users** page, click **New User**.
- ii. On the **New User** page, configure the parameters. For example, set the **First name** parameter to Jack, the **Last name** parameter to Lee, the **Username** parameter to jacklee, the **Email** parameter to jacklee@example.com, and then click **Save User**.
- iii. On the page that appears, move the pointer over **More Actions** in the upper-right corner and select **Change Password** from the drop-down list. Configure a password for the user and click **Update**.

The user can log on to OneLogin by using the password.

4. In the **Custom Fields** section of the page that appears, configure the **Aliyun Roles for SSO** parameter.

The value of the **Aliyun Roles for SSO** parameter consists of the ARN of the RAM role and the ARN of the IdP. The ARNs are separated by commas (,). The value must be in the `acs:ram::<account_id>:role/RoleName,acs:ram::<account_id>:saml-provider/ProviderName` format. The ARN of the RAM role is obtained from [Step 3: Create a RAM role in the Alibaba Cloud Management Console](#), the ARN of the IdP is obtained from [Step 2: Create an IdP in the Alibaba Cloud Management Console](#), and `<account_id>` is the ID of the Alibaba Cloud account.


 **Note** If a user corresponds to multiple RAM roles, you can configure more than one value. The values are separated by semicolons (;). For example, you can set `acs:ram::125022144354****:role/reader-onelogin,acs:ram::125022144354****:saml-provider/OneLogin;acs:ram::125022144354****:role/administrator-onelogin,acs:ram::125022144354****:saml-provider/OneLogin;acs:ram::158622887609****:role/finance,acs:ram::158622887609****:saml-provider/OneLogin2` for the **Aliyun Roles for SSO** parameter.

5. Assign the application to the user.
 - i. On the **Applications** page, click the  icon.
 - ii. Select **LoginToAliyun** created in [Step 1: Create an application in OneLogin](#) and click **Continue**.
 - iii. In the dialog box that appears, click **Save**.
6. In the upper-right corner of the **Users** page, click **Save User**.
7. Repeat to to configure the **Aliyun Roles for SSO** parameter for other users of the enterprise and assign **LoginToAliyun** to the users.

Step 6: Test role-based SSO

1. Log on to [OneLogin](#) by using the user jacklee that is created in [Step 5: Create a user in OneLogin and assign the application to the user](#).
2. Click **LoginToAliyun**.

The logon succeeds if one of the following pages appear: the page to which the URL entered for the **RelayState** parameter points and the homepage of the Alibaba Cloud Management Console.

 **Note** If you configure more than one value for the **Aliyun Roles for SSO** parameter in [Step 5: Create a user in OneLogin and assign the application to the user](#), you must select a specific RAM role before you can access Alibaba Cloud.

4.2. Role-based SSO by using OIDC

4.2.1. Overview of OIDC-based SSO

OpenID Connect (OIDC) is an authentication protocol that is developed based on OAuth 2.0. Alibaba Cloud Resource Access Management (RAM) supports OIDC-based single sign-on (SSO).

Terms

Term	Description
OIDC	An authentication protocol that is developed based on Open Authorization (OAuth) 2.0. For more information, see OIDC and OAuth 2.0 . OAuth is an authorization protocol. OIDC adds an identity layer to extend OAuth. This way, OIDC can use OAuth for authorization. OIDC also allows clients to verify the identities of users and use an HTTP RESTful API to obtain basic information about the users.
OIDC token	An identity token that is issued by OIDC to an application. An OIDC token is an identity token that indicates a logon user. An OIDC token can be used to obtain the basic information about a logon user.
STS token	A temporary identity credential that is provided by Alibaba Cloud Security Token Service (STS). STS allows you to manage temporary credentials for your Alibaba Cloud resources. You can configure a validity period and specify access permissions for an STS token. For more information about STS, see What is STS?
URL of an issuer	The URL of an issuer that is provided by an external IdP. The URL is indicated by the <code>iss</code> field in an OIDC token. The URL of the issuer must start with https and be in the valid URL format. The URL cannot contain query parameters that follow a question mark (<code>?</code>) or logon information that is identified by at signs (<code>@</code>). The URL cannot be a fragment URL that contains number signs (<code>#</code>).
fingerprint	The fingerprint that is generated based on the HTTPS certificate of an external IdP. You can use a fingerprint to prevent the URL of the issuer from being hijacked or tampered with. Alibaba Cloud calculates the fingerprint. We recommend that you calculate the fingerprint on your computer. For example, you can use OpenSSL to calculate the fingerprint. Then, you can compare the calculation result with the calculation result provided by Alibaba Cloud. For more information about OpenSSL, visit the official website of OpenSSL . If the calculation results are different, the URL of the issuer may have been attacked. Make sure that you enter a valid fingerprint.
client ID	An ID that is generated for an application when you register the application in an external IdP. When you apply for an OIDC token from an external IdP, you must use a client ID. The client ID is specified in the <code>aud</code> field of the OIDC token that is issued. When you create an OIDC IdP, you must configure the client ID. If you want to use the OIDC token to obtain an STS token, Alibaba Cloud checks whether the client ID that is included in the <code>aud</code> field is the same as the client ID that you configured in the OIDC IdP. You can assume a RAM role only when the client IDs are the same.

Scenarios

If applications of enterprises use fixed AccessKey pairs to frequently access Alibaba Cloud resources and the enterprises lacks security protection measures, potential risks may arise due to AccessKey pair leaks. To resolve this issue, the enterprises register applications in self-managed OIDC IdPs or third-party OIDC IdPs, such as Google G Suite and Okta. This way, the OIDC IdPs can generate OIDC tokens for the applications. Then, the applications can use the OIDC tokens to obtain STS tokens to access Alibaba Cloud resources in a secure manner.

In addition, individual developers or employees of small and medium-sized enterprises are allowed to log on to the Alibaba Cloud Management Console by using the identities that are registered in websites, such as social networking websites. If the websites support OIDC tokens, the individual developers or employees can use RAM to implement OIDC-based SSO.

Process

OIDC-based SSO flowchart

1. Register an application in an external IdP and obtain the client ID of the application.
2. In the RAM console, create an OIDC IdP and configure a trust relationship between Alibaba Cloud and the external IdP.
For more information, see [Create an OIDC IdP](#).
3. In the RAM console, create a RAM role whose trusted entity is an OIDC IdP and grant permissions to the RAM role.
For more information, see [Create a RAM role for an OIDC IdP](#) and [Grant permissions to a RAM role](#).
4. Apply for an OIDC token from the external IdP.
For more information, see the documentation of the external IdP.
5. Use the OIDC token to obtain an STS token.
For more information, see [AssumeRoleWithOIDC](#).
6. Use the STS token to access Alibaba Cloud resources.

Configuration example

Implement OIDC-based SSO from Okta

Limits

Item	Upper limit
The number of OIDC IdPs that can be created within an Alibaba Cloud account	100
The number of client IDs that can be added to an OIDC IdP	20
The number of fingerprints that can be added to an OIDC IdP	5

4.2.2. Manage an OIDC IdP

This topic describes how to manage an OpenID Connect (OIDC) identity provider (IdP). Before you implement OIDC-based single sign-on (SSO), you must create an OIDC IdP.

Create an OIDC IdP

1. Log on to the [RAM console](#) by using your Alibaba Cloud account.
2. In the left-side navigation pane, click **SSO**.
3. On the **Role-based SSO** tab, click the **OIDC** tab. Then, click **Create IdP**.
4. On the **Create IdP** page, configure the following parameters.

Parameter	Description
IdP Name	The name must be unique within an Alibaba Cloud account.
IdP URL	The URL of the issuer that is provided by an external IdP. The URL of the issuer must start with <code>https</code> and be in the valid URL format. The URL cannot contain query parameters that follow a question mark (<code>?</code>) or logon information that is identified by at signs (<code>@</code>). The URL cannot be a fragment URL that contains number signs (<code>#</code>).
Fingerprint	The fingerprint that is generated based on the HTTPS certificate of an external IdP. You can use a fingerprint to prevent the URL of the issuer from being hijacked or tampered with. Alibaba Cloud calculates the fingerprint. We recommend that you calculate the fingerprint on your computer. For example, you can use OpenSSL to calculate the fingerprint. Then, you can compare the calculation result with the calculation result provided by Alibaba Cloud. For more information about OpenSSL, visit the official website of OpenSSL . If the calculation results are different, the URL of the issuer may have been attacked. Make sure that you enter a valid fingerprint.
Client ID	<p>The ID that is generated for an application when you register the application in the external IdP. When you apply for an OIDC token from an external IdP, you must use the client ID. The client ID is specified in the <code>aud</code> field of the OIDC token that is issued. When you create an OIDC IdP, you must configure the client ID. If you want to use the OIDC token to obtain an STS token, Alibaba Cloud checks whether the client ID that is included in the <code>aud</code> field is the same as the client ID that you configured in the OIDC IdP. You can assume a RAM role only when the client IDs are the same.</p> <p>If multiple clients need to access Alibaba Cloud resources, you can configure multiple client IDs. You can configure a maximum of 20 client IDs.</p>
Remarks	The description of the OIDC IdP.

5. Click **OK**.

View the information about an OIDC IdP

1. Log on to the [RAM console](#) by using your Alibaba Cloud account.

2. In the left-side navigation pane, click **SSO**.
3. On the **Role-based SSO** tab, click the **OIDC** tab. Then, click the name of the OIDC IdP whose information that you want to view.
4. In the **Details** section of the page that appears, view **IdP Name**, **IdP Type**, **Created At**, **Updated At**, **Remarks**, **ARN**, and **URL**.

Modify the information about an OIDC IdP

1. Log on to the **RAM console** by using your Alibaba Cloud account.
2. In the left-side navigation pane, click **SSO**.
3. On the **Role-based SSO** tab, click the **OIDC** tab. Then, click the name of the OIDC IdP whose information that you want to view.
4. In the **Details** section of the page that appears, click **Edit** to the right of **Remarks** to modify the description of the OIDC IdP.
5. In the **Client ID** section, click **Add** or **Delete** to add or remove a client ID.

 **Note** You can add a maximum of 20 client IDs. You must retain at least one client ID.

6. In the **Fingerprint** section, click **Add** or **Delete** to add or delete a fingerprint.

 **Note** You can add a maximum of five client IDs. You must retain at least one fingerprint.

Delete an OIDC IdP

1. Log on to the **RAM console** by using your Alibaba Cloud account.
2. In the left-side navigation pane, click **SSO**.
3. On the **Role-based SSO** tab, click the **OIDC** tab. Then, find the OIDC IdP that you want to delete and click **Delete** in the **Actions** column.
4. In the **Delete** message, click **OK**.

4.2.3. Implement OIDC-based SSO from Okta

This topic provides an example on how to implement OpenID Connect (OIDC)-based single sign-on (SSO) from Okta to Alibaba Cloud. Then, applications that are registered in Okta can access Alibaba Cloud resources by using Security Token Service (STS) tokens in a secure manner.

Prerequisites

An OIDC application is registered in Okta. The URL of the issuer and the client ID of the application are obtained. The following data is used in this example:

- The URL of the issuer is `https://dev-xxxxxx.okta.com`.
- The client ID is `00a294vi1vJoClev****`.

Step 1: Create an OIDC identity provider (IdP) in Alibaba Cloud

In this step, an OIDC IdP named `TestOidcProvider` is created. The URL of the issuer is `https://dev-xxxxxx.okta.com` and the client ID is `00a294vi1vJoClev****`.

1. Log on to the **RAM console** by using your Alibaba Cloud account.

2. In the left-side navigation pane, click **SSO**.
3. On the **Role-based SSO** tab, click the **OIDC** tab. Then, click **Create IdP**.
4. On the **Create IdP** page, configure the following parameters.

Parameter	Description
IdP Name	The name must be unique within an Alibaba Cloud account.
IdP URL	The URL of the issuer that is provided by an external IdP. The URL of the issuer must start with <code>https</code> and be in the valid URL format. The URL cannot contain query parameters that follow a question mark (<code>?</code>) or logon information that is identified by at signs (<code>@</code>). The URL cannot be a fragment URL that contains number signs (<code>#</code>).
Fingerprint	The fingerprint that is generated based on the HTTPS certificate of an external IdP. You can use a fingerprint to prevent the URL of the issuer from being hijacked or tampered with. Alibaba Cloud calculates the fingerprint. We recommend that you calculate the fingerprint on your computer. For example, you can use OpenSSL to calculate the fingerprint. Then, you can compare the calculation result with the calculation result provided by Alibaba Cloud. For more information about OpenSSL, visit the official website of OpenSSL . If the calculation results are different, the URL of the issuer may have been attacked. Make sure that you enter a valid fingerprint.
Client ID	<p>The ID that is generated for an application when you register the application in the external IdP. When you apply for an OIDC token from an external IdP, you must use the client ID. The client ID is specified in the <code>aud</code> field of the OIDC token that is issued. When you create an OIDC IdP, you must configure the client ID. If you want to use the OIDC token to obtain an STS token, Alibaba Cloud checks whether the client ID that is included in the <code>aud</code> field is the same as the client ID that you configured in the OIDC IdP. You can assume a RAM role only when the client IDs are the same.</p> <p>If multiple clients need to access Alibaba Cloud resources, you can configure multiple client IDs. You can configure a maximum of 20 client IDs.</p>
Remarks	The description of the OIDC IdP.

5. Click **OK**.

Step 2: Create a RAM role for the OIDC IdP in Alibaba Cloud

In this step, a RAM role named `testoidc` is created and the `TestOidcProvider` OIDC IdP that you created in [Step 1](#) is selected.

1. Log on to the [RAM console](#) by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Roles**.

3. On the **Roles** page, click **Create Role**.
4. In the **Create Role** panel, select **IdP** for Select Trusted Entity and click **Next**.
5. Specify the **RAM Role Name** and **Note** parameters.
6. Select **OIDC** for IdP Type.
7. Select a trusted IdP, specify the conditions in the Conditions section, and then click **OK**.

The following table describes the supported conditions.

Condition key	Description	Required	Example
oidc:iss	<p>The issuer. You can assume the RAM role only if the iss field of the OIDC token that you want to use to assume the RAM role meets this condition.</p> <p>The conditional operator must be StringEquals. The value must be the URL of the issuer that you specify for the selected OIDC IdP. You can specify this condition to ensure that you can use the OIDC token to assume the RAM role only if the OIDC token is issued by a trusted IdP.</p>	Yes	https://dev-xxxxxx.okta.com
oidc:aud	<p>The audience. You can assume the RAM role only if the aud field of the OIDC token that you want to use to assume the RAM role meets this condition.</p> <p>The conditional operator must be StringEquals. The value can be one or more client IDs that you specify for the selected OIDC IdP. You can specify this condition to ensure that you can use the OIDC token to assume the RAM role only if the OIDC token is generated by using the client ID that you specify.</p>	Yes	00a294vi1vJoClev****
oidc:sub	<p>The subject. You can assume the RAM role only if the sub field of the OIDC token that you want to use to assume the RAM role meets this condition.</p> <p>The conditional operator can be a string of all types. The value can be up to 10 subjects. You can specify this condition to further limit the identity that you can use to assume the RAM role. You can also leave this condition unspecified.</p>	No	00u294e3mzNXt4Hi****

8. Click **Close**.

Step 3: Grant permissions to the RAM role

You can grant permissions to the RAM role named `testoidc` that you created in [Step 2](#) to access Alibaba Cloud resources based on your business requirements.

Step 4: Issue an OIDC token in Okta

You cannot log on to the Alibaba Cloud Management Console by using OIDC. Therefore, you must implement OIDC-based SSO by using programmatic access. To obtain an OIDC token, you must complete authorization by using Open Authorization (OAuth). Therefore, you must use OAuth 2.0 to obtain an OIDC token from an OIDC IdP such as Okta. OAuth supports a variety of flows, such as the authorization code flow. For more information, see [Authorization Code Flow](#). However, the authorization code flow is complex. In the following sections, the implicit flow is used to describe how to obtain an OIDC token and implement SSO. Some operations in the implicit flow are not described in this topic. For more information about the implicit flow, see [Implicit Flow](#).

1. Build a web application to receive an OIDC token that is issued by Okta.

In this example, a simple web application that is built by using Java Spring Boot and Thymeleaf is used. The web application is deployed on your computer and is accessible over port 8080, and the localhost is resolved to 127.0.0.1. Therefore, you can enter localhost:8080 in a browser on your computer to access the web application. The following sample code is provided:

- Sample code for a static page

OAuth 2.0 requires that the callback information that Okta sends to the web application is passed in the fragment component of the callback URL. You can create a web page and obtain the OIDC token from the fragment component. In this example, a simple static page is created. Then, you can transparently pass the fragment component. The complete URL of this page is `http://localhost:8080/accessTokenCallback`, which is also the callback URL `redirect_uri` configured for the application in Okta.

```
<!DOCTYPE HTML>
<html xmlns:th="http://www.thymeleaf.org">
  <head>
    <script>
      window.onload = function () {
        let fragment = window.location.hash.substring(1);
        window.location.href = "/receiveAccessToken?" + fragment;
      };
    </script>
  </head>
</html>
```

- Sample code for a class

A class is created as the controller of the static page.

```
package com.aliyun.oauthtest;
import org.springframework.stereotype.Controller;
import org.springframework.web.bind.annotation.RequestMapping;
@Controller
public class CallbackController {
    @RequestMapping("accessTokenCallback")
    public String callback() {
        return "accessTokenCallback";
    }
}
```

2. Log on to Okta and apply for an OIDC token from Okta.

You must log on to Okta. Then, you can construct and access the URL `https://dev-xxxxxx.okta.com/oauth2/v1/authorize?client_id=0oa294vi1vJoClev****&scope=openid&response_type=token%20id_token&state=testState&nonce=a_unique_nonce_1&redirect_uri=http%3A%2F%2Flocalhost%3A8080%2FaccessTokenCallback` by using the web application that is built in [Step 1](#).

The following list describes the parameters in the URL:

- `client_id` : Set this parameter to the client ID of the OIDC application that is registered in Okta.
- `scope` : Set this parameter to `openid`.
- `response_type` : Set this parameter to `token id_token` in the implicit flow.
- `state` : specifies the current status of the OIDC application. You can configure this parameter based on your business requirements.
- `nonce` : This parameter is used to prevent replay attacks. You can configure this parameter based on your business requirements.
- `redirect_uri` : Set this parameter to the callback URL that is used to receive `access_token` or `id_token`. In this example, set this parameter to the URL of the web application that you created in Substep 1.

In this example, you have logged on to Okta. Therefore, the system redirects you to the callback URL based on the specified `redirect_uri`. The value of `id_token` in the following URL is the OIDC token.

```
HTTP/1.1 302 Found
Location: http://localhost:8080/accessTokenCallback#id_token=eyJraWQiOiJ6OUV0e****&access_token=eyJraWQiOiJseEQ3R****&token_type=Bearer&expires_in=3600&scope=openid&state=testState
```

3. Parse the OIDC token.

You can parse the results that you obtained in Substep 2 and query the details about `header` and `payload`.

Sample request:


```

package com.aliyun.oauth2test;
import java.util.Base64;
import java.util.Base64.Decoder;
import java.util.HashMap;
import java.util.Map;
import java.util.TreeMap;
import com.alibaba.fastjson.JSON;
import com.alibaba.fastjson.JSONObject;
import org.springframework.web.bind.annotation.RequestMapping;
import org.springframework.web.bind.annotation.RequestMethod;
import org.springframework.web.bind.annotation.RequestParam;
import org.springframework.web.bind.annotation.RestController;
@RestController
public class ClientAppController {
    @RequestMapping(value = "/receiveAccessToken", method = {RequestMethod.POST, RequestMethod.GET}),
        produces = "application/json")
    public Map<String, Object> receiveAccessToken(@RequestParam("access_token") String
accessToken,
                                                @RequestParam("id_token") String idTo
ken,
                                                @RequestParam("token_type") String to
kenType,
                                                @RequestParam("expires_in") Long expi
reTime,
                                                @RequestParam("scope") String scope,
                                                @RequestParam("state") String state)
    {
        Map<String, Object> result = new TreeMap<>();
        result.put("access_token", accessToken);
        result.put("id_token", idToken);
        result.put("token_type", tokenType);
        result.put("expires_in", "" + expireTime);
        result.put("scope", scope);
        result.put("state", state);
        String[] jwt = idToken.split("\\.");
        Decoder decoder = Base64.getDecoder();
        result.put(" id token jwt header", JSON.parse(new String(decoder.decode(jwt[0])
)));
        result.put(" id token jwt payload", JSON.parse(new String(decoder.decode(jwt[1]
))));
        result.put(" id token jwt signature", jwt[2]);
        return result;
    }
}

```

Sample response:

```
{
  " id token jwt header": {
    "kid": "z9EtyT345d-JLIJo2-5ySD027LG4FPeOotbwJPT****",
    "alg": "RS256"
  },
  " id token jwt payload": {
    "at_hash": "KKsdN3prZWtvBEMn-g****",
    "sub": "00u294e3mzNXt4Hi****",
    "aud": "0oa294vilvJoClev****",
    "ver": 1,
    "idp": "0oa294iehxjUCZIO****",
    "amr": [
      "pwd"
    ],
    "auth_time": 1636373097,
    "iss": "https://dev-xxxxxx.okta.com",
    "exp": 1636377759,
    "iat": 1636374159,
    "nonce": "a_unique_nonce_1",
    "jti": "ID.lmSU5AD2iKLCVu6_KLMIr52dpCprncxW38v-NCA****"
  },
  "id token jwt signature": "ZEJEGIV4Zoau63****",
  "access_token": "eyJraWQiOiJseEQ3R****",
  "expires_in": "3600",
  "id_token": "eyJraWQiOiJ6OUV0e****",
  "scope": "openid",
  "state": "testState",
  "token_type": "Bearer"
}
```

Step 5: Use the OIDC token to obtain an STS token

To obtain an STS token, call the [AssumeRoleWithOIDC](#) operation. In the request, specify the unparsed OIDC token that you obtained in [Step 4](#).

Sample request:

```
public static void main(String[] args)
{
    IAcsClient client = initialization();
    String jwtToken = "eyJraWQiOiJ6OUV0e****"; //The unparsed OIDC token that you obtained
    from Okta. The token is the value of id_token.
    AssumeRoleWithOIDCRequest request = new AssumeRoleWithOIDCRequest();
    request.setDurationSeconds(3600L);
    request.setOIDCProviderArn("acs:ram::113511544585****:oidc-provider/TestOidcProvider");
    request.setOIDCToken(jwtToken);
    request.setRoleArn("acs:ram::113511544585****:role/testoidc");
    request.setRoleSessionName("TestOidcAssumedRoleSession");
    try
    {
        AssumeRoleWithOIDCResponse resp = client.getAcsResponse(request);
        System.out.println("success requestId: " + resp.getRequestId());
        System.out.println("success assume role arn: " + resp.getAssumedRoleUser().getArn()
    );
        System.out.println("success sts credential accessKey id: " + resp.getCredentials().
    getAccessKeyId());
        System.out.println("success sts credential accessKey secret: " + resp.getCredential
    s().getAccessKeySecret());
        System.out.println("success resp: " + JSON.toJSONString(resp));
    }
    catch(ClientException | SystemException e)
    {
        e.printStackTrace();
    }
}
```

Sample response:

```

success requestId: 3D57EAD2-8723-1F26-B69C-F8707D8B565D
success assume role arn: acs:ram::113511544585****:role/testoidc/TestOidcAssumedRoleSession
success sts credential accessKey id: STS.NUGYrLnoC37mZCnNAbez****
success sts credential accessKey secret: CVwjCkNzTMupZ8NbTCxCBRq3K16jtcWFTJAYBEv2****
success resp:
{
  "AssumedRoleUser":
  {
    "Arn": "acs:ram::113511544585****:role/testoidc/TestOidcAssumedRoleSession",
    "AssumedRoleId": "33157794895460****:TestOidcAssumedRoleSession"
  },
  "Credentials":
  {
    "AccessKeyId": "STS.NUGYrLnoC37mZCnNAbez****",
    "AccessKeySecret": "CVwjCkNzTMupZ8NbTCxCBRq3K16jtcWFTJAYBEv2****",
    "Expiration": "2021-10-20T04:27:09Z",
    "SecurityToken": "CAIShwJlq6Ft5B2yfSjIr****"
  },
  "OIDCTokenInfo":
  {
    "ClientIds": "00a294vilvJoClev****",
    "Issuer": "https://dev-xxxxxx.okta.com",
    "Subject": "00u294e3mzNXt4Hi****"
  },
  "RequestId": "3D57EAD2-8723-1F26-B69C-F8707D8B565D"
}

```

The information in `Credentials` is the information about the STS token.

Step 6: Use the STS token to access Alibaba Cloud resources

Use the STS token that you obtained from [Step 5](#) to access the Alibaba Cloud resources on which you have permissions.