

Alibaba Cloud Resource Access Management

API Reference (STS)

Issue: 20190715

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 due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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 contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information 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.
	This warning information 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 restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus, page names, and other UI elements.	Click OK.
<code>Courier</code> font	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>switch {stand slave}</code>

Contents

Legal disclaimer.....	I
Generic conventions.....	I
1 What is STS?.....	1
2 Calling method.....	2
2.1 Request Structure.....	2
3 Operation interfaces.....	3
3.1 AssumeRole.....	3
3.2 GetCallerIdentity.....	7
3.3 AssumeRoleWithSAML.....	9

1 What is STS?

Alibaba Cloud Security Token Service (STS) provides short-term access management for Alibaba Cloud accounts or RAM users.

Features

STS grants temporary access tokens to authorized RAM entities (RAM users, RAM user groups, or RAM roles). The validity period and access permissions of these temporary access tokens can be customized as needed. Authorized RAM entities with temporary STS tokens can access Alibaba Cloud resources by using either of the following methods:

- Call Alibaba Cloud API actions.
- Log on to the Alibaba Cloud console.

Endpoint

The endpoint of STS that is used to call API actions is `https://sts.aliyuncs.com`.

Commonly used terms

RAM role	A virtual RAM user.
ARN	The Alibaba Cloud Resource Name (ARN) of a RAM role. Each role has a unique ARN. Format: <code>acs:ram::\$accountID:role/\$roleName</code>
Trusted entity	The trusted entity that can assume a RAM role. You must specify a trusted entity when you create a RAM role. Only trusted entities can assume roles. The trusted entity can be an Alibaba Cloud account, Alibaba Cloud service, or identity provider (IdP).
Role assuming	The method for entity users to obtain security tokens of RAM roles. By calling the AssumeRole action, an entity user can obtain the security token of a role and use the token to access Alibaba Cloud service APIs.

2 Calling method

2.1 Request Structure

Endpoint

For the STS service address, see [Service address](#).

Communication protocol

To ensure communication security, the STS service uses only the HTTPS secure channel to send requests.

HTTP request methods

The system allows you to send HTTP GET/POST requests. In this method, the request parameters must be included in the request URL. (The size of a GET request cannot exceed 4 KB, and the size of a POST requests cannot exceed 10 MB.)

Request parameters

You must use an “Action” parameter (such as “AddUser”) in each request to specify the operation to perform, and meanwhile you must add public request parameters and interface-specified request parameters that each operation interface requires.

Character encoding

Requests and responses are encoded using UTF-8.

3 Operation interfaces

3.1 AssumeRole

Obtains a temporary identity for assuming a role.

Request parameters

Parameter	Type	Required?	Example value	Description
Action	String	Yes	AssumeRole	The name of this action. Value: AssumeRole
RoleArn	String	Yes	acs:ram::123456789012****:role/adminrole	The Alibaba Cloud Resource Name (ARN) of a RAM role. Pattern: <code>acs : ram :: \$ accountID : role / \$ roleName</code>
RoleSessionName	String	Yes	alice	The role session name. This parameter can be customized to identify the user who assumes a role. Pattern: <code>^[a-zA-Z0-9\.\@\-_]+\$</code>  Note: This parameter must be 2 to 32 characters in length.

Parameter	Type	Required ?	Example value	Description
Policy	String	No	<code>{"Statement": [{"Action": ["*"], "Effect": "Allow", "Resource": ["*"]}], "Version": "1"}</code>	The policy. It must be 1 to 1024 bytes in length. This parameter can be used to specify the permission of an STS token. If this parameter is left unspecified, the returned STS token has all permissions of a specific role.
DurationSeconds	Integer	No	3,600	The expiration duration. Unit: second Value range: 900 to 3,600 Default value: 3,600

Response parameters

Parameter	Type	Example value	Description
RequestId	String	6894B13B-6D71-4EF5-88FA-F32781734A7F	The request ID.
Credentials	N/A	N/A	The access credential.
AccessKeyId	String	STS.L4aBSCSJVMuKg5U1****	The access key ID.
AccessKeySecret	String	wyLTSmsyPGP1ohvww8xYgB29dlGI8KMih2pK****	The access key secret.
SecurityToken	String	*****	The security token.

Parameter	Type	Example value	Description
Expiration	String	2015-04-09T11:52:19Z	The date and time when the identity expires.
AssumedRoleUser	N/A	N/A	The temporary identity for assuming a role.
Arn	String	acs:sts::123456789012****:assumed-role/AdminRole/alice	The ARN of a specific role. Pattern: <code>acs : ram :: \$accountID : role / \$ roleName</code>
AssumedRoleUserId	String	34458433936495****:alice	The ID of the temporary identity for assuming a role.

Example

Request example

```
https://sts.aliyuncs.com?Action=AssumeRole
&RoleArn=acs:ram::123456789012****:role/adminrole
&RoleSessionName=alice
&DurationSeconds=3600
&Policy=<url_encode_d_policy>
&<CommonParameters>
```

Response example

XML format

```
<AssumeRoleResponse>
  <RequestId>6894B13B-6D71-4EF5-88FA-F32781734A7F</RequestId>
  <AssumedRoleUser>
    <arn>acs:sts::123456789012****:assumed-role/AdminRole/alice</arn>
    <AssumedRoleUserId>34458433936495****:alice</AssumedRoleUserId>
  </AssumedRoleUser>
  <Credentials>
    <AccessKeyId>STS.L4aBSCSJVMuKg5U1****</AccessKeyId>
    <AccessKeySecret>wyLTSmsyPGP1ohvww8xYgB29dlGI8KMih2pK****</AccessKeySecret>
    <SecurityToken>*****</SecurityToken>
    <Expiration>2015-04-09T11:52:19Z</Expiration>
  </Credentials>
```

```
</ AssumeRole Response >
```

JSON format

```
{
  "Credentials": {
    "AccessKeyId": "STS.L4aBSCSJVM.uKg5U1 ****",
    "AccessKeySecret": "wyLTSmsyPG.P1ohvvw8xY.gB29dlGI8KMiH2pK ****",
    "Expiration": "2015-04-09T11:52:19Z",
    "SecurityToken": "*****"
  },
  "AssumedRoleUser": {
    "Arn": "acs:sts::1234567890:12****:assumed-role/AdminRole/alice",
    "AssumedRoleUserId": "3445843393:6495****:alice"
  },
  "RequestId": "6894B13B-6D71-4EF5-88FA-F32781734A7F"
}
```

Errors

Error code	Error message	HTTP status code	Meaning
InvalidParameter	The parameter RoleArn is wrongly formed.	400	The ARN format of the role is incorrect.
InvalidParameter.RoleArn	The parameter RoleArn is wrongly formed.	400	The ARN format of the role is incorrect.
InvalidParameter.RoleSessionName	The parameter RoleSessionName is wrongly formed.	400	The value of the RoleSessionName parameter is incorrect. This parameter must be 2 to 32 characters in length. The allowed pattern is <code>^[a-zA-Z0-9\.\@\-_]+</code>.

Error code	Error message	HTTP status code	Meaning
InvalidParameter. DurationSeconds	The Min/Max value of DurationSeconds is 15min/1hr.	400	The value of the DurationSeconds parameter is incorrect. The value ranges from 900 to 3,600, in seconds.
InvalidParameter. PolicyGrammar	The parameter Policy has not passed grammar check.	400	The policy grammar is incorrect.
InvalidParameter. PolicySize	The size of Policy must be smaller than 1024 bytes.	400	The policy cannot exceed 1024 bytes.
NoPermission	You are not authorized to do this action. You should be authorized by RAM.	403	The STS token does not have the required permission.
InternalError	STS Server Internal Error happened.	500	An internal server error occurs.

3.2 GetCallerIdentity

Obtains the identity of the user who is calling the API action.

Request parameters

Parameter	Type	Required ?	Example value	Description
Action	String	Yes	GetCallerIdentity	The name of this action. Value: GetCallerIdentity

Response parameters

Parameter	Type	Example value	Description
RequestId	String	2C9BE469-4A35-44D5-9529-CAA280B11603	The request ID.
Arn	String	acs:ram::196813200012****:user/admin	The Alibaba Cloud Resource Name (ARN) of the user who is calling the API action.
AccountId	String	196813200012****	The ID of the Alibaba Cloud account to which the user who is calling the API action belongs.
UserId	String	216959339000****	The ID of the user who is calling the API action. If the user is the owner of an Alibaba Cloud account, the AccountId parameter is returned.

Example**Request example**

```
https://sts.aliyuncs.com?Action=GetCallerIdentity
&<CommonParameters>
```

Response example**XML format**

```
<GetCallerIdentityResponse>
  <RequestId>2C9BE469-4A35-44D5-9529-CAA280B11603</RequestId>
  <AccountId>196813200012****</AccountId>
  <UserId>216959339000****</UserId>
  <Arn>acs:ram::196813200012****:user/admin</Arn>
</GetCallerIdentityResponse>
```

JSON format

```
{
  "RequestId": "2C9BE469-4A35-44D5-9529-CAA280B11603",
  "AccountId": "196813200012****",
  "UserId": "216959339000****",
  "Arn": "acs:ram::196813200012****:user/admin"
}
```

Errors

None.

3.3 AssumeRoleWithSAML

Obtains a temporary identity for assuming a role during role-based Single Sign On (SSO).

Request parameters

Parameter	Type	Required?	Example value	Description
Action	String	Yes	AssumeRoleWithSAML	The name of this action. Value: AssumeRoleWithSAML
SAMLProviderArn	String	Yes	acs:ram::123456789012****:saml-provider/company1	The Alibaba Cloud Resource Name (ARN) of the identity provider (IdP) created in RAM. Pattern: <code>acs : ram :: \$ account_ID : saml - provider /\$ saml_provider_ID</code>
RoleArn	String	Yes	acs:ram::123456789012****:role/adminrole	The ARN of the role to be assumed. Pattern: <code>acs : ram :: \$ accountID : role /\$ roleName</code>
SAMLEnvironment	String	Yes	<base64_encoded_saml_assertion>	The SAML assertion that is encoded by using Base64. The value must be 4 to 100000 bytes in length.
Policy	String	No	<url_encoded_policy>	The policy that specifies the permission of the STS token . If this parameter is left unspecified, the STS token has all permissions of a specific role. This parameter must be 1 to 1024 bytes in length.

Parameter	Type	Required ?	Example value	Description
DurationSeconds	String	No	3,600	The expiration time. Unit: second Value range: 900 to 3,600 Default value: 3,600

Response parameters

Parameter	Type	Example value	Description
RequestId	String	6894B13B-6D71-4EF5-88FA-F32781734A7F	The request ID.
Credentials	N/A	N/A	The access credential.
AccessKeyId	String	STS.L4aBSCSJVMuKg5U1****	The access key ID.
AccessKeySecret	String	wyLTSmsyPGP1ohvww8xYgB29dlGI8KMih2pK****	The access key secret.
SecurityToken	String	*****	The security token.
Expiration	String	2015-04-09T11:52:19Z	The expiration time.
AssumedRoleUser	N/A	N/A	The temporary identity to assume the role.

Parameter	Type	Example value	Description
└ Arn	String	acs:sts::123456789012****:assumed-role/AdminRole/alice	The ARN of the temporary identity to assume the role. Pattern: <code>acs : ram :: \$accountID : assumed - role / \$ roleName / \$ roleSessionName</code>
└ AssumedRoleUserId	String	34458433936495****:alice	The ID of the temporary identity to assume the role.
SAMLAAssertionInfo	N/A	N/A	The information in the SAML assertion.
└ SubjectType	String	persistent	The format of the <code>NameID</code> field in the SAML assertion. If the <code>NameID</code> contains the <code>urn : oasis : names : tc : SAML : 2 . 0 : nameid - format : prefix</code> , the prefix will be removed. For example, if the prefix is <code>urn : oasis : names : tc : SAML : 2 . 0 : nameid - format : persistant / transient</code> , only <code>persistant / transient</code> is displayed.
└ Subject	String	alice@example.com	The value of the <code>Subject - NameID</code> field in the SAML assertion.
└ Recipient	String	https://signin.aliyun.com/saml-role/SSO	The <code>Recipient</code> attribute of the <code>Subject - SubjectConfirmation - SubjectConfirmationData</code> field in the SAML assertion.
└ Issuer	String	http://example.com/adfs/services/trust	The value of the <code>Issuer</code> field in the SAML assertion.

Example



Note:

The `SAMLAAssertion` parameter may have a large amount of body text. Therefore, we recommend that you use POST rather than GET when sending a request.

Response example

XML format

```
< AssumeRole Response >
  < RequestId > 6894B13B - 6D71 - 4EF5 - 88FA - F32781734A 7F </
  RequestId >
    < AssumedRoleUser >
      < arn > acs : sts :: 1234567890 12 ****: assumed - role /
      AdminRole / alice </ arn >
      < AssumedRoleUserId > 3445843393 6495 ****: alice <
      AssumedRoleUserId >
    </ AssumedRoleUser >
    < Credentials >
      < AccessKeyId > STS . L4aBSCSJVM uKg5U1 ****</ AccessKeyId >
      < AccessKeySecret > wyLTSmsyPG P1ohvww8xY gB29dlGI8K
      MiH2pK ****</ AccessKeySecret >
      < SecurityToken > *****</ SecurityToken >
      < Expiration > 2015 - 04 - 09T11 : 52 : 19Z </ Expiration >
    </ Credentials >
    < SAMLAssertionInfo >
      < SubjectType > persistent </ SubjectType >
      < Subject > alice @ example . com </ Subject >
      < Recipient > https :// signin . aliyun . com / saml - role /
      SSO </ Recipient >
      < Issuer > http :// example . com / adfs / services / trust </
      Issuer >
    </ SAMLAssertionInfo >
  </ AssumeRole Response >
```

JSON format

```
{
  "Credentials": {
    "AccessKeyId": "STS . L4aBSCSJVM uKg5U1 ****",
    "AccessKeySecret": "wyLTSmsyPG P1ohvww8xY gB29dlGI8K
    MiH2pK ****",
    "Expiration": " 2015 - 04 - 09T11 : 52 : 19Z ",
    "SecurityToken": "*****"
  },
  "AssumedRoleUser": {
    "arn": " acs : sts :: 1234567890 123456 : assumed - role /
    AdminRole / alice ",
    "AssumedRoleUserId": " 3445843393 6495 ****: alice "
  },
  "SAMLAssertionInfo": {
    "SubjectType": " persistent ",
    "Subject": " alice @ example . com ",
    "Recipient": " https :// signin . aliyun . com / saml - role
    / SSO ",
  }
```

```

    "Issuer": "http://example.com/adfs/services/trust",
    "RequestId": "6894B13B - 6D71 - 4EF5 - 88FA - F32781734A 7F"
  }

```

Errors

Error code	Error message	HTTP status code	Meaning
MissingParameter.SAMLAssertion	Parameter SAMLAssertion is required.	400	The SAMLAssertion parameter is required.
MissingParameter.SAMLProviderArn	Parameter SAMLProviderArn is required.	400	The SAMLProviderArn parameter is required.
MissingParameter.RoleArn	Parameter RoleArn is required.	400	The RoleArn parameter is required.
InvalidParameter.PolicyGrammar	Invalid Policy.	400	The policy is invalid.
InvalidParameter.PolicySize	The max size of policy string is 1024.	400	The policy cannot exceed 1024 bytes.
InvalidParameter.RoleSessionName	The RoleSessionName is invalid.	400	The role session name is invalid.
InvalidParameter.DurationSeconds	The DurationSeconds is invalid.	400	The DurationSeconds parameter is invalid.
EntityNotExist.SAMLProvider	Can not find SAML provider.	404	The SAML IdP does not exist.
EntityNotExist.RoleArn	The specified Role does not exist.	404	The specified role does not exist.
AuthenticationFail.IDPMetadata.Invalid	The IdP Metadata of your SAML Provider is invalid.	401	The metadata of your SAML IdP is invalid.
AuthenticationFail.SAMLAssertion.Expired	The SAML Assertion is expired.	401	The SAML assertion has expired.

Error code	Error message	HTTP status code	Meaning
AuthenticationFail .SAMLAssertion. Invalid	The SAML Assertion is invalid.	401	The SAML assertion is invalid.