ALIBABA CLOUD

Alibaba Cloud

Resource Access Management
API Reference (STS)

Document Version: 20201117

Alibaba Cloud

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 `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.What is STS?

Alibaba Cloud Security Token Service (STS) allows you to manage short-term access from other users to your Alibaba Cloud resources.

Features

You can use STS to grant temporary access tokens to RAM entities (RAM users and RAM roles). You can customize the validity period and access permissions of these STS tokens. Authorized RAM entities can use the STS tokens to access Alibaba Cloud resources by using one of the following methods:

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

Endpoints

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

Terms

RAM role
A virtual RAM user.

ARN
The Alibaba Cloud Resource Name (ARN) of a RAM role. In Alibaba Cloud, each role has a unique ARN. Format: `acs:ram::$accountID:role/$roleName`.

trusted entity
An entity that is entrusted to assume a RAM role. You must specify a trusted entity when you create a RAM role. Only trusted entities can assume the RAM role. A trusted entity can be an Alibaba Cloud account, Alibaba Cloud service, or identity provider (IdP).

role assuming
A method for entities to obtain STS tokens of RAM roles. An entity can obtain an STS token by calling the AssumeRole STS API operation. Then, the entity can use the STS token to call Alibaba Cloud API operations.

2.Request structure

This topic describes the details about the request structure, including the endpoints of Security Token Service (STS), communications protocols, HTTP request methods, and request parameters.

Endpoints

For information about STS endpoints, see Endpoints.

Communications protocols

To ensure communication security, STS only allows you to send requests over HTTPS.

HTTP request methods

STS allows you to send HTTP GET and POST requests.

> **Note** The size of each HTTP GET request cannot exceed 4 KB. The size of each HTTP POST request cannot exceed 10 MB.

Request parameters

You must specify the following parameters for each API request:

- The Action parameter. It specifies the API operation you want to perform.
- The common request parameters.
- The request parameters that are specific to the API operation.

Character encoding

Requests and responses are UTF-8 encoded.

3.Endpoints

This topic lists all the endpoints of Security Token Service (STS). You can use the listed endpoints to access the STS service. We recommend that you use the endpoint in the region where you call the STS service.

The following tables list the STS endpoint in each region. Two endpoint types are available:

- Internet endpoint: You can use the endpoints of this type to access the STS service from the Internet.
- VPC endpoint: You can use the endpoints of this type to access the STS service from virtual private clouds (VPCs) that reside in the corresponding region. You do not need to allow access to the STS service from the Internet.

Asia Pacific

Region	Region ID	Endpoint
Mainland China	N/A	Internet: sts.aliyuncs.com **Note** To access STS in a region inside mainland China, you can use the unified Internet endpoint or the endpoint that is specific to the region.
China (Hangzhou)	cn-hangzhou	• Internet: sts.cn-hangzhou.aliyuncs.com • VPC: sts-vpc.cn-hangzhou.aliyuncs.com
China (Shanghai)	cn-shanghai	• Internet: sts.cn-shanghai.aliyuncs.com • VPC: sts-vpc.cn-shanghai.aliyuncs.com
China (Shenzhen)	cn-shenzhen	• Internet: sts.cn-shenzhen.aliyuncs.com • VPC: sts-vpc.cn-shenzhen.aliyuncs.com
China (Heyuan)	cn-heyuan	Internet: sts.cn-heyuan.aliyuncs.com
China (Qingdao)	cn-qingdao	Internet: sts.cn-qingdao.aliyuncs.com

Region	Region ID	Endpoint
China (Beijing)	cn-beijing	• Internet: sts.cn-beijing.aliyuncs.com • VPC: sts-vpc.cn-beijing.aliyuncs.com
China (Zhangjiakou-Beijing Winter Olympics)	cn-zhangjiakou	• Internet: sts.cn-zhangjiakou.aliyuncs.com • VPC: sts-vpc.cn-zhangjiakou.aliyuncs.com
China (Hohhot)	cn-huhehaote	• Internet: sts.cn-huhehaote.aliyuncs.com • VPC: sts-vpc.cn-huhehaote.aliyuncs.com
China (Chengdu)	cn-chengdu	• Internet: sts.cn-chengdu.aliyuncs.com • VPC: sts-vpc.cn-chengdu.aliyuncs.com
China (Hong Kong)	cn-hongkong	• Internet: sts.cn-hongkong.aliyuncs.com • VPC: sts-vpc.cn-hongkong.aliyuncs.com
Singapore (Singapore)	ap-southeast-1	• Internet: sts.ap-southeast-1.aliyuncs.com • VPC: sts-vpc.ap-southeast-1.aliyuncs.com
Australia (Sydney)	ap-southeast-2	• Internet: sts.ap-southeast-2.aliyuncs.com • VPC: sts-vpc.ap-southeast-2.aliyuncs.com
Malaysia (Kuala Lumpur)	ap-southeast-3	• Internet: sts.ap-southeast-3.aliyuncs.com • VPC: sts-vpc.ap-southeast-3.aliyuncs.com
Indonesia (Jakarta)	ap-southeast-5	• Internet: sts.ap-southeast-5.aliyuncs.com • VPC: sts-vpc.ap-southeast-5.aliyuncs.com

Region	Region ID	Endpoint
Japan (Tokyo)	ap-northeast-1	• Internet: sts.ap-northeast-1.aliyuncs.com • VPC: sts-vpc.ap-northeast-1.aliyuncs.com

Europe & Americas

Region	Region ID	Endpoint
US (Silicon Valley)	us-west-1	• Internet: sts.us-west-1.aliyuncs.com • VPC: sts-vpc.us-west-1.aliyuncs.com
US (Virginia)	us-east-1	• Internet: sts.us-east-1.aliyuncs.com • VPC: sts-vpc.us-east-1.aliyuncs.com
Germany (Frankfurt)	eu-central-1	• Internet: sts.eu-central-1.aliyuncs.com • VPC: sts-vpc.eu-central-1.aliyuncs.com
UK (London)	eu-west-1	• Internet: sts.eu-west-1.aliyuncs.com • VPC: sts-vpc.eu-west-1.aliyuncs.com

Middle East & India

Region	Region ID	Endpoint
India (Mumbai)	ap-south-1	• Internet: sts.ap-south-1.aliyuncs.com • VPC: sts-vpc.ap-south-1.aliyuncs.com
UAE (Dubai)	me-east-1	Internet: sts.me-east-1.aliyuncs.com

4.Common parameters

Common parameters include common request parameters and common response parameters.

Common request parameters

Parameter	Type	Required	Description
Format	String	No	The format in which to return the response. Valid values: JSON and XML. Default value: *JSON*.
Version	String	Yes	The version number of the API. The parameter value is in the YYYY-MM-DD format. Set the value to 2015-04-01.
Signature	String	Yes	The signature string of the current request.
SignatureMethod	String	Yes	The encryption method of the signature string. Set the value to HMAC-SHA1.
SignatureNonce	String	Yes	A unique, random number used to prevent replay attacks. You must use different random numbers for different requests.
SignatureVersion	String	Yes	The version of the signature encryption algorithm. Set the value to 1.0.
AccessKeyId	String	Yes	The AccessKey ID provided to you by Alibaba Cloud.

Parameter	Type	Required	Description
Timestamp	String	Yes	The timestamp of the request. Specify the time in the ISO 8601 standard in the yyyy-MM-ddTHH:mm:ssZ format. The time must be in UTC. For example, 2013-01-10T12:00:00Z specifies 20:00:00 on January 10, 2013 (UTC+8).

Sample requests

```
https://sts.aliyuncs.com?Action=AssumeRole
&Format=xml
&Version=2015-04-01
&Signature=Pc5WB8gokVn0xfeu%2FZV%2BiNM1dg****
&SignatureMethod=HMAC-SHA1
&SignatureNonce=1521552885****
&SignatureVersion=1.0
&AccessKeyId=LTAI4GENiH2u8MVj7Khh****
&Timestamp=2015-06-01T12:00:00Z
```

Common response parameters

Responses can be returned in either the JSON or XML format. You can specify the response format in the request. The default response format is XML. Every response returns a unique RequestId regardless of whether the call is successful.

- A `2xx` HTTP status code indicates a successful call.
- A `4xx` or `5xx` HTTP status code indicates a failed call.

Sample success responses

- XML format

```
<? xml version="1.0" encoding="utf-8"? >
  <!—Result Root Node-->
  <Interface Name+Response>
    <!—Return Request Tag-->
    <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
    <!—Return Result Data-->
  </Interface Name+Response>
```

- JSON format

```
{
  "RequestId":"4C467B38-3910-447D-87BC-AC049166F216"
  /*Return Result Data*/
}
```

5.Request signatures

You must sign all API requests to ensure security. Alibaba Cloud uses the request signature to verify the identity of the API caller. Each API request must contain the signature, regardless of whether it is sent over HTTP or HTTPS.

Overview

For an RPC API, you must add the signature to the API request in the following format:

```
https://Endpoint/?SignatureVersion=1.0&SignatureMethod=HMAC-SHA1&Signature=CT9X0VtwR86fNWSnsc6v8YGOjuE%3D&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
```

where:

- SignatureMethod: the encryption method of the signature string. Set the value to HMAC-SHA1.
- SignatureVersion: the version of the signature encryption algorithm. Set the value to 1.0.
- SignatureNonce: a unique, random number used to prevent replay attacks. You must use different random numbers for different requests. We recommend that you use universally unique identifiers (UUIDs).
- Signature: the signature generated after the request has been symmetrically encrypted by using the AccessKey secret.

The signature encryption algorithm complies with RFC 2104 HMAC-SHA1 specifications. The AccessKey secret is used to calculate the hash-based message authentication code (HMAC) value of the encoded and sorted query string, and the HMAC value is used as the signature string. Request signatures include operation-specific parameters. Therefore, the signature of a request varies based on the request parameters. To calculate a signature, follow the steps in this topic.

```
Signature = Base64( HMAC-SHA1( AccessKey Secret, UTF-8-Encoding-Of(StringToSign)) )
```

Step 1: Compose and encode a string-to-sign

1. Use request parameters to construct a canonicalized query string.
   i. Create a canonicalized query string by arranging the request parameters (including all common and operation-specific parameters except Signature) in alphabetical order.

      > **Note** If you use the GET method to submit the request, these parameters are the part located after the question mark (?) and connected by the ampersands (&) in the request uniform resource identifier (URI).

   ii. Encode the canonicalized query string in UTF-8. The following table describes the encoding rules.

Character	Encoding rule
Uppercase letters, lowercase letters, digits, hyphens (-), underscores (_), periods (.), and tildes (~)	These characters do not need to be encoded.
Other characters	These characters must be percent encoded in `%XY` format. `XY` represents the ASCII code of the characters in hexadecimal notation. For example, double quotation marks (") are encoded as `%22`.
Extended UTF-8 characters	These characters are encoded in `%XY%ZA...` format.

Spaces	Spaces must be encoded as `%20`. Do not encode spaces as plus signs (+).
	This encoding method is different from the `application/x-www-form-urlencoded` MIME encoding algorithm (such as the `java.net.URLEncoder` class provided by the Java standard library). However, you can apply the encoding algorithm and replace the plus sign (+) in the encoded string with `%20`, the asterisk (*) with `%2A`, and `%7E` with the tilde (~). To do this, you can use the following `percentEncode` method:
	`private static final String ENCODING = "UTF-8";`
	`private static String percentEncode(String value) throws UnsupportedEncodingException`
	`{`
	`return value ! = null ? URLEncoder.encode(value, ENCODING)`
	`.replace("+", "%20").replace("*", "%2A").replace("%7E", "~")`
	`: null;`
	`}`

iii. Connect the encoded parameter names and their values by using equal signs (=).

iv. Sort the connected parameter name and value pairs in the order specified in step i and connect the pairs by using ampersands (&) to obtain the canonicalized query string.

2. Use the canonicalized query string to construct a string-to-sign in the following way:

```
StringToSign=
    HTTPMethod + "&" +
    percentEncode("/") + "&" +
     percentEncode(CanonicalizedQueryString)
```

where:

- HTTPMethod: the HTTP method used to submit a request, such as GET.
- percentEncode("/"): specifies the encoded value (%2F) of a forward slash (/). The encoding follows the URL encoding rules.
- percentEncode(CanonicalizedQueryString): specifies the encoded canonicalized query string based on the URL encoding rules.

Step 2: Calculate the signature string

1. Calculate the HMAC value of the string-to-sign based on RFC 2104.

> **Note** Use the SHA1 algorithm to calculate the HMAC value of the string-to-sign. The combination of your AccessKey secret and an ampersand (&) (ASCII code 38) that follows the secret is used as the key for the HMAC calculation.

2. Encode the HMAC value in Base64 to obtain the signature string.
3. Add the signature string to the request as the Signature parameter.

> **Note** When the obtained signature value is submitted as the final request parameter value, the value must be URL-encoded like other parameters based on rules defined in RFC 3986.

Examples

This section uses the AssumeRole API operation as an example to introduce the signature method.

Request URL before the request is signed:

```
https://sts.aliyuncs.com/?SignatureVersion=1.0&Format=JSON&Timestamp=2015-09-01T05%3A57%3A34Z&
RoleArn=acs%3Aram%3A%3A1234567890123%3Arole%2Ffirstrole&RoleSessionName=client&AccessKeyId=t
estid&SignatureMethod=HMAC-SHA1&Version=2015-04-01&Action=AssumeRole&SignatureNonce=571f8fb8-
506e-11e5-8e12-b8e8563dc8d2
```

The `StringToSign`:

```
GET&%2F&AccessKeyId%3Dtestid%26Action%3DAssumeRole%26Format%3DJSON%26RoleArn%3Dacs%253Aram%253A%253A1234567890123%253Arole%252Ffirstrole%26RoleSessionName%3Dclient%26SignatureMethod%3DHMAC-SHA1%26SignatureNonce%3D571f8fb8-506e-11e5-8e12-b8e8563dc8d2%26SignatureVersion%3D1.0%26Timestamp%3D2015-09-01T05%253A57%253A34Z%26Version%3D2015-04-01
```

Assume that the AccessKey ID is testid and the AccessKey secret is testsecret. The key that is used to calculate the HMAC value of the string-to-sign is testsecret&.

The calculated signature string is `gNI7b0AyKZHxDgjBGPDgJ1Ce3L4=` .

Request URL after the request is signed:

```
https://sts.aliyuncs.com/?SignatureVersion=1.0&Format=JSON&Timestamp=2015-09-01T05%3A57%3A34Z&RoleArn=acs%3Aram%3A%3A1234567890123%3Arole%2Ffirstrole&RoleSessionName=client&AccessKeyId=testid&SignatureMethod=HMAC-SHA1&Version=2015-04-01&Signature=gNI7b0AyKZHxDgjBGPDgJ1Ce3L4%3D&Action=AssumeRole&SignatureNonce=571f8fb8-506e-11e5-8e12-b8e8563dc8d2
```

6.Responses

After STS API operations are called, data is returned in a unified format. The returned data is in either the XML or JSON format, and the XML format is the default option. Sample responses in API documents are formatted in a way that is easier for you to read. The actual responses are not formatted with line breaks or indentation.

Sample success responses

An HTTP status code `2xx` indicates that the API operation is successful.

- XML format

```
<? xml version="1.0" encoding="utf-8"? >
<!--Result Root Node-->
<Operation name+Response>
  <!--Return Request Tag-->
  <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
  <!--Return Result Data-->
</Operation Name+Response>
```

- JSON format

```
{
  "RequestId": "4C467B38-3910-447D-87BC-AC049166F216",
  /* Return Result Data */
}
```

Sample error responses

An HTTP status code `4xx` or `5xx` indicates that the API operation failed and no result data is returned. The returned message body contains the specific error code, the error message, the `RequestId` parameter, and the `HostId` parameter. The RequestId parameter indicates the globally unique ID of the API request. The HostId parameter indicates the ID of the host to which your API request is sent. You can locate the error by using the error code.

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<Error>
  <RequestId>8906582E-6722-409A-A6C4-0E7863B733A5</RequestId>
  <HostId>sts.aliyuncs.com</HostId>
  <Code>InvalidParameter</Code>
  <Message>The specified parameter "Action or Version" is not valid. </Message>
</Error>
```

- JSON format

```
{
  "RequestId": "7463B73D-35CC-4D19-A010-6B8D65D242EF",
  "HostId": "sts.aliyuncs.com",
  "Code": "InvalidParameter",
  "Message": "The specified parameter \"Action or Version\" is not valid."
}
```

7.Operation interfaces

7.1. AssumeRole

Obtains a temporary identity to assume a RAM role. This topic uses a RAM role whose trusted entity is an Alibaba Cloud account as an example.

> **Note**
>
> The AssumeRole operation can be called up to 100 times per second for each Alibaba Cloud account. API requests that are sent by using RAM users and RAM roles under the Alibaba Cloud account are also counted. If the number of API requests exceeds 100, the following error message is returned:
>
> ```
> Request was denied due to user flow control.
> ```

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	AssumeRole	The operation that you want to perform. Set the value to AssumeRole.

Parameter	Type	Required	Example	Description
RoleArn	String	Yes	acs:ram::123456789012****:role/adminrole	The Alibaba Cloud Resource Name (ARN) of the RAM role. Format: `acs:ram::$accountID:role/$roleName`. **Note** • `$accountID`: the ID of the Alibaba Cloud account that owns the RAM role. To view the account ID, perform the following steps: Log on to the Alibaba Cloud Management Console, move the pointer over your profile picture in the upper-right corner, and then click **Security Settings**. • `$roleName`: the name of the RAM role. To view the RAM role name, perform the following steps: Log on to the RAM console. In the left-side navigation pane, click **RAM Roles**. On the page that appears, view the name in the **RAM Role Name** column.

Parameter	Type	Required	Example	Description
RoleSessionName	String	Yes	alice	The customized role session name. This parameter can be used to identify the RAM user who assumes the role. The name must be 2 to 32 characters in length and can contain letters, digits, periods (.), at signs (@), hyphens (-), and underscores (_).
Policy	String	No	{"Statement": [{"Action": ["*"],"Effect": "Allow","Resource": ["*"]}],"Version":"1"}	The policy that specifies the permissions of the returned STS token. You can use this parameter to grant the STS token fewer permissions than those granted to the RAM role. If you do not specify this parameter, the returned STS token has all permissions on the RAM role. The value must be 1 to 1,024 characters in length.
DurationSeconds	Long	No	3600	The validity period. Unit: seconds. Minimum value: 900. Maximum value: the value of the MaxSessionDuration parameter. Default value: 3600. **Note** You can call the CreateRole or UpdateRole operation to set the MaxSessionDuration parameter. For more information, see CreateRole and UpdateRole.

Response parameters

Parameter	Type	Example	Description
RequestId	String	6894B13B-6D71-4EF5-88FA-F32781734A7F	The ID of the request.
Credentials			The access credentials.
└AccessKeyId	String	STS.L4aBSCSJVMuKg5U1****	The AccessKey ID provided to you by Alibaba Cloud.

Parameter	Type	Example	Description
└AccessKeySecret	String	wyLTSmsyPGP1ohvvw8xYgB29dlGI8KMiH2pK****	The AccessKey secret provided to you by Alibaba Cloud.
└SecurityToken	String	********	The STS token.
└Expiration	String	2015-04-09T11:52:19Z	The time when the STS token expires.
AssumedRoleUser			The temporary identity that you use to assume the role.
└Arn	String	acs:ram::123456789012****:role/adminrole/alice	The ARN of the RAM role. Format: `acs:ram::$accountID:role/$roleName/$RoleSessionName`. **Note** • `$accountID`: the ID of the Alibaba Cloud account that owns the RAM role. To view the account ID, perform the following steps: Log on to the Alibaba Cloud Management Console, move the pointer over your profile picture in the upper-right corner, and then click **Security Settings**. • `$roleName`: the name of the RAM role. To view the RAM role name, perform the following steps: Log on to the RAM console. In the left-side navigation pane, click **RAM Roles**. On the page that appears, view the name in the **RAM Role Name** column.
└AssumedRoleId	String	34458433936495****:alice	The ID of the temporary identity that you use to assume the role.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<AssumeRoleResponse>
  <RequestId>6894B13B-6D71-4EF5-88FA-F32781734A7F</RequestId>
  <AssumedRoleUser>
    <Arn>acs:ram::123456789012****:role/adminrole/alice</arn>
    <AssumedRoleId>344584339364 95****:alice</AssumedRoleId>
  </AssumedRoleUser>
  <Credentials>
    <AccessKeyId>STS.L4aBSCSJVMuKg5U1****</AccessKeyId>
    <AccessKeySecret>wyLTSmsyPGP1ohvvw8xYgB29dlGI8KMiH2pK****</AccessKeySecret>
    <SecurityToken>********</SecurityToken>
    <Expiration>2015-04-09T11:52:19Z</Expiration>
  </Credentials>
</AssumeRoleResponse>
```

`JSON` format

```
{
  "Credentials": {
    "AccessKeyId": "STS.L4aBSCSJVMuKg5U1****",
    "AccessKeySecret": "wyLTSmsyPGP1ohvvw8xYgB29dlGI8KMiH2pK****",
    "Expiration": "2015-04-09T11:52:19Z",
    "SecurityToken": "********"
  },
  "AssumedRoleUser": {
    "Arn": "acs:ram::123456789012****:role/adminrole/alice",
    "AssumedRoleId":"344584339364 95****:alice"
    },
  "RequestId": "6894B13B-6D71-4EF5-88FA-F32781734A7F"
}
```

Error codes

HttpCode	Error code	Error message	Description
400	InvalidParameter	The parameter RoleArn is wrongly formed.	The error message returned because the ARN format of the RAM role is invalid.
400	InvalidParameter.RoleArn	The parameter RoleArn is wrongly formed.	The error message returned because the ARN format of the RAM role is invalid.
400	InvalidParameter.RoleSessionName	The parameter RoleSessionName is wrongly formed.	The error message returned because the format of the RoleSessionName parameter is invalid. The value must be 2 to 32 characters in length and can contain letters, digits, periods (.), at signs (@), hyphens (-), and underscores (_).
400	InvalidParameter.DurationSeconds	The Min/Max value of DurationSeconds is 15min/1hr.	The error message returned because the value of the DurationSeconds parameter is invalid. The minimum value is 900, and the maximum value is equal to the value of the MaxSessionDuration parameter.
400	InvalidParameter.PolicyGrammar	The parameter Policy has not passed grammar check.	The error message returned because the syntax of the policy is invalid.
400	InvalidParameter.PolicySize	The size of Policy must be smaller than 1024 bytes.	The error message returned because the length of the specified policy string exceeds the upper limit. The policy string can be up to 1,024 bytes in length.

HttpCode	Error code	Error message	Description
403	NoPermission	You are not authorized to do this action. You should be authorized by RAM.	The error message returned because the STS token does not have the required permissions. For more information about how to handle the error, see FAQ about RAM roles and STS tokens.
404	EntityNotExist.Role	The specified Role not exists.	The error message returned because the specified RAM role does not exist.
500	InternalError	STS Server Internal Error happened.	The error message returned because an internal server error occurred.

7.2. GetCallerIdentity

Queries the identity of the user who is making the API request.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	GetCallerIdentity	The operation that you want to perform. Set the value to GetCallerIdentity.

Response parameters

Parameter	Type	Example	Description
RequestId	String	2C9BE469-4A35-44D5-9529-CAA280B11603	The ID of the request.
Arn	String	acs:ram::1968132000012****:user/admin	The Alibaba Cloud Resource Name (ARN) of the user who is calling the API operation.
AccountId	String	196813200012****	The ID of the Alibaba Cloud account that is used to call the API operation, or the ID of the Alibaba Cloud account to which the RAM user who is calling the API operation belongs. The ID only consists of digits.

Parameter	Type	Example	Description
UserId	String	216959339000****	• The ID of the RAM user if a RAM user is calling the API operation. • The ID of the Alibaba Cloud account if an Alibaba Cloud account user is calling the API operation.
RoleId	String	33537620082992****	The ID of the RAM role. This parameter is returned only if the user who is calling the API operation assumes a RAM role.
PrincipalId	String	28877424437521****	The ID of the principal.
IdentityType	String	RAMUser	The type of the identity.

Examples

Sample requests

```
https://sts.aliyuncs.com?Action=GetCallerIdentity
&<Common request parameters>
```

Sample success responses

`XML` format

```
<GetCallerIdentityResponse>
  <RequestId>2C9BE469-4A35-44D5-9529-CAA280B11603</RequestId>
  <AccountId>196813200012****</AccountId>
  <UserId>216959339000****</UserId>
  <IdentityType>RAMUser</IdentityType>
  <PrincipalId>28877424437521****</PrincipalId>
  <Arn>acs:ram::196813200012****:user/admin</Arn>
</GetCallerIdentityResponse>
```

`JSON` format

```
{
  "RequestId": "2C9BE469-4A35-44D5-9529-CAA280B11603",
  "AccountId": "196813200012****",
  "UserId": "216959339000****",
  "IdentityType": "RAMUser",
  "PrincipalId": "28877424437521****",
  "Arn": "acs:ram::196813200012****:user/admin"
}
```


Error codes

None.

7.3. AssumeRoleWithSAML

Obtains a temporary identity to assume a RAM role during role-based single sign-on (SSO).

Request parameters

> **Note** Anonymous users can call the AssumeRoleWithSAML API operation because authentication for this operation is performed based on SAML assertions. Therefore, you do not need to specify the following common parameters: Signature, SignatureMethod, SignatureVersion, and AccessKeyId.

Parameter	Type	Required	Example	Description
Action	String	Yes	AssumeRoleWithSAML	The operation that you want to perform. Set the value to AssumeRoleWithSAML.
SAMLProviderArn	String	Yes	acs:ram::123456789012****:saml-provider/company1	The Alibaba Cloud Resource Name (ARN) of the identity provider (IdP). The IdP must be configured in the RAM console. Format: `acs:ram::$account_ID:saml-provider/$saml_provider_ID`.
RoleArn	String	Yes	acs:ram::123456789012****:role/adminrole	The ARN of the RAM role to be assumed. Format: `acs:ram::$accountID:role/$roleName`.

Parameter	Type	Required	Example	Description
SAMLAssertion	String	Yes	<base64_encoded_saml_assertion>	The Base64-encoded SAML assertion. The value must be 4 to 100,000 characters in length. **Note** A complete SAML response instead of a single SAMLAssertion field must be retrieved from the IdP.
Policy	String	No	<url_encoded_policy>	The policy that specifies the permissions of the returned STS token. You can use this parameter to grant the STS token fewer permissions than those granted to the RAM role. If you do not specify this parameter, the returned STS token has all permissions of the RAM role. The value must be 1 to 1,024 characters in length.
DurationSeconds	Long	No	3600	The validity period of the STS token. Unit: seconds. Minimum value: 900. Maximum value: the value of the MaxSessionDuration parameter. Default value: 3600. **Note** You can call the CreateRole or UpdateRole operation to set the MaxSessionDuration parameter. For more information, see CreateRole and UpdateRole.

Response parameters

Parameter	Type	Example	Description
RequestId	String	6894B13B-6D71-4EF5-88FA-F32781734A7F	The ID of the request.
Credentials			The access credentials.
└AccessKeyId	String	STS.L4aBSCSJVMuKg5U1****	The AccessKey ID.

Parameter	Type	Example	Description
└AccessKeySecret	String	wyLTSmsyPGP1ohvvw8xYgB29dlGI8KMiH2pK****	The AccessKey secret.
└SecurityToken	String	********	The STS token.
└Expiration	String	2015-04-09T11:52:19Z	The time when the STS token expires.
AssumedRoleUser			The temporary identity that you use to assume the RAM role.
└Arn	String	acs:sts::123456789012****:assumed-role/AdminRole/alice	The ARN of the temporary identity that you use to assume the RAM role. Format: `acs:ram::$accountID:assumed-role/$roleName/$roleSessionName`.
└AssumedRoleUserId	String	34458433936495****:alice	The ID of the temporary identity that you use to assume the RAM role.
SAMLAssertionInfo			The information in the SAML assertion.
└SubjectType	String	persistent	The Format attribute of the `NameID` element in the SAML assertion. If the Format attribute is prefixed with `urn:oasis:names:tc:SAML:2.0:nameid-format:`, the prefix is not included in the value of this parameter. For example, if the value of the Format attribute is urn:oasis:names:tc:SAML:2.0:nameid-format:persistant/transient, the value of this parameter is `persistant/transient`.
└Subject	String	alice@example.com	The value in the NameID sub-element of the `Subject` element in the SAML assertion.
└Recipient	String	https://signin.aliyun.com/saml-role/SSO	The `Recipient` attribute of the SubjectConfirmationData sub-element. SubjectConfirmationData is a sub-element of the `Subject` element in the SAML assertion.
└Issuer	String	http://example.com/adfs/services/trust	The value in the `Issuer` element in the SAML assertion.

Examples

> **Note** If you use the GET method to send an API request and the SAMLAssertion parameter in the API request is set to a value with a large size, the API request may fail. We recommend that you use the POST method to send the API request.

Sample success responses

`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>wyLTSmsyPGP1ohvvw8xYgB29dlGI8KMiH2pK****</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>
</AssumeRoleResponse>
```

`JSON` format

```
{
  "Credentials": {
    "AccessKeyId": "STS.L4aBSCSJVMuKg5U1****",
    "AccessKeySecret": "wyLTSmsyPGP1ohvvw8xYgB29dlGI8KMiH2pK****",
    "Expiration": "2015-04-09T11:52:19Z",
    "SecurityToken": "********"
  },
  "AssumedRoleUser": {
    "arn": "acs:sts::1234567890123456:assumed-role/AdminRole/alice",
    "AssumedRoleUserId":"34458433936495****: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-F32781734A7F"
}
```


Error codes

HTTP status code	Error code	Error message	Description
400	MissingParameter.SAMLAssertion	Parameter SAMLAssertion is required.	The error message returned because the SAMLAssertion parameter is not specified.
400	MissingParameter.SAMLProviderArn	Parameter SAMLProviderArn is required.	The error message returned because the SAMLProviderArn parameter is not specified.
400	MissingParameter.RoleArn	Parameter RoleArn is required.	The error message returned because the RoleArn parameter is not specified.
400	InvalidParameter.PolicyGrammar	Invalid Policy.	The error message returned because the specified policy is invalid.

HTTP status code	Error code	Error message	Description
400	InvalidParameter.PolicySize	The max size of policy string is 1024.	The error message returned because the length of the specified policy script has reached the upper limit. The policy script can be up to 1,024 characters in length.
400	InvalidParameter.RoleSessionName	The RoleSessionName is invalid.	The error message returned because the specified role session name is invalid.
400	InvalidParameter.DurationSeconds	The DurationSeconds is invalid.	The error message returned because the specified value for the DurationSeconds parameter is invalid.
404	EntityNotExist.SAMLProvider	Can not find SAML provider.	The error message returned because the specified SAML IdP does not exist.
404	EntityNotExist.RoleArn	The specified Role does not exists.	The error message returned because the specified RAM role does not exist.
401	AuthenticationFail.IDPMetadata.Invalid	The IdP Metadata of your SAML Provider is invalid.	The error message returned because the metadata of the SAML IdP is invalid.
401	AuthenticationFail.SAMLAssertion.Expired	The SAML Assertion is expired.	The error message returned because the SAML assertion has expired.
401	AuthenticationFail.SAMLAssertion.Invalid	The SAML Assertion is invalid.	The error message returned because the SAML assertion is invalid.