Alibaba Cloud
Resource Access Management

API Reference (STS)

Issue: 20190916

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.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

Contents

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: `acs:ram::$accountID:role/$roleName`
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 #unique_4 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

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

Endpoints

For more information about the STS endpoints, see Endpoints.

Communications protocol

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, and 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 operation you want to perform.
- The common request parameters.
- The request parameters that are specific to the specified API operation.

Character encoding

Requests and responses are encoded by using the UTF-8 character set.

2.2 Endpoints

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

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

- Endpoint for public networks: indicates the endpoint that you use to access the STS service from public networks.
- Endpoint for VPCs: indicates the endpoint that you use to access the STS service from the virtual private clouds (VPCs) of the corresponding region. You do not need to make the STS service accessible from public networks.

IDCs in Mainland China

Region	Endpoint
Mainland China	Public network: sts.aliyuncs.com

Greater China

Region	Region ID	Endpoint
China (Hangzhou)	cn-hangzhou	· Public network: sts.cn-hangzhou.aliyuncs.com · VPC: sts-vpc.cn-hangzhou.aliyuncs.com
China (Shanghai)	cn-shanghai	· Public network: sts.cn-shanghai.aliyuncs.com · VPC: sts-vpc.cn-shanghai.aliyuncs.com
China (Shenzhen)	cn-shenzhen	· Public network: sts.cn-shenzhen.aliyuncs.com · VPC: sts-vpc.cn-shenzhen.aliyuncs.com
China (Qingdao)	cn-qingdao	Public network: sts.cn-qingdao.aliyuncs.com

Region	Region ID	Endpoint
China (Beijing)	cn-beijing	· Public network: sts.cn-beijing.aliyuncs.com · VPC: sts-vpc.cn-beijing.aliyuncs.com
China (Zhangjiakou)	cn-zhangjiakou	· Public network: sts.cn-zhangjiakou.aliyuncs.com · VPC: sts-vpc.cn-zhangjiakou.aliyuncs.com
China (Hohhot)	cn-huhehaote	· Public network: sts.cn-huhehaote.aliyuncs.com · VPC: sts-vpc.cn-huhehaote.aliyuncs.com
China (Hong Kong)	cn-hongkong	· Public network: sts.cn-hongkong.aliyuncs.com · VPC: sts-vpc.cn-hongkong.aliyuncs.com

Asia Pacific

Region	Region ID	Endpoint
Singapore	ap-southeast-1	Public network: sts.ap-southeast-1.aliyuncs.com
Australia (Sydney)	ap-southeast-2	Public network: sts.ap-southeast-2.aliyuncs.com
Malaysia (Kuala Lumpur)	ap-southeast-3	Public network: sts.ap-southeast-3.aliyuncs.com
Indonesia (Jakarta)	ap-southeast-5	Public network: sts.ap-southeast-5.aliyuncs.com
Japan (Tokyo)	ap-northeast-1	Public network: sts.ap-northeast-1.aliyuncs.com
India (Mumbai)	ap-south-1	Public network: sts.ap-south-1.aliyuncs.com

Europe and Americas

Region	Region ID	Endpoint
US (Silicon Valley)	us-west-1	Public network: sts.us-west-1.aliyuncs.com
US (Virginia)	us-east-1	Public network: sts.us-east-1.aliyuncs.com
Germany (Frankfurt)	eu-central-1	Public network: sts.eu-central-1.aliyuncs.com
UAE (Dubai)	me-east-1	Public network: sts.me-east-1.aliyuncs.com
UK (London)	eu-west-1	Public network: sts.eu-west-1.aliyuncs.com

2.3 Common parameters

This topic describes the common parameters, including the common request parameters and common response parameters.

Common request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform.
Format	String	No	The format to return the response values in. Valid values: `JSON` and `XML`. Default value: `XML`.
Version	String	Yes	The version number of the API. Specify the version in the YYYY-MM-DD format. Set this parameter to 2015-04-01.

Parameter	Type	Required	Description
Signature	String	Yes	The signature string of the current request.
SignatureMethod	String	Yes	The encryption method of the signature string. Set this parameter to HMAC-SHA1.
SignatureNonce	String	Yes	A unique, random number used to prevent replay attacks. You must use different numbers for different requests.
SignatureVersion	String	Yes	The version of the signature encryption algorithm. Set this parameter to 1.0.
AccessKeyId	String	Yes	The AccessKey ID provided to you by Alibaba Cloud.
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.

Common response parameters

Parameter	Type	Description
RequestId	String	The ID of the request. The system returns a unique request ID for each API request. This request ID is used to identify each API request.

Sample requests

```
 https :// sts . aliyuncs . com /? Action = XXXXXX
?  Format = xml
& Version = 2015 - 04 - 01
& Signature = Pc5WB8gokV  n0xfeu % 2FZV % 2BiNM1dg ****
& SignatureM  ethod = HMAC - SHA1
& SignatureN  once = 1521552885 ****
& SignatureV  ersion = 1 . 0
& AccessKeyI  d = key - test
& Timestamp = 2012 - 06 - 01T12 : 00 : 00Z
…
```

Sample responses

- XML format

```
<?  xml   version =" 1 . 0 "  encoding =" utf - 8 "? >
<!— Response   root   node -->
< API   operation   name + response >
  <!— Request   ID -->
  < RequestId > 4C467B38 - 3910 - 447D - 87BC - AC049166F2  16 </
 RequestId >
  <!— Result   data -->
</ API   operation   name + response >
```

- JSON format

```
{
  " RequestId ": " 4C467B38 - 3910 - 447D - 87BC - AC049166F2  16 "
  /*  Result   data  */
}
```

2.4 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 choice.

Sample responses in our 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

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

- XML format

```
<?  xml   version =" 1 . 0 "  encoding =" utf - 8 "? >
<!— Response   root   node -->
< API   operation   name + response >
    <!— Request   ID -->
    < RequestId > 4C467B38 - 3910 - 447D - 87BC - AC049166F2  16 </
 RequestId >
    <!— Result   data -->
</ API   operation   name + response >
```

- JSON format

```
{
    " RequestId ": " 4C467B38 - 3910 - 447D - 87BC - AC049166F2  16
 ",
    /*  Result   data  */
}
```

Sample error responses

The 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, error message, the value of the `RequestId` parameter, and the value of the `HostId` parameter. The RequestId parameter indicates the globally unique ID of the API request, and the HostId parameter indicates the ID of the host to which your API request is sent. You can locate the errors by using the error codes.

- XML format

```
<?  xml   version =" 1 . 0 "  encoding =" UTF - 8 "? >
< Error >
   < RequestId > 8906582E - 6722 - 409A - A6C4 - 0E7863B733  A5 </
 RequestId >
   < HostId > sts . aliyuncs . com </ HostId >
   < Code > InvalidPar  ameter </ Code >
   < Message > The   specified   parameter  " Action   or   Version
 "  is   not   valid . </ Message >
</ Error >
```

- JSON format

```
{
    " RequestId ": " 7463B73D - 35CC - 4D19 - A010 - 6B8D65D242  EF
 ",
    " HostId ": " sts . aliyuncs . com ",
    " Code ": " InvalidPar  ameter ",
```

```
    " Message ": " The   specified   parameter  \" Action   or
 Version \"  is   not   valid ."
}
```

3 Operation interfaces

3.1 AssumeRole

You can call this operation to obtain a temporary identity for assuming a role. In this topic, RAM users can only assume the RAM roles of the trusted Alibaba Cloud account.

Request parameters

Parameter	Type	Required	Example	Description
`Action`	String	Yes	AssumeRole	The operation that you want to perform. Set this parameter to AssumeRole.
`RoleArn`	String	Yes	acs:ram::1234567890 12****:role/adminrole	The Alibaba Cloud Resource Name (ARN) of the specified RAM role. Format: `acs : ram ::$ accountID : role /$ roleName` . Note: • `$ accountID` : specifies the Alibaba Cloud account ID. To view the account ID, log on to the Alibaba Cloud console, move your pointer over your profile picture in the upper-right corner, and then click Security Settings. • `$ roleName` : specifies the name of the RAM role. To view the role name, log on to the RAM console, and click RAM Roles in the left-side navigation pane. In the RAM Role Name column, you can view the name of the target RAM role.

Parameter	Type	Required	Example	Description
RoleSessionName	String	Yes	alice	The role session name that is specified by the user. This parameter can be used to identify the RAM user who assumes the role. Format: ^[a - zA - Z0 - 9 \. @\- _]+ $. Note: The value must be 2 to 32 characters in length. If you enter only one character, an error occurs.
Policy	String	No	{"Statement": [{"Action": ["*"],"Effect": "Allow","Resource": ["*"]}],"Version":"1"}	The policy that specifies the permissions of the generated STS token. The value can be up to 1,024 bytes in length. If you do not specify this parameter, the STS token has all permissions of the specified RAM role.
DurationSeconds	Long	No	3600	The validity period of the STS token. Unit: seconds. Valid values: 900 to 3600. Default value: 3600.

Response parameters

Parameter	Type	Example	Description
RequestId	String	6894B13B-6D71-4EF5-88FA-F32781734A7F	The ID of the request.
Credentials			The access credential.
└ 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:sts::123456789012****:assumed-role/AdminRole/alice	The ARN of the specified RAM role. Format: `acs : ram ::$ accountID : role /$ roleName` . Note: • `$ accountID` : specifies the Alibaba Cloud account ID. To view the account ID, log on to the Alibaba Cloud console, move your pointer over your profile picture in the upper-right corner, and then click Security Settings. • `$ roleName` : specifies the name of the RAM role. To view the role name, log on to the RAM console, and click RAM Roles in the left-side navigation pane. In the RAM Role Name column, you can view the name of the target RAM role.
└ AssumedRoleUserId	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 :: 1234567890  12 ****: role / adminrole
& RoleSessio  nName = alice
& DurationSe  conds = 3600
& Policy =< url_encode  d_policy >
&< Common   request   parameters >
```

Sample responses

`XML` format

```
< AssumeRole  Response >
    < RequestId > 6894B13B - 6D71 - 4EF5 - 88FA - F32781734A  7F </
 RequestId >
    < AssumedRol  eUser >
        < arn > acs : sts :: 1234567890  12 ****: assumed - role /
 AdminRole / alice </ arn >
        < AssumedRol  eUserId > 3445843393  6495 ****: alice </
 AssumedRol  eUserId >
    </ AssumedRol  eUser >
    < Credential  s >
        < AccessKeyI  d > STS . L4aBSCSJVM  uKg5U1 ****</ AccessKeyI
 d >
        < AccessKeyS  ecret > wyLTSmsyPG  P1ohvvw8xY  gB29dlGI8K
 MiH2pK ****</ AccessKeyS  ecret >
        < SecurityTo  ken >********</ SecurityTo  ken >
        < Expiration > 2015 - 04 - 09T11 : 52 : 19Z </ Expiration >
    </ Credential  s >
</ AssumeRole  Response >
```

`JSON` format

```
{
    " Credential  s ": {
        " AccessKeyI  d ": " STS . L4aBSCSJVM  uKg5U1 ****",
        " AccessKeyS  ecret ": " wyLTSmsyPG  P1ohvvw8xY  gB29dlGI8K
 MiH2pK ****",
        " Expiration ": " 2015 - 04 - 09T11 : 52 : 19Z ",
        " SecurityTo  ken ": "********"
    },
    " AssumedRol  eUser ": {
        " arn ": " acs : sts :: 1234567890  12 ****: assumed - role /
 AdminRole / alice ",
        " AssumedRol  eUserId ":" 3445843393  6495 ****: alice "
        },
    " RequestId ": " 6894B13B - 6D71 - 4EF5 - 88FA - F32781734A  7F "
```

```
}
```

Error codes

HTTP status code	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. Enter a value in the format of `^[ a - zA - Z0 - 9 \. @\- _ ]+ $`, and try again.
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 value range is from 900 to 3600.
400	InvalidParameter.PolicyGrammar	The parameter Policy has not passed grammar check.	The error message returned because the policy syntax is incorrect.

HTTP status code	Error code	Error message	Description
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 has reached the upper limit. The policy string can be up to 1,024 bytes in length.
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 permission.
500	InternalError	STS Server Internal Error happened.	The error message returned because an internal server error has occurred.

3.2 GetCallerIdentity

You can call this operation to query 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 this parameter to GetCallerIdentity.

Response parameters

Parameter	Type	Example	Description
RequestId	String	2C9BE469-4A35-44D5-9529-CAA280B11603	The ID of the request.

Parameter	Type	Example	Description
Arn	String	acs:ram::196813200012****: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 to which the user who is calling the API operation belongs. The ID only consists of digits.
UserId	String	216959339000****	· The ID of the user who is calling the API operation. If the user is a RAM user under an Alibaba Cloud account, this parameter and the AccountId parameter are returned. · If the user is the owner of an Alibaba Cloud account, the AccountId parameter is returned. The UserId parameter is not returned.
RoleId	String	33537620082992****	The ID of the RAM role that is assumed by the user who is calling the API operation. If the user uses a RAM role to call the API operation, this parameter and the AccountId parameter are returned.
PrincipalId	String	28877424437521****	The ID of the principle.
IdentityType	String	RAMUser	The type of the identity.

Examples

Sample requests

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

Sample responses

`XML` format

```
< GetCallerI  dentityRes  ponse >
```

```
    < RequestId > 2C9BE469 - 4A35 - 44D5 - 9529 - CAA280B116  03 </
 RequestId >
    < AccountId > 1968132000  12 ****</ AccountId >
    < UserId > 2169593390  00 ****</ UserId >
    < IdentityTy  pe > RAMUser </ IdentityTy  pe >
    < PrincipalI  d > 2887742443  7521 ****</ PrincipalI  d >
    < Arn > acs : ram :: 1968132000  12 ****: user / admin </ Arn >
</ GetCallerI  dentityRes  ponse >
```

`JSON` format

```
{
    " RequestId ": " 2C9BE469 - 4A35 - 44D5 - 9529 - CAA280B116  03 ",
    " AccountId ": " 1968132000  12 ****",
    " UserId ": " 2169593390  00 ****",
    " IdentityTy  pe ": " RAMUser ",
    " PrincipalI  d ": " 2887742443  7521 ****",
    " Arn ": " acs : ram :: 1968132000  12 ****: user / admin "
}
```

Error codes

None.

3.3 AssumeRoleWithSAML

You can call this operation to obtain a temporary identity for assuming a role during the role-based single sign-on (SSO).

Request parameters

Parameter	Type	Required	Example	Description
`Action`	String	Yes	AssumeRoleWithSAML	The operation that you want to perform. Set this parameter to AssumeRoleWithSAML.
`SAMLProviderArn`	String	Yes	acs:ram::1234567890 12****:saml-provider/company1	The Alibaba Cloud Resource Name (ARN) of the identity provider (IdP) that is created in the RAM console. Format: `acs : ram ::$ account_ID : saml - provider /$ saml_provi  der_ID` .
`RoleArn`	String	Yes	acs:ram::1234567890 12****:role/adminrole	The ARN of the role to be assumed. Format: `acs : ram ::$ accountID : role /$ roleName` .

Parameter	Type	Required	Example	Description
SAMLAssertion	String	Yes	<base64_encoded_saml_assertion>	The SAML assertion that is encoded by using Base64 encoding. The value must be 4 to 100,000 bytes in length.
Policy	String	No	<url_encoded_policy>	The policy that specifies the permissions of the generated STS token. The value can be up to 1,024 bytes in length . If you do not specify this parameter, the STS token has all permissions of the specified RAM role.
DurationSeconds	Long	No	3600	The validity period of the STS token. Unit: seconds. Valid values: 900 to 3600. Default value: 3600.

Response parameters

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

Parameter	Type	Example	Description
AssumedRoleUser			The temporary identity that you use to assume the role.
└ Arn	String	acs:sts::123456789012****:assumed-role/AdminRole/alice	The ARN of the temporary identity that you use to assume the role. Format: `acs : ram ::$accountID : assumed - role /$roleName /$ roleSessio nName`.
└ AssumedRoleUserId	String	34458433936495****:alice	The ID of the temporary identity to assume the role.
SAMLAssertionInfo			The information in the SAML assertion.
└ SubjectType	String	persistent	The format of the `NameID` value in the SAML assertion. If a name ID contains the `urn : oasis : names : tc : SAML : 2 . 0 : nameid - format :` prefix, the prefix is removed from the ID. For example, if the ID is urn:oasis:names:tc:SAML:2.0:nameid-format:persistant/transient, only `persistant / transient` is displayed.
└ Subject	String	alice@example.com	The value of the `Subject - NameID` field in the SAML assertion.
└ Recipient	String	https://signin.aliyun.com/saml-role/SSO	The `Recipient` attribute of the `Subject - SubjectCon firmation - SubjectCon firmationD ata` field in the SAML assertion.
└ Issuer	String	http://example.com/adfs/services/trust	The value of the `Issuer` field in the SAML assertion.

Examples

Note:

If the `SAMLAssert ion` parameter has a large amount of body text and you use the GET method to send the API request, an error may occur. Therefore, we recommend that you use the POST method to send the API request.

Sample responses

`XML` format

```
< AssumeRole  Response >
    < RequestId > 6894B13B - 6D71 - 4EF5 - 88FA - F32781734A  7F </
 RequestId >
    < AssumedRol  eUser >
        < arn > acs : sts :: 1234567890  12 ****: assumed - role /
 AdminRole / alice </ arn >
        < AssumedRol  eUserId > 3445843393  6495 ****: alice </
 AssumedRol  eUserId >
    </ AssumedRol  eUser >
    < Credential  s >
        < AccessKeyI  d > STS . L4aBSCSJVM  uKg5U1 ****</ AccessKeyI
 d >
        < AccessKeyS  ecret > wyLTSmsyPG  P1ohvvw8xY  gB29dlGI8K
 MiH2pK ****</ AccessKeyS  ecret >
        < SecurityTo  ken >*********</ SecurityTo  ken >
        < Expiration > 2015 - 04 - 09T11 : 52 : 19Z </ Expiration >
    </ Credential  s >
    < SAMLAssert  ionInfo >
        < SubjectTyp  e > persistent </ SubjectTyp  e >
        < Subject > alice @ example . com </ Subject >
        < Recipient > https :// signin . aliyun . com / saml - role /
 SSO </ Recipient >
        < Issuer > http :// example . com / adfs / services / trust </
 Issuer >
    </ SAMLAssert  ionInfo >
</ AssumeRole  Response >
```

`JSON` format

```
{
    " Credential  s ": {
        " AccessKeyI  d ": " STS . L4aBSCSJVM  uKg5U1 ****",
        " AccessKeyS  ecret ": " wyLTSmsyPG  P1ohvvw8xY  gB29dlGI8K
 MiH2pK ****",
        " Expiration ": " 2015 - 04 - 09T11 : 52 : 19Z ",
        " SecurityTo  ken ": "********"
    },
    " AssumedRol  eUser ": {
        " arn ": " acs : sts :: 1234567890  123456 : assumed - role /
 AdminRole / alice ",
        " AssumedRol  eUserId ":" 3445843393  6495 ****: alice "
        },
    " SAMLAssert  ionInfo ": {
        " SubjectTyp  e ": " 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 "
}
```

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 permission policy is invalid.
400	InvalidParameter.PolicySize	The max size of policy string is 1024 .	The error message returned because the length of the specified policy string has reached the upper limit. The policy string can be up to 1,024 bytes in length.

HTTP status code	Error code	Error message	Description
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 name 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.