Search in this guide
Contact Us English ▼ Create an AWS Account
AWS > Documentation > AWS Security Token Service > API Reference
Feedback Preferences

AWS Security Token Service
API Reference

GetSessionToken

PDF

Returns a set of temporary credentials for an AWS account or IAM user. The credentials consist of an access key ID, a secret access key, and a security token. Typically, you use `GetSessionToken` if you want to use MFA to protect programmatic calls to specific AWS API operations like Amazon EC2 `StopInstances`.

MFA-enabled IAM users must call `GetSessionToken` and submit an MFA code that is associated with their MFA device. Using the temporary security credentials that the call returns, IAM users can then make programmatic calls to API operations that require MFA authentication. An incorrect MFA code causes the API to return an access denied error. For a comparison of `GetSessionToken` with the other API operations that produce temporary credentials, see Requesting Temporary Security Credentials and Compare AWS STS credentials in the *IAM User Guide*.

> **Note**
>
> No permissions are required for users to perform this operation. The purpose of the `sts:GetSessionToken` operation is to authenticate the user using MFA. You cannot use policies to control authentication operations. For more information, see Permissions for GetSessionToken in the *IAM User Guide*.

Session Duration

The `GetSessionToken` operation must be called by using the long-term AWS security credentials of an IAM user. Credentials that are created by IAM users are valid for the duration that you specify. This duration can range from 900 seconds (15 minutes) up to a maximum of 129,600 seconds (36 hours), with a default of 43,200 seconds (12 hours). Credentials based on account credentials can range from 900 seconds

The temporary security credentials created by `GetSessionToken` can be used to make API calls to any AWS service with the following exceptions:

- You cannot call any IAM API operations unless MFA authentication information is included in the request.
- You cannot call any AWS STS API *except* `AssumeRole` or `GetCallerIdentity`.

The credentials that `GetSessionToken` returns are based on permissions associated with the IAM user whose credentials were used to call the operation. The temporary credentials have the same permissions as the IAM user.

> **Note**
>
> Although it is possible to call `GetSessionToken` using the security credentials of an AWS account root user rather than an IAM user, we do not recommend it. If `GetSessionToken` is called using root user credentials, the temporary credentials have root user permissions. For more information, see Safeguard your root user credentials and don't use them for everyday tasks in the *IAM User Guide*

For more information about using `GetSessionToken` to create temporary credentials, see Temporary Credentials for Users in Untrusted Environments in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

DurationSeconds

The duration, in seconds, that the credentials should remain valid. Acceptable durations for IAM user sessions range from 900 seconds (15 minutes) to 129,600 seconds (36 hours), with 43,200 seconds (12 hours) as the default. Sessions for owners defaults to one hour.

Type: Integer

Valid Range: Minimum value of 900. Maximum value of 129600.

Required: No

SerialNumber

The identification number of the MFA device that is associated with the IAM user who is making the `GetSessionToken` call. Specify this value if the IAM user has a policy that requires MFA authentication. The value is either the serial number for a hardware device (such as `GAHT12345678`) or an Amazon Resource Name (ARN) for a virtual device (such as `arn:aws:iam::123456789012:mfa/user`). You can find the device for an IAM user by going to the AWS Management Console and viewing the user's security credentials.

The regex used to validate this parameter is a string of characters consisting of upper- and lower-case alphanumeric characters with no spaces. You can also include underscores or any of the following characters: =,.@:/-

Type: String

Length Constraints: Minimum length of 9. Maximum length of 256.

Pattern: `[\w+=/:,.@-]*`

Required: No

TokenCode

The value provided by the MFA device, if MFA is required. If any policy requires the IAM user to submit an MFA code, specify this value. If MFA authentication is required, the user must provide a code when requesting a set of temporary security credentials. A user who fails to provide the code receives an "access denied" response when requesting resources that require MFA authentication.

The format for this parameter, as described by its regex pattern, is a sequence of six numeric digits.

Required: No

Response Elements

The following element is returned by the service.

Credentials

The temporary security credentials, which include an access key ID, a secret access key, and a security (or session) token.

> **Note**
>
> The size of the security token that AWS STS API operations return is not fixed. We strongly recommend that you make no assumptions about the maximum size.

Type: Credentials object

Errors

For information about the errors that are common to all actions, see Common Errors.

RegionDisabled

AWS STS is not activated in the requested region for the account that is being asked to generate credentials. The account administrator must use the IAM console to activate AWS STS in that region. For more information, see Activating and Deactivating AWS STS in an AWS Region in the *IAM User Guide*.

HTTP Status Code: 403

Examples

Example

This example illustrates one usage of GetSessionToken.

Sample Request

```
&DurationSeconds=3600
&Tags.member.1.Key=Project
&Tags.member.1.Value=Unicorn
&Tags.member.2.Key=Cost-Center
&Tags.member.2.Value=12345
&SerialNumber=YourMFADeviceSeria
&TokenCode=123456
&AUTHPARAMS
```

Sample Response

```
<GetSessionTokenResponse xmlns="
  <GetSessionTokenResult>
    <Credentials>
      <SessionToken>
       AQoEXAMPLEH4aoAH0gNCAPyJx
       To6UDdyJwOOvEVPvLXCrrrUtd
       rkuWJOgQs8IZZaIv2BXIa2R4C
       Z3CYWFXG8C5zqx37wnOE49mRl
      </SessionToken>
      <SecretAccessKey>
      wJalrXUtnFEMI/K7MDENG/bPxR
      </SecretAccessKey>
      <Expiration>2011-07-11T19:
      <AccessKeyId>ASIAIOSFODNN7
    </Credentials>
  </GetSessionTokenResult>
  <ResponseMetadata>
    <RequestId>58c5dbae-abef-11e
  </ResponseMetadata>
</GetSessionTokenResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Did this page help you?

Yes

Next topic: Data Types

Previous topic: GetFederationToken

IQ expert