AWS Identity and Access Management

API Reference

API Version 2010-05-08

AWS Identity and Access Management: API Reference

Table of Contents

Welcome

AWS Identity and Access Management (IAM) is a web service that you can use to manage users and user permissions under your AWS account. This guide provides descriptions of IAM actions that you can call programmatically. For general information about IAM, see AWS Identity and Access Management (IAM). For the user guide for IAM, see Using IAM.

> **Note**
> AWS provides SDKs that consist of libraries and sample code for various programming languages and platforms (Java, Ruby, .NET, iOS, Android, etc.). The SDKs provide a convenient way to create programmatic access to IAM and AWS. For example, the SDKs take care of tasks such as cryptographically signing requests (see below), managing errors, and retrying requests automatically. For information about the AWS SDKs, including how to download and install them, see the Tools for Amazon Web Services page.

We recommend that you use the AWS SDKs to make programmatic API calls to IAM. However, you can also use the IAM Query API to make direct calls to the IAM web service. To learn more about the IAM Query API, see Making Query Requests in the *Using IAM* guide. IAM supports GET and POST requests for all actions. That is, the API does not require you to use GET for some actions and POST for others. However, GET requests are subject to the limitation size of a URL. Therefore, for operations that require larger sizes, use a POST request.

Signing Requests

Requests must be signed using an access key ID and a secret access key. We strongly recommend that you do not use your AWS account access key ID and secret access key for everyday work with IAM. You can use the access key ID and secret access key for an IAM user or you can use the AWS Security Token Service to generate temporary security credentials and use those to sign requests.

To sign requests, we recommend that you use Signature Version 4. If you have an existing application that uses Signature Version 2, you do not have to update it to use Signature Version 4. However, some operations now require Signature Version 4. The documentation for operations that require version 4 indicate this requirement.

Additional Resources

For more information, see the following:

- AWS Security Credentials. This topic provides general information about the types of credentials used for accessing AWS.
- IAM Best Practices. This topic presents a list of suggestions for using the IAM service to help secure your AWS resources.
- Signing AWS API Requests. This set of topics walk you through the process of signing a request using an access key ID and secret access key.

This document was last published on December 10, 2016.

Actions

The following actions are supported:

AddClientIDToOpenIDConnectProvider

Adds a new client ID (also known as audience) to the list of client IDs already registered for the specified IAM OpenID Connect (OIDC) provider resource.

This action is idempotent; it does not fail or return an error if you add an existing client ID to the provider.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

ClientID

The client ID (also known as audience) to add to the IAM OpenID Connect provider resource.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Required: Yes

OpenIDConnectProviderArn

The Amazon Resource Name (ARN) of the IAM OpenID Connect (OIDC) provider resource to add the client ID to. You can get a list of OIDC provider ARNs by using the ListOpenIDConnectProviders (p. 178) action.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=AddClientIDToOpenIDConnectProvider
&ClientID=my-application-ID
```

```
&OpenIDConnectProviderArn=arn:aws:iam::123456789012:oidc-provider/
server.example.com
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<AddClientIDToOpenIDConnectProviderResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>e4bdcdae-4f66-11e4-aefa-bfd6aEXAMPLE</RequestId>
  </ResponseMetadata>
</AddClientIDToOpenIDConnectProviderResponse>
```

AddRoleToInstanceProfile

Adds the specified IAM role to the specified instance profile.

Note

The caller of this API must be granted the `PassRole` permission on the IAM role by a permission policy.

For more information about roles, go to Working with Roles. For more information about instance profiles, go to About Instance Profiles.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

InstanceProfileName

The name of the instance profile to update.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

RoleName

The name of the role to add.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=AddRoleToInstanceProfile
&InstanceProfileName=Webserver
&RoleName=S3Access
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<AddRoleToInstanceProfileResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>12657608-99f2-11e1-a4c3-27EXAMPLE804</RequestId>
  </ResponseMetadata>
</AddRoleToInstanceProfileResponse>
```

AddUserToGroup

Adds the specified user to the specified group.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

GroupName

The name of the group to update.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

UserName

The name of the user to add.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=AddUserToGroup
&GroupName=Managers
```

```
&UserName=Bob
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<AddUserToGroupResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</AddUserToGroupResponse>
```

AttachGroupPolicy

Attaches the specified managed policy to the specified IAM group.

You use this API to attach a managed policy to a group. To embed an inline policy in a group, use PutGroupPolicy (p. 207).

For more information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

GroupName

The name (friendly name, not ARN) of the group to attach the policy to.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

PolicyArn

The Amazon Resource Name (ARN) of the IAM policy you want to attach.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=AttachGroupPolicy
&GroupName=Finance
&PolicyArn=arn:aws:iam::aws:policy/ReadOnlyAccess
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<AttachGroupPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>f8a7b7b9-3d01-11e4-bfad-8d1c6EXAMPLE</RequestId>
  </ResponseMetadata>
</AttachGroupPolicyResponse>
```

AttachRolePolicy

Attaches the specified managed policy to the specified IAM role.

When you attach a managed policy to a role, the managed policy becomes part of the role's permission (access) policy. You cannot use a managed policy as the role's trust policy. The role's trust policy is created at the same time as the role, using CreateRole (p. 38). You can update a role's trust policy using UpdateAssumeRolePolicy (p. 239).

Use this API to attach a *managed* policy to a role. To embed an inline policy in a role, use PutRolePolicy (p. 209). For more information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

PolicyArn

The Amazon Resource Name (ARN) of the IAM policy you want to attach.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

RoleName

The name (friendly name, not ARN) of the role to attach the policy to.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=AttachRolePolicy
&PolicyArn=arn:aws:iam::aws:policy/ReadOnlyAccess
&RoleName=ReadOnlyRole
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<AttachRolePolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>37a87673-3d07-11e4-bfad-8d1c6EXAMPLE</RequestId>
  </ResponseMetadata>
</AttachRolePolicyResponse>
```

AttachUserPolicy

Attaches the specified managed policy to the specified user.

You use this API to attach a *managed* policy to a user. To embed an inline policy in a user, use PutUserPolicy (p. 211).

For more information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

PolicyArn

The Amazon Resource Name (ARN) of the IAM policy you want to attach.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

UserName

The name (friendly name, not ARN) of the IAM user to attach the policy to.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=AttachUserPolicy
&PolicyArn=arn:aws:iam::aws:policy/AdministratorAccess
&UserName=Alice
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<AttachUserPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>ed7e72d3-3d07-11e4-bfad-8d1c6EXAMPLE</RequestId>
  </ResponseMetadata>
</AttachUserPolicyResponse>
```

ChangePassword

Changes the password of the IAM user who is calling this action. The root account password is not affected by this action.

To change the password for a different user, see UpdateLoginProfile (p. 243). For more information about modifying passwords, see Managing Passwords in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

NewPassword

The new password. The new password must conform to the AWS account's password policy, if one exists.

The regex pattern used to validate this parameter is a string of characters consisting of almost any printable ASCII character from the space (\u0020) through the end of the ASCII character range (\u00FF). You can also include the tab (\u0009), line feed (\u000A), and carriage return (\u000D) characters. Although any of these characters are valid in a password, note that many tools, such as the AWS Management Console, might restrict the ability to enter certain characters because they have special meaning within that tool.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

OldPassword

The IAM user's current password.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

EntityTemporarilyUnmodifiable

The request was rejected because it referenced an entity that is temporarily unmodifiable, such as a user name that was deleted and then recreated. The error indicates that the request is likely to succeed if you try again after waiting several minutes. The error message describes the entity.

HTTP Status Code: 409

InvalidUserType

The request was rejected because the type of user for the transaction was incorrect.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

PasswordPolicyViolation

The request was rejected because the provided password did not meet the requirements imposed by the account password policy.

HTTP Status Code: 400

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=ChangePassword
&OldPassword=U79}kgds4?
&NewPassword=Lb0*1(9xpN
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ChangePasswordResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</ChangePasswordResponse>
```

CreateAccessKey

Creates a new AWS secret access key and corresponding AWS access key ID for the specified user. The default status for new keys is `Active`.

If you do not specify a user name, IAM determines the user name implicitly based on the AWS access key ID signing the request. Because this action works for access keys under the AWS account, you can use this action to manage root credentials even if the AWS account has no associated users.

For information about limits on the number of keys you can create, see Limitations on IAM Entities in the *IAM User Guide*.

Important
To ensure the security of your AWS account, the secret access key is accessible only during key and user creation. You must save the key (for example, in a text file) if you want to be able to access it again. If a secret key is lost, you can delete the access keys for the associated user and then create new keys.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

UserName

The name of the IAM user that the new key will belong to.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: No

Response Elements

The following element is returned by the service.

AccessKey

A structure with details about the access key.

Type: AccessKey (p. 269) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=CreateAccessKey
&UserName=Bob
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<CreateAccessKeyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <CreateAccessKeyResult>
    <AccessKey>
      <UserName>Bob</UserName>
      <AccessKeyId>AKIAIOSFODNN7EXAMPLE</AccessKeyId>
      <Status>Active</Status>
      <SecretAccessKey>wJalrXUtnFEMI/K7MDENG/bPxRfiCYzEXAMPLEKEY
      </SecretAccessKey>
    </AccessKey>
  </CreateAccessKeyResult>
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</CreateAccessKeyResponse>
```

CreateAccountAlias

Creates an alias for your AWS account. For information about using an AWS account alias, see Using an Alias for Your AWS Account ID in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

AccountAlias

The account alias to create.

The regex pattern used to validate this parameter is a string of characters consisting of lowercase letters, digits, and dashes. You cannot start or finish with a dash, nor can you have two dashes in a row.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 63.

Pattern: `^[a-z0-9](([a-z0-9]|-(?!-))*[a-z0-9])?$`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=CreateAccountAlias
&AccountAlias=example-corporation
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<CreateAccountAliasResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>36b5db08-f1b0-11df-8fbe-45274EXAMPLE</RequestId>
  </ResponseMetadata>
```

```
</CreateAccountAliasResponse>
```

CreateGroup

Creates a new group.

For information about the number of groups you can create, see Limitations on IAM Entities in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

GroupName

The name of the group to create. Do not include the path in this value.

The regex pattern used to validate this parameter is a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: =,.@-. The group name must be unique within the account. Group names are not distinguished by case. For example, you cannot create groups named both "ADMINS" and "admins".

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Path

The path to the group. For more information about paths, see IAM Identifiers in the *IAM User Guide*.

This parameter is optional. If it is not included, it defaults to a slash (/).

The regex pattern used to validate this parameter is a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes, containing any ASCII character from the ! (\u0021) thru the DEL character (\u007F), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: No

Response Elements

The following element is returned by the service.

Group

A structure containing details about the new group.

Type: Group (p. 276) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=CreateGroup
&GroupName=Admins
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<CreateGroupResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <CreateGroupResult>
    <Group>
      <Path>/</Path>
      <GroupName>Admins</GroupName>
      <GroupId>AGPACKCEVSQ6C2EXAMPLE</GroupId>
      <Arn>arn:aws:iam::123456789012:group/Admins</Arn>
    </Group>
  </CreateGroupResult>
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</CreateGroupResponse>
```

CreateInstanceProfile

Creates a new instance profile. For information about instance profiles, go to About Instance Profiles.

For information about the number of instance profiles you can create, see Limitations on IAM Entities in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

InstanceProfileName

The name of the instance profile to create.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Path

The path to the instance profile. For more information about paths, see IAM Identifiers in the *IAM User Guide*.

This parameter is optional. If it is not included, it defaults to a slash (/).

The regex pattern used to validate this parameter is a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes, containing any ASCII character from the ! (\u0021) thru the DEL character (\u007F), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: No

Response Elements

The following element is returned by the service.

InstanceProfile

A structure containing details about the new instance profile.

Type: InstanceProfile (p. 278) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=CreateInstanceProfile
&InstanceProfileName=Webserver
&Path=/application_abc/component_xyz/
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<CreateInstanceProfileResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <CreateInstanceProfileResult>
    <InstanceProfile>
      <InstanceProfileId>AIPAD5ARO2C5EXAMPLE3G</InstanceProfileId>
      <Roles/>
      <InstanceProfileName>Webserver</InstanceProfileName>
      <Path>/application_abc/component_xyz/</Path>
      <Arn>arn:aws:iam::123456789012:instance-profile/application_abc/
component_xyz/Webserver</Arn>
      <CreateDate>2012-05-09T16:11:10.222Z</CreateDate>
    </InstanceProfile>
  </CreateInstanceProfileResult>
  <ResponseMetadata>
    <RequestId>974142ee-99f1-11e1-a4c3-27EXAMPLE804</RequestId>
  </ResponseMetadata>
</CreateInstanceProfileResponse>
```

CreateLoginProfile

Creates a password for the specified user, giving the user the ability to access AWS services through the AWS Management Console. For more information about managing passwords, see Managing Passwords in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

Password

The new password for the user.

The regex pattern used to validate this parameter is a string of characters consisting of almost any printable ASCII character from the space (\u0020) through the end of the ASCII character range (\u00FF). You can also include the tab (\u0009), line feed (\u000A), and carriage return (\u000D) characters. Although any of these characters are valid in a password, note that many tools, such as the AWS Management Console, might restrict the ability to enter certain characters because they have special meaning within that tool.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

PasswordResetRequired

Specifies whether the user is required to set a new password on next sign-in.

Type: Boolean

Required: No

UserName

The name of the IAM user to create a password for. The user must already exist.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

Response Elements

The following element is returned by the service.

LoginProfile

A structure containing the user name and password create date.

Type: LoginProfile (p. 279) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

PasswordPolicyViolation

The request was rejected because the provided password did not meet the requirements imposed by the account password policy.

HTTP Status Code: 400

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=CreateLoginProfile
&UserName=Bob
&Password=h]6EszR}vJ*m
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<CreateLoginProfileResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <CreateLoginProfileResult>
    <LoginProfile>
      <PasswordResetRequired>false</PasswordResetRequired>
      <UserName>Bob</UserName>
      <CreateDate>2015-03-25T20:48:52.558Z</CreateDate>
    </LoginProfile>
  </CreateLoginProfileResult>
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</CreateLoginProfileResponse>
```

CreateOpenIDConnectProvider

Creates an IAM entity to describe an identity provider (IdP) that supports OpenID Connect (OIDC).

The OIDC provider that you create with this operation can be used as a principal in a role's trust policy to establish a trust relationship between AWS and the OIDC provider.

When you create the IAM OIDC provider, you specify the URL of the OIDC identity provider (IdP) to trust, a list of client IDs (also known as audiences) that identify the application or applications that are allowed to authenticate using the OIDC provider, and a list of thumbprints of the server certificate(s) that the IdP uses. You get all of this information from the OIDC IdP that you want to use for access to AWS.

> **Note**
> Because trust for the OIDC provider is ultimately derived from the IAM provider that this action creates, it is a best practice to limit access to the CreateOpenIDConnectProvider (p. 29) action to highly-privileged users.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

ClientIDList.member.N

A list of client IDs (also known as audiences). When a mobile or web app registers with an OpenID Connect provider, they establish a value that identifies the application. (This is the value that's sent as the `client_id` parameter on OAuth requests.)

You can register multiple client IDs with the same provider. For example, you might have multiple applications that use the same OIDC provider. You cannot register more than 100 client IDs with a single IAM OIDC provider.

There is no defined format for a client ID. The `CreateOpenIDConnectProviderRequest` action accepts client IDs up to 255 characters long.

Type: array of Strings

Length Constraints: Minimum length of 1. Maximum length of 255.

Required: No

ThumbprintList.member.N

A list of server certificate thumbprints for the OpenID Connect (OIDC) identity provider's server certificate(s). Typically this list includes only one entry. However, IAM lets you have up to five thumbprints for an OIDC provider. This lets you maintain multiple thumbprints if the identity provider is rotating certificates.

The server certificate thumbprint is the hex-encoded SHA-1 hash value of the X.509 certificate used by the domain where the OpenID Connect provider makes its keys available. It is always a 40-character string.

You must provide at least one thumbprint when creating an IAM OIDC provider. For example, if the OIDC provider is `server.example.com` and the provider stores its keys at "https://keys.server.example.com/openid-connect", the thumbprint string would be the hex-encoded SHA-1 hash value of the certificate used by https://keys.server.example.com.

For more information about obtaining the OIDC provider's thumbprint, see Obtaining the Thumbprint for an OpenID Connect Provider in the *IAM User Guide*.

Type: array of Strings

Length Constraints: Fixed length of 40.

Required: Yes

Url

The URL of the identity provider. The URL must begin with "https://" and should correspond to the `iss` claim in the provider's OpenID Connect ID tokens. Per the OIDC standard, path components are allowed but query parameters are not. Typically the URL consists of only a host name, like "https://server.example.org" or "https://example.com".

You cannot register the same provider multiple times in a single AWS account. If you try to submit a URL that has already been used for an OpenID Connect provider in the AWS account, you will get an error.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Required: Yes

Response Elements

The following element is returned by the service.

OpenIDConnectProviderArn

The Amazon Resource Name (ARN) of the new IAM OpenID Connect provider that is created. For more information, see OpenIDConnectProviderListEntry (p. 283).

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=CreateOpenIDConnectProvider
&ThumbprintList.list.1=c3768084dfb3d2b68b7897bf5f565da8eEXAMPLE
&ClientIDList.list.1=my-application-ID
&Url=https://server.example.com
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<CreateOpenIDConnectProviderResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
```

```
  <CreateOpenIDConnectProviderResult>
    <OpenIDConnectProviderArn>
      arn:aws:iam::123456789012:oidc-provider/server.example.com
    </OpenIDConnectProviderArn>
  </CreateOpenIDConnectProviderResult>
  <ResponseMetadata>
    <RequestId>f248366a-4f64-11e4-aefa-bfd6aEXAMPLE</RequestId>
  </ResponseMetadata>
</CreateOpenIDConnectProviderResponse>
```

CreatePolicy

Creates a new managed policy for your AWS account.

This operation creates a policy version with a version identifier of `v1` and sets v1 as the policy's default version. For more information about policy versions, see Versioning for Managed Policies in the *IAM User Guide*.

For more information about managed policies in general, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

Description

A friendly description of the policy.

Typically used to store information about the permissions defined in the policy. For example, "Grants access to production DynamoDB tables."

The policy description is immutable. After a value is assigned, it cannot be changed.

Type: String

Length Constraints: Maximum length of 1000.

Required: No

Path

The path for the policy.

For more information about paths, see IAM Identifiers in the *IAM User Guide*.

This parameter is optional. If it is not included, it defaults to a slash (/).

The regex pattern used to validate this parameter is a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes, containing any ASCII character from the ! (\u0021) thru the DEL character (\u007F), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Pattern: `((/[A-Za-z0-9\.,\+@=_-]+)*)/`

Required: No

PolicyDocument

The JSON policy document that you want to use as the content for the new policy.

The regex pattern used to validate this parameter is a string of characters consisting of any printable ASCII character ranging from the space character (\u0020) through end of the ASCII character range (\u00FF). It also includes the special characters tab (\u0009), line feed (\u000A), and carriage return (\u000D).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

PolicyName

The friendly name of the policy.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Response Elements

The following element is returned by the service.

Policy

A structure containing details about the new policy.

Type: Policy (p. 286) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

MalformedPolicyDocument

The request was rejected because the policy document was malformed. The error message describes the specific error.

HTTP Status Code: 400

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=CreatePolicy
&PolicyDocument={"Version":"2012-10-17","Statement":
[{"Effect":"Allow","Action":"s3:ListAllMyBuckets",
"Resource":"arn:aws:s3:::*"},{"Effect":"Allow","Action":
["s3:Get*","s3:List*"],"Resource":
["arn:aws:s3:::EXAMPLE-BUCKET","arn:aws:s3:::EXAMPLE-BUCKET/*"]}]}
&PolicyName=S3-read-only-example-bucket
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<CreatePolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <CreatePolicyResult>
    <Policy>
      <PolicyName>S3-read-only-example-bucket</PolicyName>
      <DefaultVersionId>v1</DefaultVersionId>
      <PolicyId>AGPACKCEVSQ6C2EXAMPLE</PolicyId>
      <Path>/</Path>
      <Arn>arn:aws:iam::123456789012:policy/S3-read-only-example-bucket</Arn>
      <AttachmentCount>0</AttachmentCount>
      <CreateDate>2014-09-15T17:36:14.673Z</CreateDate>
      <UpdateDate>2014-09-15T17:36:14.673Z</UpdateDate>
    </Policy>
  </CreatePolicyResult>
  <ResponseMetadata>
    <RequestId>ca64c9e1-3cfe-11e4-bfad-8d1c6EXAMPLE</RequestId>
  </ResponseMetadata>
</CreatePolicyResponse>
```

CreatePolicyVersion

Creates a new version of the specified managed policy. To update a managed policy, you create a new policy version. A managed policy can have up to five versions. If the policy has five versions, you must delete an existing version using DeletePolicyVersion (p. 66) before you create a new version.

Optionally, you can set the new version as the policy's default version. The default version is the version that is in effect for the IAM users, groups, and roles to which the policy is attached.

For more information about managed policy versions, see Versioning for Managed Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

PolicyArn

The Amazon Resource Name (ARN) of the IAM policy to which you want to add a new version.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

PolicyDocument

The JSON policy document that you want to use as the content for this new version of the policy.

The regex pattern used to validate this parameter is a string of characters consisting of any printable ASCII character ranging from the space character (\u0020) through end of the ASCII character range (\u00FF). It also includes the special characters tab (\u0009), line feed (\u000A), and carriage return (\u000D).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

SetAsDefault

Specifies whether to set this version as the policy's default version.

When this parameter is `true`, the new policy version becomes the operative version; that is, the version that is in effect for the IAM users, groups, and roles that the policy is attached to.

For more information about managed policy versions, see Versioning for Managed Policies in the *IAM User Guide*.

Type: Boolean

Required: No

Response Elements

The following element is returned by the service.

PolicyVersion

A structure containing details about the new policy version.

Type: PolicyVersion (p. 292) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

MalformedPolicyDocument

The request was rejected because the policy document was malformed. The error message describes the specific error.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=CreatePolicyVersion
&PolicyArn=arn:aws:iam::123456789012:policy/S3-read-only-example-bucket
&PolicyDocument={"Version":"2012-10-17","Statement":
[{"Effect":"Allow","Action":"s3:ListAllMyBuckets",
"Resource":"arn:aws:s3:::*"},{"Effect":"Allow","Action":
["s3:Get*","s3:List*"],"Resource":
["arn:aws:s3:::EXAMPLE-BUCKET","arn:aws:s3:::EXAMPLE-BUCKET/*"]},
{"Effect":"Deny","Action":"s3:*",
"Resource":["arn:aws:s3:::EXAMPLE-BUCKET","arn:aws:s3:::EXAMPLE-BUCKET/
*"],"Condition":{"StringLike":
{"s3:prefix":["SENSITIVE-FILES*"]}}}]}
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<CreatePolicyVersionResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <CreatePolicyVersionResult>
    <PolicyVersion>
      <IsDefaultVersion>false</IsDefaultVersion>
      <VersionId>v2</VersionId>
      <CreateDate>2014-09-15T19:58:59.430Z</CreateDate>
    </PolicyVersion>
  </CreatePolicyVersionResult>
  <ResponseMetadata>
    <RequestId>bb551b92-3d12-11e4-bfad-8d1c6EXAMPLE</RequestId>
  </ResponseMetadata>
```

```
</CreatePolicyVersionResponse>
```

CreateRole

Creates a new role for your AWS account. For more information about roles, go to Working with Roles. For information about limitations on role names and the number of roles you can create, go to Limitations on IAM Entities in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

AssumeRolePolicyDocument

The trust relationship policy document that grants an entity permission to assume the role.

The regex pattern used to validate this parameter is a string of characters consisting of any printable ASCII character ranging from the space character (\u0020) through end of the ASCII character range (\u00FF). It also includes the special characters tab (\u0009), line feed (\u000A), and carriage return (\u000D).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

Path

The path to the role. For more information about paths, see IAM Identifiers in the *IAM User Guide*.

This parameter is optional. If it is not included, it defaults to a slash (/).

The regex pattern used to validate this parameter is a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes, containing any ASCII character from the ! (\u0021) thru the DEL character (\u007F), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: No

RoleName

The name of the role to create.

The regex pattern used to validate this parameter is a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: =,.@-. Role names are not distinguished by case. For example, you cannot create roles named both "PRODROLE" and "prodrole".

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

Response Elements

The following element is returned by the service.

Role

A structure containing details about the new role.

Type: Role (p. 295) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

MalformedPolicyDocument

The request was rejected because the policy document was malformed. The error message describes the specific error.

HTTP Status Code: 400

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=CreateRole
&RoleName=S3Access
&Path=/application_abc/component_xyz/
&AssumeRolePolicyDocument={"Version":"2012-10-17","Statement":
[{"Effect":"Allow","Principal":{"Service":["ec2.amazonaws.com"]},"Action":
["sts:AssumeRole"]}]}
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<CreateRoleResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <CreateRoleResult>
    <Role>
      <Path>/application_abc/component_xyz/</Path>
      <Arn>arn:aws:iam::123456789012:role/application_abc/component_xyz/
S3Access</Arn>
      <RoleName>S3Access</RoleName>
      <AssumeRolePolicyDocument>
        {"Version":"2012-10-17","Statement":[{"Effect":"Allow",
        "Principal":{"Service":["ec2.amazonaws.com"]},"Action":
["sts:AssumeRole"]}]}
      </AssumeRolePolicyDocument>
      <CreateDate>2012-05-08T23:34:01.495Z</CreateDate>
      <RoleId>AROADBQP57FF2AEXAMPLE</RoleId>
    </Role>
  </CreateRoleResult>
  <ResponseMetadata>
    <RequestId>4a93ceee-9966-11e1-b624-b1aEXAMPLE7c</RequestId>
  </ResponseMetadata>
```

```
</CreateRoleResponse>
```

CreateSAMLProvider

Creates an IAM resource that describes an identity provider (IdP) that supports SAML 2.0.

The SAML provider resource that you create with this operation can be used as a principal in an IAM role's trust policy to enable federated users who sign-in using the SAML IdP to assume the role. You can create an IAM role that supports Web-based single sign-on (SSO) to the AWS Management Console or one that supports API access to AWS.

When you create the SAML provider resource, you upload an a SAML metadata document that you get from your IdP and that includes the issuer's name, expiration information, and keys that can be used to validate the SAML authentication response (assertions) that the IdP sends. You must generate the metadata document using the identity management software that is used as your organization's IdP.

> **Note**
> This operation requires Signature Version 4.

For more information, see Enabling SAML 2.0 Federated Users to Access the AWS Management Console and About SAML 2.0-based Federation in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

Name

The name of the provider to create.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w._-]+`

Required: Yes

SAMLMetadataDocument

An XML document generated by an identity provider (IdP) that supports SAML 2.0. The document includes the issuer's name, expiration information, and keys that can be used to validate the SAML authentication response (assertions) that are received from the IdP. You must generate the metadata document using the identity management software that is used as your organization's IdP.

For more information, see About SAML 2.0-based Federation in the *IAM User Guide*

Type: String

Length Constraints: Minimum length of 1000. Maximum length of 10000000.

Required: Yes

Response Elements

The following element is returned by the service.

SAMLProviderArn

The Amazon Resource Name (ARN) of the new SAML provider resource in IAM.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=CreateSAMLProvider
&Name=MyUniversity
&SAMLProviderDocument=VGhpcyBpcyB3aGVyZSB5b3UgcHV0IHRoZSBTQU1MIHByb3ZpZGVyIG1ldGFkYXRhIGRvY
LCBCYXNlNjQtZW5jb2RlZCBpbnRvIGEgYmlnIHN0cmluZy4=
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<CreateSAMLProviderResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <CreateSAMLProviderResult>
    <SAMLProviderArn>arn:aws:iam::123456789012:saml-provider/MyUniversity</
SAMLProviderArn>
  </CreateSAMLProviderResult>
  <ResponseMetadata>
    <RequestId>29f47818-99f5-11e1-a4c3-27EXAMPLE804</RequestId>
  </ResponseMetadata>
</CreateSAMLProviderResponse>
```

CreateUser

Creates a new IAM user for your AWS account.

For information about limitations on the number of IAM users you can create, see Limitations on IAM Entities in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

Path

The path for the user name. For more information about paths, see IAM Identifiers in the *IAM User Guide*.

This parameter is optional. If it is not included, it defaults to a slash (/).

The regex pattern used to validate this parameter is a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes, containing any ASCII character from the ! (\u0021) thru the DEL character (\u007F), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: No

UserName

The name of the user to create.

The regex pattern used to validate this parameter is a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: =,.@-. User names are not distinguished by case. For example, you cannot create users named both "TESTUSER" and "testuser".

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

Response Elements

The following element is returned by the service.

User

A structure with details about the new IAM user.

Type: User (p. 305) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=CreateUser
&Path=/division_abc/subdivision_xyz/
&UserName=Bob
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<CreateUserResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <CreateUserResult>
    <User>
      <Path>/division_abc/subdivision_xyz/</Path>
      <UserName>Bob</UserName>
      <UserId>AIDACKCEVSQ6C2EXAMPLE</UserId>
      <Arn>arn:aws:iam::123456789012:user/division_abc/subdivision_xyz/Bob</
Arn>
    </User>
  </CreateUserResult>
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</CreateUserResponse>
```

CreateVirtualMFADevice

Creates a new virtual MFA device for the AWS account. After creating the virtual MFA, use EnableMFADevice (p. 92) to attach the MFA device to an IAM user. For more information about creating and working with virtual MFA devices, go to Using a Virtual MFA Device in the *IAM User Guide*.

For information about limits on the number of MFA devices you can create, see Limitations on Entities in the *IAM User Guide*.

> **Important**
> The seed information contained in the QR code and the Base32 string should be treated like any other secret access information, such as your AWS access keys or your passwords. After you provision your virtual device, you should ensure that the information is destroyed following secure procedures.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

Path

The path for the virtual MFA device. For more information about paths, see IAM Identifiers in the *IAM User Guide*.

This parameter is optional. If it is not included, it defaults to a slash (/).

The regex pattern used to validate this parameter is a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes, containing any ASCII character from the ! (\u0021) thru the DEL character (\u007F), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: No

VirtualMFADeviceName

The name of the virtual MFA device. Use with path to uniquely identify a virtual MFA device.

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

Type: String

Length Constraints: Minimum length of 1.

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

Required: Yes

Response Elements

The following element is returned by the service.

VirtualMFADevice

A structure containing details about the new virtual MFA device.

Type: VirtualMFADevice (p. 309) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=CreateVirtualMFADevice
&VirtualMFADeviceName=ExampleName
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<CreateVirtualMFADeviceResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <CreateVirtualMFADeviceResult>
    <VirtualMFADevice>
      <SerialNumber>arn:aws:iam::123456789012:mfa/ExampleName</SerialNumber>
      <Base32StringSeed>
        2K5K5XTLA7GGE75TQLYEXAMPLEEXAMPLEEXAMPLECHDFW4KJYZ6UFQ75LL7COCYKM
      </Base32StringSeed>
      <QRCodePNG>
        89504E470D0A1A0AASDFAHSDFKJKLJFKALSDFJASDF <!-- byte array of png
 file -->
      </QRCodePNG>
    </VirtualMFADevice>
  </CreateVirtualMFADeviceResult>
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</CreateVirtualMFADeviceResponse>
```

DeactivateMFADevice

Deactivates the specified MFA device and removes it from association with the user name for which it was originally enabled.

For more information about creating and working with virtual MFA devices, go to Using a Virtual MFA Device in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

SerialNumber

The serial number that uniquely identifies the MFA device. For virtual MFA devices, the serial number is the device ARN.

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

Type: String

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

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

Required: Yes

UserName

The name of the user whose MFA device you want to deactivate.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

EntityTemporarilyUnmodifiable

The request was rejected because it referenced an entity that is temporarily unmodifiable, such as a user name that was deleted and then recreated. The error indicates that the request is likely to succeed if you try again after waiting several minutes. The error message describes the entity.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=DeactivateMFADevice
&UserName=Bob
&SerialNumber=R1234
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeactivateMFADeviceResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</DeactivateMFADeviceResponse>
```

DeleteAccessKey

Deletes the access key pair associated with the specified IAM user.

If you do not specify a user name, IAM determines the user name implicitly based on the AWS access key ID signing the request. Because this action works for access keys under the AWS account, you can use this action to manage root credentials even if the AWS account has no associated users.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

AccessKeyId

The access key ID for the access key ID and secret access key you want to delete.

The regex pattern used to validate this parameter is a string of characters that can consist of any upper or lowercased letter or digit.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: `[\w]+`

Required: Yes

UserName

The name of the user whose access key pair you want to delete.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: No

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteAccessKey
```

```
&UserName=Bob
&AccessKeyId=AKIAIOSFODNN7EXAMPLE
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteAccessKeyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</DeleteAccessKeyResponse>
```

DeleteAccountAlias

Deletes the specified AWS account alias. For information about using an AWS account alias, see Using an Alias for Your AWS Account ID in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

AccountAlias

The name of the account alias to delete.

The regex pattern used to validate this parameter is a string of characters consisting of lowercase letters, digits, and dashes. You cannot start or finish with a dash, nor can you have two dashes in a row.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 63.

Pattern: `^[a-z0-9](([a-z0-9]|-(?!-))*[a-z0-9])?$`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteAccountAlias
&AccountAlias=ExampleCorp
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteAccountAliasResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</DeleteAccountAliasResponse>
```

DeleteAccountPasswordPolicy

Deletes the password policy for the AWS account. There are no parameters.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteAccountPasswordPolicy
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteAccountPasswordPolicyResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</DeleteAccountPasswordPolicyResponse>
```

DeleteGroup

Deletes the specified IAM group. The group must not contain any users or have any attached policies.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

GroupName

The name of the IAM group to delete.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

DeleteConflict

The request was rejected because it attempted to delete a resource that has attached subordinate entities. The error message describes these entities.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteGroup
&GroupName=Test
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteGroupResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
```

```
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</DeleteGroupResponse>
```

DeleteGroupPolicy

Deletes the specified inline policy that is embedded in the specified IAM group.

A group can also have managed policies attached to it. To detach a managed policy from a group, use DetachGroupPolicy (p. 86). For more information about policies, refer to Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

GroupName

The name (friendly name, not ARN) identifying the group that the policy is embedded in.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

PolicyName

The name identifying the policy document to delete.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteGroupPolicy
&GroupName=Admins
&PolicyName=AdminFullAccess
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteGroupPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</DeleteGroupPolicyResponse>
```

DeleteInstanceProfile

Deletes the specified instance profile. The instance profile must not have an associated role.

> **Important**
>
> Make sure you do not have any Amazon EC2 instances running with the instance profile you are about to delete. Deleting a role or instance profile that is associated with a running instance will break any applications running on the instance.

For more information about instance profiles, go to About Instance Profiles.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

InstanceProfileName

The name of the instance profile to delete.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

DeleteConflict

The request was rejected because it attempted to delete a resource that has attached subordinate entities. The error message describes these entities.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteInstanceProfile
&InstanceProfileName=Webserver
&Version=2010-05-08
```

```
&AUTHPARAMS
```

Sample Response

```
<DeleteInstanceProfileResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>90c18667-99f3-11e1-a4c3-27EXAMPLE804</RequestId>
  </ResponseMetadata>
</DeleteInstanceProfileResponse>
```

DeleteLoginProfile

Deletes the password for the specified IAM user, which terminates the user's ability to access AWS services through the AWS Management Console.

Important
Deleting a user's password does not prevent a user from accessing AWS through the command line interface or the API. To prevent all user access you must also either make any access keys inactive or delete them. For more information about making keys inactive or deleting them, see UpdateAccessKey (p. 234) and DeleteAccessKey (p. 49).

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

UserName

The name of the user whose password you want to delete.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

EntityTemporarilyUnmodifiable

The request was rejected because it referenced an entity that is temporarily unmodifiable, such as a user name that was deleted and then recreated. The error indicates that the request is likely to succeed if you try again after waiting several minutes. The error message describes the entity.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteLoginProfile
```

```
&UserName=Bob
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteLoginProfileResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</DeleteLoginProfileResponse>
```

DeleteOpenIDConnectProvider

Deletes an OpenID Connect identity provider (IdP) resource object in IAM.

Deleting an IAM OIDC provider resource does not update any roles that reference the provider as a principal in their trust policies. Any attempt to assume a role that references a deleted provider fails.

This action is idempotent; it does not fail or return an error if you call the action for a provider that does not exist.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

OpenIDConnectProviderArn

The Amazon Resource Name (ARN) of the IAM OpenID Connect provider resource object to delete. You can get a list of OpenID Connect provider resource ARNs by using the ListOpenIDConnectProviders (p. 178) action.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteOpenIDConnectProvider
&OpenIDConnectProviderArn=arn:aws:iam::123456789012:oidc-provider/
server.example.com
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteOpenIDConnectProviderResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
```

```
  <ResponseMetadata>
    <RequestId>b5e49e29-4f64-11e4-aefa-bfd6aEXAMPLE</RequestId>
  </ResponseMetadata>
</DeleteOpenIDConnectProviderResponse>
```

DeletePolicy

Deletes the specified managed policy.

Before you can delete a managed policy, you must first detach the policy from all users, groups, and roles that it is attached to, and you must delete all of the policy's versions. The following steps describe the process for deleting a managed policy:

- Detach the policy from all users, groups, and roles that the policy is attached to, using the DetachUserPolicy (p. 90), DetachGroupPolicy (p. 86), or DetachRolePolicy (p. 88) APIs. To list all the users, groups, and roles that a policy is attached to, use ListEntitiesForPolicy (p. 160).
- Delete all versions of the policy using DeletePolicyVersion (p. 66). To list the policy's versions, use ListPolicyVersions (p. 182). You cannot use DeletePolicyVersion (p. 66) to delete the version that is marked as the default version. You delete the policy's default version in the next step of the process.
- Delete the policy (this automatically deletes the policy's default version) using this API.

For information about managed policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

PolicyArn

The Amazon Resource Name (ARN) of the IAM policy you want to delete.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

DeleteConflict

The request was rejected because it attempted to delete a resource that has attached subordinate entities. The error message describes these entities.

HTTP Status Code: 409

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=DeletePolicy
&PolicyArn=arn:aws:iam::123456789012:policy/S3-read-only-example-bucket
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeletePolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>4706281b-3d19-11e4-a4a0-cffb9EXAMPLE</RequestId>
  </ResponseMetadata>
</DeletePolicyResponse>
```

DeletePolicyVersion

Deletes the specified version from the specified managed policy.

You cannot delete the default version from a policy using this API. To delete the default version from a policy, use DeletePolicy (p. 64). To find out which version of a policy is marked as the default version, use ListPolicyVersions (p. 182).

For information about versions for managed policies, see Versioning for Managed Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

PolicyArn

The Amazon Resource Name (ARN) of the IAM policy from which you want to delete a version.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

VersionId

The policy version to delete.

The regex pattern used to validate this parameter is a string of characters that consists of the lowercase letter 'v' followed by one or two digits, and optionally followed by a period '.' and a string of letters and digits.

For more information about managed policy versions, see Versioning for Managed Policies in the *IAM User Guide*.

Type: String

Pattern: `v[1-9][0-9]*(\.[A-Za-z0-9-]*)?`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

DeleteConflict

The request was rejected because it attempted to delete a resource that has attached subordinate entities. The error message describes these entities.

HTTP Status Code: 409

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=DeletePolicyVersion
&PolicyArn=arn:aws:iam::123456789012:policy/S3-read-only-example-bucket
&VersionId=v2
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeletePolicyVersionResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>268e1556-3d19-11e4-a4a0-cffb9EXAMPLE</RequestId>
  </ResponseMetadata>
</DeletePolicyVersionResponse>
```

DeleteRole

Deletes the specified role. The role must not have any policies attached. For more information about roles, go to Working with Roles.

Important
Make sure you do not have any Amazon EC2 instances running with the role you are about to delete. Deleting a role or instance profile that is associated with a running instance will break any applications running on the instance.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

RoleName

The name of the role to delete.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

DeleteConflict

The request was rejected because it attempted to delete a resource that has attached subordinate entities. The error message describes these entities.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteRole
&RoleName=S3Access
&Version=2010-05-08
```

```
&AUTHPARAMS
```

Sample Response

```
<DeleteRoleResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>913e3f37-99ed-11e1-a4c3-270EXAMPLE04</RequestId>
  </ResponseMetadata>
</DeleteRoleResponse>
```

DeleteRolePolicy

Deletes the specified inline policy that is embedded in the specified IAM role.

A role can also have managed policies attached to it. To detach a managed policy from a role, use DetachRolePolicy (p. 88). For more information about policies, refer to Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

PolicyName

The name of the inline policy to delete from the specified IAM role.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

RoleName

The name (friendly name, not ARN) identifying the role that the policy is embedded in.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteRolePolicy
&PolicyName=S3AccessPolicy
&RoleName=S3Access
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteRolePolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>c749ee7f-99ef-11e1-a4c3-27EXAMPLE804</RequestId>
  </ResponseMetadata>
</DeleteRolePolicyResponse>
```

DeleteSAMLProvider

Deletes a SAML provider resource in IAM.

Deleting the provider resource from IAM does not update any roles that reference the SAML provider resource's ARN as a principal in their trust policies. Any attempt to assume a role that references a non-existent provider resource ARN fails.

Note

This operation requires Signature Version 4.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

SAMLProviderArn

The Amazon Resource Name (ARN) of the SAML provider to delete.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteSAMLProvider
&SAMLProviderArn=arn:aws:iam::123456789012:saml-provider/MyUniversity
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteSAMLProviderResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>c749ee7f-99ef-11e1-a4c3-27EXAMPLE804</RequestId>
  </ResponseMetadata>
</DeleteSAMLProviderResponse>
```

DeleteServerCertificate

Deletes the specified server certificate.

For more information about working with server certificates, including a list of AWS services that can use the server certificates that you manage with IAM, go to Working with Server Certificates in the *IAM User Guide*.

> **Important**
> If you are using a server certificate with Elastic Load Balancing, deleting the certificate could have implications for your application. If Elastic Load Balancing doesn't detect the deletion of bound certificates, it may continue to use the certificates. This could cause Elastic Load Balancing to stop accepting traffic. We recommend that you remove the reference to the certificate from Elastic Load Balancing before using this command to delete the certificate. For more information, go to DeleteLoadBalancerListeners in the *Elastic Load Balancing API Reference*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

ServerCertificateName

The name of the server certificate you want to delete.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

DeleteConflict

The request was rejected because it attempted to delete a resource that has attached subordinate entities. The error message describes these entities.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteServerCertificate
&ServerCertificateName=ProdServerCert
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteServerCertificateResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</DeleteServerCertificateResponse>
```

DeleteSigningCertificate

Deletes a signing certificate associated with the specified IAM user.

If you do not specify a user name, IAM determines the user name implicitly based on the AWS access key ID signing the request. Because this action works for access keys under the AWS account, you can use this action to manage root credentials even if the AWS account has no associated IAM users.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

CertificateId

The ID of the signing certificate to delete.

The format of this parameter, as described by its regex pattern, is a string of characters that can be upper- or lower-cased letters or digits.

Type: String

Length Constraints: Minimum length of 24. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

UserName

The name of the user the signing certificate belongs to.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: No

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteSigningCertificate
```

```
&UserName=Bob
&CertificateId=TA7SMP42TDN5Z26OBPJE7EXAMPLE
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteSigningCertificateResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</DeleteSigningCertificateResponse>
```

DeleteSSHPublicKey

Deletes the specified SSH public key.

The SSH public key deleted by this action is used only for authenticating the associated IAM user to an AWS CodeCommit repository. For more information about using SSH keys to authenticate to an AWS CodeCommit repository, see Set up AWS CodeCommit for SSH Connections in the *AWS CodeCommit User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

SSHPublicKeyId

The unique identifier for the SSH public key.

The regex pattern used to validate this parameter is a string of characters that can consist of any upper or lowercased letter or digit.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

UserName

The name of the IAM user associated with the SSH public key.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

Example

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteSSHPublicKey
&SSHPublicKeyId=APKAEIVFHP46CEXAMPLE
&UserName=Jane
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteSSHPublicKeyResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>1a21282e-f36e-11e4-a53b-6b544EXAMPLE</RequestId>
  </ResponseMetadata>
</DeleteSSHPublicKeyResponse>
```

DeleteUser

Deletes the specified IAM user. The user must not belong to any groups or have any access keys, signing certificates, or attached policies.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

UserName

The name of the user to delete.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

DeleteConflict

The request was rejected because it attempted to delete a resource that has attached subordinate entities. The error message describes these entities.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteUser
&UserName=Bob
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteUserResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</DeleteUserResponse>
```

DeleteUserPolicy

Deletes the specified inline policy that is embedded in the specified IAM user.

A user can also have managed policies attached to it. To detach a managed policy from a user, use DetachUserPolicy (p. 90). For more information about policies, refer to Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

PolicyName

The name identifying the policy document to delete.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

UserName

The name (friendly name, not ARN) identifying the user that the policy is embedded in.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteUserPolicy
&UserName=Bob
&PolicyName=AllAccessPolicy
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteUserPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</DeleteUserPolicyResponse>
```

DeleteVirtualMFADevice

Deletes a virtual MFA device.

Note
You must deactivate a user's virtual MFA device before you can delete it. For information about deactivating MFA devices, see DeactivateMFADevice (p. 47).

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

SerialNumber

The serial number that uniquely identifies the MFA device. For virtual MFA devices, the serial number is the same as the ARN.

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

Type: String

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

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

DeleteConflict

The request was rejected because it attempted to delete a resource that has attached subordinate entities. The error message describes these entities.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteVirtualMFADevice
&SerialNumber=arn:aws:iam::123456789012:mfa/ExampleName
&Version=2010-05-08
```

```
&AUTHPARAMS
```

Sample Response

```
<DeleteVirtualMFADeviceResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</DeleteVirtualMFADeviceResponse>
```

DetachGroupPolicy

Removes the specified managed policy from the specified IAM group.

A group can also have inline policies embedded with it. To delete an inline policy, use the DeleteGroupPolicy (p. 56) API. For information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

GroupName

The name (friendly name, not ARN) of the IAM group to detach the policy from.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

PolicyArn

The Amazon Resource Name (ARN) of the IAM policy you want to detach.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=DetachGroupPolicy
&GroupName=Finance
&PolicyArn=arn:aws:iam::aws:policy/ReadOnlyAccess
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DetachGroupPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>d4faa7aa-3d1d-11e4-a4a0-cffb9EXAMPLE</RequestId>
  </ResponseMetadata>
</DetachGroupPolicyResponse>
```

DetachRolePolicy

Removes the specified managed policy from the specified role.

A role can also have inline policies embedded with it. To delete an inline policy, use the DeleteRolePolicy (p. 70) API. For information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

PolicyArn

The Amazon Resource Name (ARN) of the IAM policy you want to detach.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

RoleName

The name (friendly name, not ARN) of the IAM role to detach the policy from.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=DetachRolePolicy
&PolicyArn=arn:aws:iam::aws:policy/ReadOnlyAccess
&RoleName=ReadOnlyRole
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DetachRolePolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>4c80ccf4-3d1e-11e4-a4a0-cffb9EXAMPLE</RequestId>
  </ResponseMetadata>
</DetachRolePolicyResponse>
```

DetachUserPolicy

Removes the specified managed policy from the specified user.

A user can also have inline policies embedded with it. To delete an inline policy, use the DeleteUserPolicy (p. 82) API. For information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

PolicyArn

The Amazon Resource Name (ARN) of the IAM policy you want to detach.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

UserName

The name (friendly name, not ARN) of the IAM user to detach the policy from.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=DetachUserPolicy
&PolicyArn=arn:aws:iam::aws:policy/AdministratorAccess
&UserName=Alice
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DetachUserPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>85ba31fa-3d1f-11e4-a4a0-cffb9EXAMPLE</RequestId>
  </ResponseMetadata>
</DetachUserPolicyResponse>
```

EnableMFADevice

Enables the specified MFA device and associates it with the specified IAM user. When enabled, the MFA device is required for every subsequent login by the IAM user associated with the device.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

AuthenticationCode1

An authentication code emitted by the device.

The format for this parameter is a string of 6 digits.

Type: String

Length Constraints: Fixed length of 6.

Pattern: `[\d]+`

Required: Yes

AuthenticationCode2

A subsequent authentication code emitted by the device.

The format for this parameter is a string of 6 digits.

Type: String

Length Constraints: Fixed length of 6.

Pattern: `[\d]+`

Required: Yes

SerialNumber

The serial number that uniquely identifies the MFA device. For virtual MFA devices, the serial number is the device ARN.

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

Type: String

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

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

Required: Yes

UserName

The name of the IAM user for whom you want to enable the MFA device.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

EntityTemporarilyUnmodifiable

The request was rejected because it referenced an entity that is temporarily unmodifiable, such as a user name that was deleted and then recreated. The error indicates that the request is likely to succeed if you try again after waiting several minutes. The error message describes the entity.

HTTP Status Code: 409

InvalidAuthenticationCode

The request was rejected because the authentication code was not recognized. The error message describes the specific error.

HTTP Status Code: 403

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=EnableMFADevice
&UserName=Bob
&SerialNumber=R1234
&AuthenticationCode1=234567
&AuthenticationCode2=987654
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<EnableMFADeviceResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</EnableMFADeviceResponse>
```

GenerateCredentialReport

Generates a credential report for the AWS account. For more information about the credential report, see Getting Credential Reports in the *IAM User Guide*.

Response Elements

The following elements are returned by the service.

Description

Information about the credential report.

Type: String

State

Information about the state of the credential report.

Type: String

Valid Values: `STARTED | INPROGRESS | COMPLETE`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=GenerateCredentialReport
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GenerateCredentialReportResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <GenerateCredentialReportResult>
    <Description>No report exists. Starting a new report generation task</
Description>
    <State>STARTED</State>
  </GenerateCredentialReportResult>
  <ResponseMetadata>
    <RequestId>29f47818-99f5-11e1-a4c3-27EXAMPLE804</RequestId>
  </ResponseMetadata>
</GenerateCredentialReportResponse>
```

GetAccessKeyLastUsed

Retrieves information about when the specified access key was last used. The information includes the date and time of last use, along with the AWS service and region that were specified in the last request made with that key.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

AccessKeyId

The identifier of an access key.

The regex pattern used to validate this parameter is a string of characters that can consist of any upper or lowercased letter or digit.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: `[\w]+`

Required: Yes

Response Elements

The following elements are returned by the service.

AccessKeyLastUsed

Contains information about the last time the access key was used.

Type: AccessKeyLastUsed (p. 270) object

UserName

The name of the AWS IAM user that owns this access key.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

Example

Sample Request

```
https://iam.amazonaws.com/
?Action=GetAccessKeyLastUsed
&AccessKeyId=AKIAIOSFODNN7EXAMPLE
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetAccessKeyLastUsedResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <GetAccessKeyLastUsedResult>
    <AccessKeyLastUsed>
      <Region>us-west-2</Region>
      <LastUsedDate>2015-03-13T10:45:00Z</LastUsedDate>
      <ServiceName>s3</ServiceName>
    </AccessKeyLastUsed>
    <UserName>bob</UserName>
  </GetAccessKeyLastUsedResult>
  <ResponseMetadata>
    <RequestId>510a6abf-d022-11e4-abe8-9b0ebEXAMPLE</RequestId>
  </ResponseMetadata>
</GetAccessKeyLastUsedResponse>
```

GetAccountAuthorizationDetails

Retrieves information about all IAM users, groups, roles, and policies in your AWS account, including their relationships to one another. Use this API to obtain a snapshot of the configuration of IAM permissions (users, groups, roles, and policies) in your account.

You can optionally filter the results using the `Filter` parameter. You can paginate the results using the `MaxItems` and `Marker` parameters.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

Filter.member.N

A list of entity types used to filter the results. Only the entities that match the types you specify are included in the output. Use the value `LocalManagedPolicy` to include customer managed policies.

The format for this parameter is a comma-separated (if more than one) list of strings. Each string value in the list must be one of the valid values listed below.

Type: array of Strings

Valid Values: `User | Role | Group | LocalManagedPolicy | AWSManagedPolicy`

Required: No

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

This parameter is optional. If you do not include it, it defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true` and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

Response Elements

The following elements are returned by the service.

GroupDetailList.member.N

A list containing information about IAM groups.

Type: array of GroupDetail (p. 277) objects

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Policies.member.N

A list containing information about managed policies.

Type: array of ManagedPolicyDetail (p. 280) objects

RoleDetailList.member.N

A list containing information about IAM roles.

Type: array of RoleDetail (p. 296) objects

UserDetailList.member.N

A list containing information about IAM users.

Type: array of UserDetail (p. 307) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=GetAccountAuthorizationDetails
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetAccountAuthorizationDetailsResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <GetAccountAuthorizationDetailsResult>
    <IsTruncated>true</IsTruncated>
    <UserDetailList>
      <member>
        <GroupList>
          <member>Admins</member>
        </GroupList>
        <AttachedManagedPolicies/>
        <UserId>AIDACKCEVSQ6C2EXAMPLE</UserId>
        <Path>/</Path>
        <UserName>Alice</UserName>
        <Arn>arn:aws:iam::123456789012:user/Alice</Arn>
        <CreateDate>2013-10-14T18:32:24Z</CreateDate>
      </member>
      <member>
        <GroupList>
          <member>Admins</member>
        </GroupList>
        <AttachedManagedPolicies/>
        <UserPolicyList>
          <member>
            <PolicyName>DenyBillingAndIAMPolicy</PolicyName>
            <PolicyDocument>
              {"Version":"2012-10-17","Statement":{"Effect":"Deny","Action":
              ["aws-portal:*","iam:*"],"Resource":"*"}}
            </PolicyDocument>
          </member>
        </UserPolicyList>
        <UserId>AIDACKCEVSQ6C3EXAMPLE</UserId>
        <Path>/</Path>
        <UserName>Bob</UserName>
        <Arn>arn:aws:iam::123456789012:user/Bob</Arn>
        <CreateDate>2013-10-14T18:32:25Z</CreateDate>
      </member>
      <member>
        <GroupList>
          <member>Dev</member>
        <AttachedManagedPolicies/>
        </GroupList>
        <UserId>AIDACKCEVSQ6C4EXAMPLE</UserId>
        <Path>/</Path>
        <UserName>Charlie</UserName>
        <Arn>arn:aws:iam::123456789012:user/Charlie</Arn>
        <CreateDate>2013-10-14T18:33:56Z</CreateDate>
      </member>
      <member>
        <GroupList>
          <member>Dev</member>
        </GroupList>
        <AttachedManagedPolicies/>
        <UserId>AIDACKCEVSQ6C5EXAMPLE</UserId>
        <Path>/</Path>
        <UserName>Danielle</UserName>
        <Arn>arn:aws:iam::123456789012:user/Danielle</Arn>
        <CreateDate>2013-10-14T18:33:56Z</CreateDate>
      </member>
      <member>
        <GroupList>
          <member>Finance</member>
        </GroupList>
        <AttachedManagedPolicies/>
        <UserId>AIDACKCEVSQ6C6EXAMPLE</UserId>
        <Path>/</Path>
        <UserName>Elaine</UserName>
        <Arn>arn:aws:iam::123456789012:user/Elaine</Arn>
        <CreateDate>2013-10-14T18:57:48Z</CreateDate>
      </member>
    </UserDetailList>
    <Marker>
      EXAMPLEkakv9BCuUNFDtxWSyfzetYwEx2ADc8dnzfvERF5S6YMvXKx41t6gCl/
eeaCX3Jo94/
```

```
      bKqezEAg8TEVS99EKFLxm3jtbpl25FDWEXAMPLE
    </Marker>
    <GroupDetailList>
      <member>
        <GroupId>AIDACKCEVSQ6C7EXAMPLE</GroupId>
        <AttachedManagedPolicies>
          <member>
            <PolicyName>AdministratorAccess</PolicyName>
            <PolicyArn>arn:aws:iam::aws:policy/AdministratorAccess</
PolicyArn>
          </member>
        </AttachedManagedPolicies>
        <GroupName>Admins</GroupName>
        <Path>/</Path>
        <Arn>arn:aws:iam::123456789012:group/Admins</Arn>
        <CreateDate>2013-10-14T18:32:24Z</CreateDate>
        <GroupPolicyList/>
      </member>
      <member>
        <GroupId>AIDACKCEVSQ6C8EXAMPLE</GroupId>
        <AttachedManagedPolicies>
          <member>
            <PolicyName>PowerUserAccess</PolicyName>
            <PolicyArn>arn:aws:iam::aws:policy/PowerUserAccess</PolicyArn>
          </member>
        </AttachedManagedPolicies>
        <GroupName>Dev</GroupName>
        <Path>/</Path>
        <Arn>arn:aws:iam::123456789012:group/Dev</Arn>
        <CreateDate>2013-10-14T18:33:55Z</CreateDate>
        <GroupPolicyList/>
      </member>
      <member>
        <GroupId>AIDACKCEVSQ6C9EXAMPLE</GroupId>
        <AttachedManagedPolicies/>
        <GroupName>Finance</GroupName>
        <Path>/</Path>
        <Arn>arn:aws:iam::123456789012:group/Finance</Arn>
        <CreateDate>2013-10-14T18:57:48Z</CreateDate>
        <GroupPolicyList>
          <member>
            <PolicyName>policygen-201310141157</PolicyName>
            <PolicyDocument>
              {"Version":"2012-10-17","Statement":[{"Action":["aws-
portal:*"],
              "Sid":"Stmt1381777017000","Resource":["*"],"Effect":"Allow"}]}
            </PolicyDocument>
          </member>
        </GroupPolicyList>
      </member>
    </GroupDetailList>
    <RoleDetailList>
      <member>
        <RolePolicyList/>
        <AttachedManagedPolicies>
          <member>
            <PolicyName>AmazonS3FullAccess</PolicyName>
            <PolicyArn>arn:aws:iam::aws:policy/AmazonS3FullAccess</PolicyArn>
          </member>
          <member>
            <PolicyName>AmazonDynamoDBFullAccess</PolicyName>
            <PolicyArn>arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess</
PolicyArn>
          </member>
        </AttachedManagedPolicies>
        <InstanceProfileList>
          <member>
            <InstanceProfileName>EC2role</InstanceProfileName>
            <Roles>
              <member>
                <Path>/</Path>
                <Arn>arn:aws:iam::123456789012:role/EC2role</Arn>
                <RoleName>EC2role</RoleName>
                <AssumeRolePolicyDocument>
                  {"Version":"2012-10-17","Statement":[{"Sid":"",
                  "Effect":"Allow","Principal":
{"Service":"ec2.amazonaws.com"},
                  "Action":"sts:AssumeRole"}]}
                </AssumeRolePolicyDocument>
                <CreateDate>2014-07-30T17:09:20Z</CreateDate>
                <RoleId>AROAFP4BKI7Y7TEXAMPLE</RoleId>
              </member>
            </Roles>
            <Path>/</Path>
            <Arn>arn:aws:iam::123456789012:instance-profile/EC2role</Arn>
            <InstanceProfileId>AIPAFFYRBHWXW2EXAMPLE</InstanceProfileId>
            <CreateDate>2014-07-30T17:09:20Z</CreateDate>
          </member>
        </InstanceProfileList>
        <Path>/</Path>
        <Arn>arn:aws:iam::123456789012:role/EC2role</Arn>
        <RoleName>EC2role</RoleName>
        <AssumeRolePolicyDocument>
          {"Version":"2012-10-17","Statement":[{"Sid":"","Effect":"Allow",
          "Principal":{"Service":"ec2.amazonaws.com"},
          "Action":"sts:AssumeRole"}]}
        </AssumeRolePolicyDocument>
        <CreateDate>2014-07-30T17:09:20Z</CreateDate>
        <RoleId>AROAFP4BKI7Y7TEXAMPLE</RoleId>
      </member>
    </RoleDetailList>
    <Policies>
      <member>
        <PolicyName>create-update-delete-set-managed-policies</PolicyName>
        <DefaultVersionId>v1</DefaultVersionId>
        <PolicyId>ANPAJ2UCCR6DPCEXAMPLE</PolicyId>
        <Path>/</Path>
        <PolicyVersionList>
          <member>
            <Document>
              {"Version":"2012-10-17","Statement":{"Effect":"Allow",
              "Action":["iam:CreatePolicy","iam:CreatePolicyVersion",
              "iam:DeletePolicy","iam:DeletePolicyVersion","iam:GetPolicy",
              "iam:GetPolicyVersion","iam:ListPolicies",
              "iam:ListPolicyVersions","iam:SetDefaultPolicyVersion"],
              "Resource":"*"}}
            </Document>
            <IsDefaultVersion>true</IsDefaultVersion>
            <VersionId>v1</VersionId>
            <CreateDate>2015-02-06T19:58:34Z</CreateDate>
          </member>
        </PolicyVersionList>
        <Arn>
          arn:aws:iam::123456789012:policy/create-update-delete-set-managed-
policies
        </Arn>
        <AttachmentCount>1</AttachmentCount>
        <CreateDate>2015-02-06T19:58:34Z</CreateDate>
        <IsAttachable>true</IsAttachable>
        <UpdateDate>2015-02-06T19:58:34Z</UpdateDate>
      </member>
      <member>
        <PolicyName>S3-read-only-specific-bucket</PolicyName>
        <DefaultVersionId>v1</DefaultVersionId>
        <PolicyId>ANPAJ4AE5446DAEXAMPLE</PolicyId>
        <Path>/</Path>
        <PolicyVersionList>
          <member>
            <Document>
              {"Version":"2012-10-17","Statement":
[{"Effect":"Allow","Action":
              ["s3:Get*","s3:List*"],"Resource":["arn:aws:s3:::example-
bucket",
              "arn:aws:s3:::example-bucket/*"]}]}
            </Document>
            <IsDefaultVersion>true</IsDefaultVersion>
            <VersionId>v1</VersionId>
            <CreateDate>2015-01-21T21:39:41Z</CreateDate>
          </member>
        </PolicyVersionList>
        <Arn>arn:aws:iam::123456789012:policy/S3-read-only-specific-bucket</
Arn>
        <AttachmentCount>1</AttachmentCount>
        <CreateDate>2015-01-21T21:39:41Z</CreateDate>
        <IsAttachable>true</IsAttachable>
        <UpdateDate>2015-01-21T23:39:41Z</UpdateDate>
      </member>
      <member>
        <PolicyName>AWSOpsWorksRole</PolicyName>
        <DefaultVersionId>v1</DefaultVersionId>
        <PolicyId>ANPAE376NQ77WV6KGJEBE</PolicyId>
        <Path>/service-role/</Path>
        <PolicyVersionList>
          <member>
            <Document>
              {"Version":"2012-10-17","Statement":
[{"Effect":"Allow","Action":

 ["cloudwatch:GetMetricStatistics","ec2:DescribeAccountAttributes",
              "ec2:DescribeAvailabilityZones","ec2:DescribeInstances",

 "ec2:DescribeKeyPairs","ec2:DescribeSecurityGroups","ec2:DescribeSubnets",

 "ec2:DescribeVpcs","elasticloadbalancing:DescribeInstanceHealth",

 "elasticloadbalancing:DescribeLoadBalancers","iam:GetRolePolicy",
              "iam:ListInstanceProfiles","iam:ListRoles","iam:ListUsers",
              "iam:PassRole","opsworks:*","rds:*"],"Resource":["*"]}]}
            </Document>
            <IsDefaultVersion>true</IsDefaultVersion>
            <VersionId>v1</VersionId>
            <CreateDate>2014-12-10T22:57:47Z</CreateDate>
          </member>
        </PolicyVersionList>
        <Arn>arn:aws:iam::aws:policy/service-role/AWSOpsWorksRole</Arn>
        <AttachmentCount>1</AttachmentCount>
        <CreateDate>2015-02-06T18:41:27Z</CreateDate>
        <IsAttachable>true</IsAttachable>
        <UpdateDate>2015-02-06T18:41:27Z</UpdateDate>
      </member>
      <member>
        <PolicyName>AmazonEC2FullAccess</PolicyName>
        <DefaultVersionId>v1</DefaultVersionId>
        <PolicyId>ANPAE3QWE5YT46TQ34WLG</PolicyId>
        <Path>/</Path>
        <PolicyVersionList>
          <member>
            <Document>
              {"Version":"2012-10-17","Statement":[{"Action":"ec2:*",
              "Effect":"Allow","Resource":"*"},{"Effect":"Allow",
              "Action":"elasticloadbalancing:*","Resource":"*"},
{"Effect":"Allow",
              "Action":"cloudwatch:*","Resource":"*"},{"Effect":"Allow",
              "Action":"autoscaling:*","Resource":"*"}]}
            </Document>
            <IsDefaultVersion>true</IsDefaultVersion>
            <VersionId>v1</VersionId>
            <CreateDate>2014-10-30T20:59:46Z</CreateDate>
          </member>
        </PolicyVersionList>
        <Arn>arn:aws:iam::aws:policy/AmazonEC2FullAccess</Arn>
        <AttachmentCount>1</AttachmentCount>
        <CreateDate>2015-02-06T18:40:15Z</CreateDate>
        <IsAttachable>true</IsAttachable>
        <UpdateDate>2015-02-06T18:40:15Z</UpdateDate>
      </member>
    </Policies>
  </GetAccountAuthorizationDetailsResult>
  <ResponseMetadata>
    <RequestId>92e79ae7-7399-11e4-8c85-4b53eEXAMPLE</RequestId>
  </ResponseMetadata>
</GetAccountAuthorizationDetailsResponse>
```

GetAccountPasswordPolicy

Retrieves the password policy for the AWS account. For more information about using a password policy, go to Managing an IAM Password Policy.

Response Elements

The following element is returned by the service.

PasswordPolicy

Contains information about the account password policy.

Type: PasswordPolicy (p. 284) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=GetAccountPasswordPolicy
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetAccountPasswordPolicyResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <GetAccountPasswordPolicyResult>
    <PasswordPolicy>
      <AllowUsersToChangePassword>true</AllowUsersToChangePassword>
      <RequireUppercaseCharacters>true</RequireUppercaseCharacters>
      <RequireSymbols>true</RequireSymbols>
      <ExpirePasswords>false</ExpirePasswords>
      <PasswordReusePrevention>12</PasswordReusePrevention>
      <RequireLowercaseCharacters>true</RequireLowercaseCharacters>
      <MaxPasswordAge>90</MaxPasswordAge>
      <HardExpiry>false</HardExpiry>
      <RequireNumbers>true</RequireNumbers>
      <MinimumPasswordLength>12</MinimumPasswordLength>
    </PasswordPolicy>
  </GetAccountPasswordPolicyResult>
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</GetAccountPasswordPolicyResponse>
```

GetAccountSummary

Retrieves information about IAM entity usage and IAM quotas in the AWS account.

For information about limitations on IAM entities, see Limitations on IAM Entities in the *IAM User Guide*.

Response Elements

The following element is returned by the service.

SummaryMap , SummaryMap.entry.N.key (key), SummaryMapentry.N.value (value)

A set of key value pairs containing information about IAM entity usage and IAM quotas.

Type: String to Integer map

Valid Map Keys: `Users | UsersQuota | Groups | GroupsQuota | ServerCertificates | ServerCertificatesQuota | UserPolicySizeQuota | GroupPolicySizeQuota | GroupsPerUserQuota | SigningCertificatesPerUserQuota | AccessKeysPerUserQuota | MFADevices | MFADevicesInUse | AccountMFAEnabled | AccountAccessKeysPresent | AccountSigningCertificatesPresent | AttachedPoliciesPerGroupQuota | AttachedPoliciesPerRoleQuota | AttachedPoliciesPerUserQuota | Policies | PoliciesQuota | PolicySizeQuota | PolicyVersionsInUse | PolicyVersionsInUseQuota | VersionsPerPolicyQuota`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=GetAccountSummary
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetAccountSummaryResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <GetAccountSummaryResult>
    <SummaryMap>
      <entry>
        <key>Users</key>
        <value>32</value>
      </entry>
      <entry>
        <key>GroupPolicySizeQuota</key>
        <value>10240</value>
      </entry>
      <entry>
        <key>PolicyVersionsInUseQuota</key>
        <value>10000</value>
      </entry>
      <entry>
        <key>ServerCertificatesQuota</key>
        <value>20</value>
      </entry>
      <entry>
        <key>AccountSigningCertificatesPresent</key>
        <value>0</value>
      </entry>
      <entry>
        <key>AccountAccessKeysPresent</key>
        <value>0</value>
      </entry>
      <entry>
        <key>Groups</key>
        <value>7</value>
      </entry>
      <entry>
        <key>UsersQuota</key>
        <value>150</value>
      </entry>
      <entry>
        <key>RolePolicySizeQuota</key>
        <value>2048</value>
      </entry>
      <entry>
        <key>UserPolicySizeQuota</key>
        <value>10240</value>
      </entry>
      <entry>
        <key>GroupsPerUserQuota</key>
        <value>10</value>
      </entry>
      <entry>
        <key>AssumeRolePolicySizeQuota</key>
        <value>2048</value>
      </entry>
      <entry>
        <key>AttachedPoliciesPerGroupQuota</key>
        <value>2</value>
      </entry>
      <entry>
        <key>Roles</key>
        <value>18</value>
      </entry>
      <entry>
        <key>VersionsPerPolicyQuota</key>
        <value>5</value>
      </entry>
      <entry>
        <key>GroupsQuota</key>
        <value>50</value>
      </entry>
      <entry>
        <key>PolicySizeQuota</key>
        <value>5120</value>
      </entry>
```

```
      <entry>
        <key>Policies</key>
        <value>22</value>
      </entry>
      <entry>
        <key>RolesQuota</key>
        <value>250</value>
      </entry>
      <entry>
        <key>ServerCertificates</key>
        <value>1</value>
      </entry>
      <entry>
        <key>AttachedPoliciesPerRoleQuota</key>
        <value>2</value>
      </entry>
      <entry>
        <key>MFADevicesInUse</key>
        <value>4</value>
      </entry>
      <entry>
        <key>PoliciesQuota</key>
        <value>1000</value>
      </entry>
      <entry>
        <key>AccountMFAEnabled</key>
        <value>1</value>
      </entry>
      <entry>
        <key>Providers</key>
        <value>3</value>
      </entry>
      <entry>
        <key>InstanceProfilesQuota</key>
        <value>100</value>
      </entry>
      <entry>
        <key>MFADevices</key>
        <value>4</value>
      </entry>
      <entry>
        <key>AccessKeysPerUserQuota</key>
        <value>2</value>
      </entry>
      <entry>
        <key>AttachedPoliciesPerUserQuota</key>
        <value>2</value>
      </entry>
      <entry>
        <key>SigningCertificatesPerUserQuota</key>
        <value>2</value>
      </entry>
      <entry>
        <key>PolicyVersionsInUse</key>
        <value>27</value>
      </entry>
      <entry>
        <key>InstanceProfiles</key>
        <value>12</value>
      </entry>
    </SummaryMap>
  </GetAccountSummaryResult>
  <ResponseMetadata>
    <RequestId>85cb9b90-ac28-11e4-a88d-97964EXAMPLE</RequestId>
  </ResponseMetadata>
</GetAccountSummaryResponse>
```

GetContextKeysForCustomPolicy

Gets a list of all of the context keys referenced in the input policies. The policies are supplied as a list of one or more strings. To get the context keys from policies associated with an IAM user, group, or role, use GetContextKeysForPrincipalPolicy (p. 112).

Context keys are variables maintained by AWS and its services that provide details about the context of an API query request, and can be evaluated by testing against a value specified in an IAM policy. Use GetContextKeysForCustomPolicy to understand what key names and values you must supply when you call SimulateCustomPolicy (p. 223). Note that all parameters are shown in unencoded form here for clarity, but must be URL encoded to be included as a part of a real HTML request.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

PolicyInputList.member.N

A list of policies for which you want the list of context keys referenced in those policies. Each document is specified as a string containing the complete, valid JSON text of an IAM policy.

The regex pattern used to validate this parameter is a string of characters consisting of any printable ASCII character ranging from the space character (\u0020) through end of the ASCII character range (\u00FF). It also includes the special characters tab (\u0009), line feed (\u000A), and carriage return (\u000D).

Type: array of Strings

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

Response Elements

The following element is returned by the service.

ContextKeyNames.member.N

The list of context keys that are referenced in the input policies.

Type: array of Strings

Length Constraints: Minimum length of 5. Maximum length of 256.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

Example

Example 1

In the following example, the request includes a policy as a string. The response shows that the policies use both `aws:CurrentTime` and `aws:username`.

Sample Request

```
https://iam.amazonaws.com/?Action=GetContextKeysForCustomPolicy
&PolicyInputList.member.1='{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "dynamodb:*",
    "Resource": "arn:aws:dynamodb:us-east-1:ACCOUNT-ID-WITHOUT-HYPHENS:table/
${aws:username}",
    "Condition":{"DateGreaterThan":
{"aws:CurrentTime":"2015-08-16T12:00:00Z"}}
  }
}'
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetContextKeysForCustomPolicyResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <GetContextKeysForCustomPolicyResult>
    <ContextKeyNames>
      <member>aws:username</member>
      <member>aws:CurrentTime</member>
    </ContextKeyNames>
  </GetContextKeysForCustomPolicyResult>
  <ResponseMetadata>
    <RequestId>d6808605-4c06-11e5-b121-bd8c7EXAMPLE</RequestId>
  </ResponseMetadata>
</GetContextKeysForCustomPolicyResponse>
```

GetContextKeysForPrincipalPolicy

Gets a list of all of the context keys referenced in all of the IAM policies attached to the specified IAM entity. The entity can be an IAM user, group, or role. If you specify a user, then the request also includes all of the policies attached to groups that the user is a member of.

You can optionally include a list of one or more additional policies, specified as strings. If you want to include *only* a list of policies by string, use GetContextKeysForCustomPolicy (p. 110) instead.

Note: This API discloses information about the permissions granted to other users. If you do not want users to see other user's permissions, then consider allowing them to use GetContextKeysForCustomPolicy (p. 110) instead.

Context keys are variables maintained by AWS and its services that provide details about the context of an API query request, and can be evaluated by testing against a value in an IAM policy. Use GetContextKeysForPrincipalPolicy (p. 112) to understand what key names and values you must supply when you call SimulatePrincipalPolicy (p. 228).

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

PolicyInputList.member.N

An optional list of additional policies for which you want the list of context keys that are referenced.

The regex pattern used to validate this parameter is a string of characters consisting of any printable ASCII character ranging from the space character (\u0020) through end of the ASCII character range (\u00FF). It also includes the special characters tab (\u0009), line feed (\u000A), and carriage return (\u000D).

Type: array of Strings

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: No

PolicySourceArn

The ARN of a user, group, or role whose policies contain the context keys that you want listed. If you specify a user, the list includes context keys that are found in all policies attached to the user as well as to all groups that the user is a member of. If you pick a group or a role, then it includes only those context keys that are found in policies attached to that entity. Note that all parameters are shown in unencoded form here for clarity, but must be URL encoded to be included as a part of a real HTML request.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Response Elements

The following element is returned by the service.

ContextKeyNames.member.N

The list of context keys that are referenced in the input policies.

Type: array of Strings

Length Constraints: Minimum length of 5. Maximum length of 256.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

Example

Example 1

In the following example, the request includes the ARN for a user named Dave, and includes one additional policy. This enables you to evaluate the impact that policy would have if you attached it to the user. The response includes five context keys, four from policies attached to the user and one from the added policy. Note that all parameters are shown in unencoded form here for clarity, but must be URL encoded to be included as a part of a real HTML request.

Sample Request

```
https://iam.amazonaws.com/?Action=GetContextKeysForPrincipalPolicy
&PolicySourceArn=arn:aws:iam::123456789012:user/Dave
&PolicyInputList.member.1='{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "dynamodb:*",
    "Resource": "arn:aws:dynamodb:us-east-1:ACCOUNT-ID-WITHOUT-HYPHENS:table/
${aws:username}",
    "Condition":{"DateGreaterThan":
{"aws:CurrentTime":"2015-08-16T12:00:00Z"}}
  }
}'
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetContextKeysForPrincipalPolicyResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <GetContextKeysForPrincipalPolicyResult>
    <ContextKeyNames>
      <member>aws:username</member>
      <member>aws:CurrentTime</member>
      <member>aws:username</member>
      <member>ec2:InstanceType</member>
      <member>aws:CurrentTime</member>
    </ContextKeyNames>
  </GetContextKeysForPrincipalPolicyResult>
  <ResponseMetadata>
    <RequestId>7ec754ab-4c08-11e5-b121-bd8c7EXAMPLE</RequestId>
  </ResponseMetadata>
</GetContextKeysForPrincipalPolicyResponse>
```

GetCredentialReport

Retrieves a credential report for the AWS account. For more information about the credential report, see Getting Credential Reports in the *IAM User Guide*.

Response Elements

The following elements are returned by the service.

Content

Contains the credential report. The report is Base64-encoded.

Type: Base64-encoded binary data

GeneratedTime

The date and time when the credential report was created, in ISO 8601 date-time format.

Type: Timestamp

ReportFormat

The format (MIME type) of the credential report.

Type: String

Valid Values: `text/csv`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

ReportExpired

The request was rejected because the most recent credential report has expired. To generate a new credential report, use GenerateCredentialReport (p. 94). For more information about credential report expiration, see Getting Credential Reports in the *IAM User Guide*.

HTTP Status Code: 410

ReportInProgress

The request was rejected because the credential report is still being generated.

HTTP Status Code: 404

ReportNotPresent

The request was rejected because the credential report does not exist. To generate a credential report, use GenerateCredentialReport (p. 94).

HTTP Status Code: 410

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=GetCredentialReport
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetCredentialReportResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
<GetCredentialReportResult>
  <Content>BASE-64 ENCODED FILE CONTENTS</Content>
  <ReportFormat>text/csv</ReportFormat>
  <GeneratedTime>2014-08-28T21:42:50Z</GeneratedTime>
</GetCredentialReportResult>
<ResponseMetadata>
  <RequestId>29f47818-99f5-11e1-a4c3-27EXAMPLE804</RequestId>
</ResponseMetadata>
</GetCredentialReportResponse>
```

GetGroup

Returns a list of IAM users that are in the specified IAM group. You can paginate the results using the `MaxItems` and `Marker` parameters.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

GroupName

The name of the group.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

This parameter is optional. If you do not include it, it defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true` and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

Response Elements

The following elements are returned by the service.

Group

A structure that contains details about the group.

Type: Group (p. 276) object

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Users.member.N

A list of users in the group.

Type: array of User (p. 305) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=GetGroup
&GroupName=Admins
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetGroupResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
 <GetGroupResult>
    <Group>
       <Path>/</Path>
       <GroupName>Admins</GroupName>
       <GroupId>AGPACKCEVSQ6C2EXAMPLE</GroupId>
       <Arn>arn:aws:iam::123456789012:group/Admins</Arn>
    </Group>
    <Users>
       <member>
          <Path>/division_abc/subdivision_xyz/</Path>
          <UserName>Bob</UserName>
          <UserId>AIDACKCEVSQ6C2EXAMPLE</UserId>
          <Arn>
          arn:aws:iam::123456789012:user/division_abc/subdivision_xyz/Bob
          </Arn>
       </member>
       <member>
          <Path>/division_abc/subdivision_xyz/</Path>
          <UserName>Susan</UserName>
          <UserId>AIDACKCEVSQ6C2EXAMPLE</UserId>
          <Arn>
          arn:aws:iam::123456789012:user/division_abc/subdivision_xyz/Susan
          </Arn>
       </member>
    </Users>
    <IsTruncated>false</IsTruncated>
 </GetGroupResult>
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</GetGroupResponse>
```

GetGroupPolicy

Retrieves the specified inline policy document that is embedded in the specified IAM group.

> **Note**
> Policies returned by this API are URL-encoded compliant with RFC 3986. You can use a URL decoding method to convert the policy back to plain JSON text. For example, if you use Java, you can use the `decode` method of the `java.net.URLDecoder` utility class in the Java SDK. Other languages and SDKs provide similar functionality.

An IAM group can also have managed policies attached to it. To retrieve a managed policy document that is attached to a group, use GetPolicy (p. 128) to determine the policy's default version, then use GetPolicyVersion (p. 130) to retrieve the policy document.

For more information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

GroupName

The name of the group the policy is associated with.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

PolicyName

The name of the policy document to get.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Response Elements

The following elements are returned by the service.

GroupName

The group the policy is associated with.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

PolicyDocument

The policy document.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

PolicyName

The name of the policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=GetGroupPolicy
&GroupName=Admins
&PolicyName=AdminRoot
&AUTHPARAMS
```

Sample Response

```
<GetGroupPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
 <GetGroupPolicyResult>
    <GroupName>Admins</GroupName>
    <PolicyName>AdminRoot</PolicyName>
    <PolicyDocument>
    {"Version":"2012-10-17","Statement":
{"Effect":"Allow","Action":"*","Resource":"*"}}
    </PolicyDocument>
 </GetGroupPolicyResult>
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</GetGroupPolicyResponse>
```

GetInstanceProfile

Retrieves information about the specified instance profile, including the instance profile's path, GUID, ARN, and role. For more information about instance profiles, see About Instance Profiles in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

InstanceProfileName

The name of the instance profile to get information about.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Response Elements

The following element is returned by the service.

InstanceProfile

A structure containing details about the instance profile.

Type: InstanceProfile (p. 278) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=GetInstanceProfile
&InstanceProfileName=Webserver
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetInstanceProfileResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
<GetInstanceProfileResult>
  <InstanceProfile>
    <InstanceProfileId>AIPAD5ARO2C5EXAMPLE3G</InstanceProfileId>
    <Roles>
      <member>
        <Path>/application_abc/component_xyz/</Path>
        <Arn>arn:aws:iam::123456789012:role/application_abc/component_xyz/
S3Access</Arn>
        <RoleName>S3Access</RoleName>
        <AssumeRolePolicyDocument>
          {"Version":"2012-10-17","Statement":[{"Effect":"Allow",
          "Principal":{"Service":["ec2.amazonaws.com"]},"Action":
["sts:AssumeRole"]}]}
        </AssumeRolePolicyDocument>
        <CreateDate>2012-05-09T15:45:35Z</CreateDate>
        <RoleId>AROACVYKSVTSZFEXAMPLE</RoleId>
      </member>
    </Roles>
    <InstanceProfileName>Webserver</InstanceProfileName>
    <Path>/application_abc/component_xyz/</Path>
    <Arn>arn:aws:iam::123456789012:instance-profile/application_abc/
component_xyz/Webserver</Arn>
    <CreateDate>2012-05-09T16:11:10Z</CreateDate>
  </InstanceProfile>
</GetInstanceProfileResult>
<ResponseMetadata>
  <RequestId>37289fda-99f2-11e1-a4c3-27EXAMPLE804</RequestId>
</ResponseMetadata>
</GetInstanceProfileResponse>
```

GetLoginProfile

Retrieves the user name and password-creation date for the specified IAM user. If the user has not been assigned a password, the action returns a 404 (`NoSuchEntity`) error.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

UserName

The name of the user whose login profile you want to retrieve.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

Response Elements

The following element is returned by the service.

LoginProfile

A structure containing the user name and password create date for the user.

Type: LoginProfile (p. 279) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=GetLoginProfile
&UserName=Bob
&AUTHPARAMS
```

Sample Response

```
<GetLoginProfileResponse>
```

```
 <GetLoginProfileResult>
    <LoginProfile>
       <UserName>Bob</UserName>
       <CreateDate>2011-09-19T23:00:56Z</CreateDate>
    </LoginProfile>
 </GetLoginProfileResult>
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</GetLoginProfileResponse>
```

GetOpenIDConnectProvider

Returns information about the specified OpenID Connect (OIDC) provider resource object in IAM.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

OpenIDConnectProviderArn

The Amazon Resource Name (ARN) of the OIDC provider resource object in IAM to get information for. You can get a list of OIDC provider resource ARNs by using the ListOpenIDConnectProviders (p. 178) action.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Response Elements

The following elements are returned by the service.

ClientIDList.member.N

A list of client IDs (also known as audiences) that are associated with the specified IAM OIDC provider resource object. For more information, see CreateOpenIDConnectProvider (p. 29).

Type: array of Strings

Length Constraints: Minimum length of 1. Maximum length of 255.

CreateDate

The date and time when the IAM OIDC provider resource object was created in the AWS account.

Type: Timestamp

ThumbprintList.member.N

A list of certificate thumbprints that are associated with the specified IAM OIDC provider resource object. For more information, see CreateOpenIDConnectProvider (p. 29).

Type: array of Strings

Length Constraints: Fixed length of 40.

Url

The URL that the IAM OIDC provider resource object is associated with. For more information, see CreateOpenIDConnectProvider (p. 29).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=GetOpenIDConnectProvider
&OpenIDConnectProviderArn=arn:aws:iam::123456789012:oidc-provider/example.com
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetOpenIDConnectProviderResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <GetOpenIDConnectProviderResult>
    <ThumbprintList>
      <member>c3768084dfb3d2b68b7897bf5f565da8eEXAMPLE</member>
    </ThumbprintList>
    <CreateDate>2014-10-09T03:32:51.398Z</CreateDate>
    <ClientIDList>
      <member>my-application-ID</member>
    </ClientIDList>
    <Url>server.example.com</Url>
  </GetOpenIDConnectProviderResult>
  <ResponseMetadata>
    <RequestId>2c91531b-4f65-11e4-aefa-bfd6aEXAMPLE</RequestId>
  </ResponseMetadata>
</GetOpenIDConnectProviderResponse>
```

GetPolicy

Retrieves information about the specified managed policy, including the policy's default version and the total number of IAM users, groups, and roles to which the policy is attached. To retrieve the list of the specific users, groups, and roles that the policy is attached to, use the ListEntitiesForPolicy (p. 160) API. This API returns metadata about the policy. To retrieve the actual policy document for a specific version of the policy, use GetPolicyVersion (p. 130).

This API retrieves information about managed policies. To retrieve information about an inline policy that is embedded with an IAM user, group, or role, use the GetUserPolicy (p. 144), GetGroupPolicy (p. 120), or GetRolePolicy (p. 134) API.

For more information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

PolicyArn

The Amazon Resource Name (ARN) of the managed policy that you want information about.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Response Elements

The following element is returned by the service.

Policy

A structure containing details about the policy.

Type: Policy (p. 286) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=GetPolicy
&PolicyArn=arn:aws:iam::123456789012:policy/S3-read-only-example-bucket
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <GetPolicyResult>
    <Policy>
      <PolicyName>S3-read-only-example-bucket</PolicyName>
      <Description>Allows read-only access to the example bucket</
Description>
      <DefaultVersionId>v1</DefaultVersionId>
      <PolicyId>AGPACKCEVSQ6C2EXAMPLE</PolicyId>
      <Path>/</Path>
      <Arn>arn:aws:iam::123456789012:policy/S3-read-only-example-bucket</Arn>
      <AttachmentCount>9</AttachmentCount>
      <CreateDate>2014-09-15T17:36:14Z</CreateDate>
      <UpdateDate>2014-09-15T20:31:47Z</UpdateDate>
    </Policy>
  </GetPolicyResult>
  <ResponseMetadata>
    <RequestId>684f0917-3d22-11e4-a4a0-cffb9EXAMPLE</RequestId>
  </ResponseMetadata>
</GetPolicyResponse>
```

GetPolicyVersion

Retrieves information about the specified version of the specified managed policy, including the policy document.

> **Note**
> Policies returned by this API are URL-encoded compliant with RFC 3986. You can use a URL decoding method to convert the policy back to plain JSON text. For example, if you use Java, you can use the `decode` method of the `java.net.URLDecoder` utility class in the Java SDK. Other languages and SDKs provide similar functionality.

To list the available versions for a policy, use ListPolicyVersions (p. 182).

This API retrieves information about managed policies. To retrieve information about an inline policy that is embedded in a user, group, or role, use the GetUserPolicy (p. 144), GetGroupPolicy (p. 120), or GetRolePolicy (p. 134) API.

For more information about the types of policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

For more information about managed policy versions, see Versioning for Managed Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

PolicyArn

The Amazon Resource Name (ARN) of the managed policy that you want information about.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

VersionId

Identifies the policy version to retrieve.

The regex pattern used to validate this parameter is a string of characters that consists of the lowercase letter 'v' followed by one or two digits, and optionally followed by a period '.' and a string of letters and digits.

Type: String

Pattern: `v[1-9][0-9]*(\.[A-Za-z0-9-]*)?`

Required: Yes

Response Elements

The following element is returned by the service.

PolicyVersion

A structure containing details about the policy version.

Type: PolicyVersion (p. 292) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=GetPolicyVersion
&PolicyArn=arn:aws:iam::123456789012:policy/S3-read-only-example-bucket
&VersionId=v1
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetPolicyVersionResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <GetPolicyVersionResult>
    <PolicyVersion>
      <Document>
      {"Version":"2012-10-17","Statement":[{"Effect":"Allow","Action":
["s3:Get*","s3:List*"],
      "Resource":["arn:aws:s3:::EXAMPLE-BUCKET","arn:aws:s3:::EXAMPLE-BUCKET/
*"]}]}
      </Document>
      <IsDefaultVersion>true</IsDefaultVersion>
      <VersionId>v1</VersionId>
      <CreateDate>2014-09-15T20:31:47Z</CreateDate>
    </PolicyVersion>
  </GetPolicyVersionResult>
  <ResponseMetadata>
    <RequestId>d472f28e-3d23-11e4-a4a0-cffb9EXAMPLE</RequestId>
  </ResponseMetadata>
</GetPolicyVersionResponse>
```

GetRole

Retrieves information about the specified role, including the role's path, GUID, ARN, and the role's trust policy that grants permission to assume the role. For more information about roles, see Working with Roles.

Note

Policies returned by this API are URL-encoded compliant with RFC 3986. You can use a URL decoding method to convert the policy back to plain JSON text. For example, if you use Java, you can use the `decode` method of the `java.net.URLDecoder` utility class in the Java SDK. Other languages and SDKs provide similar functionality.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

RoleName

The name of the IAM role to get information about.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

Response Elements

The following element is returned by the service.

Role

A structure containing details about the IAM role.

Type: Role (p. 295) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=GetRole
```

```
&RoleName=S3Access
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetRoleResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
<GetRoleResult>
  <Role>
    <Path>/application_abc/component_xyz/</Path>
    <Arn>arn:aws:iam::123456789012:role/application_abc/component_xyz/
S3Access</Arn>
    <RoleName>S3Access</RoleName>
    <AssumeRolePolicyDocument>
      {"Version":"2012-10-17","Statement":[{"Effect":"Allow",
      "Principal":{"Service":["ec2.amazonaws.com"]},"Action":
["sts:AssumeRole"]}]}
    </AssumeRolePolicyDocument>
    <CreateDate>2012-05-08T23:34:01Z</CreateDate>
    <RoleId>AROADBQP57FF2AEXAMPLE</RoleId>
  </Role>
</GetRoleResult>
<ResponseMetadata>
  <RequestId>df37e965-9967-11e1-a4c3-270EXAMPLE04</RequestId>
</ResponseMetadata>
</GetRoleResponse>
```

GetRolePolicy

Retrieves the specified inline policy document that is embedded with the specified IAM role.

> **Note**
> Policies returned by this API are URL-encoded compliant with RFC 3986. You can use a URL decoding method to convert the policy back to plain JSON text. For example, if you use Java, you can use the `decode` method of the `java.net.URLDecoder` utility class in the Java SDK. Other languages and SDKs provide similar functionality.

An IAM role can also have managed policies attached to it. To retrieve a managed policy document that is attached to a role, use GetPolicy (p. 128) to determine the policy's default version, then use GetPolicyVersion (p. 130) to retrieve the policy document.

For more information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

For more information about roles, see Using Roles to Delegate Permissions and Federate Identities.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

PolicyName

The name of the policy document to get.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

RoleName

The name of the role associated with the policy.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

Response Elements

The following elements are returned by the service.

PolicyDocument

The policy document.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

PolicyName

The name of the policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

RoleName

The role the policy is associated with.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=GetRolePolicy
&PolicyName=S3AccessPolicy
&RoleName=S3Access
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetRolePolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
<GetRolePolicyResult>
  <PolicyName>S3AccessPolicy</PolicyName>
  <RoleName>S3Access</RoleName>
  <PolicyDocument>
  {"Version":"2012-10-17","Statement":[{"Effect":"Allow","Action":
["s3:*"],"Resource":["*"]}]}
  </PolicyDocument>
</GetRolePolicyResult>
<ResponseMetadata>
  <RequestId>7e7cd8bc-99ef-11e1-a4c3-27EXAMPLE804</RequestId>
</ResponseMetadata>
</GetRolePolicyResponse>
```

GetSAMLProvider

Returns the SAML provider metadocument that was uploaded when the IAM SAML provider resource object was created or updated.

Note
This operation requires Signature Version 4.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

SAMLProviderArn

The Amazon Resource Name (ARN) of the SAML provider resource object in IAM to get information about.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Response Elements

The following elements are returned by the service.

CreateDate

The date and time when the SAML provider was created.

Type: Timestamp

SAMLMetadataDocument

The XML metadata document that includes information about an identity provider.

Type: String

Length Constraints: Minimum length of 1000. Maximum length of 10000000.

ValidUntil

The expiration date and time for the SAML provider.

Type: Timestamp

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=GetSAMLProvider
&Name=arn:aws:iam::123456789012:saml-provider/MyUniversity
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetSAMLProviderResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
<GetSAMLProviderResult>
  <CreateDate>2012-05-09T16:27:11Z</CreateDate>
  <ValidUntil>2015-12-31T211:59:59Z</ValidUntil>
  <SAMLMetadataDocument>Pd9fexDssTkRgGNqs...DxptfEs==</SAMLMetadataDocument>
</GetSAMLProviderResult>
<ResponseMetadata>
  <RequestId>29f47818-99f5-11e1-a4c3-27EXAMPLE804</RequestId>
</ResponseMetadata>
</GetSAMLProviderResponse>
```

GetServerCertificate

Retrieves information about the specified server certificate stored in IAM.

For more information about working with server certificates, including a list of AWS services that can use the server certificates that you manage with IAM, go to Working with Server Certificates in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

ServerCertificateName

The name of the server certificate you want to retrieve information about.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Response Elements

The following element is returned by the service.

ServerCertificate

A structure containing details about the server certificate.

Type: ServerCertificate (p. 299) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=GetServerCertificate
&ServerCertificateName=ProdServerCert
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetServerCertificateResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
<GetServerCertificateResult>
  <ServerCertificate>
    <ServerCertificateMetadata>
      <ServerCertificateName>ProdServerCert</ServerCertificateName>
      <Path>/company/servercerts/</Path>
      <Arn>arn:aws:iam::123456789012:server-certificate/company/servercerts/
ProdServerCert</Arn>
      <UploadDate>2010-05-08T01:02:03.004Z</UploadDate>
      <ServerCertificateId>ASCACKCEVSQ6C2EXAMPLE</ServerCertificateId>
      <Expiration>2012-05-08T01:02:03.004Z</Expiration>
    </ServerCertificateMetadata>
    <CertificateBody>
-----BEGIN CERTIFICATE-----
MIICdzCCAeCgAwIBAgIGANc+Ha2wMA0GCSqGSIb3DQEBBQUAMFMxCzAJBgNVBAYT
AlVTMRMwEQYDVQQKEwpBbWF6b24uY29tMQwwCgYDVQQLEwNBV1MxITAfBgNVBAMT
GEFXUyBMaW1pdGVkLUFzc3VyYW5jZSBDQTAeFw0wOTAyMDQxNzE5MjdaFw0xMDAy
MDQxNzE5MjdaMFIxCzAJBgNVBAYTAlVTMRMwEQYDVQQKEwpBbWF6b24uY29tMRcw
FQYDVQQLEw5BV1MtRGV2ZWxvcGVyczEVMBMGA1UEAxMMNTdxNDl0c3ZwYjRtMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpB/vsOwmT/O0td1RqzKjttSBaPjbr
dqwNe9BrOyB08fw2+Ch5oonZYXfGUrT6mkYXH5fQot9HvASrzAKHO596FdJA6DmL
ywdWe1Oggk7zFSXO1Xv+3vPrJtaYxYo3eRIp7w80PMkiOv6M0XK8ubcTouODeJbf
suDqcLnLDxwsvwIDAQABo1cwVTAOBgNVHQ8BAf8EBAMCBaAwFgYDVR0lAQH/BAww
CgYIKwYBBQUHAwIwDAYDVR0TAQH/BAIwADAdBgNVHQ4EFgQULGNaBphBumaKbDRK
CAi0mH8B3mowDQYJKoZIhvcNAQEFBQADgYEAuKxhkXaCLGcqDuweKtO/AEw9ZePH
wr0XqsaIK2HZboqruebXEGsojK4Ks0WzwgrEynuHJwTn760xe39rSqXWIOGrOBaX
wFpWHVjTFMKk+tSDG1lssLHyYWWdFFU4AnejRGORJYNaRHgVTKjHphc5jEhHm0BX
AEaHzTpmEXAMPLE=
-----END CERTIFICATE-----
    </CertificateBody>
  </ServerCertificate>
</GetServerCertificateResult>
<ResponseMetadata>
  <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
</ResponseMetadata>
</GetServerCertificateResponse>
```

GetSSHPublicKey

Retrieves the specified SSH public key, including metadata about the key.

The SSH public key retrieved by this action is used only for authenticating the associated IAM user to an AWS CodeCommit repository. For more information about using SSH keys to authenticate to an AWS CodeCommit repository, see Set up AWS CodeCommit for SSH Connections in the *AWS CodeCommit User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

Encoding

Specifies the public key encoding format to use in the response. To retrieve the public key in ssh-rsa format, use `SSH`. To retrieve the public key in PEM format, use `PEM`.

Type: String

Valid Values: `SSH | PEM`

Required: Yes

SSHPublicKeyId

The unique identifier for the SSH public key.

The regex pattern used to validate this parameter is a string of characters that can consist of any upper or lowercased letter or digit.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

UserName

The name of the IAM user associated with the SSH public key.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

Response Elements

The following element is returned by the service.

SSHPublicKey

A structure containing details about the SSH public key.

Type: SSHPublicKey (p. 302) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

UnrecognizedPublicKeyEncoding

The request was rejected because the public key encoding format is unsupported or unrecognized.

HTTP Status Code: 400

Example

Sample Request

```
https://iam.amazonaws.com/?Action=GetSSHPublicKey
&Encoding=PEM
&SSHPublicKeyId=APKAEIVFHP46CEXAMPLE
&UserName=Jane
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetSSHPublicKeyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <GetSSHPublicKeyResult>
    <SSHPublicKey>
      <UploadDate>2015-06-05T20:56:46Z</UploadDate>
      <Fingerprint>7a:1d:ea:9e:b0:80:ac:f8:ec:d8:dc:e6:a7:2c:fc:51</
Fingerprint>
      <UserName>Jane</UserName>
      <SSHPublicKeyId>APKAEIVFHP46CEXAMPLE</SSHPublicKeyId>
      <Status>Active</Status>
      <SSHPublicKeyBody>
        -----BEGIN PUBLIC KEY-----
        MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsu+WpO9hhmqGTctHI1BE
        SJ/pq4GtAt9JJpIsDnjeB+mLbwnVJLFaaYzzoZuPOVhUc7yHMWjBLmfSEgJKfAH3
        n8m8R9D3UFoRC0rtKR2jJwAwFO3Tp9wgnqzvPtLMnG7uBEuD/nHStanrd6bbBv83
        kDSy5jiuc4yEWtTAEtyp8C8BxFTxHuCQ/sX4IbjtJ8M1IKZ3hjcJO5u6ooWCxZzQ
        hXXlPDniK/RZnO+YOaJR5umaAv23HAB7qx5H3A6WpyUyzXy0eTo9eAmUrET+JDXZ
        vqHufiDzO/MOCfb+KV1OJos2AxNtRuIFA1cTq7NF+upTIoV+gK1YJhCvjSuRkIJ/
        cwIDAQAB
        -----END PUBLIC KEY-----
      </SSHPublicKeyBody>
    </SSHPublicKey>
  </GetSSHPublicKeyResult>
  <ResponseMetadata>
    <RequestId>4817ee13-f36d-11e4-97db-33c4eEXAMPLE</RequestId>
  </ResponseMetadata>
</GetSSHPublicKeyResponse>
```

GetUser

Retrieves information about the specified IAM user, including the user's creation date, path, unique ID, and ARN.

If you do not specify a user name, IAM determines the user name implicitly based on the AWS access key ID used to sign the request to this API.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

UserName

The name of the user to get information about.

This parameter is optional. If it is not included, it defaults to the user making the request. The regex pattern used to validate this parameter is a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: =,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: No

Response Elements

The following element is returned by the service.

User

A structure containing details about the IAM user.

Type: User (p. 305) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=GetUser
&UserName=Bob
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetUserResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <GetUserResult>
    <User>
      <UserId>AIDACKCEVSQ6C2EXAMPLE</UserId>
      <Path>/division_abc/subdivision_xyz/</Path>
      <UserName>Bob</UserName>
      <Arn>arn:aws:iam::123456789012:user/division_abc/subdivision_xyz/Bob</
Arn>
      <CreateDate>2013-10-02T17:01:44Z</CreateDate>
      <PasswordLastUsed>2014-10-10T14:37:51Z</PasswordLastUsed>
    </User>
  </GetUserResult>
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</GetUserResponse>
```

GetUserPolicy

Retrieves the specified inline policy document that is embedded in the specified IAM user.

> **Note**
> Policies returned by this API are URL-encoded compliant with RFC 3986. You can use a URL decoding method to convert the policy back to plain JSON text. For example, if you use Java, you can use the `decode` method of the `java.net.URLDecoder` utility class in the Java SDK. Other languages and SDKs provide similar functionality.

An IAM user can also have managed policies attached to it. To retrieve a managed policy document that is attached to a user, use GetPolicy (p. 128) to determine the policy's default version, then use GetPolicyVersion (p. 130) to retrieve the policy document.

For more information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

PolicyName

The name of the policy document to get.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

UserName

The name of the user who the policy is associated with.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Response Elements

The following elements are returned by the service.

PolicyDocument

The policy document.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

PolicyName

The name of the policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

UserName

The user the policy is associated with.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=GetUserPolicy
&UserName=Bob
&PolicyName=AllAccessPolicy
&AUTHPARAMS
```

Sample Response

```
<GetUserPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
 <GetUserPolicyResult>
    <UserName>Bob</UserName>
    <PolicyName>AllAccessPolicy</PolicyName>
    <PolicyDocument>
    {"Version":"2012-10-17","Statement":
[{"Effect":"Allow","Action":"*","Resource":"*"}]}
    </PolicyDocument>
 </GetUserPolicyResult>
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</GetUserPolicyResponse>
```

ListAccessKeys

Returns information about the access key IDs associated with the specified IAM user. If there are none, the action returns an empty list.

Although each user is limited to a small number of keys, you can still paginate the results using the `MaxItems` and `Marker` parameters.

If the `UserName` field is not specified, the UserName is determined implicitly based on the AWS access key ID used to sign the request. Because this action works for access keys under the AWS account, you can use this action to manage root credentials even if the AWS account has no associated users.

> **Note**
> To ensure the security of your AWS account, the secret access key is accessible only during key and user creation.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

This parameter is optional. If you do not include it, it defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true` and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

UserName

The name of the user.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: No

Response Elements

The following elements are returned by the service.

AccessKeyMetadata.member.N

A list of objects containing metadata about the access keys.

Type: array of AccessKeyMetadata (p. 271) objects

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=ListAccessKeys
&UserName=Bob
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListAccessKeysResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ListAccessKeysResult>
    <UserName>Bob</UserName>
    <AccessKeyMetadata>
       <member>
          <UserName>Bob</UserName>
          <AccessKeyId>AKIA1234567890EXAMPLE</AccessKeyId>
          <Status>Active</Status>
       </member>
       <member>
          <UserName>Susan</UserName>
          <AccessKeyId>AKIA2345678901EXAMPLE</AccessKeyId>
          <Status>Inactive</Status>
       </member>
    </AccessKeyMetadata>
    <IsTruncated>false</IsTruncated>
  </ListAccessKeysResult>
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</ListAccessKeysResponse>
```

ListAccountAliases

Lists the account alias associated with the AWS account (Note: you can have only one). For information about using an AWS account alias, see Using an Alias for Your AWS Account ID in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

This parameter is optional. If you do not include it, it defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true` and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

Response Elements

The following elements are returned by the service.

AccountAliases.member.N

A list of aliases associated with the account. AWS supports only one alias per account.

Type: array of Strings

Length Constraints: Minimum length of 3. Maximum length of 63.

Pattern: `^[a-z0-9](([a-z0-9]|-(?!-))*[a-z0-9])?$`

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=ListAccountAliases
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListAccountAliasesResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
<ListAccountAliasesResult>
  <IsTruncated>false</IsTruncated>
  <AccountAliases>
    <member>example-corporation</member>
  </AccountAliases>
</ListAccountAliasesResult>
<ResponseMetadata>
  <RequestId>c5a076e9-f1b0-11df-8fbe-45274EXAMPLE</RequestId>
</ResponseMetadata>
</ListAccountAliasesResponse>
```

ListAttachedGroupPolicies

Lists all managed policies that are attached to the specified IAM group.

An IAM group can also have inline policies embedded with it. To list the inline policies for a group, use the ListGroupPolicies (p. 163) API. For information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

You can paginate the results using the `MaxItems` and `Marker` parameters. You can use the `PathPrefix` parameter to limit the list of policies to only those matching the specified path prefix. If there are no policies attached to the specified group (or none that match the specified path prefix), the action returns an empty list.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

GroupName

The name (friendly name, not ARN) of the group to list attached policies for.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

This parameter is optional. If you do not include it, it defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true` and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

PathPrefix

The path prefix for filtering the results. This parameter is optional. If it is not included, it defaults to a slash (/), listing all policies.

The regex pattern used to validate this parameter is a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes, containing any ASCII character from the ! (\u0021) thru the DEL character (\u007F), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Pattern: `((/[A-Za-z0-9\.,\+@=_-]+)*)/`

Required: No

Response Elements

The following elements are returned by the service.

AttachedPolicies.member.N

A list of the attached policies.

Type: array of AttachedPolicy (p. 272) objects

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=ListAttachedGroupPolicies
&GroupName=ReadOnlyUsers
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListAttachedGroupPoliciesResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <ListAttachedGroupPoliciesResult>
    <AttachedPolicies>
      <member>
        <PolicyName>ReadOnlyAccess</PolicyName>
        <PolicyArn>arn:aws:iam::aws:policy/ReadOnlyAccess</PolicyArn>
      </member>
    </AttachedPolicies>
    <IsTruncated>false</IsTruncated>
  </ListAttachedGroupPoliciesResult>
  <ResponseMetadata>
    <RequestId>710f2d3f-3df1-11e4-9d0d-6f969EXAMPLE</RequestId>
  </ResponseMetadata>
</ListAttachedGroupPoliciesResponse>
```

ListAttachedRolePolicies

Lists all managed policies that are attached to the specified IAM role.

An IAM role can also have inline policies embedded with it. To list the inline policies for a role, use the ListRolePolicies (p. 185) API. For information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

You can paginate the results using the `MaxItems` and `Marker` parameters. You can use the `PathPrefix` parameter to limit the list of policies to only those matching the specified path prefix. If there are no policies attached to the specified role (or none that match the specified path prefix), the action returns an empty list.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

This parameter is optional. If you do not include it, it defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true` and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

PathPrefix

The path prefix for filtering the results. This parameter is optional. If it is not included, it defaults to a slash (/), listing all policies.

The regex pattern used to validate this parameter is a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes, containing any ASCII character from the ! (\u0021) thru the DEL character (\u007F), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Pattern: `((/[A-Za-z0-9\.,\+@=_-]+)*)/`

Required: No

RoleName

The name (friendly name, not ARN) of the role to list attached policies for.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

Response Elements

The following elements are returned by the service.

AttachedPolicies.member.N

A list of the attached policies.

Type: array of AttachedPolicy (p. 272) objects

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=ListAttachedRolePolicies
&RoleName=ReadOnlyRole
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListAttachedRolePoliciesResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <ListAttachedRolePoliciesResult>
    <AttachedPolicies>
      <member>
        <PolicyName>ReadOnlyAccess</PolicyName>
        <PolicyArn>arn:aws:iam::aws:policy/ReadOnlyAccess</PolicyArn>
      </member>
    </AttachedPolicies>
    <IsTruncated>false</IsTruncated>
  </ListAttachedRolePoliciesResult>
  <ResponseMetadata>
    <RequestId>9a3b490d-3ea5-11e4-9d0d-6f969EXAMPLE</RequestId>
  </ResponseMetadata>
</ListAttachedRolePoliciesResponse>
```

ListAttachedUserPolicies

Lists all managed policies that are attached to the specified IAM user.

An IAM user can also have inline policies embedded with it. To list the inline policies for a user, use the ListUserPolicies (p. 199) API. For information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

You can paginate the results using the `MaxItems` and `Marker` parameters. You can use the `PathPrefix` parameter to limit the list of policies to only those matching the specified path prefix. If there are no policies attached to the specified group (or none that match the specified path prefix), the action returns an empty list.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

This parameter is optional. If you do not include it, it defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true` and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

PathPrefix

The path prefix for filtering the results. This parameter is optional. If it is not included, it defaults to a slash (/), listing all policies.

The regex pattern used to validate this parameter is a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes, containing any ASCII character from the ! (\u0021) thru the DEL character (\u007F), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Pattern: `((/[A-Za-z0-9\.,\+@=_-]+)*)/`

Required: No

UserName

The name (friendly name, not ARN) of the user to list attached policies for.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

Response Elements

The following elements are returned by the service.

AttachedPolicies.member.N

A list of the attached policies.

Type: array of AttachedPolicy (p. 272) objects

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=ListAttachedUserPolicies
&UserName=Alice
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListAttachedUserPoliciesResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <ListAttachedUserPoliciesResult>
    <AttachedPolicies>
      <member>
        <PolicyName>AdministratorAccess</PolicyName>
        <PolicyArn>arn:aws:iam::aws:policy/AdministratorAccess</PolicyArn>
      </member>
    </AttachedPolicies>
    <IsTruncated>false</IsTruncated>
  </ListAttachedUserPoliciesResult>
  <ResponseMetadata>
    <RequestId>75980e78-3ea6-11e4-9d0d-6f969EXAMPLE</RequestId>
  </ResponseMetadata>
</ListAttachedUserPoliciesResponse>
```

ListEntitiesForPolicy

Lists all IAM users, groups, and roles that the specified managed policy is attached to.

You can use the optional `EntityFilter` parameter to limit the results to a particular type of entity (users, groups, or roles). For example, to list only the roles that are attached to the specified policy, set `EntityFilter` to `Role`.

You can paginate the results using the `MaxItems` and `Marker` parameters.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

EntityFilter

The entity type to use for filtering the results.

For example, when `EntityFilter` is `Role`, only the roles that are attached to the specified policy are returned. This parameter is optional. If it is not included, all attached entities (users, groups, and roles) are returned. The argument for this parameter must be one of the valid values listed below.

Type: String

Valid Values: `User | Role | Group | LocalManagedPolicy | AWSManagedPolicy`

Required: No

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

This parameter is optional. If you do not include it, it defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true` and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

PathPrefix

The path prefix for filtering the results. This parameter is optional. If it is not included, it defaults to a slash (/), listing all entities.

The regex pattern used to validate this parameter is a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes, containing any ASCII character from the ! (\u0021) thru the DEL character (\u007F), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: No

PolicyArn

The Amazon Resource Name (ARN) of the IAM policy for which you want the versions.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Response Elements

The following elements are returned by the service.

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

PolicyGroups.member.N

A list of IAM groups that the policy is attached to.

Type: array of PolicyGroup (p. 289) objects

PolicyRoles.member.N

A list of IAM roles that the policy is attached to.

Type: array of PolicyRole (p. 290) objects

PolicyUsers.member.N

A list of IAM users that the policy is attached to.

Type: array of PolicyUser (p. 291) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=ListEntitiesForPolicy
&PolicyArn=arn:aws:iam::123456789012:policy/EC2-Devs
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListEntitiesForPolicyResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <ListEntitiesForPolicyResult>
    <PolicyRoles>
      <member>
        <RoleName>DevRole</RoleName>
      </member>
    </PolicyRoles>
    <PolicyGroups>
      <member>
        <GroupName>Dev</GroupName>
      </member>
    </PolicyGroups>
    <IsTruncated>false</IsTruncated>
    <PolicyUsers>
      <member>
        <UserName>Alice</UserName>
      </member>
      <member>
        <UserName>Bob</UserName>
      </member>
    </PolicyUsers>
  </ListEntitiesForPolicyResult>
  <ResponseMetadata>
    <RequestId>eb358e22-9d1f-11e4-93eb-190ecEXAMPLE</RequestId>
  </ResponseMetadata>
</ListEntitiesForPolicyResponse>
```

ListGroupPolicies

Lists the names of the inline policies that are embedded in the specified IAM group.

An IAM group can also have managed policies attached to it. To list the managed policies that are attached to a group, use ListAttachedGroupPolicies (p. 151). For more information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

You can paginate the results using the `MaxItems` and `Marker` parameters. If there are no inline policies embedded with the specified group, the action returns an empty list.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

GroupName

The name of the group to list policies for.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

This parameter is optional. If you do not include it, it defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true` and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

Response Elements

The following elements are returned by the service.

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

PolicyNames.member.N

A list of policy names.

Type: array of Strings

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=ListGroupPolicies
&GroupName=Admins
&AUTHPARAMS
```

Sample Response

```
<ListGroupPoliciesResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
 <ListGroupPoliciesResult>
    <PolicyNames>
       <member>AdminRoot</member>
       <member>KeyPolicy</member>
    </PolicyNames>
    <IsTruncated>false</IsTruncated>
 </ListGroupPoliciesResult>
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</ListGroupPoliciesResponse>
```

ListGroups

Lists the IAM groups that have the specified path prefix.

You can paginate the results using the `MaxItems` and `Marker` parameters.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

This parameter is optional. If you do not include it, it defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true` and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

PathPrefix

The path prefix for filtering the results. For example, the prefix `/division_abc/subdivision_xyz/` gets all groups whose path starts with `/division_abc/subdivision_xyz/`.

This parameter is optional. If it is not included, it defaults to a slash (/), listing all groups. The regex pattern used to validate this parameter is a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes, containing any ASCII character from the ! (\u0021) thru the DEL character (\u007F), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `\u002F[\u0021-\u007F]*`

Required: No

Response Elements

The following elements are returned by the service.

Groups.member.N

A list of groups.

Type: array of Group (p. 276) objects

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more

items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=ListGroups
&PathPrefix=/division_abc/subdivision_xyz/
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListGroupsResponse>
  <ListGroupsResult>
    <Groups>
       <member>
          <Path>/division_abc/subdivision_xyz/</Path>
          <GroupName>Admins</GroupName>
          <GroupId>AGPACKCEVSQ6C2EXAMPLE</GroupId>
          <Arn>arn:aws:iam::123456789012:group/Admins</Arn>
       </member>
       <member>
          <Path>/division_abc/subdivision_xyz/product_1234/engineering/
          </Path>
          <GroupName>Test</GroupName>
          <GroupId>AGP2MAB8DPLSRHEXAMPLE</GroupId>
          <Arn>arn:aws:iam::123456789012:group
          /division_abc/subdivision_xyz/product_1234/engineering/Test</Arn>
       </member>
       <member>
          <Path>/division_abc/subdivision_xyz/product_1234/</Path>
          <GroupName>Managers</GroupName>
          <GroupId>AGPIODR4TAW7CSEXAMPLE</GroupId>
          <Arn>arn:aws:iam::123456789012
          :group/division_abc/subdivision_xyz/product_1234/Managers</Arn>
       </member>
    </Groups>
    <IsTruncated>false</IsTruncated>
  </ListGroupsResult>
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</ListGroupsResponse>
```

ListGroupsForUser

Lists the IAM groups that the specified IAM user belongs to.

You can paginate the results using the `MaxItems` and `Marker` parameters.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

This parameter is optional. If you do not include it, it defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true` and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

UserName

The name of the user to list groups for.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Response Elements

The following elements are returned by the service.

Groups.member.N

A list of groups.

Type: array of Group (p. 276) objects

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=ListGroupsForUser
&UserName=Bob
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListGroupsForUserResponse>
  <ListGroupsForUserResult>
    <Groups>
       <member>
          <Path>/</Path>
          <GroupName>Admins</GroupName>
          <GroupId>AGPACKCEVSQ6C2EXAMPLE</GroupId>
          <Arn>arn:aws:iam::123456789012:group/Admins</Arn>
       </member>
    </Groups>
    <IsTruncated>false</IsTruncated>
  </ListGroupsForUserResult>
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</ListGroupsForUserResponse>
```

ListInstanceProfiles

Lists the instance profiles that have the specified path prefix. If there are none, the action returns an empty list. For more information about instance profiles, go to About Instance Profiles.

You can paginate the results using the `MaxItems` and `Marker` parameters.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

This parameter is optional. If you do not include it, it defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true` and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

PathPrefix

The path prefix for filtering the results. For example, the prefix `/application_abc/component_xyz/` gets all instance profiles whose path starts with `/application_abc/component_xyz/`.

This parameter is optional. If it is not included, it defaults to a slash (/), listing all instance profiles. The regex pattern used to validate this parameter is a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes, containing any ASCII character from the ! (\u0021) thru the DEL character (\u007F), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `\u002F[\u0021-\u007F]*`

Required: No

Response Elements

The following elements are returned by the service.

InstanceProfiles.member.N

A list of instance profiles.

Type: array of InstanceProfile (p. 278) objects

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=ListInstanceProfiles
&MaxItems=100
&PathPrefix=/application_abc/
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListInstanceProfilesResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
<ListInstanceProfilesResult>
  <IsTruncated>false</IsTruncated>
  <InstanceProfiles>
    <member>
      <InstanceProfileId>AIPA1234567890EXAMPLE</InstanceProfileId>
      <Roles>
        <member>
          <AssumeRolePolicyDocument>{  …  JSON POLICY DOCUMENT HERE … }</
AssumeRolePolicyDocument>
          <RoleId>AROA1234567890EXAMPLE</RoleId>
          <CreateDate>2016-04-27T21:18:27Z</CreateDate>
          <RoleName>ec2instancerole-MyADFSTestServer</RoleName>
          <Path>/</Path>,
          <Arn>arn:aws:iam::123456789012:role/ec2instancerole-
MyADFSTestServer</Arn>
        </member>
      </Roles>
      <InstanceProfileName>Database</InstanceProfileName>
      <Path>/application_abc/component_xyz/</Path>
      <Arn>arn:aws:iam::123456789012:instance-profile/application_abc/
component_xyz/Database</Arn>
      <CreateDate>2012-05-09T16:27:03Z</CreateDate>
    </member>
    <member>
      <InstanceProfileId>AIPA2345678901EXAMPLE</InstanceProfileId>
      <Roles/>
      <InstanceProfileName>Webserver</InstanceProfileName>
      <Path>/application_abc/component_xyz/</Path>
      <Arn>arn:aws:iam::123456789012:instance-profile/application_abc/
component_xyz/Webserver</Arn>
      <CreateDate>2012-05-09T16:27:11Z</CreateDate>
    </member>
  </InstanceProfiles>
</ListInstanceProfilesResult>
<ResponseMetadata>
  <RequestId>fd74fa8d-99f3-11e1-a4c3-27EXAMPLE804</RequestId>
</ResponseMetadata>
</ListInstanceProfilesResponse>
```

ListInstanceProfilesForRole

Lists the instance profiles that have the specified associated IAM role. If there are none, the action returns an empty list. For more information about instance profiles, go to About Instance Profiles.

You can paginate the results using the `MaxItems` and `Marker` parameters.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

This parameter is optional. If you do not include it, it defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true` and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

RoleName

The name of the role to list instance profiles for.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

Response Elements

The following elements are returned by the service.

InstanceProfiles.member.N

A list of instance profiles.

Type: array of InstanceProfile (p. 278) objects

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=ListInstanceProfilesForRole
&MaxItems=100
&RoleName=S3Access
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListInstanceProfilesForRoleResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
<ListInstanceProfilesForRoleResult>
  <IsTruncated>false</IsTruncated>
  <InstanceProfiles>
    <member>
      <Id>AIPACZLS2EYYXMEXAMPLE</Id>
      <Roles>
        <member>
          <Path>/application_abc/component_xyz/</Path>
          <Arn>arn:aws:iam::123456789012:role/application_abc/component_xyz/
S3Access</Arn>
          <RoleName>S3Access</RoleName>
          <AssumeRolePolicyDocument>
            {"Version":"2012-10-17","Statement":[{"Effect":"Allow",
            "Principal":{"Service":["ec2.amazonaws.com"]},"Action":
["sts:AssumeRole"]}]}
          </AssumeRolePolicyDocument>
          <CreateDate>2012-05-09T15:45:35Z</CreateDate>
          <RoleId>AROACVSVTSZYK3EXAMPLE</RoleId>
        </member>
      </Roles>
      <InstanceProfileName>Webserver</InstanceProfileName>
      <Path>/application_abc/component_xyz/</Path>
      <Arn>arn:aws:iam::123456789012:instance-profile/application_abc/
component_xyz/Webserver</Arn>
      <CreateDate>2012-05-09T16:27:11Z</CreateDate>
    </member>
  </InstanceProfiles>
</ListInstanceProfilesForRoleResult>
<ResponseMetadata>
  <RequestId>6a8c3992-99f4-11e1-a4c3-27EXAMPLE804</RequestId>
</ResponseMetadata>
</ListInstanceProfilesForRoleResponse>
```

ListMFADevices

Lists the MFA devices for an IAM user. If the request includes a IAM user name, then this action lists all the MFA devices associated with the specified user. If you do not specify a user name, IAM determines the user name implicitly based on the AWS access key ID signing the request for this API.

You can paginate the results using the `MaxItems` and `Marker` parameters.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

This parameter is optional. If you do not include it, it defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true` and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

UserName

The name of the user whose MFA devices you want to list.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: No

Response Elements

The following elements are returned by the service.

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

MFADevices.member.N

A list of MFA devices.

Type: array of MFADevice (p. 282) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=ListMFADevices
&UserName=Bob
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListMFADevicesResponse>
  <ListMFADevicesResult>
    <MFADevices>
       <member>
          <UserName>Bob</UserName>
          <SerialNumber>R1234</SerialNumber>
       </member>
    </MFADevices>
    <IsTruncated>false</IsTruncated>
  </ListMFADevicesResult>
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</ListMFADevicesResponse>
```

ListOpenIDConnectProviders

Lists information about the IAM OpenID Connect (OIDC) provider resource objects defined in the AWS account.

Response Elements

The following element is returned by the service.

OpenIDConnectProviderList.member.N

The list of IAM OIDC provider resource objects defined in the AWS account.

Type: array of OpenIDConnectProviderListEntry (p. 283) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=ListOpenIDConnectProviders
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListOpenIDConnectProvidersResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <ListOpenIDConnectProvidersResult>
    <OpenIDConnectProviderList>
      <member>
        <Arn>arn:aws:iam::123456789012:oidc-provider/server.example.com</Arn>
      </member>
      <member>
        <Arn>arn:aws:iam::123456789012:oidc-provider/server.example.org</Arn>
      </member>
    </OpenIDConnectProviderList>
  </ListOpenIDConnectProvidersResult>
  <ResponseMetadata>
    <RequestId>de2c0228-4f63-11e4-aefa-bfd6aEXAMPLE</RequestId>
  </ResponseMetadata>
</ListOpenIDConnectProvidersResponse>
```

ListPolicies

Lists all the managed policies that are available in your AWS account, including your own customer-defined managed policies and all AWS managed policies.

You can filter the list of policies that is returned using the optional `OnlyAttached`, `Scope`, and `PathPrefix` parameters. For example, to list only the customer managed policies in your AWS account, set `Scope` to `Local`. To list only AWS managed policies, set `Scope` to `AWS`.

You can paginate the results using the `MaxItems` and `Marker` parameters.

For more information about managed policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

This parameter is optional. If you do not include it, it defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true` and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

OnlyAttached

A flag to filter the results to only the attached policies.

When `OnlyAttached` is `true`, the returned list contains only the policies that are attached to an IAM user, group, or role. When `OnlyAttached` is `false`, or when the parameter is not included, all policies are returned.

Type: Boolean

Required: No

PathPrefix

The path prefix for filtering the results. This parameter is optional. If it is not included, it defaults to a slash (/), listing all policies. The regex pattern used to validate this parameter is a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes, containing any ASCII character from the ! (\u0021) thru the DEL character (\u007F), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Pattern: `((/[A-Za-z0-9\.,\+@=_-]+)*)/`

Required: No

Scope

The scope to use for filtering the results.

To list only AWS managed policies, set `Scope` to `AWS`. To list only the customer managed policies in your AWS account, set `Scope` to `Local`.

This parameter is optional. If it is not included, or if it is set to `All`, all policies are returned.

Type: String

Valid Values: `All | AWS | Local`

Required: No

Response Elements

The following elements are returned by the service.

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Policies.member.N

A list of policies.

Type: array of Policy (p. 286) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=ListPolicies
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListPoliciesResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ListPoliciesResult>
    <IsTruncated>true</IsTruncated>
    <Marker>EXAMPLEkakv9BCuUNFDtxWSyfzetYwEx2ADc8dnzfvERF5S6YMvXKx41t6gCl/
eeaCX3Jo94/bKqezEAg8TEVS
    99EKFLxm3jtbpl25FDWEXAMPLE
    </Marker>
    <Policies>
      <member>
        <PolicyName>ExamplePolicy</PolicyName>
        <DefaultVersionId>v1</DefaultVersionId>
        <PolicyId>AGPACKCEVSQ6C2EXAMPLE</PolicyId>
        <Path>/</Path>
        <Arn>arn:aws:iam::123456789012:policy/ExamplePolicy</Arn>
        <AttachmentCount>2</AttachmentCount>
        <CreateDate>2014-09-15T17:36:14Z</CreateDate>
        <UpdateDate>2014-09-15T20:31:47Z</UpdateDate>
      </member>
      <member>
        <PolicyName>PowerUserAccess</PolicyName>
        <DefaultVersionId>v1</DefaultVersionId>
        <PolicyId>AGPACKCEVSQ6C2EXAMPLE</PolicyId>
        <Path>/</Path>
        <Arn>arn:aws:iam::aws:policy/PowerUserAccess</Arn>
        <AttachmentCount>0</AttachmentCount>
        <CreateDate>2014-08-21T20:25:01Z</CreateDate>
        <UpdateDate>2014-08-21T20:25:01Z</UpdateDate>
      </member>
      <member>
        <PolicyName>AdministratorAccess</PolicyName>
        <DefaultVersionId>v1</DefaultVersionId>
        <PolicyId>AGPACKCEVSQ6C2EXAMPLE</PolicyId>
        <Path>/</Path>
        <Arn>arn:aws:iam::aws:policy/AdministratorAccess</Arn>
        <AttachmentCount>1</AttachmentCount>
        <CreateDate>2014-08-21T20:11:25Z</CreateDate>
        <UpdateDate>2014-08-21T20:11:25Z</UpdateDate>
      </member>
      <member>
        <PolicyName>ReadOnlyAccess</PolicyName>
        <DefaultVersionId>v1</DefaultVersionId>
        <PolicyId>AGPACKCEVSQ6C2EXAMPLE</PolicyId>
        <Path>/</Path>
        <Arn>arn:aws:iam::aws:policy/ReadOnlyAccess</Arn>
        <AttachmentCount>6</AttachmentCount>
        <CreateDate>2014-08-21T20:31:44Z</CreateDate>
        <UpdateDate>2014-08-21T20:31:44Z</UpdateDate>
      </member>
    </Policies>
  </ListPoliciesResult>
  <ResponseMetadata>
    <RequestId>6207e832-3eb7-11e4-9d0d-6f969EXAMPLE</RequestId>
  </ResponseMetadata>
</ListPoliciesResponse>
```

ListPolicyVersions

Lists information about the versions of the specified managed policy, including the version that is currently set as the policy's default version.

For more information about managed policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

This parameter is optional. If you do not include it, it defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true` and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

PolicyArn

The Amazon Resource Name (ARN) of the IAM policy for which you want the versions.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Response Elements

The following elements are returned by the service.

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Versions.member.N

A list of policy versions.

For more information about managed policy versions, see Versioning for Managed Policies in the *IAM User Guide*.

Type: array of PolicyVersion (p. 292) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=ListPolicyVersions
&PolicyArn=arn:aws:iam::123456789012:policy/S3-read-only-example-bucket
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListPolicyVersionsResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <ListPolicyVersionsResult>
    <Versions>
      <member>
        <IsDefaultVersion>false</IsDefaultVersion>
        <VersionId>v3</VersionId>
        <CreateDate>2014-09-17T22:32:43Z</CreateDate>
      </member>
      <member>
        <IsDefaultVersion>true</IsDefaultVersion>
        <VersionId>v2</VersionId>
        <CreateDate>2014-09-15T20:31:47Z</CreateDate>
      </member>
      <member>
```

```
        <IsDefaultVersion>false</IsDefaultVersion>
        <VersionId>v1</VersionId>
        <CreateDate>2014-09-15T17:36:14Z</CreateDate>
      </member>
    </Versions>
    <IsTruncated>false</IsTruncated>
  </ListPolicyVersionsResult>
  <ResponseMetadata>
    <RequestId>a31d1a86-3eba-11e4-9d0d-6f969EXAMPLE</RequestId>
  </ResponseMetadata>
</ListPolicyVersionsResponse>
```

ListRolePolicies

Lists the names of the inline policies that are embedded in the specified IAM role.

An IAM role can also have managed policies attached to it. To list the managed policies that are attached to a role, use ListAttachedRolePolicies (p. 154). For more information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

You can paginate the results using the `MaxItems` and `Marker` parameters. If there are no inline policies embedded with the specified role, the action returns an empty list.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

This parameter is optional. If you do not include it, it defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true` and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

RoleName

The name of the role to list policies for.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

Response Elements

The following elements are returned by the service.

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

PolicyNames.member.N

A list of policy names.

Type: array of Strings

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=ListRolePolicies
&RoleName=S3Access
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListRolePoliciesResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
<ListRolePoliciesResult>
  <PolicyNames>
    <member>CloudwatchPutMetricPolicy</member>
    <member>S3AccessPolicy</member>
  </PolicyNames>
  <IsTruncated>false</IsTruncated>
</ListRolePoliciesResult>
<ResponseMetadata>
  <RequestId>8c7e1816-99f0-11e1-a4c3-27EXAMPLE804</RequestId>
</ResponseMetadata>
</ListRolePoliciesResponse>
```

ListRoles

Lists the IAM roles that have the specified path prefix. If there are none, the action returns an empty list. For more information about roles, go to Working with Roles.

You can paginate the results using the `MaxItems` and `Marker` parameters.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

This parameter is optional. If you do not include it, it defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true` and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

PathPrefix

The path prefix for filtering the results. For example, the prefix `/application_abc/component_xyz/` gets all roles whose path starts with `/application_abc/component_xyz/`.

This parameter is optional. If it is not included, it defaults to a slash (/), listing all roles. The regex pattern used to validate this parameter is a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes, containing any ASCII character from the ! (\u0021) thru the DEL character (\u007F), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `\u002F[\u0021-\u007F]*`

Required: No

Response Elements

The following elements are returned by the service.

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Roles.member.N

A list of roles.

Type: array of Role (p. 295) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=ListRoles
&MaxItems=100
&PathPrefix=/application_abc/
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListRolesResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
<ListRolesResult>
  <IsTruncated>false</IsTruncated>
  <Roles>
    <member>
      <Path>/application_abc/component_xyz/</Path>
      <Arn>arn:aws:iam::123456789012:role/application_abc/component_xyz/
S3Access</Arn>
      <RoleName>S3Access</RoleName>
      <AssumeRolePolicyDocument>
        {"Version":"2012-10-17","Statement":[{"Effect":"Allow",
        "Principal":{"Service":["ec2.amazonaws.com"]},"Action":
["sts:AssumeRole"]}]}
      </AssumeRolePolicyDocument>
      <CreateDate>2012-05-09T15:45:35Z</CreateDate>
      <RoleId>AROACVSVTSZYEXAMPLEYK</RoleId>
    </member>
    <member>
      <Path>/application_abc/component_xyz/</Path>
      <Arn>arn:aws:iam::123456789012:role/application_abc/component_xyz/
SDBAccess</Arn>
```

```
      <RoleName>SDBAccess</RoleName>
      <AssumeRolePolicyDocument>
        {"Version":"2012-10-17","Statement":[{"Effect":"Allow",
        "Principal":{"Service":["ec2.amazonaws.com"]},"Action":
["sts:AssumeRole"]}]}
      </AssumeRolePolicyDocument>
      <CreateDate>2012-05-09T15:45:45Z</CreateDate>
      <RoleId>AROAC2ICXG32EXAMPLEWK</RoleId>
    </member>
  </Roles>
</ListRolesResult>
<ResponseMetadata>
  <RequestId>20f7279f-99ee-11e1-a4c3-27EXAMPLE804</RequestId>
</ResponseMetadata>
</ListRolesResponse>
```

ListSAMLProviders

Lists the SAML provider resource objects defined in IAM in the account.

Note
This operation requires Signature Version 4.

Response Elements

The following element is returned by the service.

SAMLProviderList.member.N

The list of SAML provider resource objects defined in IAM for this AWS account.

Type: array of SAMLProviderListEntry (p. 298) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=ListSAMLProviders
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListSAMLProvidersResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
<ListSAMLProvidersResult>
  <SAMLProviderList>
    <member>
      <Arn>arn:aws:iam::123456789012:saml-provider/MyUniversity</Arn>
      <ValidUntil>2032-05-09T16:27:11Z</ValidUntil>
      <CreateDate>2012-05-09T16:27:03Z</CreateDate>
    </member>
    <member>
      <Arn>arn:aws:iam::123456789012:saml-provider/MyUniversity</Arn>
      <ValidUntil>2015-03-11T13:11:02Z</ValidUntil>
      <CreateDate>2012-05-09T16:27:11Z</CreateDate>
    </member>
  </SAMLProviderList>
</ListSAMLProvidersResult>
<ResponseMetadata>
  <RequestId>fd74fa8d-99f3-11e1-a4c3-27EXAMPLE804</RequestId>
</ResponseMetadata>
</ListSAMLProvidersResponse>
```

ListServerCertificates

Lists the server certificates stored in IAM that have the specified path prefix. If none exist, the action returns an empty list.

You can paginate the results using the `MaxItems` and `Marker` parameters.

For more information about working with server certificates, including a list of AWS services that can use the server certificates that you manage with IAM, go to Working with Server Certificates in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

This parameter is optional. If you do not include it, it defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true` and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

PathPrefix

The path prefix for filtering the results. For example: `/company/servercerts` would get all server certificates for which the path starts with `/company/servercerts`.

This parameter is optional. If it is not included, it defaults to a slash (/), listing all server certificates. The regex pattern used to validate this parameter is a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes, containing any ASCII character from the ! (\u0021) thru the DEL character (\u007F), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `\u002F[\u0021-\u007F]*`

Required: No

Response Elements

The following elements are returned by the service.

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more

items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

ServerCertificateMetadataList.member.N

A list of server certificates.

Type: array of ServerCertificateMetadata (p. 300) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=ListServerCertificates
&PathPrefix=/company/servercerts
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListServerCertificatesResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
<ListServerCertificatesResult>
  <IsTruncated>false</IsTruncated>
  <ServerCertificateMetadataList>
    <member>
      <ServerCertificateMetadata>
        <ServerCertificateName>ProdServerCert</ServerCertificateName>
        <Path>/company/servercerts/</Path>
        <Arn>arn:aws:iam::123456789012:server-certificate/company/
servercerts/ProdServerCert</Arn>
        <UploadDate>2010-05-08T01:02:03.004Z</UploadDate>
        <ServerCertificateId>ASCACKCEVSQ6CEXAMPLE1</ServerCertificateId>
        <Expiration>2012-05-08T01:02:03.004Z</Expiration>
      </ServerCertificateMetadata>
    </member>
    <member>
      <ServerCertificateMetadata>
        <ServerCertificateName>BetaServerCert</ServerCertificateName>
        <Path>/company/servercerts/</Path>
        <Arn>arn:aws:iam::123456789012:server-certificate/company/
servercerts/BetaServerCert</Arn>
        <UploadDate>2010-05-08T02:03:01.004Z</UploadDate>
        <ServerCertificateId>ASCACKCEVSQ6CEXAMPLE2</ServerCertificateId>
        <Expiration>2012-05-08T02:03:01.004Z</Expiration>
      </ServerCertificateMetadata>
    </member>
    <member>
      <ServerCertificateMetadata>
        <ServerCertificateName>TestServerCert</ServerCertificateName>
        <Path>/company/servercerts/</Path>
        <Arn>arn:aws:iam::123456789012:server-certificate/company/
servercerts/TestServerCert</Arn>
        <UploadDate>2010-05-08T03:01:02.004Z</UploadDate>
        <ServerCertificateId>ASCACKCEVSQ6CEXAMPLE3</ServerCertificateId>
        <Expiration>2012-05-08T03:01:02.004Z</Expiration>
      </ServerCertificateMetadata>
    </member>
  </ServerCertificateMetadataList>
</ListServerCertificatesResult>
<ResponseMetadata>
  <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
</ResponseMetadata>
</ListServerCertificatesResponse>
```

ListSigningCertificates

Returns information about the signing certificates associated with the specified IAM user. If there are none, the action returns an empty list.

Although each user is limited to a small number of signing certificates, you can still paginate the results using the `MaxItems` and `Marker` parameters.

If the `UserName` field is not specified, the user name is determined implicitly based on the AWS access key ID used to sign the request for this API. Because this action works for access keys under the AWS account, you can use this action to manage root credentials even if the AWS account has no associated users.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

This parameter is optional. If you do not include it, it defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true` and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

UserName

The name of the IAM user whose signing certificates you want to examine.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: No

Response Elements

The following elements are returned by the service.

Certificates.member.N

A list of the user's signing certificate information.

Type: array of SigningCertificate (p. 301) objects

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=ListSigningCertificates
&UserName=Bob
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListSigningCertificatesResponse>
  <ListSigningCertificatesResult>
    <UserName>Bob</UserName>
    <Certificates>
       <member>
          <UserName>Bob</UserName>
          <CertificateId>TA7SMEXAMPLEZ26OBPJE7EXAMPLE</CertificateId>
          <CertificateBody>
-----BEGIN CERTIFICATE-----
MIICdzCCAeCgAwIBAgIGANc+Ha2wMA0GCSqGSIb3DQEBBQUAMFMxCzAJBgNVBAYT
AlVTMRMwEQYDVQQKEwpBbWF6b24uY29tMQwwCgYDVQQLEwNBV1MxITAfBgNVBAMT
GEFXUyBMaW1pdGVkLUFzc3VyYW5jZSBDQTAeFw0wOTAyMDQxNzE5MjdaFw0xMDAy
MDQxNzE5MjdaMFIxCzAJBgNVBAYTAlVTMRMwEQYDVQQKEwpBbWF6b24uY29tMRcw
FQYDVQQLEw5BV1MtRGV2ZWxvcGVyczEVMBMGA1UEAxMMNTdxNDl0c3ZwYjRtMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpB/vsOwmT/O0td1RqzKjttSBaPjbr
```

```
dqwNe9BrOyB08fw2+Ch5oonZYXfGUrT6mkYXH5fQot9HvASrzAKHO596FdJA6DmL
ywdWe1Oggk7zFSXO1Xv+3vPrJtaYxYo3eRIp7w80PMkiOv6M0XK8ubcTouODeJbf
suDqcLnLDxwsvwIDAQABo1cwVTAOBgNVHQ8BAf8EBAMCBaAwFgYDVR0lAQH/BAww
CgYIKwYBBQUHAwIwDAYDVR0TAQH/BAIwADAdBgNVHQ4EFgQULGNaBphBumaKbDRK
CAi0mH8B3mowDQYJKoZIhvcNAQEFBQADgYEAuKxhkXaCLGcqDuweKtO/AEw9ZePH
wr0XqsaIK2HZboqruebXEGsojK4Ks0WzwgrEynuHJwTn760xe39rSqXWIOGrOBaX
wFpWHVjTFMKk+tSDG1lssLHyYWWdFFU4AnejRGORJYNaRHgVTKjHphc5jEhHm0BX
AEaHzTpmEXAMPLE=
-----END CERTIFICATE-----
          </CertificateBody>
          <Status>Active</Status>
       </member>
    </Certificates>
    <IsTruncated>false</IsTruncated>
 </ListSigningCertificatesResult>
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</ListSigningCertificatesResponse>
```

ListSSHPublicKeys

Returns information about the SSH public keys associated with the specified IAM user. If there are none, the action returns an empty list.

The SSH public keys returned by this action are used only for authenticating the IAM user to an AWS CodeCommit repository. For more information about using SSH keys to authenticate to an AWS CodeCommit repository, see Set up AWS CodeCommit for SSH Connections in the *AWS CodeCommit User Guide*.

Although each user is limited to a small number of keys, you can still paginate the results using the `MaxItems` and `Marker` parameters.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

This parameter is optional. If you do not include it, it defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true` and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

UserName

The name of the IAM user to list SSH public keys for. If none is specified, the UserName field is determined implicitly based on the AWS access key used to sign the request.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: No

Response Elements

The following elements are returned by the service.

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more

items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

SSHPublicKeys.member.N

A list of the SSH public keys assigned to IAM user.

Type: array of SSHPublicKeyMetadata (p. 303) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

Example

Sample Request

```
https://iam.amazonaws.com/?Action=ListSSHPublicKeys
&UserName=Jane
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListSSHPublicKeysResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ListSSHPublicKeysResult>
    <IsTruncated>false</IsTruncated>
    <SSHPublicKeys>
      <member>
        <UploadDate>2015-06-05T20:56:46Z</UploadDate>
        <UserName>Jane</UserName>
        <SSHPublicKeyId>APKAEIVFHP46CEXAMPLE</SSHPublicKeyId>
        <Status>Active</Status>
      </member>
    </SSHPublicKeys>
  </ListSSHPublicKeysResult>
  <ResponseMetadata>
    <RequestId>9f8e2d77-f36c-11e4-97db-33c4eEXAMPLE</RequestId>
  </ResponseMetadata>
</ListSSHPublicKeysResponse>
```

ListUserPolicies

Lists the names of the inline policies embedded in the specified IAM user.

An IAM user can also have managed policies attached to it. To list the managed policies that are attached to a user, use ListAttachedUserPolicies (p. 157). For more information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

You can paginate the results using the `MaxItems` and `Marker` parameters. If there are no inline policies embedded with the specified user, the action returns an empty list.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

This parameter is optional. If you do not include it, it defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true` and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

UserName

The name of the user to list policies for.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Response Elements

The following elements are returned by the service.

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

PolicyNames.member.N

A list of policy names.

Type: array of Strings

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=ListUserPolicies
&UserName=Bob
&AUTHPARAMS
```

Sample Response

```
<ListUserPoliciesResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
 <ListUserPoliciesResult>
    <PolicyNames>
       <member>AllAccessPolicy</member>
       <member>KeyPolicy</member>
    </PolicyNames>
    <IsTruncated>false</IsTruncated>
 </ListUserPoliciesResult>
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</ListUserPoliciesResponse>
```

ListUsers

Lists the IAM users that have the specified path prefix. If no path prefix is specified, the action returns all users in the AWS account. If there are none, the action returns an empty list.

You can paginate the results using the `MaxItems` and `Marker` parameters.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

This parameter is optional. If you do not include it, it defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true` and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

PathPrefix

The path prefix for filtering the results. For example: `/division_abc/subdivision_xyz/`, which would get all user names whose path starts with `/division_abc/subdivision_xyz/`.

This parameter is optional. If it is not included, it defaults to a slash (/), listing all user names. The regex pattern used to validate this parameter is a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes, containing any ASCII character from the ! (\u0021) thru the DEL character (\u007F), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `\u002F[\u0021-\u007F]*`

Required: No

Response Elements

The following elements are returned by the service.

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Users.member.N

A list of users.

Type: array of User (p. 305) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=ListUsers
&PathPrefix=/division_abc/subdivision_xyz/product_1234/engineering/
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListUsersResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
 <ListUsersResult>
    <Users>
       <member>
          <UserId>AID2MAB8DPLSRHEXAMPLE</UserId>
          <Path>/division_abc/subdivision_xyz/engineering/</Path>
          <UserName>Andrew</UserName>
          <Arn>arn:aws:iam::123456789012:user/division_abc/subdivision_xyz/
engineering/Andrew</Arn>
          <CreateDate>2012-09-05T19:38:48Z</CreateDate>
          <PasswordLastUsed>2014-09-08T21:47:36Z</PasswordLastUsed>
       </member>
       <member>
          <UserId>AIDIODR4TAW7CSEXAMPLE</UserId>
          <Path>/division_abc/subdivision_xyz/engineering/</Path>
          <UserName>Jackie</UserName>
          <Arn>arn:aws:iam::123456789012:user/division_abc/subdivision_xyz/
engineering/Jackie</Arn>
          <CreateDate>2014-04-09T15:43:45Z</CreateDate>
          <PasswordLastUsed>2014-09-24T16:18:07Z</PasswordLastUsed>
       </member>
    </Users>
    <IsTruncated>false</IsTruncated>
 </ListUsersResult>
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</ListUsersResponse>
```

ListVirtualMFADevices

Lists the virtual MFA devices defined in the AWS account by assignment status. If you do not specify an assignment status, the action returns a list of all virtual MFA devices. Assignment status can be `Assigned`, `Unassigned`, or `Any`.

You can paginate the results using the `MaxItems` and `Marker` parameters.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

AssignmentStatus

The status (`Unassigned` or `Assigned`) of the devices to list. If you do not specify an `AssignmentStatus`, the action defaults to `Any` which lists both assigned and unassigned virtual MFA devices.

Type: String

Valid Values: `Assigned | Unassigned | Any`

Required: No

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

This parameter is optional. If you do not include it, it defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true` and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

Response Elements

The following elements are returned by the service.

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

VirtualMFADevices.member.N

The list of virtual MFA devices in the current account that match the `AssignmentStatus` value that was passed in the request.

Type: array of VirtualMFADevice (p. 309) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

Example

Sample Request

```
https://iam.amazonaws.com/?Action=ListVirtualMFADevices
&AssignmentStatus=Any
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListVirtualMFADevicesResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
<ListVirtualMFADevicesResult>
  <IsTruncated>false</IsTruncated>
  <VirtualMFADevices>
    <member>
      <SerialNumber>
      arn:aws:iam::123456789012:mfa/MFAdeviceName
      </SerialNumber>
    </member>
    <member>
      <SerialNumber>
      arn:aws:iam::123456789012:mfa/RootMFAdeviceName
      </SerialNumber>
      <EnableDate>2011-10-20T20:49:03Z</EnableDate>
      <User>
        <UserId>123456789012</UserId>
        <Arn>arn:aws:iam::123456789012:root</Arn>
        <CreateDate>2009-10-13T22:00:36Z</CreateDate>
      </User>
    </member>
    <member>
      <SerialNumber>
      arn:aws:iam:::mfa/ExampleUserMFAdeviceName
      </SerialNumber>
      <EnableDate>2011-10-31T20:45:02Z</EnableDate>
      <User>
        <UserId>AIDEXAMPLE4EXAMPLEXYZ</UserId>
        <Path>/</Path>
        <UserName>ExampleUser</UserName>
        <Arn>arn:aws:iam::111122223333:user/ExampleUser</Arn>
        <CreateDate>2011-07-01T17:23:07Z</CreateDate>
      </User>
    </member>
  </VirtualMFADevices>
</ListVirtualMFADevicesResult>
<ResponseMetadata>
  <RequestId>b61ce1b1-0401-11e1-b2f8-2dEXAMPLEbfc</RequestId>
</ResponseMetadata>
</ListVirtualMFADevicesResponse>
```

PutGroupPolicy

Adds or updates an inline policy document that is embedded in the specified IAM group.

A user can also have managed policies attached to it. To attach a managed policy to a group, use AttachGroupPolicy (p. 11). To create a new managed policy, use CreatePolicy (p. 32). For information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

For information about limits on the number of inline policies that you can embed in a group, see Limitations on IAM Entities in the *IAM User Guide*.

> **Note**
> Because policy documents can be large, you should use POST rather than GET when calling `PutGroupPolicy`. For general information about using the Query API with IAM, go to Making Query Requests in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

GroupName

The name of the group to associate the policy with.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

PolicyDocument

The policy document.

The regex pattern used to validate this parameter is a string of characters consisting of any printable ASCII character ranging from the space character (\u0020) through end of the ASCII character range (\u00FF). It also includes the special characters tab (\u0009), line feed (\u000A), and carriage return (\u000D).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

PolicyName

The name of the policy document.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

MalformedPolicyDocument

The request was rejected because the policy document was malformed. The error message describes the specific error.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=PutGroupPolicy
&GroupName=Admins
&PolicyName=AdminRoot
&PolicyDocument={"Version":"2012-10-17","Statement":
{"Effect":"Allow","Action":"*","Resource":"*"}}
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<PutGroupPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</PutGroupPolicyResponse>
```

PutRolePolicy

Adds or updates an inline policy document that is embedded in the specified IAM role.

When you embed an inline policy in a role, the inline policy is used as part of the role's access (permissions) policy. The role's trust policy is created at the same time as the role, using CreateRole (p. 38). You can update a role's trust policy using UpdateAssumeRolePolicy (p. 239). For more information about IAM roles, go to Using Roles to Delegate Permissions and Federate Identities.

A role can also have a managed policy attached to it. To attach a managed policy to a role, use AttachRolePolicy (p. 13). To create a new managed policy, use CreatePolicy (p. 32). For information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

For information about limits on the number of inline policies that you can embed with a role, see Limitations on IAM Entities in the *IAM User Guide*.

> **Note**
> Because policy documents can be large, you should use POST rather than GET when calling `PutRolePolicy`. For general information about using the Query API with IAM, go to Making Query Requests in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

PolicyDocument

The policy document.

The regex pattern used to validate this parameter is a string of characters consisting of any printable ASCII character ranging from the space character (\u0020) through end of the ASCII character range (\u00FF). It also includes the special characters tab (\u0009), line feed (\u000A), and carriage return (\u000D).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

PolicyName

The name of the policy document.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

RoleName

The name of the role to associate the policy with.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

MalformedPolicyDocument

The request was rejected because the policy document was malformed. The error message describes the specific error.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=PutRolePolicy
&RoleName=S3Access
&PolicyName=S3AccessPolicy
&PolicyDocument={"Version":"2012-10-17","Statement":
{"Effect":"Allow","Action":"s3:*","Resource":"*"}}
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<PutRolePolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</PutRolePolicyResponse>
```

PutUserPolicy

Adds or updates an inline policy document that is embedded in the specified IAM user.

An IAM user can also have a managed policy attached to it. To attach a managed policy to a user, use AttachUserPolicy (p. 15). To create a new managed policy, use CreatePolicy (p. 32). For information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

For information about limits on the number of inline policies that you can embed in a user, see Limitations on IAM Entities in the *IAM User Guide*.

> **Note**
> Because policy documents can be large, you should use POST rather than GET when calling `PutUserPolicy`. For general information about using the Query API with IAM, go to Making Query Requests in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

PolicyDocument

The policy document.

The regex pattern used to validate this parameter is a string of characters consisting of any printable ASCII character ranging from the space character (\u0020) through end of the ASCII character range (\u00FF). It also includes the special characters tab (\u0009), line feed (\u000A), and carriage return (\u000D).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

PolicyName

The name of the policy document.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

UserName

The name of the user to associate the policy with.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

MalformedPolicyDocument

The request was rejected because the policy document was malformed. The error message describes the specific error.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=PutUserPolicy
&UserName=Bob
&PolicyName=AllAccessPolicy
&PolicyDocument={"Version":"2012-10-17","Statement":
{"Effect":"Allow","Action":"*","Resource":"*"}}
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<PutUserPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</PutUserPolicyResponse>
```

RemoveClientIDFromOpenIDConnectProvider

Removes the specified client ID (also known as audience) from the list of client IDs registered for the specified IAM OpenID Connect (OIDC) provider resource object.

This action is idempotent; it does not fail or return an error if you try to remove a client ID that does not exist.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

ClientID

The client ID (also known as audience) to remove from the IAM OIDC provider resource. For more information about client IDs, see CreateOpenIDConnectProvider (p. 29).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Required: Yes

OpenIDConnectProviderArn

The Amazon Resource Name (ARN) of the IAM OIDC provider resource to remove the client ID from. You can get a list of OIDC provider ARNs by using the ListOpenIDConnectProviders (p. 178) action.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=RemoveClientIDFromOpenIDConnectProvider
&ClientID=my-application-ID
```

```
&OpenIDConnectProviderArn=arn:aws:iam::123456789012:oidc-provider/
server.example.com
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<RemoveClientIDFromOpenIDConnectProviderResponse xmlns="https://
iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>1a5214df-4f67-11e4-aefa-bfd6aEXAMPLE</RequestId>
  </ResponseMetadata>
</RemoveClientIDFromOpenIDConnectProviderResponse>
```

RemoveRoleFromInstanceProfile

Removes the specified IAM role from the specified EC2 instance profile.

> **Important**
> Make sure you do not have any Amazon EC2 instances running with the role you are about to remove from the instance profile. Removing a role from an instance profile that is associated with a running instance break any applications running on the instance.

For more information about IAM roles, go to Working with Roles. For more information about instance profiles, go to About Instance Profiles.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

InstanceProfileName

The name of the instance profile to update.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

RoleName

The name of the role to remove.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=RemoveRoleFromInstanceProfile
&InstanceProfileName=Webserver
&RoleName=S3Access
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<RemoveRoleFromInstanceProfileResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
<ResponseMetadata>
  <RequestId>29f47818-99f5-11e1-a4c3-27EXAMPLE804</RequestId>
</ResponseMetadata>
</RemoveRoleFromInstanceProfileResponse>
```

RemoveUserFromGroup

Removes the specified user from the specified group.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

GroupName

The name of the group to update.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

UserName

The name of the user to remove.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=RemoveUserFromGroup
&GroupName=Managers
```

```
&UserName=Bob
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<RemoveUserFromGroupResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</RemoveUserFromGroupResponse>
```

ResyncMFADevice

Synchronizes the specified MFA device with its IAM resource object on the AWS servers.

For more information about creating and working with virtual MFA devices, go to Using a Virtual MFA Device in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

AuthenticationCode1

An authentication code emitted by the device.

The format for this parameter is a sequence of six digits.

Type: String

Length Constraints: Fixed length of 6.

Pattern: `[\d]+`

Required: Yes

AuthenticationCode2

A subsequent authentication code emitted by the device.

The format for this parameter is a sequence of six digits.

Type: String

Length Constraints: Fixed length of 6.

Pattern: `[\d]+`

Required: Yes

SerialNumber

Serial number that uniquely identifies the MFA device.

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

Type: String

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

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

Required: Yes

UserName

The name of the user whose MFA device you want to resynchronize.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidAuthenticationCode

The request was rejected because the authentication code was not recognized. The error message describes the specific error.

HTTP Status Code: 403

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=ResyncMFADevice
&UserName=Bob
&SerialNumber=R1234
&AuthenticationCode1=234567
&AuthenticationCode2=987654
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ResyncMFADeviceResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</ResyncMFADeviceResponse>
```

SetDefaultPolicyVersion

Sets the specified version of the specified policy as the policy's default (operative) version.

This action affects all users, groups, and roles that the policy is attached to. To list the users, groups, and roles that the policy is attached to, use the ListEntitiesForPolicy (p. 160) API.

For information about managed policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

PolicyArn

The Amazon Resource Name (ARN) of the IAM policy whose default version you want to set.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

VersionId

The version of the policy to set as the default (operative) version.

For more information about managed policy versions, see Versioning for Managed Policies in the *IAM User Guide*.

Type: String

Pattern: `v[1-9][0-9]*(\.[A-Za-z0-9-]*)?`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=SetDefaultPolicyVersion
&PolicyArn=arn:aws:iam::123456789012:policy/S3-read-only-example-bucket
&VersionId=v3
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<SetDefaultPolicyVersionResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>35f241af-3ebc-11e4-9d0d-6f969EXAMPLE</RequestId>
  </ResponseMetadata>
</SetDefaultPolicyVersionResponse>
```

SimulateCustomPolicy

Simulate how a set of IAM policies and optionally a resource-based policy works with a list of API actions and AWS resources to determine the policies' effective permissions. The policies are provided as strings.

The simulation does not perform the API actions; it only checks the authorization to determine if the simulated policies allow or deny the actions.

If you want to simulate existing policies attached to an IAM user, group, or role, use SimulatePrincipalPolicy (p. 228) instead.

Context keys are variables maintained by AWS and its services that provide details about the context of an API query request. You can use the `Condition` element of an IAM policy to evaluate context keys. To get the list of context keys that the policies require for correct simulation, use GetContextKeysForCustomPolicy (p. 110).

If the output is long, you can use `MaxItems` and `Marker` parameters to paginate the results.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

ActionNames.member.N

A list of names of API actions to evaluate in the simulation. Each action is evaluated against each resource. Each action must include the service identifier, such as `iam:CreateUser`.

Type: array of Strings

Length Constraints: Minimum length of 3. Maximum length of 128.

Required: Yes

CallerArn

The ARN of the IAM user that you want to use as the simulated caller of the APIs. `CallerArn` is required if you include a `ResourcePolicy` so that the policy's `Principal` element has a value to use in evaluating the policy.

You can specify only the ARN of an IAM user. You cannot specify the ARN of an assumed role, federated user, or a service principal.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

ContextEntries.member.N

A list of context keys and corresponding values for the simulation to use. Whenever a context key is evaluated in one of the simulated IAM permission policies, the corresponding value is supplied.

Type: array of ContextEntry (p. 273) objects

Required: No

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

This parameter is optional. If you do not include it, it defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true` and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

PolicyInputList.member.N

A list of policy documents to include in the simulation. Each document is specified as a string containing the complete, valid JSON text of an IAM policy. Do not include any resource-based policies in this parameter. Any resource-based policy must be submitted with the `ResourcePolicy` parameter. The policies cannot be "scope-down" policies, such as you could include in a call to GetFederationToken or one of the AssumeRole APIs to restrict what a user can do while using the temporary credentials.

The regex pattern used to validate this parameter is a string of characters consisting of any printable ASCII character ranging from the space character (\u0020) through end of the ASCII character range (\u00FF). It also includes the special characters tab (\u0009), line feed (\u000A), and carriage return (\u000D).

Type: array of Strings

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

ResourceArns.member.N

A list of ARNs of AWS resources to include in the simulation. If this parameter is not provided then the value defaults to `*` (all resources). Each API in the `ActionNames` parameter is evaluated for each resource in this list. The simulation determines the access result (allowed or denied) of each combination and reports it in the response.

The simulation does not automatically retrieve policies for the specified resources. If you want to include a resource policy in the simulation, then you must include the policy as a string in the `ResourcePolicy` parameter.

If you include a `ResourcePolicy`, then it must be applicable to all of the resources included in the simulation or you receive an invalid input error.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: array of Strings

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

ResourceHandlingOption

Specifies the type of simulation to run. Different APIs that support resource-based policies require different combinations of resources. By specifying the type of simulation to run, you enable the policy simulator to enforce the presence of the required resources to ensure reliable simulation results. If your simulation does not match one of the following scenarios, then you can omit this parameter. The following list shows each of the supported scenario values and the resources that you must define to run the simulation.

Each of the EC2 scenarios requires that you specify instance, image, and security-group resources. If your scenario includes an EBS volume, then you must specify that volume as a resource. If the EC2 scenario includes VPC, then you must supply the network-interface resource. If it includes an IP subnet, then you must specify the subnet resource. For more information on the EC2 scenario options, see Supported Platforms in the *AWS EC2 User Guide*.

- **EC2-Classic-InstanceStore**

  instance, image, security-group
- **EC2-Classic-EBS**

  instance, image, security-group, volume

- **EC2-VPC-InstanceStore**

  instance, image, security-group, network-interface
- **EC2-VPC-InstanceStore-Subnet**

  instance, image, security-group, network-interface, subnet
- **EC2-VPC-EBS**

  instance, image, security-group, network-interface, volume
- **EC2-VPC-EBS-Subnet**

  instance, image, security-group, network-interface, subnet, volume

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Required: No

ResourceOwner

An AWS account ID that specifies the owner of any simulated resource that does not identify its owner in the resource ARN, such as an S3 bucket or object. If `ResourceOwner` is specified, it is also used as the account owner of any `ResourcePolicy` included in the simulation. If the `ResourceOwner` parameter is not specified, then the owner of the resources and the resource policy defaults to the account of the identity provided in `CallerArn`. This parameter is required only if you specify a resource-based policy and account that owns the resource is different from the account that owns the simulated calling user `CallerArn`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

ResourcePolicy

A resource-based policy to include in the simulation provided as a string. Each resource in the simulation is treated as if it had this policy attached. You can include only one resource-based policy in a simulation.

The regex pattern used to validate this parameter is a string of characters consisting of any printable ASCII character ranging from the space character (\u0020) through end of the ASCII character range (\u00FF). It also includes the special characters tab (\u0009), line feed (\u000A), and carriage return (\u000D).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: No

Response Elements

The following elements are returned by the service.

EvaluationResults.member.N

The results of the simulation.

Type: array of EvaluationResult (p. 274) objects

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

PolicyEvaluation

The request failed because a provided policy could not be successfully evaluated. An additional detail message indicates the source of the failure.

HTTP Status Code: 500

Example

Example

This example specifies a policy by string and supplies a `ContextEntry` to use for the context key that the policy references. Note that all parameters are shown in unencoded form here for clarity but must be URL encoded to be included as a part of a real HTML request. The results show that the policy allows `s3:ListBucket` access to the S3 bucket named `teambucket`.

Sample Request

```
https://iam.amazonaws.com/Action=SimulateCustomPolicy
&ActionNames.member.1=s3:ListBucket
&ResourceArns.member.1=arn:aws:s3:::teambucket
&ContextEntries.member.1.ContextKeyName=aws:MultiFactorAuthPresent
&ContextEntries.member.1.ContextKeyType=boolean
&ContextEntries.member.1.ContextKeyValues.member.1=true
&PolicyInputList.member.1='{
  "Version":"2012-10-17",
  "Statement":{
    "Effect":"Allow",
    "Action":"s3:ListBucket",
    "Resource":"arn:aws:s3:::teambucket",
    "Condition":{
      "Bool":{"aws:MultiFactorAuthPresent":"true"}
    }
  }
}'
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<SimulateCustomPolicyResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
```

```
  <SimulateCustomPolicyResult>
    <IsTruncated>false</IsTruncated>
    <EvaluationResults>
      <member>
        <MatchedStatements>
          <member>
            <SourcePolicyId>PolicyInputList.1</SourcePolicyId>
            <EndPosition>
              <Column>4</Column>
              <Line>11</Line>
            </EndPosition>
            <StartPosition>
              <Column>16</Column>
              <Line>4</Line>
            </StartPosition>
          </member>
        </MatchedStatements>
        <MissingContextValues/>
        <EvalResourceName>arn:aws:s3:::teambucket</EvalResourceName>
        <EvalDecision>allowed</EvalDecision>
        <EvalActionName>s3:ListBucket</EvalActionName>
      </member>
    </EvaluationResults>
  </SimulateCustomPolicyResult>
  <ResponseMetadata>
    <RequestId>1cdb5b0a-4c15-11e5-b121-bd8c7EXAMPLE</RequestId>
  </ResponseMetadata>
</SimulateCustomPolicyResponse>
```

SimulatePrincipalPolicy

Simulate how a set of IAM policies attached to an IAM entity works with a list of API actions and AWS resources to determine the policies' effective permissions. The entity can be an IAM user, group, or role. If you specify a user, then the simulation also includes all of the policies that are attached to groups that the user belongs to .

You can optionally include a list of one or more additional policies specified as strings to include in the simulation. If you want to simulate only policies specified as strings, use SimulateCustomPolicy (p. 223) instead.

You can also optionally include one resource-based policy to be evaluated with each of the resources included in the simulation.

The simulation does not perform the API actions, it only checks the authorization to determine if the simulated policies allow or deny the actions.

Note: This API discloses information about the permissions granted to other users. If you do not want users to see other user's permissions, then consider allowing them to use SimulateCustomPolicy (p. 223) instead.

Context keys are variables maintained by AWS and its services that provide details about the context of an API query request. You can use the `Condition` element of an IAM policy to evaluate context keys. To get the list of context keys that the policies require for correct simulation, use GetContextKeysForPrincipalPolicy (p. 112).

If the output is long, you can use the `MaxItems` and `Marker` parameters to paginate the results.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

ActionNames.member.N

A list of names of API actions to evaluate in the simulation. Each action is evaluated for each resource. Each action must include the service identifier, such as `iam:CreateUser`.

Type: array of Strings

Length Constraints: Minimum length of 3. Maximum length of 128.

Required: Yes

CallerArn

The ARN of the IAM user that you want to specify as the simulated caller of the APIs. If you do not specify a `CallerArn`, it defaults to the ARN of the user that you specify in `PolicySourceArn`, if you specified a user. If you include both a `PolicySourceArn` (for example, `arn:aws:iam::123456789012:user/David`) and a `CallerArn` (for example, `arn:aws:iam::123456789012:user/Bob`), the result is that you simulate calling the APIs as Bob, as if Bob had David's policies.

You can specify only the ARN of an IAM user. You cannot specify the ARN of an assumed role, federated user, or a service principal.

`CallerArn` is required if you include a `ResourcePolicy` and the `PolicySourceArn` is not the ARN for an IAM user. This is required so that the resource-based policy's `Principal` element has a value to use in evaluating the policy.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

ContextEntries.member.N

A list of context keys and corresponding values for the simulation to use. Whenever a context key is evaluated in one of the simulated IAM permission policies, the corresponding value is supplied.

Type: array of ContextEntry (p. 273) objects

Required: No

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

This parameter is optional. If you do not include it, it defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true` and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

PolicyInputList.member.N

An optional list of additional policy documents to include in the simulation. Each document is specified as a string containing the complete, valid JSON text of an IAM policy.

The regex pattern used to validate this parameter is a string of characters consisting of any printable ASCII character ranging from the space character (\u0020) through end of the ASCII character range (\u00FF). It also includes the special characters tab (\u0009), line feed (\u000A), and carriage return (\u000D).

Type: array of Strings

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: No

PolicySourceArn

The Amazon Resource Name (ARN) of a user, group, or role whose policies you want to include in the simulation. If you specify a user, group, or role, the simulation includes all policies that are associated with that entity. If you specify a user, the simulation also includes all policies that are attached to any groups the user belongs to.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

ResourceArns.member.N

A list of ARNs of AWS resources to include in the simulation. If this parameter is not provided then the value defaults to `*` (all resources). Each API in the `ActionNames` parameter is evaluated for each resource in this list. The simulation determines the access result (allowed or denied) of each combination and reports it in the response.

The simulation does not automatically retrieve policies for the specified resources. If you want to include a resource policy in the simulation, then you must include the policy as a string in the `ResourcePolicy` parameter.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: array of Strings

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

ResourceHandlingOption

Specifies the type of simulation to run. Different APIs that support resource-based policies require different combinations of resources. By specifying the type of simulation to run, you enable the policy simulator to enforce the presence of the required resources to ensure reliable simulation results. If your simulation does not match one of the following scenarios, then you can omit this parameter. The following list shows each of the supported scenario values and the resources that you must define to run the simulation.

Each of the EC2 scenarios requires that you specify instance, image, and security-group resources. If your scenario includes an EBS volume, then you must specify that volume as a resource. If the EC2 scenario includes VPC, then you must supply the network-interface resource. If it includes an IP subnet, then you must specify the subnet resource. For more information on the EC2 scenario options, see Supported Platforms in the *AWS EC2 User Guide*.

- **EC2-Classic-InstanceStore**

  instance, image, security-group
- **EC2-Classic-EBS**

  instance, image, security-group, volume
- **EC2-VPC-InstanceStore**

  instance, image, security-group, network-interface
- **EC2-VPC-InstanceStore-Subnet**

  instance, image, security-group, network-interface, subnet
- **EC2-VPC-EBS**

  instance, image, security-group, network-interface, volume
- **EC2-VPC-EBS-Subnet**

  instance, image, security-group, network-interface, subnet, volume

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Required: No

ResourceOwner

An AWS account ID that specifies the owner of any simulated resource that does not identify its owner in the resource ARN, such as an S3 bucket or object. If `ResourceOwner` is specified, it is also used as the account owner of any `ResourcePolicy` included in the simulation. If the `ResourceOwner` parameter is not specified, then the owner of the resources and the resource policy defaults to the account of the identity provided in `CallerArn`. This parameter is required only if you specify a resource-based policy and account that owns the resource is different from the account that owns the simulated calling user `CallerArn`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

ResourcePolicy

A resource-based policy to include in the simulation provided as a string. Each resource in the simulation is treated as if it had this policy attached. You can include only one resource-based policy in a simulation.

The regex pattern used to validate this parameter is a string of characters consisting of any printable ASCII character ranging from the space character (\u0020) through end of the ASCII character range (\u00FF). It also includes the special characters tab (\u0009), line feed (\u000A), and carriage return (\u000D).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: No

Response Elements

The following elements are returned by the service.

EvaluationResults.member.N

The results of the simulation.

Type: array of EvaluationResult (p. 274) objects

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

PolicyEvaluation

The request failed because a provided policy could not be successfully evaluated. An additional detail message indicates the source of the failure.

HTTP Status Code: 500

Example

Example

This example simulates calling the Amazon S3 APIs GetObject, PutObject, and DeleteObject for a specific S3 bucket. The simulation includes all policies that are attached to the user Jill. In this example, the user Jill has only the managed policy "AmazonS3ReadOnlyAccess" attached. Note that all parameters are shown in unencoded form here for clarity but must be URL encoded to be included as a part of a real HTML request. In the results, the simulation shows that Jill can add new files to the bucket because of the additional policy specified as a string parameter. In addition, she can read from the bucket because of the managed policy attached to the user. However, she cannot delete anything from the S3 bucket because of the default `implicitDeny`.

Sample Request

```
https://iam.amazonaws.com/Action=SimulatePrincipalPolicy
&ActionNames.member.1=s3:PutObject
&ActionNames.member.2=s3:GetObject
&ActionNames.member.3=s3:DeleteObject
&ResourceArns.member.1="arn:aws:s3:::my-test-bucket"
&PolicySourceArn=arn:aws:iam:::user/Jill
&PolicyInputList.member.1='{
  "Version":"2012-10-17",
  "Statement":{
    "Effect":"Allow",
    "Action":"s3:PutObject",
    "Resource":"arn:aws:s3:::my-test-bucket"
  }
}'
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<SimulatePrincipalPolicyResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <SimulatePrincipalPolicyResult>
    <IsTruncated>false</IsTruncated>
    <EvaluationResults>
      <member>
        <MatchedStatements>
          <member>
            <SourcePolicyId>PolicyInputList.1</SourcePolicyId>
            <EndPosition>
              <Column>4</Column>
              <Line>7</Line>
            </EndPosition>
            <StartPosition>
              <Column>16</Column>
              <Line>3</Line>
            </StartPosition>
          </member>
        </MatchedStatements>
        <MissingContextValues/>
        <EvalResourceName>arn:aws:s3:::my-test-bucket</EvalResourceName>
        <EvalDecision>allowed</EvalDecision>
        <EvalActionName>s3:PutObject</EvalActionName>
      </member>
      <member>
        <MatchedStatements>
          <member>
            <SourcePolicyId>AmazonS3ReadOnlyAccess</SourcePolicyId>
            <EndPosition>
              <Column>6</Column>
              <Line>11</Line>
            </EndPosition>
            <StartPosition>
```

```
              <Column>17</Column>
              <Line>3</Line>
            </StartPosition>
          </member>
        </MatchedStatements>
        <MissingContextValues/>
        <EvalResourceName>arn:aws:s3:::my-test-bucket</EvalResourceName>
        <EvalDecision>allowed</EvalDecision>
        <EvalActionName>s3:GetObject</EvalActionName>
      </member>
      <member>
        <MatchedStatements/>
        <MissingContextValues/>
        <EvalResourceName>arn:aws:s3:::my-test-bucket</EvalResourceName>
        <EvalDecision>implicitDeny</EvalDecision>
        <EvalActionName>s3:DeleteObject</EvalActionName>
      </member>
    </EvaluationResults>
  </SimulatePrincipalPolicyResult>
  <ResponseMetadata>
    <RequestId>004d7059-4c14-11e5-b121-bd8c7EXAMPLE</RequestId>
  </ResponseMetadata>
</SimulatePrincipalPolicyResponse>
```

UpdateAccessKey

Changes the status of the specified access key from Active to Inactive, or vice versa. This action can be used to disable a user's key as part of a key rotation work flow.

If the `UserName` field is not specified, the UserName is determined implicitly based on the AWS access key ID used to sign the request. Because this action works for access keys under the AWS account, you can use this action to manage root credentials even if the AWS account has no associated users.

For information about rotating keys, see Managing Keys and Certificates in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

AccessKeyId

The access key ID of the secret access key you want to update.

The regex pattern used to validate this parameter is a string of characters that can consist of any upper or lowercased letter or digit.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: `[\w]+`

Required: Yes

Status

The status you want to assign to the secret access key. `Active` means the key can be used for API calls to AWS, while `Inactive` means the key cannot be used.

Type: String

Valid Values: `Active | Inactive`

Required: Yes

UserName

The name of the user whose key you want to update.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: No

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=UpdateAccessKey
&UserName=Bob
&AccessKeyId=AKIAIOSFODNN7EXAMPLE
&Status=Inactive
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UpdateAccessKeyResponse>
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</UpdateAccessKeyResponse>
```

UpdateAccountPasswordPolicy

Updates the password policy settings for the AWS account.

> **Note**
> This action does not support partial updates. No parameters are required, but if you do not specify a parameter, that parameter's value reverts to its default value. See the **Request Parameters** section for each parameter's default value.

For more information about using a password policy, see Managing an IAM Password Policy in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

AllowUsersToChangePassword

Allows all IAM users in your account to use the AWS Management Console to change their own passwords. For more information, see Letting IAM Users Change Their Own Passwords in the *IAM User Guide*.

Default value: false

Type: Boolean

Required: No

HardExpiry

Prevents IAM users from setting a new password after their password has expired.

Default value: false

Type: Boolean

Required: No

MaxPasswordAge

The number of days that an IAM user password is valid. The default value of 0 means IAM user passwords never expire.

Default value: 0

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1095.

Required: No

MinimumPasswordLength

The minimum number of characters allowed in an IAM user password.

Default value: 6

Type: Integer

Valid Range: Minimum value of 6. Maximum value of 128.

Required: No

PasswordReusePrevention

Specifies the number of previous passwords that IAM users are prevented from reusing. The default value of 0 means IAM users are not prevented from reusing previous passwords.

Default value: 0

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 24.

Required: No

RequireLowercaseCharacters

Specifies whether IAM user passwords must contain at least one lowercase character from the ISO basic Latin alphabet (a to z).

Default value: false

Type: Boolean

Required: No

RequireNumbers

Specifies whether IAM user passwords must contain at least one numeric character (0 to 9).

Default value: false

Type: Boolean

Required: No

RequireSymbols

Specifies whether IAM user passwords must contain at least one of the following non-alphanumeric characters:

! @ # $ % ^ &amp; * ( ) _ + - = [ ] { } | '

Default value: false

Type: Boolean

Required: No

RequireUppercaseCharacters

Specifies whether IAM user passwords must contain at least one uppercase character from the ISO basic Latin alphabet (A to Z).

Default value: false

Type: Boolean

Required: No

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

MalformedPolicyDocument

The request was rejected because the policy document was malformed. The error message describes the specific error.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=UpdateAccountPasswordPolicy
&AllowUsersToChangePassword=true
&HardExpiry=false
&MaxPasswordAge=90
```

```
&MinimumPasswordLength=12
&PasswordReusePrevention=12
&RequireLowercaseCharacters=true
&RequireNumbers=true
&RequireSymbols=true
&RequireUppercaseCharacters=true
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UpdateAccountPasswordPolicyResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</UpdateAccountPasswordPolicyResponse>
```

UpdateAssumeRolePolicy

Updates the policy that grants an IAM entity permission to assume a role. This is typically referred to as the "role trust policy". For more information about roles, go to Using Roles to Delegate Permissions and Federate Identities.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

PolicyDocument

The policy that grants an entity permission to assume the role.

The regex pattern used to validate this parameter is a string of characters consisting of any printable ASCII character ranging from the space character (\u0020) through end of the ASCII character range (\u00FF). It also includes the special characters tab (\u0009), line feed (\u000A), and carriage return (\u000D).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

RoleName

The name of the role to update with the new policy.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

MalformedPolicyDocument

The request was rejected because the policy document was malformed. The error message describes the specific error.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=UpdateAssumeRolePolicy
&PolicyDocument={"Version":"2012-10-17","Statement":[{"Effect":"Allow",
"Principal":{"Service":["ec2.amazonaws.com"]},"Action":["sts:AssumeRole"]}]}
&RoleName=S3AccessForEC2Instances
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UpdateAssumeRolePolicyResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
<ResponseMetadata>
  <RequestId>309c1671-99ed-11e1-a4c3-270EXAMPLE04</RequestId>
</ResponseMetadata>
</UpdateAssumeRolePolicyResponse>
```

UpdateGroup

Updates the name and/or the path of the specified IAM group.

Important

You should understand the implications of changing a group's path or name. For more information, see Renaming Users and Groups in the *IAM User Guide*.

Note

To change an IAM group name the requester must have appropriate permissions on both the source object and the target object. For example, to change "Managers" to "MGRs", the entity making the request must have permission on both "Managers" and "MGRs", or must have permission on all (*). For more information about permissions, see Permissions and Policies.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

GroupName

Name of the IAM group to update. If you're changing the name of the group, this is the original name.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

NewGroupName

New name for the IAM group. Only include this if changing the group's name.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: No

NewPath

New path for the IAM group. Only include this if changing the group's path.

The regex pattern used to validate this parameter is a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes, containing any ASCII character from the ! (\u0021) thru the DEL character (\u007F), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: No

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=UpdateGroup
&GroupName=Test
&NewGroupName=Test_1
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UpdateGroupResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</UpdateGroupResponse>
```

UpdateLoginProfile

Changes the password for the specified IAM user.

IAM users can change their own passwords by calling ChangePassword (p. 17). For more information about modifying passwords, see Managing Passwords in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

Password

The new password for the specified IAM user.

The regex pattern used to validate this parameter is a string of characters consisting of any printable ASCII character ranging from the space character (\u0020) through end of the ASCII character range (\u00FF). It also includes the special characters tab (\u0009), line feed (\u000A), and carriage return (\u000D). However, the format can be further restricted by the account administrator by setting a password policy on the AWS account. For more information, see UpdateAccountPasswordPolicy (p. 236).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: No

PasswordResetRequired

Allows this new password to be used only once by requiring the specified IAM user to set a new password on next sign-in.

Type: Boolean

Required: No

UserName

The name of the user whose password you want to update.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

EntityTemporarilyUnmodifiable

The request was rejected because it referenced an entity that is temporarily unmodifiable, such as a user name that was deleted and then recreated. The error indicates that the request is likely to succeed if you try again after waiting several minutes. The error message describes the entity.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

PasswordPolicyViolation

The request was rejected because the provided password did not meet the requirements imposed by the account password policy.

HTTP Status Code: 400

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=UpdateLoginProfile
&UserName=Bob
&Password=^L[p*#Z*8o)K
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UpdateLoginProfileResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</UpdateLoginProfileResponse>
```

UpdateOpenIDConnectProviderThumbprint

Replaces the existing list of server certificate thumbprints associated with an OpenID Connect (OIDC) provider resource object with a new list of thumbprints.

The list that you pass with this action completely replaces the existing list of thumbprints. (The lists are not merged.)

Typically, you need to update a thumbprint only when the identity provider's certificate changes, which occurs rarely. However, if the provider's certificate *does* change, any attempt to assume an IAM role that specifies the OIDC provider as a principal fails until the certificate thumbprint is updated.

> **Note**
> Because trust for the OIDC provider is ultimately derived from the provider's certificate and is validated by the thumbprint, it is a best practice to limit access to the `UpdateOpenIDConnectProviderThumbprint` action to highly-privileged users.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

OpenIDConnectProviderArn

The Amazon Resource Name (ARN) of the IAM OIDC provider resource object for which you want to update the thumbprint. You can get a list of OIDC provider ARNs by using the ListOpenIDConnectProviders (p. 178) action.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

ThumbprintList.member.N

A list of certificate thumbprints that are associated with the specified IAM OpenID Connect provider. For more information, see CreateOpenIDConnectProvider (p. 29).

Type: array of Strings

Length Constraints: Fixed length of 40.

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=UpdateOpenIDConnectProviderThumbprint
&ThumbprintList.list.1=c3768084dfb3d2b68b7897bf5f565da8eEXAMPLE
&OpenIDConnectProviderArn=arn:aws:iam::123456789012:oidc-provider/
server.example.com
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UpdateOpenIDConnectProviderThumbprintResponse xmlns="https://
iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>29b6031c-4f66-11e4-aefa-bfd6aEXAMPLE</RequestId>
  </ResponseMetadata>
</UpdateOpenIDConnectProviderThumbprintResponse>
```

UpdateSAMLProvider

Updates the metadata document for an existing SAML provider resource object.

Note
This operation requires Signature Version 4.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

SAMLMetadataDocument

An XML document generated by an identity provider (IdP) that supports SAML 2.0. The document includes the issuer's name, expiration information, and keys that can be used to validate the SAML authentication response (assertions) that are received from the IdP. You must generate the metadata document using the identity management software that is used as your organization's IdP.

Type: String

Length Constraints: Minimum length of 1000. Maximum length of 10000000.

Required: Yes

SAMLProviderArn

The Amazon Resource Name (ARN) of the SAML provider to update.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Response Elements

The following element is returned by the service.

SAMLProviderArn

The Amazon Resource Name (ARN) of the SAML provider that was updated.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=UpdateSAMLProvider
&Name=arn:aws:iam::123456789012:saml-provider/MyUniversity
&SAMLMetadataDocument=VGhpcyBpcyB3aGVyZSB5b3UgcHV0IHRoZSBTQU1MIHByb3ZpZGVyIG1ldGFkYXRhIGRvY
LCBCYXNlNjQtZW5jb2RlZCBpbnRvIGEgYmlnIHN0cmluZy4=
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UpdateSAMLProviderResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
<UpdateSAMLProviderResult>
  <SAMLProviderArn>arn:aws:iam::123456789012:saml-provider/MyUniversity</
SAMLProviderArn>
</UpdateSAMLProviderResult>
<ResponseMetadata>
  <RequestId>29f47818-99f5-11e1-a4c3-27EXAMPLE804</RequestId>
</ResponseMetadata>
</UpdateSAMLProviderResponse>
```

UpdateServerCertificate

Updates the name and/or the path of the specified server certificate stored in IAM.

For more information about working with server certificates, including a list of AWS services that can use the server certificates that you manage with IAM, go to Working with Server Certificates in the *IAM User Guide*.

Important

You should understand the implications of changing a server certificate's path or name. For more information, see Renaming a Server Certificate in the *IAM User Guide*.

Note

To change a server certificate name the requester must have appropriate permissions on both the source object and the target object. For example, to change the name from "ProductionCert" to "ProdCert", the entity making the request must have permission on "ProductionCert" and "ProdCert", or must have permission on all (*). For more information about permissions, see Access Management in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

NewPath

The new path for the server certificate. Include this only if you are updating the server certificate's path.

The regex pattern used to validate this parameter is a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes, containing any ASCII character from the ! (\u0021) thru the DEL character (\u007F), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: No

NewServerCertificateName

The new name for the server certificate. Include this only if you are updating the server certificate's name. The name of the certificate cannot contain any spaces.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: No

ServerCertificateName

The name of the server certificate that you want to update.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=UpdateServerCertificate
&ServerCertificateName=OldProdServerCertName
&NewServerCertificateName=NewProdServerCertName
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UpdateServerCertificateResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
<ResponseMetadata>
  <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
</ResponseMetadata>
</UpdateServerCertificateResponse>
```

UpdateSigningCertificate

Changes the status of the specified user signing certificate from active to disabled, or vice versa. This action can be used to disable an IAM user's signing certificate as part of a certificate rotation work flow.

If the `UserName` field is not specified, the UserName is determined implicitly based on the AWS access key ID used to sign the request. Because this action works for access keys under the AWS account, you can use this action to manage root credentials even if the AWS account has no associated users.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

CertificateId

The ID of the signing certificate you want to update.

The regex pattern used to validate this parameter is a string of characters that can consist of any upper or lowercased letter or digit.

Type: String

Length Constraints: Minimum length of 24. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

Status

The status you want to assign to the certificate. `Active` means the certificate can be used for API calls to AWS, while `Inactive` means the certificate cannot be used.

Type: String

Valid Values: `Active | Inactive`

Required: Yes

UserName

The name of the IAM user the signing certificate belongs to.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: No

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=UpdateSigningCertificate
&UserName=Bob
&CertificateId=TA7SMP42TDN5Z26OBPJE7EXAMPLE
&Status=Inactive
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UpdateSigningCertificateResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</UpdateSigningCertificateResponse>
```

UpdateSSHPublicKey

Sets the status of an IAM user's SSH public key to active or inactive. SSH public keys that are inactive cannot be used for authentication. This action can be used to disable a user's SSH public key as part of a key rotation work flow.

The SSH public key affected by this action is used only for authenticating the associated IAM user to an AWS CodeCommit repository. For more information about using SSH keys to authenticate to an AWS CodeCommit repository, see Set up AWS CodeCommit for SSH Connections in the *AWS CodeCommit User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

SSHPublicKeyId

The unique identifier for the SSH public key.

The regex pattern used to validate this parameter is a string of characters that can consist of any upper or lowercased letter or digit.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

Status

The status to assign to the SSH public key. `Active` means the key can be used for authentication with an AWS CodeCommit repository. `Inactive` means the key cannot be used.

Type: String

Valid Values: `Active | Inactive`

Required: Yes

UserName

The name of the IAM user associated with the SSH public key.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

Example

Sample Request

```
https://iam.amazonaws.com/?Action=UpdateSSHPublicKey
&SSHPublicKeyId=APKAEIVFHP46CEXAMPLE
&Status=Inactive
&UserName=Jane
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UpdateSSHPublicKeyResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>d3d9215c-f36b-11e4-97ab-c53b2EXAMPLE</RequestId>
  </ResponseMetadata>
</UpdateSSHPublicKeyResponse>
```

UpdateUser

Updates the name and/or the path of the specified IAM user.

> **Important**
> You should understand the implications of changing an IAM user's path or name. For more information, see Renaming an IAM User and Renaming an IAM Group in the *IAM User Guide*.

> **Note**
> To change a user name the requester must have appropriate permissions on both the source object and the target object. For example, to change Bob to Robert, the entity making the request must have permission on Bob and Robert, or must have permission on all (*). For more information about permissions, see Permissions and Policies.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

NewPath

New path for the IAM user. Include this parameter only if you're changing the user's path.

The regex pattern used to validate this parameter is a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes, containing any ASCII character from the ! (\u0021) thru the DEL character (\u007F), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: No

NewUserName

New name for the user. Include this parameter only if you're changing the user's name.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: No

UserName

Name of the user to update. If you're changing the name of the user, this is the original user name.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

EntityTemporarilyUnmodifiable

The request was rejected because it referenced an entity that is temporarily unmodifiable, such as a user name that was deleted and then recreated. The error indicates that the request is likely to succeed if you try again after waiting several minutes. The error message describes the entity.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=UpdateUser
&UserName=Bob
&NewUserName=Robert
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UpdateUserResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
 <UpdateUserResult>
 <User>
    <Path>/division_abc/subdivision_xyz/</Path>
    <UserName>Robert</UserName>
    <UserId>AIDACKCEVSQ6C2EXAMPLE</UserId>
    <Arn>arn:aws::123456789012:user/division_abc/subdivision_xyz/Robert
    </Arn>
 </User>
 </UpdateUserResult>
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</UpdateUserResponse>
```

UploadServerCertificate

Uploads a server certificate entity for the AWS account. The server certificate entity includes a public key certificate, a private key, and an optional certificate chain, which should all be PEM-encoded.

For more information about working with server certificates, including a list of AWS services that can use the server certificates that you manage with IAM, go to Working with Server Certificates in the *IAM User Guide*.

For information about the number of server certificates you can upload, see Limitations on IAM Entities and Objects in the *IAM User Guide*.

> **Note**
>
> Because the body of the public key certificate, private key, and the certificate chain can be large, you should use POST rather than GET when calling `UploadServerCertificate`. For information about setting up signatures and authorization through the API, go to Signing AWS API Requests in the *AWS General Reference*. For general information about using the Query API with IAM, go to Calling the API by Making HTTP Query Requests in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

CertificateBody

The contents of the public key certificate in PEM-encoded format.

The regex pattern used to validate this parameter is a string of characters consisting of any printable ASCII character ranging from the space character (\u0020) through end of the ASCII character range (\u00FF). It also includes the special characters tab (\u0009), line feed (\u000A), and carriage return (\u000D).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 16384.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

CertificateChain

The contents of the certificate chain. This is typically a concatenation of the PEM-encoded public key certificates of the chain.

The regex pattern used to validate this parameter is a string of characters consisting of any printable ASCII character ranging from the space character (\u0020) through end of the ASCII character range (\u00FF). It also includes the special characters tab (\u0009), line feed (\u000A), and carriage return (\u000D).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2097152.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: No

Path

The path for the server certificate. For more information about paths, see IAM Identifiers in the *IAM User Guide*.

This parameter is optional. If it is not included, it defaults to a slash (/). The regex pattern used to validate this parameter is a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes, containing any ASCII character from the ! (\u0021) thru the DEL character (\u007F), including most punctuation characters, digits, and upper and lowercased letters.

> **Note**
>
> If you are uploading a server certificate specifically for use with Amazon CloudFront distributions, you must specify a path using the `--path` option. The path must begin with `/cloudfront` and must include a trailing slash (for example, `/cloudfront/test/`).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: No

PrivateKey

The contents of the private key in PEM-encoded format.

The regex pattern used to validate this parameter is a string of characters consisting of any printable ASCII character ranging from the space character (\u0020) through end of the ASCII character range (\u00FF). It also includes the special characters tab (\u0009), line feed (\u000A), and carriage return (\u000D).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 16384.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

ServerCertificateName

The name for the server certificate. Do not include the path in this value. The name of the certificate cannot contain any spaces.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Response Elements

The following element is returned by the service.

ServerCertificateMetadata

The meta information of the uploaded server certificate without its certificate body, certificate chain, and private key.

Type: ServerCertificateMetadata (p. 300) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

KeyPairMismatch

The request was rejected because the public key certificate and the private key do not match.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

MalformedCertificate

The request was rejected because the certificate was malformed or expired. The error message describes the specific error.

HTTP Status Code: 400

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=UploadServerCertificate
&ServerCertificateName=ProdServerCert
&Path=/company/servercerts/
&CertificateBody=
-----BEGIN CERTIFICATE-----
MIICdzCCAeCgAwIBAgIGANc+Ha2wMA0GCSqGSIb3DQEBBQUAMFMxCzAJBgNVBAYT
AlVTMRMwEQYDVQQKEwpBbWF6b24uY29tMQwwCgYDVQQLEwNBV1MxITAfBgNVBAMT
GEFXUyBMaW1pdGVkLUFzc3VyYW5jZSBDQTAeFw0wOTAyMDQxNzE5MjdaFw0xMDAy
MDQxNzE5MjdaMFIxCzAJBgNVBAYTAlVTMRMwEQYDVQQKEwpBbWF6b24uY29tMRcw
FQYDVQQLEw5BV1MtRGV2ZWxvcGVyczEVMBMGA1UEAxMMNTdxNDl0c3ZwYjRtMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpB/vsOwmT/O0td1RqzKjttSBaPjbr
dqwNe9BrOyB08fw2+Ch5oonZYXfGUrT6mkYXH5fQot9HvASrzAKHO596FdJA6DmL
ywdWe1Oggk7zFSXO1Xv+3vPrJtaYxYo3eRIp7w80PMkiOv6M0XK8ubcTouODeJbf
suDqcLnLDxwsvwIDAQABo1cwVTAOBgNVHQ8BAf8EBAMCBaAwFgYDVR0lAQH/BAww
CgYIKwYBBQUHAwIwDAYDVR0TAQH/BAIwADAdBgNVHQ4EFgQULGNaBphBumaKbDRK
CAi0mH8B3mowDQYJKoZIhvcNAQEFBQADgYEAuKxhkXaCLGcqDuweKtO/AEw9ZePH
wr0XqsaIK2HZboqruebXEGsojK4Ks0WzwgrEynuHJwTn760xe39rSqXWIOGrOBaX
wFpWHVjTFMKk+tSDG1lssLHyYWWdFFU4AnejRGORJYNaRHgVTKjHphc5jEhHm0BX
AEaHzTpmEXAMPLE=
-----END CERTIFICATE-----
&PrivateKey=
-----BEGIN DSA PRIVATE KEY-----
MIIBugIBTTKBgQD33xToSXPJ6hr37L3+KNi3/7DgywlBcvlFPPSHIw3ORuO/22mT
8Cy5fT89WwNvZ3BPKWU6OZ38TQv3eWjNc/3U3+oqVNG2poX5nCPOtO1b96HYX2mR
3FTdH6FRKbQEhpDzZ6tRrjTHjMX6sT3JRWkBd2c4bGu+HUHO1H7QvrCTeQIVTKMs
TCKCyrLiGhUWuUGNJUMU6y6zToGTHl84Tz7TPwDGDXuy/Dk5s4jTVr+xibROC/gS
Qrs4Dzz3T1ze6lvU8S1KT9UsOB5FUJNTTPCPey+Lo4mmK6b23XdTyCIT8e2fsm2j
jHHC1pIPiTkdLS3j6ZYjF8LY6TENFng+LDY/xwPOl7TJVoD3J/WXC2J9CEYq9o34
kq6WWn3CgYTuo54nXUgnoCb3xdG8COFrg+oTbIkHTSzs3w5o/GGgKK7TDF3UlJjq
vHNyJQ6kWBrQRR1Xp5KYQ4c/Dm5kef+62mH53HpcCELguWVcffuVQpmq3EWL9Zp9
jobTJQ2VHjb5IVxiO6HRSd27di3njyrzUuJCyHSDTqwLJmTThpd6OTIUTL3Tc4m2
62TITdw53KWJEXAMPLE=
-----END DSA PRIVATE KEY-----
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UploadServerCertificateResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
<UploadServerCertificateResult>
  <ServerCertificateMetadata>
    <ServerCertificateName>ProdServerCert</ServerCertificateName>
    <Path>/company/servercerts/</Path>
    <Arn>arn:aws:iam::123456789012:server-certificate/company/servercerts/
ProdServerCert</Arn>
```

```
    <UploadDate>2010-05-08T01:02:03.004Z</UploadDate>
    <ServerCertificateId>ASCACKCEVSQ6C2EXAMPLE</ServerCertificateId>
    <Expiration>2012-05-08T01:02:03.004Z</Expiration>
  </ServerCertificateMetadata>
</UploadServerCertificateResult>
<ResponseMetadata>
  <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
</ResponseMetadata>
</UploadServerCertificateResponse>
```

UploadSigningCertificate

Uploads an X.509 signing certificate and associates it with the specified IAM user. Some AWS services use X.509 signing certificates to validate requests that are signed with a corresponding private key. When you upload the certificate, its default status is `Active`.

If the `UserName` field is not specified, the IAM user name is determined implicitly based on the AWS access key ID used to sign the request. Because this action works for access keys under the AWS account, you can use this action to manage root credentials even if the AWS account has no associated users.

> **Note**
>
> Because the body of a X.509 certificate can be large, you should use POST rather than GET when calling `UploadSigningCertificate`. For information about setting up signatures and authorization through the API, go to Signing AWS API Requests in the *AWS General Reference*. For general information about using the Query API with IAM, go to Making Query Requests in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

CertificateBody

The contents of the signing certificate.

The regex pattern used to validate this parameter is a string of characters consisting of any printable ASCII character ranging from the space character (\u0020) through end of the ASCII character range (\u00FF). It also includes the special characters tab (\u0009), line feed (\u000A), and carriage return (\u000D).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 16384.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

UserName

The name of the user the signing certificate is for.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: No

Response Elements

The following element is returned by the service.

Certificate

Information about the certificate.

Type: SigningCertificate (p. 301) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

DuplicateCertificate

The request was rejected because the same certificate is associated with an IAM user in the account.

HTTP Status Code: 409

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

InvalidCertificate

The request was rejected because the certificate is invalid.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

MalformedCertificate

The request was rejected because the certificate was malformed or expired. The error message describes the specific error.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Example

Sample Request

```
https://iam.amazonaws.com/?Action=UploadSigningCertificate
&UserName=Bob
&CertificateBody=
-----BEGIN CERTIFICATE-----
MIICdzCCAeCgAwIBAgIGANc+Ha2wMA0GCSqGSIb3DQEBBQUAMFMxCzAJBgNVBAYT
AlVTMRMwEQYDVQQKEwpBbWF6b24uY29tMQwwCgYDVQQLEwNBV1MxITAfBgNVBAMT
GEFXUyBMaW1pdGVkLUFzc3VyYW5jZSBDQTAeFw0wOTAyMDQxNzE5MjdaFw0xMDAy
MDQxNzE5MjdaMFIxCzAJBgNVBAYTAlVTMRMwEQYDVQQKEwpBbWF6b24uY29tMRcw
FQYDVQQLEw5BV1MtRGV2ZWxvcGVyczEVMBMGA1UEAxMMNTdxNDl0c3ZwYjRtMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpB/vsOwmT/O0td1RqzKjttSBaPjbr
dqwNe9BrOyB08fw2+Ch5oonZYXfGUrT6mkYXH5fQot9HvASrzAKHO596FdJA6DmL
ywdWe1Oggk7zFSXO1Xv+3vPrJtaYxYo3eRIp7w80PMkiOv6M0XK8ubcTouODeJbf
suDqcLnLDxwsvwIDAQABo1cwVTAOBgNVHQ8BAf8EBAMCBaAwFgYDVR0lAQH/BAww
CgYIKwYBBQUHAwIwDAYDVR0TAQH/BAIwADAdBgNVHQ4EFgQULGNaBphBumaKbDRK
CAi0mH8B3mowDQYJKoZIhvcNAQEFBQADgYEAuKxhkXaCLGcqDuweKtO/AEw9ZePH
wr0XqsaIK2HZboqruebXEGsojK4Ks0WzwgrEynuHJwTn760xe39rSqXWIOGrOBaX
wFpWHVjTFMKk+tSDG1lssLHyYWWdFFU4AnejRGORJYNaRHgVTKjHphc5jEhHm0BX
AEaHzTpmEXAMPLE=
-----END CERTIFICATE-----
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UploadSigningCertificateResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <UploadSigningCertificateResult>
    <Certificate>
      <UserName>Bob</UserName>
      <CertificateId>TA7SMP42TDN5Z26OBPJE7EXAMPLE</CertificateId>
      <CertificateBody>
-----BEGIN CERTIFICATE-----
MIICdzCCAeCgAwIBAgIGANc+Ha2wMA0GCSqGSIb3DQEBBQUAMFMxCzAJBgNVBAYT
AlVTMRMwEQYDVQQKEwpBbWF6b24uY29tMQwwCgYDVQQLEwNBV1MxITAfBgNVBAMT
GEFXUyBMaW1pdGVkLUFzc3VyYW5jZSBDQTAeFw0wOTAyMDQxNzE5MjdaFw0xMDAy
MDQxNzE5MjdaMFIxCzAJBgNVBAYTAlVTMRMwEQYDVQQKEwpBbWF6b24uY29tMRcw
FQYDVQQLEw5BV1MtRGV2ZWxvcGVyczEVMBMGA1UEAxMMNTdxNDl0c3ZwYjRtMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpB/vsOwmT/O0td1RqzKjttSBaPjbr
dqwNe9BrOyB08fw2+Ch5oonZYXfGUrT6mkYXH5fQot9HvASrzAKHO596FdJA6DmL
ywdWe1Oggk7zFSXO1Xv+3vPrJtaYxYo3eRIp7w80PMkiOv6M0XK8ubcTouODeJbf
suDqcLnLDxwsvwIDAQABo1cwVTAOBgNVHQ8BAf8EBAMCBaAwFgYDVR0lAQH/BAww
CgYIKwYBBQUHAwIwDAYDVR0TAQH/BAIwADAdBgNVHQ4EFgQULGNaBphBumaKbDRK
CAi0mH8B3mowDQYJKoZIhvcNAQEFBQADgYEAuKxhkXaCLGcqDuweKtO/AEw9ZePH
wr0XqsaIK2HZboqruebXEGsojK4Ks0WzwgrEynuHJwTn760xe39rSqXWIOGrOBaX
wFpWHVjTFMKk+tSDG1lssLHyYWWdFFU4AnejRGORJYNaRHgVTKjHphc5jEhHm0BX
AEaHzTpmEXAMPLE=
-----END CERTIFICATE-----
      </CertificateBody>
      <Status>Active</Status>
    </Certificate>
 </UploadSigningCertificateResult>
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</UploadSigningCertificateResponse>
```

UploadSSHPublicKey

Uploads an SSH public key and associates it with the specified IAM user.

The SSH public key uploaded by this action can be used only for authenticating the associated IAM user to an AWS CodeCommit repository. For more information about using SSH keys to authenticate to an AWS CodeCommit repository, see Set up AWS CodeCommit for SSH Connections in the *AWS CodeCommit User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 310).

SSHPublicKeyBody

The SSH public key. The public key must be encoded in ssh-rsa format or PEM format.

The regex pattern used to validate this parameter is a string of characters consisting of any printable ASCII character ranging from the space character (\u0020) through end of the ASCII character range (\u00FF). It also includes the special characters tab (\u0009), line feed (\u000A), and carriage return (\u000D).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 16384.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

UserName

The name of the IAM user to associate the SSH public key with.

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

Response Elements

The following element is returned by the service.

SSHPublicKey

Contains information about the SSH public key.

Type: SSHPublicKey (p. 302) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 312).

DuplicateSSHPublicKey

The request was rejected because the SSH public key is already associated with the specified IAM user.

HTTP Status Code: 400

InvalidPublicKey

The request was rejected because the public key is malformed or otherwise invalid.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced an entity that does not exist. The error message describes the entity.

HTTP Status Code: 404

UnrecognizedPublicKeyEncoding

The request was rejected because the public key encoding format is unsupported or unrecognized.

HTTP Status Code: 400

Example

Sample Request

```
https://iam.amazonaws.com/?Action=UploadSSHPublicKey
&SSHPublicKeyBody=ssh-rsa
 AAAAB3NzaC1yc2EAAAADAQABAAABAQCy75ak72GGaoZNy0cjUERIn
+mrga0C30kmkiwOeN4H6YtvCdUksVppjPOhm485WFRzvIcxaMEuZ9ISAkp8AfefybxH0PdQWhELSu0p
HaMnADAU7dOn3CCerO8+0sycbu4ES4P+cdK1qet3ptsG/
zeQNLLmOK5zjIRa1MAS3KnwLwHEVPEe4JD
+xfghuO0nwzUgpneGNwk7m7qihYLFnNCFdeU8OeIr9Fmc75g5olHm6ZoC/
bccAHurHkfcDpanJTLNfL
R5Oj14CZSsRP4kNdm+oe5+IPM78w4J9v4pXU4mizYDE21G4gUDVxOrs0X66lMihX6ArVgmEK
+NK5GQg
n9z jane@example.com
&UserName=Jane
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UploadSSHPublicKeyResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <UploadSSHPublicKeyResult>
    <PublicKey>
      <UploadDate>2015-06-05T20:56:46.012Z</UploadDate>
      <Fingerprint>7a:1d:ea:9e:b0:80:ac:f8:ec:d8:dc:e6:a7:2c:fc:51</
Fingerprint>
      <UserName>Jane</UserName>
      <SSHPublicKeyId>APKAEIVFHP46CEXAMPLE</SSHPublicKeyId>
      <Status>Active</Status>
      <SSHPublicKeyBody>
        ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCy75ak72GGaoZNy0cjUERIn
+mrga0C30k

 mkiwOeN4H6YtvCdUksVppjPOhm485WFRzvIcxaMEuZ9ISAkp8AfefybxH0PdQWhELSu0pHa
        MnADAU7dOn3CCerO8+0sycbu4ES4P+cdK1qet3ptsG/
zeQNLLmOK5zjIRa1MAS3KnwLwHEV
        PEe4JD+xfghuO0nwzUgpneGNwk7m7qihYLFnNCFdeU8OeIr9Fmc75g5olHm6ZoC/
bccAHur
        HkfcDpanJTLNfLR5Oj14CZSsRP4kNdm
+oe5+IPM78w4J9v4pXU4mizYDE21G4gUDVxOrs0X
```

```
        66lMihX6ArVgmEK+NK5GQgn9z jane@example.com
      </SSHPublicKeyBody>
    </PublicKey>
  </UploadSSHPublicKeyResult>
  <ResponseMetadata>
    <RequestId>3da97a2f-f369-11e4-97ab-c53b2EXAMPLE</RequestId>
  </ResponseMetadata>
</UploadSSHPublicKeyResponse>
```

Data Types

The AWS Identity and Access Management API contains several data types that various actions use. This section describes each data type in detail.

Note
The order of each element in a data type structure is not guaranteed. Applications should not assume a particular order.

The following data types are supported:

- ServerCertificate (p. 299)
- ServerCertificateMetadata (p. 300)
- SigningCertificate (p. 301)
- SSHPublicKey (p. 302)
- SSHPublicKeyMetadata (p. 303)
- Statement (p. 304)
- User (p. 305)
- UserDetail (p. 307)
- VirtualMFADevice (p. 309)

AccessKey

Contains information about an AWS access key.

This data type is used as a response element in the CreateAccessKey (p. 19) and ListAccessKeys (p. 146) actions.

> **Note**
>
> The `SecretAccessKey` value is returned only in response to CreateAccessKey (p. 19). You can get a secret access key only when you first create an access key; you cannot recover the secret access key later. If you lose a secret access key, you must create a new access key.

Contents

AccessKeyId

The ID for this access key.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: `[\w]+`

Required: Yes

CreateDate

The date when the access key was created.

Type: Timestamp

Required: No

SecretAccessKey

The secret key used to sign requests.

Type: String

Required: Yes

Status

The status of the access key. `Active` means the key is valid for API calls, while `Inactive` means it is not.

Type: String

Valid Values: `Active | Inactive`

Required: Yes

UserName

The name of the IAM user that the access key is associated with.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

AccessKeyLastUsed

Contains information about the last time an AWS access key was used.

This data type is used as a response element in the GetAccessKeyLastUsed (p. 95) action.

Contents

LastUsedDate

The date and time, in ISO 8601 date-time format, when the access key was most recently used. This field is null when:

- The user does not have an access key.
- An access key exists but has never been used, at least not since IAM started tracking this information on April 22nd, 2015.
- There is no sign-in data associated with the user

Type: Timestamp

Required: Yes

Region

The AWS region where this access key was most recently used. This field is null when:

- The user does not have an access key.
- An access key exists but has never been used, at least not since IAM started tracking this information on April 22nd, 2015.
- There is no sign-in data associated with the user

For more information about AWS regions, see Regions and Endpoints in the Amazon Web Services General Reference.

Type: String

Required: Yes

ServiceName

The name of the AWS service with which this access key was most recently used. This field is null when:

- The user does not have an access key.
- An access key exists but has never been used, at least not since IAM started tracking this information on April 22nd, 2015.
- There is no sign-in data associated with the user

Type: String

Required: Yes

AccessKeyMetadata

Contains information about an AWS access key, without its secret key.

This data type is used as a response element in the ListAccessKeys (p. 146) action.

Contents

AccessKeyId

The ID for this access key.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: `[\w]+`

Required: No

CreateDate

The date when the access key was created.

Type: Timestamp

Required: No

Status

The status of the access key. `Active` means the key is valid for API calls; `Inactive` means it is not.

Type: String

Valid Values: `Active | Inactive`

Required: No

UserName

The name of the IAM user that the key is associated with.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: No

AttachedPolicy

Contains information about an attached policy.

An attached policy is a managed policy that has been attached to a user, group, or role. This data type is used as a response element in the ListAttachedGroupPolicies (p. 151), ListAttachedRolePolicies (p. 154), ListAttachedUserPolicies (p. 157), and GetAccountAuthorizationDetails (p. 97) actions.

For more information about managed policies, refer to Managed Policies and Inline Policies in the *Using IAM* guide.

Contents

PolicyArn

The Amazon Resource Name (ARN). ARNs are unique identifiers for AWS resources.

For more information about ARNs, go to Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: No

PolicyName

The friendly name of the attached policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: No

ContextEntry

Contains information about a condition context key. It includes the name of the key and specifies the value (or values, if the context key supports multiple values) to use in the simulation. This information is used when evaluating the `Condition` elements of the input policies.

This data type is used as an input parameter to `SimulateCustomPolicy (p. 223)` and `SimulateCustomPolicy (p. 223)` .

Contents

ContextKeyName

The full name of a condition context key, including the service prefix. For example, `aws:SourceIp` or `s3:VersionId`.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 256.

Required: No

ContextKeyType

The data type of the value (or values) specified in the `ContextKeyValues` parameter.

Type: String

Valid Values: `string | stringList | numeric | numericList | boolean | booleanList | ip | ipList | binary | binaryList | date | dateList`

Required: No

ContextKeyValues.member.N

The value (or values, if the condition context key supports multiple values) to provide to the simulation for use when the key is referenced by a `Condition` element in an input policy.

Type: array of Strings

Required: No

EvaluationResult

Contains the results of a simulation.

This data type is used by the return parameter of `SimulateCustomPolicy (p. 223)` and `SimulatePrincipalPolicy (p. 228)` .

Contents

EvalActionName

The name of the API action tested on the indicated resource.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 128.

Required: Yes

EvalDecision

The result of the simulation.

Type: String

Valid Values: `allowed | explicitDeny | implicitDeny`

Required: Yes

EvalDecisionDetails , EvalDecisionDetails.entry.N.key (key), EvalDecisionDetailsentry.N.value (value)

Additional details about the results of the evaluation decision. When there are both IAM policies and resource policies, this parameter explains how each set of policies contributes to the final evaluation decision. When simulating cross-account access to a resource, both the resource-based policy and the caller's IAM policy must grant access. See How IAM Roles Differ from Resource-based Policies

Type: String to String map

Valid Values: `allowed | explicitDeny | implicitDeny`

Required: No

EvalResourceName

The ARN of the resource that the indicated API action was tested on.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

MatchedStatements.member.N

A list of the statements in the input policies that determine the result for this scenario. Remember that even if multiple statements allow the action on the resource, if only one statement denies that action, then the explicit deny overrides any allow, and the deny statement is the only entry included in the result.

Type: array of Statement (p. 304) objects

Required: No

MissingContextValues.member.N

A list of context keys that are required by the included input policies but that were not provided by one of the input parameters. This list is used when the resource in a simulation is "*", either explicitly, or when the `ResourceArns` parameter blank. If you include a list of resources, then any missing context values are instead included under the `ResourceSpecificResults` section. To discover the context keys used by a set of policies, you can call GetContextKeysForCustomPolicy (p. 110) or GetContextKeysForPrincipalPolicy (p. 112).

Type: array of Strings

Length Constraints: Minimum length of 5. Maximum length of 256.

Required: No

ResourceSpecificResults.member.N

The individual results of the simulation of the API action specified in EvalActionName on each resource.

Type: array of ResourceSpecificResult (p. 294) objects

Required: No

Group

Contains information about an IAM group entity.

This data type is used as a response element in the following actions:

- CreateGroup (p. 23)
- GetGroup (p. 117)
- ListGroups (p. 165)

Contents

Arn

The Amazon Resource Name (ARN) specifying the group. For more information about ARNs and how to use them in policies, see IAM Identifiers in the *Using IAM* guide.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

CreateDate

The date and time, in ISO 8601 date-time format, when the group was created.

Type: Timestamp

Required: Yes

GroupId

The stable and unique string identifying the group. For more information about IDs, see IAM Identifiers in the *Using IAM* guide.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: `[\w]+`

Required: Yes

GroupName

The friendly name that identifies the group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Path

The path to the group. For more information about paths, see IAM Identifiers in the *Using IAM* guide.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: Yes

GroupDetail

Contains information about an IAM group, including all of the group's policies.

This data type is used as a response element in the GetAccountAuthorizationDetails (p. 97) action.

Contents

Arn

The Amazon Resource Name (ARN). ARNs are unique identifiers for AWS resources.

For more information about ARNs, go to Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: No

AttachedManagedPolicies.member.N

A list of the managed policies attached to the group.

Type: array of AttachedPolicy (p. 272) objects

Required: No

CreateDate

The date and time, in ISO 8601 date-time format, when the group was created.

Type: Timestamp

Required: No

GroupId

The stable and unique string identifying the group. For more information about IDs, see IAM Identifiers in the *Using IAM* guide.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: `[\w]+`

Required: No

GroupName

The friendly name that identifies the group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: No

GroupPolicyList.member.N

A list of the inline policies embedded in the group.

Type: array of PolicyDetail (p. 288) objects

Required: No

Path

The path to the group. For more information about paths, see IAM Identifiers in the *Using IAM* guide.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: No

InstanceProfile

Contains information about an instance profile.

This data type is used as a response element in the following actions:

- CreateInstanceProfile (p. 25)
- GetInstanceProfile (p. 122)
- ListInstanceProfiles (p. 170)
- ListInstanceProfilesForRole (p. 173)

Contents

Arn

The Amazon Resource Name (ARN) specifying the instance profile. For more information about ARNs and how to use them in policies, see IAM Identifiers in the *Using IAM* guide.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

CreateDate

The date when the instance profile was created.

Type: Timestamp

Required: Yes

InstanceProfileId

The stable and unique string identifying the instance profile. For more information about IDs, see IAM Identifiers in the *Using IAM* guide.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: `[\w]+`

Required: Yes

InstanceProfileName

The name identifying the instance profile.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

Path

The path to the instance profile. For more information about paths, see IAM Identifiers in the *Using IAM* guide.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: Yes

Roles.member.N

The role associated with the instance profile.

Type: array of Role (p. 295) objects

Required: Yes

LoginProfile

Contains the user name and password create date for a user.

This data type is used as a response element in the CreateLoginProfile (p. 27) and GetLoginProfile (p. 124) actions.

Contents

CreateDate

The date when the password for the user was created.

Type: Timestamp

Required: Yes

PasswordResetRequired

Specifies whether the user is required to set a new password on next sign-in.

Type: Boolean

Required: No

UserName

The name of the user, which can be used for signing in to the AWS Management Console.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

ManagedPolicyDetail

Contains information about a managed policy, including the policy's ARN, versions, and the number of principal entities (users, groups, and roles) that the policy is attached to.

This data type is used as a response element in the GetAccountAuthorizationDetails (p. 97) action.

For more information about managed policies, see Managed Policies and Inline Policies in the *Using IAM* guide.

Contents

Arn

The Amazon Resource Name (ARN). ARNs are unique identifiers for AWS resources.

For more information about ARNs, go to Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: No

AttachmentCount

The number of principal entities (users, groups, and roles) that the policy is attached to.

Type: Integer

Required: No

CreateDate

The date and time, in ISO 8601 date-time format, when the policy was created.

Type: Timestamp

Required: No

DefaultVersionId

The identifier for the version of the policy that is set as the default (operative) version.

For more information about policy versions, see Versioning for Managed Policies in the *Using IAM* guide.

Type: String

Pattern: `v[1-9][0-9]*(\.[A-Za-z0-9-]*)?`

Required: No

Description

A friendly description of the policy.

Type: String

Length Constraints: Maximum length of 1000.

Required: No

IsAttachable

Specifies whether the policy can be attached to an IAM user, group, or role.

Type: Boolean

Required: No

Path

The path to the policy.

For more information about paths, see IAM Identifiers in the *Using IAM* guide.

Type: String

Pattern: `((/[A-Za-z0-9\.,\+@=_-]+)*)/`

Required: No

PolicyId

The stable and unique string identifying the policy.

For more information about IDs, see IAM Identifiers in the *Using IAM* guide.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: `[\w]+`

Required: No

PolicyName

The friendly name (not ARN) identifying the policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: No

PolicyVersionList.member.N

A list containing information about the versions of the policy.

Type: array of PolicyVersion (p. 292) objects

Required: No

UpdateDate

The date and time, in ISO 8601 date-time format, when the policy was last updated.

When a policy has only one version, this field contains the date and time when the policy was created. When a policy has more than one version, this field contains the date and time when the most recent policy version was created.

Type: Timestamp

Required: No

MFADevice

Contains information about an MFA device.

This data type is used as a response element in the ListMFADevices (p. 176) action.

Contents

EnableDate

The date when the MFA device was enabled for the user.

Type: Timestamp

Required: Yes

SerialNumber

The serial number that uniquely identifies the MFA device. For virtual MFA devices, the serial number is the device ARN.

Type: String

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

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

Required: Yes

UserName

The user with whom the MFA device is associated.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

OpenIDConnectProviderListEntry

Contains the Amazon Resource Name (ARN) for an IAM OpenID Connect provider.

Contents

Arn

The Amazon Resource Name (ARN). ARNs are unique identifiers for AWS resources.

For more information about ARNs, go to Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: No

PasswordPolicy

Contains information about the account password policy.

This data type is used as a response element in the GetAccountPasswordPolicy (p. 104) action.

Contents

AllowUsersToChangePassword

Specifies whether IAM users are allowed to change their own password.

Type: Boolean

Required: No

ExpirePasswords

Indicates whether passwords in the account expire. Returns true if MaxPasswordAge is contains a value greater than 0. Returns false if MaxPasswordAge is 0 or not present.

Type: Boolean

Required: No

HardExpiry

Specifies whether IAM users are prevented from setting a new password after their password has expired.

Type: Boolean

Required: No

MaxPasswordAge

The number of days that an IAM user password is valid.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1095.

Required: No

MinimumPasswordLength

Minimum length to require for IAM user passwords.

Type: Integer

Valid Range: Minimum value of 6. Maximum value of 128.

Required: No

PasswordReusePrevention

Specifies the number of previous passwords that IAM users are prevented from reusing.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 24.

Required: No

RequireLowercaseCharacters

Specifies whether to require lowercase characters for IAM user passwords.

Type: Boolean

Required: No

RequireNumbers

Specifies whether to require numbers for IAM user passwords.

Type: Boolean

Required: No

RequireSymbols

Specifies whether to require symbols for IAM user passwords.

Type: Boolean

Required: No

RequireUppercaseCharacters

Specifies whether to require uppercase characters for IAM user passwords.

Type: Boolean

Required: No

Policy

Contains information about a managed policy.

This data type is used as a response element in the CreatePolicy (p. 32), GetPolicy (p. 128), and ListPolicies (p. 179) actions.

For more information about managed policies, refer to Managed Policies and Inline Policies in the *Using IAM* guide.

Contents

Arn

The Amazon Resource Name (ARN). ARNs are unique identifiers for AWS resources.

For more information about ARNs, go to Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: No

AttachmentCount

The number of entities (users, groups, and roles) that the policy is attached to.

Type: Integer

Required: No

CreateDate

The date and time, in ISO 8601 date-time format, when the policy was created.

Type: Timestamp

Required: No

DefaultVersionId

The identifier for the version of the policy that is set as the default version.

Type: String

Pattern: `v[1-9][0-9]*(\.[A-Za-z0-9-]*)?`

Required: No

Description

A friendly description of the policy.

This element is included in the response to the GetPolicy (p. 128) operation. It is not included in the response to the ListPolicies (p. 179) operation.

Type: String

Length Constraints: Maximum length of 1000.

Required: No

IsAttachable

Specifies whether the policy can be attached to an IAM user, group, or role.

Type: Boolean

Required: No

Path

The path to the policy.

For more information about paths, see IAM Identifiers in the *Using IAM* guide.

Type: String

Pattern: `((/[A-Za-z0-9\.,\+@=_-]+)*)/`

Required: No

PolicyId

The stable and unique string identifying the policy.

For more information about IDs, see IAM Identifiers in the *Using IAM* guide.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: `[\w]+`

Required: No

PolicyName

The friendly name (not ARN) identifying the policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: No

UpdateDate

The date and time, in ISO 8601 date-time format, when the policy was last updated.

When a policy has only one version, this field contains the date and time when the policy was created. When a policy has more than one version, this field contains the date and time when the most recent policy version was created.

Type: Timestamp

Required: No

PolicyDetail

Contains information about an IAM policy, including the policy document.

This data type is used as a response element in the GetAccountAuthorizationDetails (p. 97) action.

Contents

PolicyDocument

The policy document.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: No

PolicyName

The name of the policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: No

PolicyGroup

Contains information about a group that a managed policy is attached to.

This data type is used as a response element in the ListEntitiesForPolicy (p. 160) action.

For more information about managed policies, refer to Managed Policies and Inline Policies in the *Using IAM* guide.

Contents

GroupId

The stable and unique string identifying the group. For more information about IDs, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: `[\w]+`

Required: No

GroupName

The name (friendly name, not ARN) identifying the group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: No

PolicyRole

Contains information about a role that a managed policy is attached to.

This data type is used as a response element in the ListEntitiesForPolicy (p. 160) action.

For more information about managed policies, refer to Managed Policies and Inline Policies in the *Using IAM* guide.

Contents

RoleId

The stable and unique string identifying the role. For more information about IDs, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: `[\w]+`

Required: No

RoleName

The name (friendly name, not ARN) identifying the role.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: No

PolicyUser

Contains information about a user that a managed policy is attached to.

This data type is used as a response element in the ListEntitiesForPolicy (p. 160) action.

For more information about managed policies, refer to Managed Policies and Inline Policies in the *Using IAM* guide.

Contents

UserId

The stable and unique string identifying the user. For more information about IDs, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: `[\w]+`

Required: No

UserName

The name (friendly name, not ARN) identifying the user.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: No

PolicyVersion

Contains information about a version of a managed policy.

This data type is used as a response element in the CreatePolicyVersion (p. 35), GetPolicyVersion (p. 130), ListPolicyVersions (p. 182), and GetAccountAuthorizationDetails (p. 97) actions.

For more information about managed policies, refer to Managed Policies and Inline Policies in the *Using IAM* guide.

Contents

CreateDate

The date and time, in ISO 8601 date-time format, when the policy version was created.

Type: Timestamp

Required: No

Document

The policy document.

The policy document is returned in the response to the GetPolicyVersion (p. 130) and GetAccountAuthorizationDetails (p. 97) operations. It is not returned in the response to the CreatePolicyVersion (p. 35) or ListPolicyVersions (p. 182) operations.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: No

IsDefaultVersion

Specifies whether the policy version is set as the policy's default version.

Type: Boolean

Required: No

VersionId

The identifier for the policy version.

Policy version identifiers always begin with `v` (always lowercase). When a policy is created, the first policy version is `v1`.

Type: String

Pattern: `v[1-9][0-9]*(\.[A-Za-z0-9-]*)?`

Required: No

Position

Contains the row and column of a location of a `Statement` element in a policy document.

This data type is used as a member of the `Statement (p. 304)` type.

Contents

Column

The column in the line containing the specified position in the document.

Type: Integer

Required: No

Line

The line containing the specified position in the document.

Type: Integer

Required: No

ResourceSpecificResult

Contains the result of the simulation of a single API action call on a single resource.

This data type is used by a member of the EvaluationResult (p. 274) data type.

Contents

EvalDecisionDetails , EvalDecisionDetails.entry.N.key (key), EvalDecisionDetailsentry.N.value (value)

Additional details about the results of the evaluation decision. When there are both IAM policies and resource policies, this parameter explains how each set of policies contributes to the final evaluation decision. When simulating cross-account access to a resource, both the resource-based policy and the caller's IAM policy must grant access.

Type: String to String map

Valid Values: `allowed | explicitDeny | implicitDeny`

Required: No

EvalResourceDecision

The result of the simulation of the simulated API action on the resource specified in `EvalResourceName`.

Type: String

Valid Values: `allowed | explicitDeny | implicitDeny`

Required: Yes

EvalResourceName

The name of the simulated resource, in Amazon Resource Name (ARN) format.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

MatchedStatements.member.N

A list of the statements in the input policies that determine the result for this part of the simulation. Remember that even if multiple statements allow the action on the resource, if *any* statement denies that action, then the explicit deny overrides any allow, and the deny statement is the only entry included in the result.

Type: array of Statement (p. 304) objects

Required: No

MissingContextValues.member.N

A list of context keys that are required by the included input policies but that were not provided by one of the input parameters. This list is used when a list of ARNs is included in the `ResourceArns` parameter instead of "*". If you do not specify individual resources, by setting `ResourceArns` to "*" or by not including the `ResourceArns` parameter, then any missing context values are instead included under the `EvaluationResults` section. To discover the context keys used by a set of policies, you can call GetContextKeysForCustomPolicy (p. 110) or GetContextKeysForPrincipalPolicy (p. 112).

Type: array of Strings

Length Constraints: Minimum length of 5. Maximum length of 256.

Required: No

Role

Contains information about an IAM role.

This data type is used as a response element in the following actions:

- CreateRole (p. 38)
- GetRole (p. 132)
- ListRoles (p. 187)

Contents

Arn

The Amazon Resource Name (ARN) specifying the role. For more information about ARNs and how to use them in policies, see IAM Identifiers in the *Using IAM* guide.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

AssumeRolePolicyDocument

The policy that grants an entity permission to assume the role.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: No

CreateDate

The date and time, in ISO 8601 date-time format, when the role was created.

Type: Timestamp

Required: Yes

Path

The path to the role. For more information about paths, see IAM Identifiers in the *Using IAM* guide.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: Yes

RoleId

The stable and unique string identifying the role. For more information about IDs, see IAM Identifiers in the *Using IAM* guide.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: `[\w]+`

Required: Yes

RoleName

The friendly name that identifies the role.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

RoleDetail

Contains information about an IAM role, including all of the role's policies.

This data type is used as a response element in the GetAccountAuthorizationDetails (p. 97) action.

Contents

Arn

The Amazon Resource Name (ARN). ARNs are unique identifiers for AWS resources.

For more information about ARNs, go to Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: No

AssumeRolePolicyDocument

The trust policy that grants permission to assume the role.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: No

AttachedManagedPolicies.member.N

A list of managed policies attached to the role. These policies are the role's access (permissions) policies.

Type: array of AttachedPolicy (p. 272) objects

Required: No

CreateDate

The date and time, in ISO 8601 date-time format, when the role was created.

Type: Timestamp

Required: No

InstanceProfileList.member.N

A list of instance profiles that contain this role.

Type: array of InstanceProfile (p. 278) objects

Required: No

Path

The path to the role. For more information about paths, see IAM Identifiers in the *Using IAM* guide.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: No

RoleId

The stable and unique string identifying the role. For more information about IDs, see IAM Identifiers in the *Using IAM* guide.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: `[\w]+`

Required: No

RoleName

The friendly name that identifies the role.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: No

RolePolicyList.member.N

A list of inline policies embedded in the role. These policies are the role's access (permissions) policies.

Type: array of PolicyDetail (p. 288) objects

Required: No

SAMLProviderListEntry

Contains the list of SAML providers for this account.

Contents

Arn

The Amazon Resource Name (ARN) of the SAML provider.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: No

CreateDate

The date and time when the SAML provider was created.

Type: Timestamp

Required: No

ValidUntil

The expiration date and time for the SAML provider.

Type: Timestamp

Required: No

ServerCertificate

Contains information about a server certificate.

This data type is used as a response element in the GetServerCertificate (p. 138) action.

Contents

CertificateBody

The contents of the public key certificate.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 16384.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

CertificateChain

The contents of the public key certificate chain.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2097152.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: No

ServerCertificateMetadata

The meta information of the server certificate, such as its name, path, ID, and ARN.

Type: ServerCertificateMetadata (p. 300) object

Required: Yes

ServerCertificateMetadata

Contains information about a server certificate without its certificate body, certificate chain, and private key.

This data type is used as a response element in the UploadServerCertificate (p. 257) and ListServerCertificates (p. 191) actions.

Contents

Arn

The Amazon Resource Name (ARN) specifying the server certificate. For more information about ARNs and how to use them in policies, see IAM Identifiers in the *Using IAM* guide.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Expiration

The date on which the certificate is set to expire.

Type: Timestamp

Required: No

Path

The path to the server certificate. For more information about paths, see IAM Identifiers in the *Using IAM* guide.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: Yes

ServerCertificateId

The stable and unique string identifying the server certificate. For more information about IDs, see IAM Identifiers in the *Using IAM* guide.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: `[\w]+`

Required: Yes

ServerCertificateName

The name that identifies the server certificate.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: Yes

UploadDate

The date when the server certificate was uploaded.

Type: Timestamp

Required: No

SigningCertificate

Contains information about an X.509 signing certificate.

This data type is used as a response element in the UploadSigningCertificate (p. 261) and ListSigningCertificates (p. 194) actions.

Contents

CertificateBody

The contents of the signing certificate.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 16384.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

CertificateId

The ID for the signing certificate.

Type: String

Length Constraints: Minimum length of 24. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

Status

The status of the signing certificate. `Active` means the key is valid for API calls, while `Inactive` means it is not.

Type: String

Valid Values: `Active | Inactive`

Required: Yes

UploadDate

The date when the signing certificate was uploaded.

Type: Timestamp

Required: No

UserName

The name of the user the signing certificate is associated with.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

SSHPublicKey

Contains information about an SSH public key.

This data type is used as a response element in the GetSSHPublicKey (p. 140) and UploadSSHPublicKey (p. 264) actions.

Contents

Fingerprint

The MD5 message digest of the SSH public key.

Type: String

Length Constraints: Fixed length of 48.

Pattern: `[:\w]+`

Required: Yes

SSHPublicKeyBody

The SSH public key.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 16384.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

SSHPublicKeyId

The unique identifier for the SSH public key.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

Status

The status of the SSH public key. `Active` means the key can be used for authentication with an AWS CodeCommit repository. `Inactive` means the key cannot be used.

Type: String

Valid Values: `Active | Inactive`

Required: Yes

UploadDate

The date and time, in ISO 8601 date-time format, when the SSH public key was uploaded.

Type: Timestamp

Required: No

UserName

The name of the IAM user associated with the SSH public key.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

SSHPublicKeyMetadata

Contains information about an SSH public key, without the key's body or fingerprint.

This data type is used as a response element in the ListSSHPublicKeys (p. 197) action.

Contents

SSHPublicKeyId

The unique identifier for the SSH public key.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

Status

The status of the SSH public key. `Active` means the key can be used for authentication with an AWS CodeCommit repository. `Inactive` means the key cannot be used.

Type: String

Valid Values: `Active | Inactive`

Required: Yes

UploadDate

The date and time, in ISO 8601 date-time format, when the SSH public key was uploaded.

Type: Timestamp

Required: Yes

UserName

The name of the IAM user associated with the SSH public key.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

Statement

Contains a reference to a `Statement` element in a policy document that determines the result of the simulation.

This data type is used by the `MatchedStatements` member of the `EvaluationResult (p. 274)` type.

Contents

EndPosition

The row and column of the end of a `Statement` in an IAM policy.

Type: Position (p. 293) object

Required: No

SourcePolicyId

The identifier of the policy that was provided as an input.

Type: String

Required: No

SourcePolicyType

The type of the policy.

Type: String

Valid Values: `user | group | role | aws-managed | user-managed | resource | none`

Required: No

StartPosition

The row and column of the beginning of the `Statement` in an IAM policy.

Type: Position (p. 293) object

Required: No

User

Contains information about an IAM user entity.

This data type is used as a response element in the following actions:

- CreateUser (p. 43)
- GetUser (p. 142)
- ListUsers (p. 201)

Contents

Arn

The Amazon Resource Name (ARN) that identifies the user. For more information about ARNs and how to use ARNs in policies, see IAM Identifiers in the *Using IAM* guide.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

CreateDate

The date and time, in ISO 8601 date-time format, when the user was created.

Type: Timestamp

Required: Yes

PasswordLastUsed

The date and time, in ISO 8601 date-time format, when the user's password was last used to sign in to an AWS website. For a list of AWS websites that capture a user's last sign-in time, see the Credential Reports topic in the *Using IAM* guide. If a password is used more than once in a five-minute span, only the first use is returned in this field. This field is null (not present) when:

- The user does not have a password
- The password exists but has never been used (at least not since IAM started tracking this information on October 20th, 2014
- there is no sign-in data associated with the user

This value is returned only in the GetUser (p. 142) and ListUsers (p. 201) actions.

Type: Timestamp

Required: No

Path

The path to the user. For more information about paths, see IAM Identifiers in the *Using IAM* guide.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: Yes

UserId

The stable and unique string identifying the user. For more information about IDs, see IAM Identifiers in the *Using IAM* guide.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: `[\w]+`

Required: Yes

UserName

The friendly name identifying the user.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: Yes

UserDetail

Contains information about an IAM user, including all the user's policies and all the IAM groups the user is in.

This data type is used as a response element in the GetAccountAuthorizationDetails (p. 97) action.

Contents

Arn

The Amazon Resource Name (ARN). ARNs are unique identifiers for AWS resources.

For more information about ARNs, go to Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: No

AttachedManagedPolicies.member.N

A list of the managed policies attached to the user.

Type: array of AttachedPolicy (p. 272) objects

Required: No

CreateDate

The date and time, in ISO 8601 date-time format, when the user was created.

Type: Timestamp

Required: No

GroupList.member.N

A list of IAM groups that the user is in.

Type: array of Strings

Length Constraints: Minimum length of 1. Maximum length of 128.

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

Required: No

Path

The path to the user. For more information about paths, see IAM Identifiers in the *Using IAM* guide.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: No

UserId

The stable and unique string identifying the user. For more information about IDs, see IAM Identifiers in the *Using IAM* guide.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: `[\w]+`

Required: No

UserName

The friendly name identifying the user.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

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

Required: No

UserPolicyList.member.N

A list of the inline policies embedded in the user.

Type: array of PolicyDetail (p. 288) objects

Required: No

VirtualMFADevice

Contains information about a virtual MFA device.

Contents

Base32StringSeed

The Base32 seed defined as specified in RFC3548. The `Base32StringSeed` is Base64-encoded.

Type: Base64-encoded binary data

Required: No

EnableDate

The date and time on which the virtual MFA device was enabled.

Type: Timestamp

Required: No

QRCodePNG

A QR code PNG image that encodes `otpauth://totp/$virtualMFADeviceName@$AccountName?secret=$Base32String` where `$virtualMFADeviceName` is one of the create call arguments, `AccountName` is the user name if set (otherwise, the account ID otherwise), and `Base32String` is the seed in Base32 format. The `Base32String` value is Base64-encoded.

Type: Base64-encoded binary data

Required: No

SerialNumber

The serial number associated with `VirtualMFADevice`.

Type: String

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

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

Required: Yes

User

The user to whom the MFA device is assigned.

Type: User (p. 305) object

Required: No

Common Parameters

The following table lists the parameters that all actions use for signing Signature Version 4 requests. Any action-specific parameters are listed in the topic for that action. To view sample requests, see Examples of Signed Signature Version 4 Requests or Signature Version 4 Test Suite in the *Amazon Web Services General Reference*.

Action

The action to be performed.

Type: string

Required: Yes

Version

The API version that the request is written for, expressed in the format YYYY-MM-DD.

Type: string

Required: Yes

X-Amz-Algorithm

The hash algorithm that you used to create the request signature.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Valid Values: `AWS4-HMAC-SHA256`

Required: Conditional

X-Amz-Credential

The credential scope value, which is a string that includes your access key, the date, the region you are targeting, the service you are requesting, and a termination string ("aws4_request"). The value is expressed in the following format: *access_key*/*YYYYMMDD*/*region*/*service*/aws4_request.

For more information, see Task 2: Create a String to Sign for Signature Version 4 in the *Amazon Web Services General Reference*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

X-Amz-Date

The date that is used to create the signature. The format must be ISO 8601 basic format (YYYYMMDD'T'HHMMSS'Z'). For example, the following date time is a valid X-Amz-Date value: `20120325T120000Z`.

Condition: X-Amz-Date is optional for all requests; it can be used to override the date used for signing requests. If the Date header is specified in the ISO 8601 basic format, X-Amz-Date is not required. When X-Amz-Date is used, it always overrides the value of the Date header. For more information, see Handling Dates in Signature Version 4 in the *Amazon Web Services General Reference*.

Type: string

Required: Conditional

X-Amz-Security-Token

The temporary security token that was obtained through a call to AWS Security Token Service. For a list of services that support AWS Security Token Service, go to Using Temporary Security Credentials to Access AWS in *Using Temporary Security Credentials*.

Condition: If you're using temporary security credentials from the AWS Security Token Service, you must include the security token.

Type: string

Required: Conditional

X-Amz-Signature

Specifies the hex-encoded signature that was calculated from the string to sign and the derived signing key.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

X-Amz-SignedHeaders

Specifies all the HTTP headers that were included as part of the canonical request. For more information about specifying signed headers, see Task 1: Create a Canonical Request For Signature Version 4 in the *Amazon Web Services General Reference*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

Common Errors

This section lists the common errors that all actions return. Any action-specific errors are listed in the topic for the action.

IncompleteSignature

The request signature does not conform to AWS standards.

HTTP Status Code: 400

InternalFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

InvalidAction

The action or operation requested is invalid. Verify that the action is typed correctly.

HTTP Status Code: 400

InvalidClientTokenId

The X.509 certificate or AWS access key ID provided does not exist in our records.

HTTP Status Code: 403

InvalidParameterCombination

Parameters that must not be used together were used together.

HTTP Status Code: 400

InvalidParameterValue

An invalid or out-of-range value was supplied for the input parameter.

HTTP Status Code: 400

InvalidQueryParameter

The AWS query string is malformed or does not adhere to AWS standards.

HTTP Status Code: 400

MalformedQueryString

The query string contains a syntax error.

HTTP Status Code: 404

MissingAction

The request is missing an action or a required parameter.

HTTP Status Code: 400

MissingAuthenticationToken

The request must contain either a valid (registered) AWS access key ID or X.509 certificate.

HTTP Status Code: 403

MissingParameter

A required parameter for the specified action is not supplied.

HTTP Status Code: 400

OptInRequired

The AWS access key ID needs a subscription for the service.

HTTP Status Code: 403

RequestExpired

The request reached the service more than 15 minutes after the date stamp on the request or more than 15 minutes after the request expiration date (such as for pre-signed URLs), or the date stamp on the request is more than 15 minutes in the future.

HTTP Status Code: 400

ServiceUnavailable

The request has failed due to a temporary failure of the server.

HTTP Status Code: 503

Throttling

The request was denied due to request throttling.

HTTP Status Code: 400

ValidationError

The input fails to satisfy the constraints specified by an AWS service.

HTTP Status Code: 400