aws

API Reference

IAM Toolbox



API Version 2018-05-10

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

IAM Toolbox: API Reference

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Services or capabilities described in AWS documentation might vary by Region. To see the differences applicable to the AWS European Sovereign Cloud Region, see the AWS European Sovereign Cloud User Guide.

Table of Contents

Welcome **1**
Actions **2**
GetRequestAuthorizationDetails 3
Request Syntax 3
URI Request Parameters 3
Request Body 4
Response Syntax 4
Response Elements 5
Errors 6
Examples 7
See Also 18
GetRequestAuthorizationPolicy 20
Request Syntax 20
URI Request Parameters 20
Request Body 21
Response Syntax 21
Response Elements 21
Errors 21
Examples 22
See Also 23
Data Types **24**
AttachedTo 25
Contents 25
See Also 25
Check 26
Contents 26
See Also 28
Evaluation 29
Contents 29
See Also 30
MatchedPolicy 32
Contents 32
See Also 32
MatchedStatement 33

Contents 33
See Also 33
PolicyInfo 34
Contents 34
See Also 35
Common Parameters 37
Common Error Types 40

Welcome

Contains APIs to work with AWS Identity and Access Management (IAM).

This document was last published on November 20, 2026.

Actions

The following actions are supported:

- GetRequestAuthorizationDetails
- GetRequestAuthorizationPolicy

GetRequestAuthorizationDetails

Retrieves the authorization details for a specific access denied request. The details include the request context, the evaluations performed, and the policies that were evaluated.

Use this operation to understand why a request was denied. Supported services include an authorization ID in the access denied error message. Pass that ID to this operation to retrieve the details.

To retrieve the content for a policy in the `policies` list, call `GetRequestAuthorizationPolicy`.

Authorization details are available for at least 24 hours after the denial.

To use this operation, you must have the `iam:GetRequestAuthorizationDetails` permission.

Request Syntax

```
GET /authorization-details/authorizationId?nextToken=nextToken HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

authorizationId

The authorization ID received in the access denied error message. This ID identifies the specific request to retrieve details for.

Length Constraints: Minimum length of 0. Maximum length of 256.

Pattern: `[0123456789abcdefghijklmnopqrstuvwxyz]+`

Required: Yes

nextToken

The pagination token from a previous call, used to retrieve the next page of evaluations. Omit this value on the first call.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "evaluations": [
      {
         "action": "string",
         "checks": [
            {
               "checkType": "string",
               "evaluatedEffect": "string",
               "matchedPolicies": [
                  {
                     "matchedStatements": [
                        {
                           "evaluatedEffect": "string",
                           "sid": "string"
                        }
                     ],
                     "uri": "string"
                  }
               ],
               "relevantPolicyTypes": [ "string" ],
               "targetArn": "string"
            }
         ],
         "context": {
            "string" : JSON value
         },
         "evaluatedEffect": "string",
         "matchedPolicies": [
            {
               "matchedStatements": [
                  {
                     "evaluatedEffect": "string",
                     "sid": "string"
                  }
```

```
                ],
                "uri": "string"
             }
          ],
          "resource": "string"
       }
    ],
    "nextToken": "string",
    "policies": [
       {
          "attachedTo": [
             {
                "arn": "string"
             }
          ],
          "inline": boolean,
          "policySource": {
             "string" : "string"
          },
          "type": "string",
          "uri": "string"
       }
    ],
    "requestContext": {
       "string" : JSON value
    }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

evaluations

The list of evaluations for this request. Each evaluation shows how a single action and resource pair was evaluated. This includes the context, the effect, and any policies that matched.

Type: Array of Evaluation objects

nextToken

The pagination token for retrieving the next page of evaluations. This value is absent when there are no more results.

Type: String

policies

The list of policies that were evaluated.

Type: Array of PolicyInfo objects

requestContext

The request context is the set of context keys and values that apply to the entire request and are shared by all evaluations.

Type: String to JSON value map

Errors

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

AccessDeniedException

The caller does not have sufficient access to perform this action.

HTTP Status Code: 403

InternalServerException

An unexpected error occurred while processing the request. Try again.

HTTP Status Code: 500

ResourceNotFoundException

The requested policy or authorization details do not exist in this region or have expired. Verify that the authorization ID from the access denied error message is correct and the call is made in the region where the denial occurred. Ensure that the calling principal belongs to the same account or organization as the original denied request. If you specified a policy URI, verify that it is from the `policies` list that `GetRequestAuthorizationDetails` returns for the same authorization ID.

HTTP Status Code: 404

ValidationException

The request is malformed or is missing one or more required parameters. Check the request parameters and try again.

HTTP Status Code: 400

Examples

Example – Retrieve authorization details for an implicitly denied iam:GetUser request

This example illustrates one usage of GetRequestAuthorizationDetails.

Sample Request

```
{
  "authorizationId": "a1b2c3d4e5f6g7h8i9j0"
}
```

Sample Response

```
{
  "evaluations": [
    {
      "action": "iam:GetUser",
      "checks": [
        {
          "checkType": "RESOURCE_CONTROL_POLICY",
          "evaluatedEffect": "ALLOW",
          "matchedPolicies": [
            {
              "matchedStatements": [
                {
                  "evaluatedEffect": "ALLOW",
                  "sid": "<Statement1>"
                }
              ],
              "uri": "arn:aws:organizations::aws:policy/resource_control_policy/p-
RCPFullAWSAccess"
```

```
            }
          ],
          "relevantPolicyTypes": [
            "RESOURCE_CONTROL_POLICY"
          ],
          "targetArn": "arn:aws:organizations::111122223333:root/o-exampleorgid/r-
examp"
        },
        {
          "checkType": "RESOURCE_CONTROL_POLICY",
          "evaluatedEffect": "ALLOW",
          "matchedPolicies": [
            {
              "matchedStatements": [
                {
                  "evaluatedEffect": "ALLOW",
                  "sid": "<Statement1>"
                }
              ],
              "uri": "arn:aws:organizations::aws:policy/resource_control_policy/p-
RCPFullAWSAccess"
            }
          ],
          "relevantPolicyTypes": [
            "RESOURCE_CONTROL_POLICY"
          ],
          "targetArn": "arn:aws:organizations::111122223333:account/o-
exampleorgid/111122223333"
        },
        {
          "checkType": "SERVICE_CONTROL_POLICY",
          "evaluatedEffect": "ALLOW",
          "matchedPolicies": [
            {
              "matchedStatements": [
                {
                  "evaluatedEffect": "ALLOW",
                  "sid": "<Statement1>"
                }
              ],
              "uri": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess"
            }
          ],
```

```
          "relevantPolicyTypes": [
            "SERVICE_CONTROL_POLICY"
          ],
          "targetArn": "arn:aws:organizations::111122223333:root/o-exampleorgid/r-
examp"
        },
        {
          "checkType": "SERVICE_CONTROL_POLICY",
          "evaluatedEffect": "ALLOW",
          "matchedPolicies": [
            {
              "matchedStatements": [
                {
                  "evaluatedEffect": "ALLOW",
                  "sid": "<Statement1>"
                }
              ],
              "uri": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess"
            }
          ],
          "relevantPolicyTypes": [
            "SERVICE_CONTROL_POLICY"
          ],
          "targetArn": "arn:aws:organizations::111122223333:account/o-
exampleorgid/111122223333"
        },
        {
          "checkType": "PRINCIPAL",
          "evaluatedEffect": "IMPLICIT_DENY",
          "matchedPolicies": [],
          "relevantPolicyTypes": [
            "IDENTITY_BASED_POLICY"
          ]
        },
        {
          "checkType": "SESSION",
          "evaluatedEffect": "ALLOW",
          "matchedPolicies": [
            {
              "matchedStatements": [
                {
                  "evaluatedEffect": "ALLOW",
                  "sid": "AllowAll"
```

```
                }
              ],
              "uri": "inline:b6cf943c21a1966b"
            }
          ],
          "relevantPolicyTypes": [
            "SESSION_POLICY"
          ]
        }
      ],
      "context": {},
      "evaluatedEffect": "IMPLICIT_DENY",
      "matchedPolicies": [
        {
          "matchedStatements": [
            {
              "evaluatedEffect": "ALLOW",
              "sid": "<Statement1>"
            }
          ],
          "uri": "arn:aws:organizations::aws:policy/resource_control_policy/p-
RCPFullAWSAccess"
        },
        {
          "matchedStatements": [
            {
              "evaluatedEffect": "ALLOW",
              "sid": "<Statement1>"
            }
          ],
          "uri": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess"
        },
        {
          "matchedStatements": [
            {
              "evaluatedEffect": "ALLOW",
              "sid": "AllowAll"
            }
          ],
          "uri": "inline:b6cf943c21a1966b"
        }
      ],
      "resource": "arn:aws:iam::111122223333:user/ExampleUser"
```

```
    }
  ],
  "policies": [
    {
      "attachedTo": [
        {
          "arn": "arn:aws:organizations::111122223333:root/o-exampleorgid/r-examp"
        },
        {
          "arn": "arn:aws:organizations::111122223333:account/o-
exampleorgid/111122223333"
        }
      ],
      "inline": false,
      "type": "RESOURCE_CONTROL_POLICY",
      "uri": "arn:aws:organizations::aws:policy/resource_control_policy/p-
RCPFullAWSAccess"
    },
    {
      "attachedTo": [
        {
          "arn": "arn:aws:organizations::111122223333:root/o-exampleorgid/r-examp"
        },
        {
          "arn": "arn:aws:organizations::111122223333:account/o-
exampleorgid/111122223333"
        }
      ],
      "inline": false,
      "type": "SERVICE_CONTROL_POLICY",
      "uri": "arn:aws:organizations::aws:policy/service_control_policy/p-FullAWSAccess"
    },
    {
      "attachedTo": [
        {
          "arn": "arn:aws:iam::111122223333:role/ImplicitDeny"
        }
      ],
      "inline": true,
      "type": "SESSION_POLICY",
      "uri": "inline:b6cf943c21a1966b"
    }
  ],
  "requestContext": {
```

```
    "aws:ViaAWSService": "false",
    "aws:MultiFactorAuthPresent": "false",
    "aws:TokenIssueTime": "2026-01-01T00:00:00Z",
    "aws:ResourceOrgPaths": "[o-exampleorgid/r-examp/]",
    "aws:UserAgent": "aws-cli/2.0.0 md/command#iam.get-user",
    "aws:UserId": "AROA123456789EXAMPLE:example-session",
    "aws:ResourceOrgID": "o-exampleorgid",
    "aws:PrincipalAccount": "111122223333",
    "aws:EpochTime": "2026-01-01T00:00:00Z",
    "aws:PrincipalARN": "arn:aws:iam::111122223333:role/ImplicitDeny",
    "aws:ViaAWSMCPService": "false",
    "aws:SourceIp": "192.0.2.1/32",
    "aws:RequestedRegion": "us-east-1",
    "aws:PrincipalIsAWSService": "false",
    "aws:SecureTransport": "true",
    "aws:PrincipalOrgPaths": "[o-exampleorgid/r-examp/]",
    "aws:PrincipalOrgID": "o-exampleorgid",
    "aws:CurrentTime": "2026-01-01T00:00:00Z"
  }
}
```

Example – Retrieve authorization details for an explicitly denied iam:GetUser request

This example illustrates one usage of GetRequestAuthorizationDetails.

Sample Request

```
{
  "authorizationId": "z9y8x7w6v5u4t3s2r1q0"
}
```

Sample Response

```
{
  "evaluations": [
    {
      "action": "iam:GetUser",
      "checks": [
        {
          "checkType": "PRINCIPAL",
          "evaluatedEffect": "EXPLICIT_DENY",
          "matchedPolicies": [
```

```
            {
              "matchedStatements": [
                {
                  "evaluatedEffect": "DENY",
                  "sid": "DenyAll"
                }
              ],
              "uri": "arn:aws:iam::aws:policy/AWSDenyAll"
            }
          ],
          "relevantPolicyTypes": [
            "IDENTITY_BASED_POLICY"
          ]
        },
        {
          "checkType": "SESSION",
          "evaluatedEffect": "ALLOW",
          "matchedPolicies": [
            {
              "matchedStatements": [
                {
                  "evaluatedEffect": "ALLOW",
                  "sid": "AllowAll"
                }
              ],
              "uri": "inline:0000000000000000"
            }
          ],
          "relevantPolicyTypes": [
            "SESSION_POLICY"
          ]
        }
      ],
      "context": {},
      "evaluatedEffect": "EXPLICIT_DENY",
      "matchedPolicies": [
        {
          "matchedStatements": [
            {
              "evaluatedEffect": "DENY",
              "sid": "DenyAll"
            }
          ],
          "uri": "arn:aws:iam::aws:policy/AWSDenyAll"
```

```
        },
        {
          "matchedStatements": [
            {
              "evaluatedEffect": "ALLOW",
              "sid": "AllowAll"
            }
          ],
          "uri": "inline:0000000000000000"
        }
      ],
      "resource": "arn:aws:iam::111122223333:user/ExampleUser"
    }
  ],
  "policies": [
    {
      "attachedTo": [
        {
          "arn": "arn:aws:iam::111122223333:role/ExplicitDeny"
        }
      ],
      "inline": false,
      "type": "IDENTITY_BASED_POLICY",
      "uri": "arn:aws:iam::aws:policy/AWSDenyAll"
    },
    {
      "attachedTo": [
        {
          "arn": "arn:aws:iam::111122223333:role/ExplicitDeny"
        }
      ],
      "inline": true,
      "type": "SESSION_POLICY",
      "uri": "inline:0000000000000000"
    }
  ],
  "requestContext": {
    "aws:UserId": "AROA123456789EXAMPLE:example-session",
    "aws:PrincipalAccount": "111122223333",
    "aws:PrincipalARN": "arn:aws:iam::111122223333:role/ExplicitDeny",
    "aws:RequestedRegion": "us-east-1"
  }
}
```

Example – Retrieve authorization details for an explicitly denied kms:Decrypt request

This example illustrates one usage of GetRequestAuthorizationDetails.

Sample Request

```
{
  "authorizationId": "m4n5o6p7q8r9s0t1u2v3"
}
```

Sample Response

```
{
  "evaluations": [
    {
      "action": "kms:Decrypt",
      "checks": [
        {
          "checkType": "RESOURCE",
          "evaluatedEffect": "EXPLICIT_DENY",
          "matchedPolicies": [
            {
              "matchedStatements": [
                {
                  "evaluatedEffect": "DENY",
                  "sid": "DenyDecrypt"
                }
              ],
              "uri": "inline:3f1c9a7e5d2b8046"
            }
          ],
          "relevantPolicyTypes": [
            "RESOURCE_BASED_POLICY"
          ]
        },
        {
          "checkType": "PRINCIPAL",
          "evaluatedEffect": "ALLOW",
          "matchedPolicies": [
            {
              "matchedStatements": [
                {
```

```
                "evaluatedEffect": "ALLOW",
                "sid": "AllowDecrypt"
              }
            ],
            "uri": "arn:aws:iam::111122223333:policy/ExampleKmsAccess"
          }
        ],
        "relevantPolicyTypes": [
          "IDENTITY_BASED_POLICY"
        ]
      },
      {
        "checkType": "SESSION",
        "evaluatedEffect": "ALLOW",
        "matchedPolicies": [
          {
            "matchedStatements": [
              {
                "evaluatedEffect": "ALLOW",
                "sid": "AllowAll"
              }
            ],
            "uri": "inline:5a8c0e2f4b6d1937"
          }
        ],
        "relevantPolicyTypes": [
          "SESSION_POLICY"
        ]
      }
    ],
    "context": {},
    "evaluatedEffect": "EXPLICIT_DENY",
    "matchedPolicies": [
      {
        "matchedStatements": [
          {
            "evaluatedEffect": "ALLOW",
            "sid": "AllowDecrypt"
          }
        ],
        "uri": "arn:aws:iam::111122223333:policy/ExampleKmsAccess"
      },
      {
        "matchedStatements": [
```

```
            {
              "evaluatedEffect": "DENY",
              "sid": "DenyDecrypt"
            }
          ],
          "uri": "inline:3f1c9a7e5d2b8046"
        },
        {
          "matchedStatements": [
            {
              "evaluatedEffect": "ALLOW",
              "sid": "AllowAll"
            }
          ],
          "uri": "inline:5a8c0e2f4b6d1937"
        }
      ],
      "resource": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ],
  "policies": [
    {
      "attachedTo": [
        {
          "arn": "arn:aws:iam::111122223333:role/ExampleRole"
        }
      ],
      "inline": false,
      "type": "IDENTITY_BASED_POLICY",
      "uri": "arn:aws:iam::111122223333:policy/ExampleKmsAccess"
    },
    {
      "attachedTo": [
        {
          "arn": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
      ],
      "inline": true,
      "policySource": {
        "type": "KMS_KEY_POLICY",
        "typeName": "KMS key policy"
      },
```

```
      "type": "RESOURCE_BASED_POLICY",
      "uri": "inline:3f1c9a7e5d2b8046"
    },
    {
      "attachedTo": [
        {
          "arn": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
      ],
      "inline": true,
      "policySource": {
        "grantId": "0c237476b39f8bc44e45212e08498fbe3151305030726c0590dd8d3e9f3d6a60",
        "type": "KMS_GRANT",
        "typeName": "KMS grant"
      },
      "type": "RESOURCE_BASED_POLICY",
      "uri": "inline:9e4d27b1c6a0f583"
    },
    {
      "attachedTo": [
        {
          "arn": "arn:aws:iam::111122223333:role/ExampleRole"
        }
      ],
      "inline": true,
      "type": "SESSION_POLICY",
      "uri": "inline:5a8c0e2f4b6d1937"
    }
  ],
  "requestContext": {
    "aws:UserId": "AROA123456789EXAMPLE:example-session",
    "aws:PrincipalAccount": "111122223333",
    "aws:PrincipalARN": "arn:aws:iam::111122223333:role/ExampleRole",
    "aws:RequestedRegion": "us-east-1"
  }
}
```


See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetRequestAuthorizationPolicy

Retrieves a policy that was evaluated for a specific access denied request. The operation returns the structured JSON document of the policy that was captured with the original authorization request. It doesn't retrieve the current version of the policy.

For some AWS services and policy types, the returned policy document includes all actions relevant to the service that processed the denied request, but might omit actions for other services.

Specify the authorization ID from the access denied error message and the policy URI returned by `GetRequestAuthorizationDetails` for the same authorization ID.

Access depends on the account and organization recorded for the principal that made the denied request. If an organization was recorded, the calling principal must belong to that organization. Otherwise, the calling principal must belong to the recorded account.

To use this operation, you must have the `iam:GetRequestAuthorizationPolicy` permission.

Request Syntax

```
GET /authorization-details/authorizationId/policy?policyUri=policyUri HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

authorizationId

The authorization ID received in the access denied error message. This ID identifies the request whose evaluated policy you want to retrieve.

Length Constraints: Minimum length of 0. Maximum length of 256.

Pattern: `[0123456789abcdefghijklmnopqrstuvwxyz]+`

Required: Yes

policyUri

The URI of the policy to retrieve. Use the `uri` value from the `policies` list returned by `GetRequestAuthorizationDetails` for the same authorization ID.

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "policyDocument": JSON value
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

policyDocument

The policy document evaluated for the denied request, returned as a JSON object.

For some AWS services and policy types, this document includes all actions relevant to the service that processed the denied request, but might omit actions for other services.

Type: JSON value

Errors

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

AccessDeniedException

The caller does not have sufficient access to perform this action.

HTTP Status Code: 403

InternalServerException

An unexpected error occurred while processing the request. Try again.

HTTP Status Code: 500

ResourceNotFoundException

The requested policy or authorization details do not exist in this region or have expired. Verify that the authorization ID from the access denied error message is correct and the call is made in the region where the denial occurred. Ensure that the calling principal belongs to the same account or organization as the original denied request. If you specified a policy URI, verify that it is from the `policies` list that `GetRequestAuthorizationDetails` returns for the same authorization ID.

HTTP Status Code: 404

ValidationException

The request is malformed or is missing one or more required parameters. Check the request parameters and try again.

HTTP Status Code: 400

Examples

Example – Retrieve the policy for an explicitly denied iam:GetUser request

This example illustrates one usage of GetRequestAuthorizationPolicy.

Sample Request

```
{
  "authorizationId": "z9y8x7w6v5u4t3s2r1q0",
  "policyUri": "arn:aws:iam::aws:policy/AWSDenyAll"
}
```

Sample Response

```
{
  "policyDocument": {
    "Version": "2012-10-17",
```

```
    "Statement": [
      {
        "Sid": "DenyAll",
        "Effect": "Deny",
        "Action": "*",
        "Resource": "*"
      }
    ]
  }
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

Data Types

The IAM Toolbox (Preview) 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:

- AttachedTo
- Check
- Evaluation
- MatchedPolicy
- MatchedStatement
- PolicyInfo

AttachedTo

An entity that a policy is attached to, identified by its ARN.

Contents

arn

The ARN of the entity that the policy is attached to. The ARN format depends on the policy type:

- For identity, session, and permissions boundary policies, this is the principal ARN (for example, an IAM role or user ARN).
- For resource-based policies, this is the resource ARN.
- For organization control policies (SCPs and RCPs), this is the AWS Organizations ARN of the account, organizational unit, or root.

Type: String

Pattern: `arn:[^:]*:[^:]*:[^:]*:[^:]*:.*`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Check

Represents one authorization requirement considered during an evaluation and its result.

Contents

checkType

The type of requirement that the check evaluates. Valid values:

- `SERVICE_CONTROL_POLICY` - The service control policies (SCPs) attached to one organization target, such as a root, organizational unit, or account, that apply to the principal.
- `RESOURCE_CONTROL_POLICY` - The resource control policies (RCPs) attached to one organization target that apply to the resource.
- `VPC_ENDPOINT` - The VPC endpoint policy for the endpoint through which the request passes.
- `RESOURCE` - The resource owner's resource-based policies, when the owner must allow the request separately, such as a cross-account request or a request to an AWS KMS key.
- `PRINCIPAL` - The principal's identity-based policies attached to the IAM user or role.
- `PERMISSIONS_BOUNDARY` - The permissions boundary on the IAM user or role.
- `SESSION` - The role session that made the request, decided by its session policies.

Type: String

Valid Values: `SERVICE_CONTROL_POLICY | RESOURCE_CONTROL_POLICY | VPC_ENDPOINT | RESOURCE | PRINCIPAL | PERMISSIONS_BOUNDARY | SESSION`

Required: Yes

evaluatedEffect

The result of evaluating this requirement. Valid values:

- `ALLOW` - A statement that applies to this check allows the request.
- `EXPLICIT_DENY` - A deny statement that applies to this check matches.
- `IMPLICIT_DENY` - The check required an allow and nothing that applies to it allows the request.
- `NO_IMPACT` - No statement in this check matched, and no allow was needed because another path allowed the request.

Type: String

Valid Values: `ALLOW | NO_IMPACT | IMPLICIT_DENY | EXPLICIT_DENY`

Required: Yes

matchedPolicies

Policies in this list have statements that matched for this check. Each URI corresponds to an entry in the top-level `policies` list. Only policies in the top-level list are included. The check effect can reflect a matched policy omitted from this list, so this list can be empty even when the effect is `ALLOW`.

Type: Array of MatchedPolicy objects

Required: No

relevantPolicyTypes

The policy types used to satisfy this check, plus the type of every policy with a statement that matched in it. `matchedPolicies` lists matching policies in the top-level `policies` list.

Type: Array of strings

Valid Values: `IDENTITY_BASED_POLICY | RESOURCE_BASED_POLICY | PERMISSIONS_BOUNDARY | SESSION_POLICY | SERVICE_CONTROL_POLICY | RESOURCE_CONTROL_POLICY | VPC_ENDPOINT_POLICY`

Required: No

targetArn

The ARN that distinguishes this check from other checks of the same type. This value is absent when the check type alone identifies the check. For SCP and RCP checks, this is the AWS Organizations ARN of the root, organizational unit, or account that the evaluated policies are attached to.

Type: String

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Evaluation

Represents an individual evaluation for a single action and resource pair. This includes the context, the resulting effect, and any policies that matched.

Contents

action

The action evaluated for this request (for example, `iam:PassRole`).

Type: String

Required: Yes

resource

The resource that the action targeted. This is typically a resource ARN, but can be a wildcard ARN that matches multiple resources, or empty for actions that are not resource-specific.

Type: String

Required: Yes

checks

`checks` contains the authorization checks that explain an evaluation result. Each check is one authorization requirement and reports its result and policies from the top-level `policies` list with matching statements. The output lists RCP checks from the organization root to the account, then SCP checks from the organization root to the account. It then lists VPC endpoint, resource, principal, permissions boundary, and session checks. When `checks` is present, an `EXPLICIT_DENY` evaluation includes an `EXPLICIT_DENY` check. When `checks` is present for an `IMPLICIT_DENY` evaluation, it includes an `IMPLICIT_DENY` check and no `EXPLICIT_DENY` check. For more information about how IAM evaluates policies, see Policy evaluation logic.

`PRINCIPAL`, `PERMISSIONS_BOUNDARY`, and `SESSION` checks appear when they apply to the principal that made the request, even if none of their policies matched. A missing allow produces `IMPLICIT_DENY`, or `NO_IMPACT` when another path already allowed the request.

Returned when the caller is in the request principal's account or organization. The absence of `checks` does not mean no authorization checks applied.

Type: Array of Check objects

Required: No

context

The context keys and values specific to this evaluation. These are applied on top of the request context.

Type: String to JSON value map

Required: No

evaluatedEffect

The result of the evaluation. Valid values:

- `ALLOW` - The action was allowed.
- `EXPLICIT_DENY` - The action was explicitly denied by a policy.
- `IMPLICIT_DENY` - The action was denied because at least one required authorization check had no matching allow statement.

Type: String

Valid Values: `ALLOW | EXPLICIT_DENY | IMPLICIT_DENY`

Required: No

matchedPolicies

`matchedPolicies` is deprecated. Use `checks` instead. This value contains the policies that matched during evaluation of this action and resource.

Type: Array of MatchedPolicy objects

Required: No

See Also

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

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

MatchedPolicy

A policy that matched during evaluation, referenced by URI. The URI corresponds to a policy in the top-level policies list.

Contents

uri

The URI of the policy. This cross-references an entry in the top-level policies list. The value depends on the policy type:

- For managed policies, this is the policy ARN.
- For inline policies, this is an opaque identifier.

Type: String

Required: Yes

matchedStatements

The statements within the policy that matched during the evaluation.

Type: Array of MatchedStatement objects

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

MatchedStatement

A statement that matched during evaluation.

Contents

evaluatedEffect

The evaluated effect of this statement. Valid values:

- `ALLOW` - The statement allows the action.
- `DENY` - The statement denies the action.

Type: String

Valid Values: `ALLOW | DENY`

Required: No

sid

The statement ID (Sid). If the statement has no Sid, one is generated for reference.

Type: String

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PolicyInfo

Contains details about a policy evaluated during authorization. Details include the policy type, whether it is inline or managed, a URI that identifies it, the entities it is attached to, and its source, if present.

Contents

attachedTo

The entities that the policy is attached to. For identity, session, and resource-based policies, this is typically a single entity. For organization control policies (SCPs and RCPs), it can be multiple entities at different levels of the organization hierarchy.

Type: Array of AttachedTo objects

Required: No

inline

Specifies whether this is an inline policy (`true`) or a managed policy (`false`).

Type: Boolean

Required: No

policySource

What the policy was built from, such as a KMS key policy or grant. Absent for other policies.

The `type` and `typeName` keys are always present. `type` identifies the policy-source kind. `typeName` is its readable name. Compare `type`, not `typeName`.

A policy source can include additional keys that depend on its type. For example, a KMS grant includes a `grantId` key that identifies the grant. A grant has no ARN. Use the grant ID with the KMS key ARN in `attachedTo` to find the grant with the AWS KMS `ListGrants` operation.

New types and keys can be added, so clients should ignore types and keys they don't recognize.

Type: String to string map

Required: No

type

The type of policy. Valid values:

- `IDENTITY_BASED_POLICY` - An identity-based policy attached to an IAM user, group, or role.
- `PERMISSIONS_BOUNDARY` - A permissions boundary for an IAM entity.
- `RESOURCE_BASED_POLICY` - A resource-based policy attached to a resource. An AWS service can evaluate and report a policy kind it defines, such as a KMS grant, as `RESOURCE_BASED_POLICY`. `policySource` identifies the kind.
- `RESOURCE_CONTROL_POLICY` - A resource control policy (RCP) in AWS Organizations.
- `SERVICE_CONTROL_POLICY` - A service control policy (SCP) in AWS Organizations.
- `SESSION_POLICY` - A session policy passed during role assumption or federation.
- `VPC_ENDPOINT_POLICY` - A VPC endpoint policy.

Type: String

Valid Values: `IDENTITY_BASED_POLICY | RESOURCE_BASED_POLICY | PERMISSIONS_BOUNDARY | SESSION_POLICY | SERVICE_CONTROL_POLICY | RESOURCE_CONTROL_POLICY | VPC_ENDPOINT_POLICY`

Required: No

uri

A URI that identifies the policy. Use this URI to cross-reference the policy with the matching policies in each evaluation. To retrieve the policy document, pass this URI as the `policyUri` parameter of `GetRequestAuthorizationPolicy`, together with the same authorization ID. The value depends on the policy type:

- For managed policies, this is the policy ARN.
- For inline policies, which have no ARN, this is an opaque identifier.

Type: String

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Common Parameters

The following list contains the parameters that all actions use for signing Signature Version 4 requests with a query string. Any action-specific parameters are listed in the topic for that action. For more information about Signature Version 4, see Signing AWS API requests in the *IAM User Guide*.

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 Create a signed AWS API request in the *IAM User Guide*.

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 Elements of an AWS API request signature in the *IAM User Guide*.

Type: string

Required: Conditional

X-Amz-Security-Token

The temporary security token that was obtained through a call to AWS Security Token Service (AWS STS). For a list of services that support temporary security credentials from AWS STS, see AWS services that work with IAM in the *IAM User Guide*.

Condition: If you're using temporary security credentials from AWS STS, 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 Create a signed AWS API request in the *IAM User Guide*.

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 Error Types

This section lists common error types that this AWS service may return. Not all services return all error types listed here. For errors specific to an API action for this service, see the topic for that API action.

AccessDeniedException

You don't have permission to perform this action. Verify that your IAM policy includes the required permissions.

HTTP Status Code: 403

ExpiredTokenException

The security token included in the request has expired. Request a new security token and try again.

HTTP Status Code: 403

IncompleteSignature

The request signature doesn't conform to AWS standards. Verify that you're using valid AWS credentials and that your request is properly formatted. If you're using an SDK, ensure it's up to date.

HTTP Status Code: 403

InternalFailure

The request can't be processed right now because of an internal server issue. Try again later. If the problem persists, contact AWS Support.

HTTP Status Code: 500

MalformedHttpRequestException

The request body can't be processed. This typically happens when the request body can't be decompressed using the specified content encoding algorithm. Verify that the content encoding header matches the compression format used.

HTTP Status Code: 400

NotAuthorized

You don't have permissions to perform this action. Verify that your IAM policy includes the required permissions.

HTTP Status Code: 401

OptInRequired

Your AWS account needs a subscription for this service. Verify that you've enabled the service in your account.

HTTP Status Code: 403

RequestAbortedException

The request was aborted before a response could be returned. This typically happens when the client closes the connection.

HTTP Status Code: 400

RequestEntityTooLargeException

The request entity is too large. Reduce the size of the request body and try again.

HTTP Status Code: 413

RequestTimeoutException

The request timed out. The server didn't receive the complete request within the expected time frame. Try again.

HTTP Status Code: 408

ServiceUnavailable

The service is temporarily unavailable. Try again later.

HTTP Status Code: 503

ThrottlingException

Your request rate is too high. The AWS SDKs automatically retry requests that receive this exception. Reduce the frequency of requests.

HTTP Status Code: 400

UnknownOperationException

The action or operation isn't recognized. Verify that the action name is spelled correctly and that it's supported by the API version you're using.

HTTP Status Code: 404

UnrecognizedClientException

The X.509 certificate or AWS access key ID you provided doesn't exist in our records. Verify that you're using valid credentials and that they haven't expired.

HTTP Status Code: 403

ValidationError

The input doesn't meet the required format or constraints. Check that all required parameters are included and that values are valid.

HTTP Status Code: 400