API Reference

AWS Security Incident Response

API Version 2018-05-10

AWS Security Incident Response: API Reference

Table of Contents

Welcome **1**
Actions **2**
BatchGetMemberAccountDetails 3
Request Syntax 3
URI Request Parameters 3
Request Body 3
Response Syntax 4
Response Elements 5
Errors 5
See Also 6
CancelMembership 7
Request Syntax 7
URI Request Parameters 7
Request Body 7
Response Syntax 7
Response Elements 7
Errors 8
See Also 9
CloseCase 10
Request Syntax 10
URI Request Parameters 10
Request Body 10
Response Syntax 10
Response Elements 10
Errors 11
See Also 12
CreateCase 13
Request Syntax 13
URI Request Parameters 14
Request Body 14
Response Syntax 17
Response Elements 17
Errors 18
See Also 19

CreateCaseComment ... 20
Request Syntax ... 20
URI Request Parameters ... 20
Request Body ... 20
Response Syntax ... 21
Response Elements ... 21
Errors ... 22
See Also ... 23
CreateMembership ... 24
Request Syntax ... 24
URI Request Parameters ... 24
Request Body ... 24
Response Syntax ... 26
Response Elements ... 26
Errors ... 27
See Also ... 28
GetCase ... 29
Request Syntax ... 29
URI Request Parameters ... 29
Request Body ... 29
Response Syntax ... 29
Response Elements ... 30
Errors ... 34
See Also ... 35
GetCaseAttachmentDownloadUrl ... 36
Request Syntax ... 36
URI Request Parameters ... 36
Request Body ... 36
Response Syntax ... 36
Response Elements ... 37
Errors ... 37
See Also ... 38
GetCaseAttachmentUploadUrl ... 39
Request Syntax ... 39
URI Request Parameters ... 39
Request Body ... 39

Response Syntax ... 40
Response Elements ... 41
Errors ... 41
See Also ... 42
GetMembership ... 43
Request Syntax ... 43
URI Request Parameters ... 43
Request Body ... 43
Response Syntax ... 43
Response Elements ... 44
Errors ... 46
See Also ... 47
ListCaseEdits ... 49
Request Syntax ... 49
URI Request Parameters ... 49
Request Body ... 49
Response Syntax ... 50
Response Elements ... 50
Errors ... 51
See Also ... 52
ListCases ... 53
Request Syntax ... 53
URI Request Parameters ... 53
Request Body ... 53
Response Syntax ... 54
Response Elements ... 54
Errors ... 55
See Also ... 56
ListComments ... 57
Request Syntax ... 57
URI Request Parameters ... 57
Request Body ... 57
Response Syntax ... 58
Response Elements ... 58
Errors ... 59
See Also ... 60

ListMemberships 61
Request Syntax 61
URI Request Parameters 61
Request Body 61
Response Syntax 62
Response Elements 62
Errors 62
See Also 63
ListTagsForResource 65
Request Syntax 65
URI Request Parameters 65
Request Body 65
Response Syntax 65
Response Elements 65
Errors 66
See Also 67
TagResource 68
Request Syntax 68
URI Request Parameters 68
Request Body 68
Response Syntax 69
Response Elements 69
Errors 69
See Also 70
UntagResource 71
Request Syntax 71
URI Request Parameters 71
Request Body 71
Response Syntax 71
Response Elements 72
Errors 72
See Also 73
UpdateCase 74
Request Syntax 74
URI Request Parameters 75
Request Body 75

Response Syntax ... 79
Response Elements ... 79
Errors ... 80
See Also ... 81
UpdateCaseComment ... 82
Request Syntax ... 82
URI Request Parameters ... 82
Request Body ... 82
Response Syntax ... 83
Response Elements ... 83
Errors ... 84
See Also ... 85
UpdateCaseStatus ... 86
Request Syntax ... 86
URI Request Parameters ... 86
Request Body ... 87
Response Syntax ... 87
Response Elements ... 87
Errors ... 88
See Also ... 89
UpdateMembership ... 90
Request Syntax ... 90
URI Request Parameters ... 90
Request Body ... 91
Response Syntax ... 91
Response Elements ... 91
Errors ... 92
See Also ... 93
UpdateResolverType ... 94
Request Syntax ... 94
URI Request Parameters ... 94
Request Body ... 94
Response Syntax ... 95
Response Elements ... 95
Errors ... 96
See Also ... 97

Data Types 98
CaseAttachmentAttributes 99
Contents 99
See Also 100
CaseEditItem 101
Contents 101
See Also 101
GetMembershipAccountDetailError 103
Contents 103
See Also 103
GetMembershipAccountDetailItem 104
Contents 104
See Also 104
ImpactedAwsRegion 106
Contents 106
See Also 106
IncidentResponder 107
Contents 107
See Also 107
ListCasesItem 109
Contents 109
See Also 111
ListCommentsItem 112
Contents 112
See Also 113
ListMembershipItem 114
Contents 114
See Also 115
OptInFeature 116
Contents 116
See Also 116
ThreatActorIp 117
Contents 117
See Also 117
ValidationExceptionField 118
Contents 118

See Also 118
Watcher 119
Contents 119
See Also 119
Common Parameters 120
Common Errors 123

Welcome

This guide documents the action and response elements for use of the service.

This document was last published on December 1, 2024.

Actions

The following actions are supported:

- BatchGetMemberAccountDetails
- CancelMembership
- CloseCase
- CreateCase
- CreateCaseComment
- CreateMembership
- GetCase
- GetCaseAttachmentDownloadUrl
- GetCaseAttachmentUploadUrl
- GetMembership
- ListCaseEdits
- ListCases
- ListComments
- ListMemberships
- ListTagsForResource
- TagResource
- UntagResource
- UpdateCase
- UpdateCaseComment
- UpdateCaseStatus
- UpdateMembership
- UpdateResolverType

BatchGetMemberAccountDetails

Provides information on whether the supplied account IDs are associated with a membership.

> **Note**
>
> AWS account ID's may appear less than 12 characters and need to be zero-prepended. An example would be `123123123` which is nine digits, and with zero-prepend would be `000123123123`. Not zero-prepending to 12 digits could result in errors.

Request Syntax

```
POST /v1/membership/membershipId/batch-member-details HTTP/1.1
Content-type: application/json

{
   "accountIds": [ "string" ]
}
```

URI Request Parameters

The request uses the following URI parameters.

membershipId

Required element used in combination with BatchGetMemberAccountDetails to identify the membership ID to query.

Length Constraints: Minimum length of 12. Maximum length of 34.

Pattern: `m-[a-z0-9]{10,32}`

Required: Yes

Request Body

The request accepts the following data in JSON format.

accountIds

Optional element to query the membership relationship status to a provided list of account IDs.

> **Note**
>
> AWS account ID's may appear less than 12 characters and need to be zero-prepended. An example would be `123123123` which is nine digits, and with zero-prepend would be `000123123123`. Not zero-prepending to 12 digits could result in errors.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 100 items.

Length Constraints: Fixed length of 12.

Pattern: `[0-9]{12}`

Required: Yes

Response Syntax

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

{
   "errors": [
      {
         "accountId": "string",
         "error": "string",
         "message": "string"
      }
   ],
   "items": [
      {
         "accountId": "string",
         "relationshipStatus": "string",
         "relationshipType": "string"
      }
   ]
```

```
}
```

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.

errors

The response element providing error messages for requests to GetMembershipAccountDetails.

Type: Array of GetMembershipAccountDetailError objects

Array Members: Minimum number of 0 items. Maximum number of 100 items.

items

The response element providing responses for requests to GetMembershipAccountDetails.

Type: Array of GetMembershipAccountDetailItem objects

Array Members: Minimum number of 0 items. Maximum number of 100 items.

Errors

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

AccessDeniedException

HTTP Status Code: 403

ConflictException

HTTP Status Code: 409

InternalServerException

HTTP Status Code: 500

InvalidTokenException

HTTP Status Code: 423

ResourceNotFoundException

HTTP Status Code: 404

SecurityIncidentResponseNotActiveException

HTTP Status Code: 400

ServiceQuotaExceededException

HTTP Status Code: 402

ThrottlingException

HTTP Status Code: 429

ValidationException

HTTP Status Code: 400

See Also

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

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

CancelMembership

Cancels an existing membership.

Request Syntax

```
PUT /v1/membership/membershipId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

membershipId

Required element used in combination with CancelMembershipRequest to identify the membership ID to cancel.

Length Constraints: Minimum length of 12. Maximum length of 34.

Pattern: `m-[a-z0-9]{10,32}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

{
   "membershipId": "string"
}
```

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.

membershipId

The response element providing responses for requests to CancelMembershipRequest.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 34.

Pattern: `m-[a-z0-9]{10,32}`

Errors

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

AccessDeniedException

HTTP Status Code: 403

ConflictException

HTTP Status Code: 409

InternalServerException

HTTP Status Code: 500

InvalidTokenException

HTTP Status Code: 423

ResourceNotFoundException

HTTP Status Code: 404

SecurityIncidentResponseNotActiveException

HTTP Status Code: 400

ServiceQuotaExceededException

HTTP Status Code: 402

ThrottlingException

HTTP Status Code: 429

ValidationException

HTTP Status Code: 400

See Also

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

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

CloseCase

Closes an existing case.

Request Syntax

```
POST /v1/cases/caseId/close-case HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

caseId

Required element used in combination with CloseCase to identify the case ID to close.

Length Constraints: Minimum length of 10. Maximum length of 32.

Pattern: `\d{10,32}.*`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

{
   "caseStatus": "string",
   "closedDate": number
}
```

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.

caseStatus

A response element providing responses for requests to CloseCase. This element responds `Closed` if successful.

Type: String

Valid Values: `Submitted | Acknowledged | Detection and Analysis | Containment, Eradication and Recovery | Post-incident Activities | Ready to Close | Closed`

closedDate

A response element providing responses for requests to CloseCase. This element responds with the ISO-8601 formatted timestamp of the moment when the case was closed.

Type: Timestamp

Errors

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

AccessDeniedException

HTTP Status Code: 403

ConflictException

HTTP Status Code: 409

InternalServerException

HTTP Status Code: 500

InvalidTokenException

HTTP Status Code: 423

ResourceNotFoundException

HTTP Status Code: 404

SecurityIncidentResponseNotActiveException

HTTP Status Code: 400

ServiceQuotaExceededException

HTTP Status Code: 402

ThrottlingException

HTTP Status Code: 429

ValidationException

HTTP Status Code: 400

See Also

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

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

CreateCase

Creates a new case.

Request Syntax

```
POST /v1/create-case HTTP/1.1
Content-type: application/json

{
   "clientToken": "string",
   "description": "string",
   "engagementType": "string",
   "impactedAccounts": [ "string" ],
   "impactedAwsRegions": [
      {
         "region": "string"
      }
   ],
   "impactedServices": [ "string" ],
   "reportedIncidentStartDate": number,
   "resolverType": "string",
   "tags": {
      "string" : "string"
   },
   "threatActorIpAddresses": [
      {
         "ipAddress": "string",
         "userAgent": "string"
      }
   ],
   "title": "string",
   "watchers": [
      {
         "email": "string",
         "jobTitle": "string",
         "name": "string"
      }
   ]
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

clientToken

> **Note**
>
> The `clientToken` field is an idempotency key used to ensure that repeated attempts for a single action will be ignored by the server during retries. A caller supplied unique ID (typically a UUID) should be provided.

Type: String

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

Required: No

description

Required element used in combination with CreateCase

to provide a description for the new case.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 8000.

Required: Yes

engagementType

Required element used in combination with CreateCase to provide an engagement type for the new cases. Available engagement types include Security Incident | Investigation

Type: String

Valid Values: `Security Incident | Investigation`

Required: Yes

impactedAccounts

Required element used in combination with CreateCase to provide a list of impacted accounts.

> **Note**
>
> AWS account ID's may appear less than 12 characters and need to be zero-prepended. An example would be `123123123` which is nine digits, and with zero-prepend would be `000123123123`. Not zero-prepending to 12 digits could result in errors.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Length Constraints: Fixed length of 12.

Pattern: `[0-9]{12}`

Required: Yes

impactedAwsRegions

An optional element used in combination with CreateCase to provide a list of impacted regions.

Type: Array of ImpactedAwsRegion objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Required: No

impactedServices

An optional element used in combination with CreateCase to provide a list of services impacted.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 600 items.

Length Constraints: Minimum length of 3. Maximum length of 50.

Pattern: `[a-zA-Z0-9 -.():]+`

Required: No

reportedIncidentStartDate

Required element used in combination with CreateCase to provide an initial start date for the unauthorized activity.

Type: Timestamp

Required: Yes

resolverType

Required element used in combination with CreateCase to identify the resolver type.

Type: String

Valid Values: `AWS | Self`

Required: Yes

tags

An optional element used in combination with CreateCase to add customer specified tags to a case.

Type: String to string map

Map Entries: Minimum number of 0 items. Maximum number of 200 items.

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

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

Required: No

threatActorIpAddresses

An optional element used in combination with CreateCase to provide a list of suspicious internet protocol addresses associated with unauthorized activity.

Type: Array of ThreatActorIp objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

title

Required element used in combination with CreateCase to provide a title for the new case.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

watchers

Required element used in combination with CreateCase to provide a list of entities to receive notifications for case updates.

Type: Array of Watcher objects

Array Members: Minimum number of 0 items. Maximum number of 30 items.

Required: Yes

Response Syntax

```
HTTP/1.1 201
Content-type: application/json

{
   "caseId": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 201 response.

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

caseId

A response element providing responses for requests to CreateCase. This element responds with the case ID.

Type: String

Length Constraints: Minimum length of 10. Maximum length of 32.

Pattern: `\d{10,32}.*`

Errors

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

AccessDeniedException

HTTP Status Code: 403

ConflictException

HTTP Status Code: 409

InternalServerException

HTTP Status Code: 500

InvalidTokenException

HTTP Status Code: 423

ResourceNotFoundException

HTTP Status Code: 404

SecurityIncidentResponseNotActiveException

HTTP Status Code: 400

ServiceQuotaExceededException

HTTP Status Code: 402

ThrottlingException

HTTP Status Code: 429

ValidationException

HTTP Status Code: 400

See Also

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

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

CreateCaseComment

Adds a comment to an existing case.

Request Syntax

```
POST /v1/cases/caseId/create-comment HTTP/1.1
Content-type: application/json

{
   "body": "string",
   "clientToken": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

caseId

Required element used in combination with CreateCaseComment to specify a case ID.

Length Constraints: Minimum length of 10. Maximum length of 32.

Pattern: `\d{10,32}.*`

Required: Yes

Request Body

The request accepts the following data in JSON format.

body

Required element used in combination with CreateCaseComment to add content for the new comment.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 12000.

Required: Yes

clientToken

> **Note**
>
> The `clientToken` field is an idempotency key used to ensure that repeated attempts for a single action will be ignored by the server during retries. A caller supplied unique ID (typically a UUID) should be provided.

Type: String

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

Required: No

Response Syntax

```
HTTP/1.1 201
Content-type: application/json

{
   "commentId": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 201 response.

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

commentId

Response element indicating the new comment ID.

Type: String

Length Constraints: Fixed length of 6.

Pattern: `\d{6}`

Errors

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

AccessDeniedException

HTTP Status Code: 403

ConflictException

HTTP Status Code: 409

InternalServerException

HTTP Status Code: 500

InvalidTokenException

HTTP Status Code: 423

ResourceNotFoundException

HTTP Status Code: 404

SecurityIncidentResponseNotActiveException

HTTP Status Code: 400

ServiceQuotaExceededException

HTTP Status Code: 402

ThrottlingException

HTTP Status Code: 429

ValidationException

HTTP Status Code: 400

See Also

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

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

CreateMembership

Creates a new membership.

Request Syntax

```
POST /v1/membership HTTP/1.1
Content-type: application/json

{
   "clientToken": "string",
   "incidentResponseTeam": [
      {
         "email": "string",
         "jobTitle": "string",
         "name": "string"
      }
   ],
   "membershipName": "string",
   "optInFeatures": [
      {
         "featureName": "string",
         "isEnabled": boolean
      }
   ],
   "tags": {
      "string" : "string"
   }
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

clientToken

> **Note**
>
> The `clientToken` field is an idempotency key used to ensure that repeated attempts for a single action will be ignored by the server during retries. A caller supplied unique ID (typically a UUID) should be provided.

Type: String

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

Required: No

incidentResponseTeam

Required element used in combination with CreateMembership to add customer incident response team members and trusted partners to the membership.

Type: Array of IncidentResponder objects

Array Members: Minimum number of 2 items. Maximum number of 10 items.

Required: Yes

membershipName

Required element used in combination with CreateMembership to create a name for the membership.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 50.

Required: Yes

optInFeatures

Optional element to enable the monitoring and investigation opt-in features for the service.

Type: Array of OptInFeature objects

Array Members: Minimum number of 1 item. Maximum number of 2 items.

Required: No

tags

Optional element for customer configured tags.

Type: String to string map

Map Entries: Minimum number of 0 items. Maximum number of 200 items.

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

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

Required: No

Response Syntax

```
HTTP/1.1 201
Content-type: application/json

{
   "membershipId": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 201 response.

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

membershipId

Response element for CreateMembership providing the newly created membership ID.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 34.

Pattern: `m-[a-z0-9]{10,32}`

Errors

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

AccessDeniedException

HTTP Status Code: 403

ConflictException

HTTP Status Code: 409

InternalServerException

HTTP Status Code: 500

InvalidTokenException

HTTP Status Code: 423

ResourceNotFoundException

HTTP Status Code: 404

SecurityIncidentResponseNotActiveException

HTTP Status Code: 400

ServiceQuotaExceededException

HTTP Status Code: 402

ThrottlingException

HTTP Status Code: 429

ValidationException

HTTP Status Code: 400

See Also

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

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

GetCase

Returns the attributes of a case.

Request Syntax

```
GET /v1/cases/caseId/get-case HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

caseId

Required element for GetCase to identify the requested case ID.

Length Constraints: Minimum length of 10. Maximum length of 32.

Pattern: `\d{10,32}.*`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

{
   "actualIncidentStartDate": number,
   "caseArn": "string",
   "caseAttachments": [
      {
         "attachmentId": "string",
         "attachmentStatus": "string",
         "createdDate": number,
```

```
            "creator": "string",
            "fileName": "string"
         }
      ],
      "caseStatus": "string",
      "closedDate": number,
      "closureCode": "string",
      "createdDate": number,
      "description": "string",
      "engagementType": "string",
      "impactedAccounts": [ "string" ],
      "impactedAwsRegions": [
         {
            "region": "string"
         }
      ],
      "impactedServices": [ "string" ],
      "lastUpdatedDate": number,
      "pendingAction": "string",
      "reportedIncidentStartDate": number,
      "resolverType": "string",
      "threatActorIpAddresses": [
         {
            "ipAddress": "string",
            "userAgent": "string"
         }
      ],
      "title": "string",
      "watchers": [
         {
            "email": "string",
            "jobTitle": "string",
            "name": "string"
         }
      ]
}
```


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.

actualIncidentStartDate

Response element for GetCase that provides the actual incident start date as identified by data analysis during the investigation.

Type: Timestamp

caseArn

Response element for GetCase that provides the case ARN

Type: String

Length Constraints: Minimum length of 12. Maximum length of 80.

Pattern: `arn:aws:security-ir:\w+?-\w+?-\d+:[0-9]{12}:case/[0-9]{10}`

caseAttachments

Response element for GetCase that provides a list of current case attachments.

Type: Array of CaseAttachmentAttributes objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

caseStatus

Response element for GetCase that provides the case status. Options for statuses include `Submitted | Detection and Analysis | Eradication, Containment and Recovery | Post-Incident Activities | Closed`

Type: String

Valid Values: `Submitted | Acknowledged | Detection and Analysis | Containment, Eradication and Recovery | Post-incident Activities | Ready to Close | Closed`

closedDate

Response element for GetCase that provides the date a specified case was closed.

Type: Timestamp

closureCode

Response element for GetCase that provides the summary code for why a case was closed.

Type: String

Valid Values: `Investigation Completed | Not Resolved | False Positive | Duplicate`

createdDate

Response element for GetCase that provides the date the case was created.

Type: Timestamp

description

Response element for GetCase that provides contents of the case description.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 8000.

engagementType

Response element for GetCase that provides the engagement type. Options for engagement type include `Active Security Event | Investigations`

Type: String

Valid Values: `Security Incident | Investigation`

impactedAccounts

Response element for GetCase that provides a list of impacted accounts.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Length Constraints: Fixed length of 12.

Pattern: `[0-9]{12}`

impactedAwsRegions

Response element for GetCase that provides the impacted regions.

Type: Array of ImpactedAwsRegion objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

impactedServices

Response element for GetCase that provides a list of impacted services.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 600 items.

Length Constraints: Minimum length of 3. Maximum length of 50.

Pattern: `[a-zA-Z0-9 -.():]+`

lastUpdatedDate

Response element for GetCase that provides the date a case was last modified.

Type: Timestamp

pendingAction

Response element for GetCase that identifies the case is waiting on customer input.

Type: String

Valid Values: `Customer | None`

reportedIncidentStartDate

Response element for GetCase that provides the customer provided incident start date.

Type: Timestamp

resolverType

Response element for GetCase that provides the current resolver types.

Type: String

Valid Values: `AWS | Self`

threatActorIpAddresses

Response element for GetCase that provides a list of suspicious IP addresses associated with unauthorized activity.

Type: Array of ThreatActorIp objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

title

Response element for GetCase that provides the case title.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

watchers

Response element for GetCase that provides a list of Watchers added to the case.

Type: Array of Watcher objects

Array Members: Minimum number of 0 items. Maximum number of 30 items.

Errors

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

AccessDeniedException

HTTP Status Code: 403

ConflictException

HTTP Status Code: 409

InternalServerException

HTTP Status Code: 500

InvalidTokenException

HTTP Status Code: 423

ResourceNotFoundException

HTTP Status Code: 404

SecurityIncidentResponseNotActiveException

HTTP Status Code: 400

ServiceQuotaExceededException

HTTP Status Code: 402

ThrottlingException

HTTP Status Code: 429

ValidationException

HTTP Status Code: 400

See Also

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

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

GetCaseAttachmentDownloadUrl

Returns a Pre-Signed URL for uploading attachments into a case.

Request Syntax

```
GET /v1/cases/caseId/get-presigned-url/attachmentId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

attachmentId

Required element for GetCaseAttachmentDownloadUrl to identify the attachment ID for downloading an attachment.

Pattern: `[0-9a-fA-F]{8}\b-[0-9a-fA-F]{4}\b-[0-9a-fA-F]{4}\b-[0-9a-fA-F]{4}\b-[0-9a-fA-F]{12}`

Required: Yes

caseId

Required element for GetCaseAttachmentDownloadUrl to identify the case ID for downloading an attachment from.

Length Constraints: Minimum length of 10. Maximum length of 32.

Pattern: `\d{10,32}.*`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 201
```

```
Content-type: application/json

{
   "attachmentPresignedUrl": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 201 response.

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

attachmentPresignedUrl

Response element providing the Amazon S3 presigned URL to download an attachment.

Type: String

Pattern: `https?://(?:www.)?[a-zA-Z0-9@:._+~#=-]{2,256}\.[a-z]{2,6}\b(?:[-a-zA-Z0-9@:%_+.~#?&/=]{0,2048})`

Errors

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

AccessDeniedException

HTTP Status Code: 403

ConflictException

HTTP Status Code: 409

InternalServerException

HTTP Status Code: 500

InvalidTokenException

HTTP Status Code: 423

ResourceNotFoundException

HTTP Status Code: 404

SecurityIncidentResponseNotActiveException

HTTP Status Code: 400

ServiceQuotaExceededException

HTTP Status Code: 402

ThrottlingException

HTTP Status Code: 429

ValidationException

HTTP Status Code: 400

See Also

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

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

GetCaseAttachmentUploadUrl

Uploads an attachment to a case.

Request Syntax

```
POST /v1/cases/caseId/get-presigned-url HTTP/1.1
Content-type: application/json

{
   "clientToken": "string",
   "contentLength": number,
   "fileName": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

caseId

Required element for GetCaseAttachmentUploadUrl to identify the case ID for uploading an attachment.

Length Constraints: Minimum length of 10. Maximum length of 32.

Pattern: `\d{10,32}.*`

Required: Yes

Request Body

The request accepts the following data in JSON format.

clientToken

> **Note**
>
> The `clientToken` field is an idempotency key used to ensure that repeated attempts for a single action will be ignored by the server during retries. A caller supplied unique ID (typically a UUID) should be provided.

Type: String

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

Required: No

contentLength

Required element for GetCaseAttachmentUploadUrl to identify the size of the file attachment.

Type: Long

Valid Range: Minimum value of 1. Maximum value of 104857600.

Required: Yes

fileName

Required element for GetCaseAttachmentUploadUrl to identify the file name of the attachment to upload.

Type: String

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

Pattern: `[a-zA-Z0-9._-]+`

Required: Yes

Response Syntax

```
HTTP/1.1 201
Content-type: application/json
```

```
{
   "attachmentPresignedUrl": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 201 response.

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

attachmentPresignedUrl

Response element providing the Amazon S3 presigned URL to upload the attachment.

Type: String

Pattern: `https?://(?:www.)?[a-zA-Z0-9@:._+~#=-]{2,256}\.[a-z]{2,6}\b(?:[-a-zA-Z0-9@:%_+.~#?&/=]{0,2048})`

Errors

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

AccessDeniedException

HTTP Status Code: 403

ConflictException

HTTP Status Code: 409

InternalServerException

HTTP Status Code: 500

InvalidTokenException

HTTP Status Code: 423

ResourceNotFoundException

HTTP Status Code: 404

SecurityIncidentResponseNotActiveException

HTTP Status Code: 400

ServiceQuotaExceededException

HTTP Status Code: 402

ThrottlingException

HTTP Status Code: 429

ValidationException

HTTP Status Code: 400

See Also

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

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

GetMembership

Returns the attributes of a membership.

Request Syntax

```
GET /v1/membership/membershipId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

membershipId

Required element for GetMembership to identify the membership ID to query.

Length Constraints: Minimum length of 12. Maximum length of 34.

Pattern: `m-[a-z0-9]{10,32}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

{
   "accountId": "string",
   "customerType": "string",
   "incidentResponseTeam": [
      {
         "email": "string",
         "jobTitle": "string",
         "name": "string"
```

```
      }
   ],
   "membershipActivationTimestamp": number,
   "membershipArn": "string",
   "membershipDeactivationTimestamp": number,
   "membershipId": "string",
   "membershipName": "string",
   "membershipStatus": "string",
   "numberOfAccountsCovered": number,
   "optInFeatures": [
      {
         "featureName": "string",
         "isEnabled": boolean
      }
   ],
   "region": "string"
}
```

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.

accountId

Response element for GetMembership that provides the account configured to manage the membership.

Type: String

Length Constraints: Fixed length of 12.

Pattern: `[0-9]{12}`

customerType

Response element for GetMembership that provides the configured membership type. Options include `Standalone | Organizations`.

Type: String

Valid Values: `Standalone | Organization`

incidentResponseTeam

Response element for GetMembership that provides the configured membership incident response team members.

Type: Array of IncidentResponder objects

Array Members: Minimum number of 2 items. Maximum number of 10 items.

membershipActivationTimestamp

Response element for GetMembership that provides the configured membership activation timestamp.

Type: Timestamp

membershipArn

Response element for GetMembership that provides the membership ARN.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 80.

Pattern: `arn:aws:security-ir:\w+?-\w+?-\d+:[0-9]{12}:membership/m-[a-z0-9]{10,32}`

membershipDeactivationTimestamp

Response element for GetMembership that provides the configured membership name deactivation timestamp.

Type: Timestamp

membershipId

Response element for GetMembership that provides the queried membership ID.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 34.

Pattern: `m-[a-z0-9]{10,32}`

membershipName

Response element for GetMembership that provides the configured membership name.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 50.

membershipStatus

Response element for GetMembership that provides the current membership status.

Type: String

Valid Values: `Active | Cancelled | Terminated`

numberOfAccountsCovered

Response element for GetMembership that provides the number of accounts in the membership.

Type: Long

optInFeatures

Response element for GetMembership that provides the if opt-in features have been enabled.

Type: Array of OptInFeature objects

Array Members: Minimum number of 1 item. Maximum number of 2 items.

region

Response element for GetMembership that provides the region configured to manage the membership.

Type: String

Valid Values: `af-south-1 | ap-east-1 | ap-northeast-1 | ap-northeast-2 | ap-northeast-3 | ap-south-1 | ap-south-2 | ap-southeast-1 | ap-southeast-2 | ap-southeast-3 | ap-southeast-4 | ap-southeast-5 | ca-central-1 | ca-west-1 | cn-north-1 | cn-northwest-1 | eu-central-1 | eu-central-2 | eu-north-1 | eu-south-1 | eu-south-2 | eu-west-1 | eu-west-2 | eu-west-3 | il-central-1 | me-central-1 | me-south-1 | sa-east-1 | us-east-1 | us-east-2 | us-west-1 | us-west-2`

Errors

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

AccessDeniedException

HTTP Status Code: 403

ConflictException

HTTP Status Code: 409

InternalServerException

HTTP Status Code: 500

InvalidTokenException

HTTP Status Code: 423

ResourceNotFoundException

HTTP Status Code: 404

SecurityIncidentResponseNotActiveException

HTTP Status Code: 400

ServiceQuotaExceededException

HTTP Status Code: 402

ThrottlingException

HTTP Status Code: 429

ValidationException

HTTP Status Code: 400

See Also

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

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

ListCaseEdits

Views the case history for edits made to a designated case.

Request Syntax

```
POST /v1/cases/caseId/list-case-edits HTTP/1.1
Content-type: application/json

{
   "maxResults": number,
   "nextToken": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

caseId

Required element used with ListCaseEdits to identify the case to query.

Length Constraints: Minimum length of 10. Maximum length of 32.

Pattern: `\d{10,32}.*`

Required: Yes

Request Body

The request accepts the following data in JSON format.

maxResults

Optional element to identify how many results to obtain. There is a maximum value of 25.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 25.

Required: No

nextToken

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2000.

Required: No

Response Syntax

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

{
   "items": [
      {
         "action": "string",
         "eventTimestamp": number,
         "message": "string",
         "principal": "string"
      }
   ],
   "nextToken": "string",
   "total": number
}
```

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.

items

Response element for ListCaseEdits that includes the action, event timestamp, message, and principal for the response.

Type: Array of CaseEditItem objects

nextToken

Type: String

total

Response element for ListCaseEdits that identifies the total number of edits.

Type: Integer

Errors

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

AccessDeniedException

HTTP Status Code: 403

ConflictException

HTTP Status Code: 409

InternalServerException

HTTP Status Code: 500

InvalidTokenException

HTTP Status Code: 423

ResourceNotFoundException

HTTP Status Code: 404

SecurityIncidentResponseNotActiveException

HTTP Status Code: 400

ServiceQuotaExceededException

HTTP Status Code: 402

ThrottlingException

HTTP Status Code: 429

ValidationException

HTTP Status Code: 400

See Also

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

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

ListCases

Lists all cases the requester has access to.

Request Syntax

```
POST /v1/list-cases HTTP/1.1
Content-type: application/json

{
   "maxResults": number,
   "nextToken": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

maxResults

Optional element for ListCases to limit the number of responses.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 25.

Required: No

nextToken

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2000.

Required: No

Response Syntax

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

{
   "items": [
      {
         "caseArn": "string",
         "caseId": "string",
         "caseStatus": "string",
         "closedDate": number,
         "createdDate": number,
         "engagementType": "string",
         "lastUpdatedDate": number,
         "pendingAction": "string",
         "resolverType": "string",
         "title": "string"
      }
   ],
   "nextToken": "string",
   "total": number
}
```

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.

items

Response element for ListCases that includes caseARN, caseID, caseStatus, closedDate, createdDate, engagementType, lastUpdatedDate, pendingAction, resolverType, and title for each response.

Type: Array of ListCasesItem objects

nextToken

Type: String

total

Response element for ListCases providing the total number of responses.

Type: Long

Errors

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

AccessDeniedException

HTTP Status Code: 403

ConflictException

HTTP Status Code: 409

InternalServerException

HTTP Status Code: 500

InvalidTokenException

HTTP Status Code: 423

ResourceNotFoundException

HTTP Status Code: 404

SecurityIncidentResponseNotActiveException

HTTP Status Code: 400

ServiceQuotaExceededException

HTTP Status Code: 402

ThrottlingException

HTTP Status Code: 429

ValidationException

HTTP Status Code: 400

See Also

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

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

ListComments

Returns comments for a designated case.

Request Syntax

```
POST /v1/cases/caseId/list-comments HTTP/1.1
Content-type: application/json

{
   "maxResults": number,
   "nextToken": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

caseId

Required element for ListComments to designate the case to query.

Length Constraints: Minimum length of 10. Maximum length of 32.

Pattern: `\d{10,32}.*`

Required: Yes

Request Body

The request accepts the following data in JSON format.

maxResults

Optional element for ListComments to limit the number of responses.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 25.

Required: No

nextToken

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2000.

Required: No

Response Syntax

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

{
   "items": [
      {
         "body": "string",
         "commentId": "string",
         "createdDate": number,
         "creator": "string",
         "lastUpdatedBy": "string",
         "lastUpdatedDate": number
      }
   ],
   "nextToken": "string",
   "total": number
}
```

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.

items

Response element for ListComments providing the body, commentID, createDate, creator, lastUpdatedBy and lastUpdatedDate for each response.

Type: Array of ListCommentsItem objects

nextToken

Type: String

total

Response element for ListComments identifying the number of responses.

Type: Integer

Errors

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

AccessDeniedException

HTTP Status Code: 403

ConflictException

HTTP Status Code: 409

InternalServerException

HTTP Status Code: 500

InvalidTokenException

HTTP Status Code: 423

ResourceNotFoundException

HTTP Status Code: 404

SecurityIncidentResponseNotActiveException

HTTP Status Code: 400

ServiceQuotaExceededException

HTTP Status Code: 402

ThrottlingException

HTTP Status Code: 429

ValidationException

HTTP Status Code: 400

See Also

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

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

ListMemberships

Returns the memberships that the calling principal can access.

Request Syntax

```
POST /v1/memberships HTTP/1.1
Content-type: application/json

{
   "maxResults": number,
   "nextToken": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

maxResults

Request element for ListMemberships to limit the number of responses.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 25.

Required: No

nextToken

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2000.

Required: No

Response Syntax

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

{
   "items": [
      {
         "accountId": "string",
         "membershipArn": "string",
         "membershipId": "string",
         "membershipStatus": "string",
         "region": "string"
      }
   ],
   "nextToken": "string"
}
```

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.

items

Request element for ListMemberships including the accountID, membershipARN, membershipID, membershipStatus, and region for each response.

Type: Array of ListMembershipItem objects

nextToken

Type: String

Errors

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

AccessDeniedException

HTTP Status Code: 403

ConflictException

HTTP Status Code: 409

InternalServerException

HTTP Status Code: 500

InvalidTokenException

HTTP Status Code: 423

ResourceNotFoundException

HTTP Status Code: 404

SecurityIncidentResponseNotActiveException

HTTP Status Code: 400

ServiceQuotaExceededException

HTTP Status Code: 402

ThrottlingException

HTTP Status Code: 429

ValidationException

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface

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

ListTagsForResource

Returns currently configured tags on a resource.

Request Syntax

```
GET /v1/tags/resourceArn HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

resourceArn

Required element for ListTagsForResource to provide the ARN to identify a specific resource.

Length Constraints: Minimum length of 12. Maximum length of 1010.

Pattern: `arn:aws:security-ir:\w+?-\w+?-\d+:[0-9]{12}:(membership/m-[a-z0-9]{10,32}|case/[0-9]{10})`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

{
   "tags": {
      "string" : "string"
   }
}
```

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.

tags

Response element for ListTagsForResource providing content for each configured tag.

Type: String to string map

Map Entries: Minimum number of 0 items. Maximum number of 200 items.

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

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

Errors

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

AccessDeniedException

HTTP Status Code: 403

ConflictException

HTTP Status Code: 409

InternalServerException

HTTP Status Code: 500

InvalidTokenException

HTTP Status Code: 423

ResourceNotFoundException

HTTP Status Code: 404

SecurityIncidentResponseNotActiveException

HTTP Status Code: 400

ServiceQuotaExceededException

HTTP Status Code: 402

ThrottlingException

HTTP Status Code: 429

ValidationException

HTTP Status Code: 400

See Also

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

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

TagResource

Adds a tag(s) to a designated resource.

Request Syntax

```
POST /v1/tags/resourceArn HTTP/1.1
Content-type: application/json

{
   "tags": {
      "string" : "string"
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

resourceArn

Required element for TagResource to identify the ARN for the resource to add a tag to.

Length Constraints: Minimum length of 12. Maximum length of 1010.

Pattern: `arn:aws:security-ir:\w+?-\w+?-\d+:[0-9]{12}:(membership/m-[a-z0-9]{10,32}|case/[0-9]{10})`

Required: Yes

Request Body

The request accepts the following data in JSON format.

tags

Required element for ListTagsForResource to provide the content for a tag.

Type: String to string map

Map Entries: Minimum number of 0 items. Maximum number of 200 items.

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

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

Required: Yes

Response Syntax

```
HTTP/1.1 204
```

Response Elements

If the action is successful, the service sends back an HTTP 204 response with an empty HTTP body.

Errors

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

AccessDeniedException

HTTP Status Code: 403

ConflictException

HTTP Status Code: 409

InternalServerException

HTTP Status Code: 500

InvalidTokenException

HTTP Status Code: 423

ResourceNotFoundException

HTTP Status Code: 404

SecurityIncidentResponseNotActiveException

HTTP Status Code: 400

ServiceQuotaExceededException

HTTP Status Code: 402

ThrottlingException

HTTP Status Code: 429

ValidationException

HTTP Status Code: 400

See Also

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

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

UntagResource

Removes a tag(s) from a designate resource.

Request Syntax

```
DELETE /v1/tags/resourceArn?tagKeys=tagKeys HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

resourceArn

Required element for UnTagResource to identify the ARN for the resource to remove a tag from.

Length Constraints: Minimum length of 12. Maximum length of 1010.

Pattern: `arn:aws:security-ir:\w+?-\w+?-\d+:[0-9]{12}:(membership/m-[a-z0-9]{10,32}|case/[0-9]{10})`

Required: Yes

tagKeys

Required element for UnTagResource to identify tag to remove.

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

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

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

Errors

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

AccessDeniedException

HTTP Status Code: 403

ConflictException

HTTP Status Code: 409

InternalServerException

HTTP Status Code: 500

InvalidTokenException

HTTP Status Code: 423

ResourceNotFoundException

HTTP Status Code: 404

SecurityIncidentResponseNotActiveException

HTTP Status Code: 400

ServiceQuotaExceededException

HTTP Status Code: 402

ThrottlingException

HTTP Status Code: 429

ValidationException

HTTP Status Code: 400

See Also

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

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

UpdateCase

Updates an existing case.

Request Syntax

```
POST /v1/cases/caseId/update-case HTTP/1.1
Content-type: application/json

{
   "actualIncidentStartDate": number,
   "description": "string",
   "engagementType": "string",
   "impactedAccountsToAdd": [ "string" ],
   "impactedAccountsToDelete": [ "string" ],
   "impactedAwsRegionsToAdd": [
      {
         "region": "string"
      }
   ],
   "impactedAwsRegionsToDelete": [
      {
         "region": "string"
      }
   ],
   "impactedServicesToAdd": [ "string" ],
   "impactedServicesToDelete": [ "string" ],
   "reportedIncidentStartDate": number,
   "threatActorIpAddressesToAdd": [
      {
         "ipAddress": "string",
         "userAgent": "string"
      }
   ],
   "threatActorIpAddressesToDelete": [
      {
         "ipAddress": "string",
         "userAgent": "string"
      }
   ],
   "title": "string",
   "watchersToAdd": [
      {
```

```
            "email": "string",
            "jobTitle": "string",
            "name": "string"
         }
      ],
      "watchersToDelete": [
         {
            "email": "string",
            "jobTitle": "string",
            "name": "string"
         }
      ]
}
```

URI Request Parameters

The request uses the following URI parameters.

caseId

Required element for UpdateCase to identify the case ID for updates.

Length Constraints: Minimum length of 10. Maximum length of 32.

Pattern: `\d{10,32}.*`

Required: Yes

Request Body

The request accepts the following data in JSON format.

actualIncidentStartDate

Optional element for UpdateCase to provide content for the incident start date field.

Type: Timestamp

Required: No

description

Optional element for UpdateCase to provide content for the description field.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 8000.

Required: No

engagementType

Optional element for UpdateCase to provide content for the engagement type field. `Available engagement types include Security Incident | Investigation.`

Type: String

Valid Values: `Security Incident | Investigation`

Required: No

impactedAccountsToAdd

Optional element for UpdateCase to provide content to add accounts impacted.

> **Note**
>
> AWS account ID's may appear less than 12 characters and need to be zero-prepended. An example would be `123123123` which is nine digits, and with zero-prepend would be `000123123123`. Not zero-prepending to 12 digits could result in errors.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Length Constraints: Fixed length of 12.

Pattern: `[0-9]{12}`

Required: No

impactedAccountsToDelete

Optional element for UpdateCase to provide content to add accounts impacted.

> **Note**
>
> AWS account ID's may appear less than 12 characters and need to be zero-prepended. An example would be `123123123` which is nine digits, and with zero-prepend would be `000123123123`. Not zero-prepending to 12 digits could result in errors.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Length Constraints: Fixed length of 12.

Pattern: `[0-9]{12}`

Required: No

impactedAwsRegionsToAdd

Optional element for UpdateCase to provide content to add regions impacted.

Type: Array of ImpactedAwsRegion objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Required: No

impactedAwsRegionsToDelete

Optional element for UpdateCase to provide content to remove regions impacted.

Type: Array of ImpactedAwsRegion objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Required: No

impactedServicesToAdd

Optional element for UpdateCase to provide content to add services impacted.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 600 items.

Length Constraints: Minimum length of 3. Maximum length of 50.

Pattern: `[a-zA-Z0-9 -.():]+`

Required: No

impactedServicesToDelete

Optional element for UpdateCase to provide content to remove services impacted.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 600 items.

Length Constraints: Minimum length of 3. Maximum length of 50.

Pattern: `[a-zA-Z0-9 -.():]+`

Required: No

reportedIncidentStartDate

Optional element for UpdateCase to provide content for the customer reported incident start date field.

Type: Timestamp

Required: No

threatActorIpAddressesToAdd

Optional element for UpdateCase to provide content to add additional suspicious IP addresses related to a case.

Type: Array of ThreatActorIp objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

threatActorIpAddressesToDelete

Optional element for UpdateCase to provide content to remove suspicious IP addresses from a case.

Type: Array of ThreatActorIp objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

title

Optional element for UpdateCase to provide content for the title field.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: No

watchersToAdd

Optional element for UpdateCase to provide content to add additional watchers to a case.

Type: Array of Watcher objects

Array Members: Minimum number of 0 items. Maximum number of 30 items.

Required: No

watchersToDelete

Optional element for UpdateCase to provide content to remove existing watchers from a case.

Type: Array of Watcher objects

Array Members: Minimum number of 0 items. Maximum number of 30 items.

Required: No

Response Syntax

```
HTTP/1.1 200
```

Response Elements

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

Errors

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

AccessDeniedException

HTTP Status Code: 403

ConflictException

HTTP Status Code: 409

InternalServerException

HTTP Status Code: 500

InvalidTokenException

HTTP Status Code: 423

ResourceNotFoundException

HTTP Status Code: 404

SecurityIncidentResponseNotActiveException

HTTP Status Code: 400

ServiceQuotaExceededException

HTTP Status Code: 402

ThrottlingException

HTTP Status Code: 429

ValidationException

HTTP Status Code: 400

See Also

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

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

UpdateCaseComment

Updates an existing case comment.

Request Syntax

```
PUT /v1/cases/caseId/update-case-comment/commentId HTTP/1.1
Content-type: application/json

{
   "body": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

caseId

Required element for UpdateCaseComment to identify the case ID containing the comment to be updated.

Length Constraints: Minimum length of 10. Maximum length of 32.

Pattern: `\d{10,32}.*`

Required: Yes

commentId

Required element for UpdateCaseComment to identify the case ID to be updated.

Length Constraints: Fixed length of 6.

Pattern: `\d{6}`

Required: Yes

Request Body

The request accepts the following data in JSON format.

body

Required element for UpdateCaseComment to identify the content for the comment to be updated.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 12000.

Required: Yes

Response Syntax

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

{
   "body": "string",
   "commentId": "string"
}
```

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.

body

Response element for UpdateCaseComment providing the updated comment content.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 12000.

commentId

Response element for UpdateCaseComment providing the updated comment ID.

Type: String

Length Constraints: Fixed length of 6.

Pattern: \d{6}

Errors

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

AccessDeniedException

HTTP Status Code: 403

ConflictException

HTTP Status Code: 409

InternalServerException

HTTP Status Code: 500

InvalidTokenException

HTTP Status Code: 423

ResourceNotFoundException

HTTP Status Code: 404

SecurityIncidentResponseNotActiveException

HTTP Status Code: 400

ServiceQuotaExceededException

HTTP Status Code: 402

ThrottlingException

HTTP Status Code: 429

ValidationException

HTTP Status Code: 400

See Also

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

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

UpdateCaseStatus

Updates the state transitions for a designated cases.

Self-managed: the following states are available for self-managed cases.

- Submitted → Detection and Analysis
- Detection and Analysis → Containment, Eradication, and Recovery
- Detection and Analysis → Post-incident Activities
- Containment, Eradication, and Recovery → Detection and Analysis
- Containment, Eradication, and Recovery → Post-incident Activities
- Post-incident Activities → Containment, Eradication, and Recovery
- Post-incident Activities → Detection and Analysis
- Any → Closed

AWS supported: You must use the `CloseCase` API to close.

Request Syntax

```
POST /v1/cases/caseId/update-case-status HTTP/1.1
Content-type: application/json

{
   "caseStatus": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

caseId

Required element for UpdateCaseStatus to identify the case to update.

Length Constraints: Minimum length of 10. Maximum length of 32.

Pattern: `\d{10,32}.*`

Required: Yes

Request Body

The request accepts the following data in JSON format.

caseStatus

Required element for UpdateCaseStatus to identify the status for a case. Options include `Submitted | Detection and Analysis | Containment, Eradication and Recovery | Post-incident Activities`.

Type: String

Valid Values: `Submitted | Detection and Analysis | Containment, Eradication and Recovery | Post-incident Activities`

Required: Yes

Response Syntax

```
HTTP/1.1 201
Content-type: application/json

{
   "caseStatus": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 201 response.

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

caseStatus

Response element for UpdateCaseStatus showing the newly configured status.

Type: String

Valid Values: `Submitted | Detection and Analysis | Containment, Eradication and Recovery | Post-incident Activities`

Errors

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

AccessDeniedException

HTTP Status Code: 403

ConflictException

HTTP Status Code: 409

InternalServerException

HTTP Status Code: 500

InvalidTokenException

HTTP Status Code: 423

ResourceNotFoundException

HTTP Status Code: 404

SecurityIncidentResponseNotActiveException

HTTP Status Code: 400

ServiceQuotaExceededException

HTTP Status Code: 402

ThrottlingException

HTTP Status Code: 429

ValidationException

HTTP Status Code: 400

See Also

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

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

UpdateMembership

Updates membership configuration.

Request Syntax

```
PUT /v1/membership/membershipId/update-membership HTTP/1.1
Content-type: application/json

{
   "incidentResponseTeam": [
      {
         "email": "string",
         "jobTitle": "string",
         "name": "string"
      }
   ],
   "membershipName": "string",
   "optInFeatures": [
      {
         "featureName": "string",
         "isEnabled": boolean
      }
   ]
}
```

URI Request Parameters

The request uses the following URI parameters.

membershipId

Required element for UpdateMembership to identify the membership to update.

Length Constraints: Minimum length of 12. Maximum length of 34.

Pattern: `m-[a-z0-9]{10,32}`

Required: Yes

Request Body

The request accepts the following data in JSON format.

incidentResponseTeam

Optional element for UpdateMembership to update the membership name.

Type: Array of IncidentResponder objects

Array Members: Minimum number of 2 items. Maximum number of 10 items.

Required: No

membershipName

Optional element for UpdateMembership to update the membership name.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 50.

Required: No

optInFeatures

Optional element for UpdateMembership to enable or disable opt-in features for the service.

Type: Array of OptInFeature objects

Array Members: Minimum number of 1 item. Maximum number of 2 items.

Required: No

Response Syntax

```
HTTP/1.1 200
```

Response Elements

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

Errors

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

AccessDeniedException

HTTP Status Code: 403

ConflictException

HTTP Status Code: 409

InternalServerException

HTTP Status Code: 500

InvalidTokenException

HTTP Status Code: 423

ResourceNotFoundException

HTTP Status Code: 404

SecurityIncidentResponseNotActiveException

HTTP Status Code: 400

ServiceQuotaExceededException

HTTP Status Code: 402

ThrottlingException

HTTP Status Code: 429

ValidationException

HTTP Status Code: 400

See Also

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

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

UpdateResolverType

Updates the resolver type for a case.

> **Important**
>
> This is a one-way action and cannot be reversed.

Request Syntax

```
POST /v1/cases/caseId/update-resolver-type HTTP/1.1
Content-type: application/json

{
   "resolverType": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

caseId

Required element for UpdateResolverType to identify the case to update.

Length Constraints: Minimum length of 10. Maximum length of 32.

Pattern: `\d{10,32}.*`

Required: Yes

Request Body

The request accepts the following data in JSON format.

resolverType

Required element for UpdateResolverType to identify the new resolver.

Type: String

Valid Values: `AWS | Self`

Required: Yes

Response Syntax

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

{
   "caseId": "string",
   "caseStatus": "string",
   "resolverType": "string"
}
```

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.

caseId

Response element for UpdateResolver identifying the case ID being updated.

Type: String

Length Constraints: Minimum length of 10. Maximum length of 32.

Pattern: `\d{10,32}.*`

caseStatus

Response element for UpdateResolver identifying the current status of the case.

Type: String

Valid Values: `Submitted | Acknowledged | Detection and Analysis | Containment, Eradication and Recovery | Post-incident Activities | Ready to Close | Closed`

resolverType

Response element for UpdateResolver identifying the current resolver of the case.

Type: String

Valid Values: `AWS | Self`

Errors

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

AccessDeniedException

HTTP Status Code: 403

ConflictException

HTTP Status Code: 409

InternalServerException

HTTP Status Code: 500

InvalidTokenException

HTTP Status Code: 423

ResourceNotFoundException

HTTP Status Code: 404

SecurityIncidentResponseNotActiveException

HTTP Status Code: 400

ServiceQuotaExceededException

HTTP Status Code: 402

ThrottlingException

HTTP Status Code: 429

ValidationException

HTTP Status Code: 400

See Also

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

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

Data Types

The Security Incident Response 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:

- CaseAttachmentAttributes
- CaseEditItem
- GetMembershipAccountDetailError
- GetMembershipAccountDetailItem
- ImpactedAwsRegion
- IncidentResponder
- ListCasesItem
- ListCommentsItem
- ListMembershipItem
- OptInFeature
- ThreatActorIp
- ValidationExceptionField
- Watcher

CaseAttachmentAttributes

Contents

attachmentId

Type: String

Pattern: `[0-9a-fA-F]{8}\b-[0-9a-fA-F]{4}\b-[0-9a-fA-F]{4}\b-[0-9a-fA-F]{4}\b-[0-9a-fA-F]{12}`

Required: Yes

attachmentStatus

Type: String

Valid Values: `Verified | Failed | Pending`

Required: Yes

createdDate

Type: Timestamp

Required: Yes

creator

Type: String

Pattern: `.*(^internal:midway:([a-z]{3,8}|svc-mw-[0-9]{12}[a-zA-Z0-9-]{5,20})$)|(^external:aws:\d{12}$).*`

Required: Yes

fileName

Type: String

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

Pattern: `[a-zA-Z0-9._-]+`

Required: Yes

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

CaseEditItem

Contents

action

Type: String

Length Constraints: Minimum length of 1. Maximum length of 100.

Required: No

eventTimestamp

Type: Timestamp

Required: No

message

Type: String

Length Constraints: Minimum length of 10. Maximum length of 4096.

Required: No

principal

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

GetMembershipAccountDetailError

Contents

accountId

Type: String

Length Constraints: Fixed length of 12.

Pattern: `[0-9]{12}`

Required: Yes

error

Type: String

Required: Yes

message

Type: String

Required: Yes

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

GetMembershipAccountDetailItem

Contents

accountId

Type: String

Length Constraints: Fixed length of 12.

Pattern: `[0-9]{12}`

Required: No

relationshipStatus

Type: String

Valid Values: `Associated | Disassociated`

Required: No

relationshipType

Type: String

Valid Values: `Organization`

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

ImpactedAwsRegion

Contents

region

Type: String

Valid Values: `af-south-1 | ap-east-1 | ap-northeast-1 | ap-northeast-2 | ap-northeast-3 | ap-south-1 | ap-south-2 | ap-southeast-1 | ap-southeast-2 | ap-southeast-3 | ap-southeast-4 | ap-southeast-5 | ca-central-1 | ca-west-1 | cn-north-1 | cn-northwest-1 | eu-central-1 | eu-central-2 | eu-north-1 | eu-south-1 | eu-south-2 | eu-west-1 | eu-west-2 | eu-west-3 | il-central-1 | me-central-1 | me-south-1 | sa-east-1 | us-east-1 | us-east-2 | us-west-1 | us-west-2`

Required: Yes

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

IncidentResponder

Contents

email

Type: String

Length Constraints: Minimum length of 6. Maximum length of 254.

Pattern: `[a-zA-Z0-9.!#$%&'*+/=?^_`{|}~-]+@[a-zA-Z0-9-]+(?:\.[a-zA-Z0-9-]+)*`

Required: Yes

jobTitle

Type: String

Length Constraints: Minimum length of 1. Maximum length of 50.

Required: Yes

name

Type: String

Length Constraints: Minimum length of 3. Maximum length of 50.

Required: Yes

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

ListCasesItem

Contents

caseId

Type: String

Length Constraints: Minimum length of 10. Maximum length of 32.

Pattern: `\d{10,32}.*`

Required: Yes

caseArn

Type: String

Length Constraints: Minimum length of 12. Maximum length of 80.

Pattern: `arn:aws:security-ir:\w+?-\w+?-\d+:[0-9]{12}:case/[0-9]{10}`

Required: No

caseStatus

Type: String

Valid Values: `Submitted | Acknowledged | Detection and Analysis | Containment, Eradication and Recovery | Post-incident Activities | Ready to Close | Closed`

Required: No

closedDate

Type: Timestamp

Required: No

createdDate

Type: Timestamp

Required: No

engagementType

Type: String

Valid Values: `Security Incident | Investigation`

Required: No

lastUpdatedDate

Type: Timestamp

Required: No

pendingAction

Type: String

Valid Values: `Customer | None`

Required: No

resolverType

Type: String

Valid Values: `AWS | Self`

Required: No

title

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

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

ListCommentsItem

Contents

commentId

Type: String

Length Constraints: Fixed length of 6.

Pattern: `\d{6}`

Required: Yes

body

Type: String

Length Constraints: Minimum length of 1. Maximum length of 12000.

Required: No

createdDate

Type: Timestamp

Required: No

creator

Type: String

Pattern: `.*(^internal:midway:([a-z]{3,8}|svc-mw-[0-9]{12}[a-zA-Z0-9-]{5,20})$)|(^external:aws:\d{12}$).*`

Required: No

lastUpdatedBy

Type: String

Pattern: `.*(^internal:midway:([a-z]{3,8}|svc-mw-[0-9]{12}[a-zA-Z0-9-]{5,20})$)|(^external:aws:\d{12}$).*`

Required: No

lastUpdatedDate

Type: Timestamp

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

ListMembershipItem

Contents

membershipId

Type: String

Length Constraints: Minimum length of 12. Maximum length of 34.

Pattern: `m-[a-z0-9]{10,32}`

Required: Yes

accountId

Type: String

Length Constraints: Fixed length of 12.

Pattern: `[0-9]{12}`

Required: No

membershipArn

Type: String

Length Constraints: Minimum length of 12. Maximum length of 80.

Pattern: `arn:aws:security-ir:\w+?-\w+?-\d+:[0-9]{12}:membership/m-[a-z0-9]{10,32}`

Required: No

membershipStatus

Type: String

Valid Values: `Active | Cancelled | Terminated`

Required: No

region

Type: String

Valid Values: `af-south-1 | ap-east-1 | ap-northeast-1 | ap-northeast-2 | ap-northeast-3 | ap-south-1 | ap-south-2 | ap-southeast-1 | ap-southeast-2 | ap-southeast-3 | ap-southeast-4 | ap-southeast-5 | ca-central-1 | ca-west-1 | cn-north-1 | cn-northwest-1 | eu-central-1 | eu-central-2 | eu-north-1 | eu-south-1 | eu-south-2 | eu-west-1 | eu-west-2 | eu-west-3 | il-central-1 | me-central-1 | me-south-1 | sa-east-1 | us-east-1 | us-east-2 | us-west-1 | us-west-2`

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

OptInFeature

Contents

featureName

Type: String

Valid Values: `Triage`

Required: Yes

isEnabled

Type: Boolean

Required: Yes

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

ThreatActorIp

Contents

ipAddress

Type: String

Pattern: `(?:(?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?))|(?:(?:[A-F0-9]{1,4}:){7}[A-F0-9]{1,4})|(?:(?:[A-F0-9]{1,4}:){6}(?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?))`

Required: Yes

userAgent

Type: String

Length Constraints: Minimum length of 0. Maximum length of 500.

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

ValidationExceptionField

Contents

message

Type: String

Required: Yes

name

Type: String

Required: Yes

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

Watcher

Contents

email

Type: String

Length Constraints: Minimum length of 6. Maximum length of 254.

Pattern: `[a-zA-Z0-9.!#$%&'*+/=?^_`{|}~-]+@[a-zA-Z0-9-]+(?:\.[a-zA-Z0-9-]+)*`

Required: Yes

jobTitle

Type: String

Length Constraints: Minimum length of 1. Maximum length of 50.

Required: No

name

Type: String

Length Constraints: Minimum length of 1. Maximum length of 50.

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*.

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 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 Errors

This section lists the errors common to the API actions of all AWS services. For errors specific to an API action for this service, see the topic for that API action.

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ExpiredTokenException

The security token included in the request is expired

HTTP Status Code: 403

IncompleteSignature

The request signature does not conform to AWS standards.

HTTP Status Code: 403

InternalFailure

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

HTTP Status Code: 500

MalformedHttpRequestException

Problems with the request at the HTTP level, e.g. we can't decompress the body according to the decompression algorithm specified by the content-encoding.

HTTP Status Code: 400

NotAuthorized

You do not have permission to perform this action.

HTTP Status Code: 401

OptInRequired

The AWS access key ID needs a subscription for the service.

HTTP Status Code: 403

RequestAbortedException

Convenient exception that can be used when a request is aborted before a reply is sent back (e.g. client closed connection).

HTTP Status Code: 400

RequestEntityTooLargeException

Problems with the request at the HTTP level. The request entity is too large.

HTTP Status Code: 413

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

RequestTimeoutException

Problems with the request at the HTTP level. Reading the Request timed out.

HTTP Status Code: 408

ServiceUnavailable

The request has failed due to a temporary failure of the server.

HTTP Status Code: 503

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 400

UnrecognizedClientException

The X.509 certificate or AWS access key ID provided does not exist in our records.

HTTP Status Code: 403

UnknownOperationException

The action or operation requested is invalid. Verify that the action is typed correctly.

HTTP Status Code: 404

ValidationError

The input fails to satisfy the constraints specified by an AWS service.

HTTP Status Code: 400