
Amazon Macie

REST API Reference



Amazon Macie: REST API Reference

Copyright © 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.

Table of Contents

Welcome	1
Finding regional endpoints	1
Managing multiple accounts	1
Signing requests	2
Logging API calls	2
Operations	3
Resources	7
Account Administration	8
URI	8
HTTP methods	8
Schemas	11
Properties	13
See also	16
Administrator	18
URI	18
HTTP methods	18
Schemas	19
Properties	20
See also	22
Administrator Disassociation	23
URI	23
HTTP methods	23
Schemas	24
Properties	25
See also	26
AWS Organizations - Macie Administrator	27
URI	27
HTTP methods	27
Schemas	30
Properties	31
See also	34
AWS Organizations - Macie Configuration	35
URI	35
HTTP methods	35
Schemas	37
Properties	38
See also	40
Classification Job Creation	41
URI	41
HTTP methods	41
Schemas	42
Properties	45
See also	58
Classification Job Description	58
URI	59
HTTP methods	59
Schemas	61
Properties	64
See also	80
Classification Job List	81
URI	81
HTTP methods	81
Schemas	82
Properties	84

See also	95
Custom Data Identifier	95
URI	95
HTTP methods	95
Schemas	97
Properties	98
See also	102
Custom Data Identifier Creation	102
URI	103
HTTP methods	103
Schemas	104
Properties	105
See also	108
Custom Data Identifier Descriptions	109
URI	109
HTTP methods	109
Schemas	110
Properties	111
See also	114
Custom Data Identifier List	114
URI	115
HTTP methods	115
Schemas	115
Properties	117
See also	120
Custom Data Identifier Testing	120
URI	120
HTTP methods	120
Schemas	121
Properties	123
See also	125
Data Sources - Amazon S3	126
URI	126
HTTP methods	126
Schemas	127
Properties	130
See also	145
Data Sources - Amazon S3 Statistics	145
URI	146
HTTP methods	146
Schemas	146
Properties	148
See also	156
Data Sources - Search	156
URI	156
HTTP methods	157
Schemas	157
Properties	160
See also	171
Export Configuration	171
URI	172
HTTP methods	172
Schemas	173
Properties	175
See also	178
Findings Descriptions	178
URI	179

HTTP methods	179
Schemas	179
Properties	186
See also	217
Findings Filter	218
URI	218
HTTP methods	218
Schemas	221
Properties	222
See also	229
Findings Filters	229
URI	230
HTTP methods	230
Schemas	231
Properties	233
See also	239
Findings List	240
URI	240
HTTP methods	240
Schemas	241
Properties	242
See also	247
Findings Publication Configuration	247
URI	248
HTTP methods	248
Schemas	249
Properties	251
See also	253
Findings Samples	254
URI	254
HTTP methods	254
Schemas	255
Properties	256
See also	258
Findings Statistics	259
URI	259
HTTP methods	259
Schemas	260
Properties	261
See also	266
Invitation Acceptance	267
URI	267
HTTP methods	267
Schemas	268
Properties	269
See also	271
Invitation Count	272
URI	272
HTTP methods	272
Schemas	273
Properties	274
See also	276
Invitation Decline	276
URI	277
HTTP methods	277
Schemas	277
Properties	279

See also	281
Invitation Deletion	282
URI	282
HTTP methods	282
Schemas	283
Properties	284
See also	287
Invitation List	287
URI	288
HTTP methods	288
Schemas	289
Properties	291
See also	295
Managed Data Identifiers	296
URI	296
HTTP methods	296
Schemas	296
Properties	297
See also	298
Master Account	298
URI	299
HTTP methods	299
Schemas	299
Properties	301
See also	303
Master Disassociation	304
URI	304
HTTP methods	304
Schemas	305
Properties	306
See also	307
Member	307
URI	308
HTTP methods	308
Schemas	310
Properties	311
See also	314
Member Disassociation	315
URI	315
HTTP methods	315
Schemas	316
Properties	317
See also	319
Member Status	319
URI	319
HTTP methods	319
Schemas	320
Properties	321
See also	323
Members	324
URI	324
HTTP methods	324
Schemas	326
Properties	328
See also	332
Tags	333
URI	333

HTTP methods	333
Schemas	335
Properties	336
See also	337
Usage Statistics	338
URI	338
HTTP methods	338
Schemas	339
Properties	340
See also	347
Usage Totals	347
URI	348
HTTP methods	348
Schemas	349
Properties	350
See also	353
AWS glossary	354
Document history	355

Welcome

Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to help you discover, monitor, and protect sensitive data in your AWS environment.

Macie automates the discovery of sensitive data, such as personally identifiable information (PII) and financial information, to provide you with a better understanding of the data that your organization stores in Amazon Simple Storage Service (Amazon S3). Macie also provides you with an inventory of your S3 buckets, and it automatically evaluates and monitors those buckets for security and access control. If Macie detects sensitive data or potential issues with the security or privacy of your data, it creates detailed findings for you to review and remediate as necessary.

This guide, the *Amazon Macie REST API Reference*, provides information about the Amazon Macie API. This includes supported resources, HTTP methods, parameters, and schemas. If you're new to Macie, you might find it helpful to also review the [Amazon Macie User Guide](#). The *Amazon Macie User Guide* explains key concepts and provides procedures that demonstrate how to use Macie features. It also provides information about topics such as integrating Macie with other AWS services.

In addition to interacting with Macie by making RESTful calls to the Amazon Macie API, you can use a current version of an AWS command line tool or SDK. AWS provides tools and SDKs that consist of libraries and sample code for various languages and platforms, such as PowerShell, Java, Go, Python, C++, and .NET. These tools and SDKs provide convenient, programmatic access to Macie and other AWS services. They also handle tasks such as signing requests, managing errors, and retrying requests automatically. For information about installing and using the AWS tools and SDKs, see [Tools to Build on AWS](#).

Finding regional endpoints

The Amazon Macie API is available in most AWS Regions and it provides an endpoint for each of these Regions. For a list of Regions and endpoints where the API is currently available, see [Amazon Macie endpoints and quotas](#) in the *Amazon Web Services General Reference*. To learn more about AWS Regions, see [Managing AWS Regions](#) in the *Amazon Web Services General Reference*.

When you send a request to the Amazon Macie API, the request applies only to the AWS Region that's currently active for your AWS account or specified in the request. If your request submits changes to configuration or other settings for your account, the changes apply only to that Region. To make the same changes in other Regions, send the request to each additional Region that you want to apply the changes to.

Managing multiple accounts

You can centrally manage multiple Amazon Macie accounts. To do this, designate a single Macie account as the *Macie administrator account* and associate other Macie accounts with it as *member accounts*. You can do this in two ways, by using AWS Organizations or by sending membership invitations from Macie. We recommend using AWS Organizations to manage multiple accounts.

If you're a user of a Macie administrator account, you can access and manage certain Macie resources for member accounts. You can also perform certain administrative tasks and choose certain settings for member accounts.

If you're a user of a member account, you can access and manage Macie resources only for your own account. You can't access or manage Macie resources for other member accounts or the Macie administrator account. For this reason, you might not be able to use certain operations of the Amazon Macie API.

For detailed information about the primary tasks that administrator and member accounts can perform, see [Managing multiple accounts](#) in the *Amazon Macie User Guide*.

Signing requests

When you send an HTTPS request to the Amazon Macie API, you have to sign the request by using your AWS access key, which consists of an access key ID and a secret access key. For everyday work with Macie, we strongly recommend that you not use the access key ID and secret key for your root AWS account. Instead, use the access key ID and secret access key for an AWS Identity and Access Management (IAM) user. You can also use the AWS Security Token Service to generate temporary security credentials that you can use to sign requests. All Amazon Macie operations require Signature Version 4.

For more information about using credentials and signing requests, see the following resources:

- [AWS security credentials](#) – This section of the Amazon Web Services General Reference provides information about the types of credentials that can be used to access AWS.
- [Temporary security credentials in IAM](#) – This section of the *IAM User Guide* describes how to create and use temporary security credentials.
- [Signing AWS API requests](#) – This section of the Amazon Web Services General Reference explains and guides you through the process of signing a request using an access key ID and secret access key.

Logging API calls

Amazon Macie integrates with AWS CloudTrail, which is a service that provides a record of actions that were taken in Macie by a user, a role, or another AWS service. This includes actions that were performed using the Amazon Macie console and programmatic calls to Amazon Macie API operations.

By using the information collected by CloudTrail, you can determine which requests were successfully sent to Macie. For each request, you can identify when it was made, the IP address from which it was made, who made it, and additional details. To learn more about CloudTrail, see the [AWS CloudTrail User Guide](#).

Operations

The Amazon Macie REST API includes the following operations.

- [AcceptInvitation](#) (p. 267)

Accepts an Amazon Macie membership invitation that was received from a specific account.

- [BatchGetCustomDataIdentifiers](#) (p. 109)

Retrieves information about one or more custom data identifiers.

- [CreateClassificationJob](#) (p. 41)

Creates and defines the settings for a classification job.

- [CreateCustomDataIdentifier](#) (p. 103)

Creates and defines the criteria and other settings for a custom data identifier.

- [CreateFindingsFilter](#) (p. 231)

Creates and defines the criteria and other settings for a findings filter.

- [CreateInvitations](#) (p. 289)

Sends an Amazon Macie membership invitation to one or more accounts.

- [CreateMember](#) (p. 325)

Associates an account with an Amazon Macie administrator account.

- [CreateSampleFindings](#) (p. 254)

Creates sample findings.

- [DeclineInvitations](#) (p. 277)

Declines Amazon Macie membership invitations that were received from specific accounts.

- [DeleteCustomDataIdentifier](#) (p. 96)

Soft deletes a custom data identifier.

- [DeleteFindingsFilter](#) (p. 219)

Deletes a findings filter.

- [DeleteInvitations](#) (p. 282)

Deletes Amazon Macie membership invitations that were received from specific accounts.

- [DeleteMember](#) (p. 309)

Deletes the association between an Amazon Macie administrator account and an account.

- [DescribeBuckets](#) (p. 126)

Retrieves (queries) statistical data and other information about one or more S3 buckets that Amazon Macie monitors and analyzes.

- [DescribeClassificationJob](#) (p. 59)

Retrieves the status and settings for a classification job.

- [DescribeOrganizationConfiguration](#) (p. 35)

Retrieves the Amazon Macie configuration settings for an AWS organization.

- [DisableMacie](#) (p. 10)

Disables an Amazon Macie account and deletes Macie resources for the account.

- [DisableOrganizationAdminAccount](#) (p. 29)

Disables an account as the delegated Amazon Macie administrator account for an AWS organization.

- [DisassociateFromAdministratorAccount](#) (p. 23)

Disassociates a member account from its Amazon Macie administrator account.

- [DisassociateFromMasterAccount](#) (p. 304)

(Deprecated) Disassociates a member account from its Amazon Macie administrator account. This operation has been replaced by the [DisassociateFromAdministratorAccount](#) (p. 23) operation.

- [DisassociateMember](#) (p. 315)

Disassociates an Amazon Macie administrator account from a member account.

- [EnableMacie](#) (p. 9)

Enables Amazon Macie and specifies the configuration settings for a Macie account.

- [EnableOrganizationAdminAccount](#) (p. 28)

Designates an account as the delegated Amazon Macie administrator account for an AWS organization.

- [GetAdministratorAccount](#) (p. 18)

Retrieves information about the Amazon Macie administrator account for an account.

- [GetBucketStatistics](#) (p. 146)

Retrieves (queries) aggregated statistical data for all the S3 buckets that Amazon Macie monitors and analyzes.

- [GetClassificationExportConfiguration](#) (p. 172)

Retrieves the configuration settings for storing data classification results.

- [GetCustomDataIdentifier](#) (p. 95)

Retrieves the criteria and other settings for a custom data identifier.

- [GetFindings](#) (p. 179)

Retrieves the details of one or more findings.

- [GetFindingsFilter](#) (p. 218)

Retrieves the criteria and other settings for a findings filter.

- [GetFindingsPublicationConfiguration](#) (p. 248)

Retrieves the configuration settings for publishing findings to AWS Security Hub.

- [GetFindingStatistics](#) (p. 259)

Retrieves (queries) aggregated statistical data about findings.

- [GetInvitationsCount](#) (p. 272)

Retrieves the count of Amazon Macie membership invitations that were received by an account.

- [GetMacieSession](#) (p. 8)

Retrieves the current status and configuration settings for an Amazon Macie account.

- [GetMasterAccount](#) (p. 299)

(Deprecated) Retrieves information about the Amazon Macie administrator account for an account. This operation has been replaced by the [GetAdministratorAccount](#) (p. 18) operation.

- [GetMember](#) (p. 308)

Retrieves information about an account that's associated with an Amazon Macie administrator account.

- [GetUsageStatistics](#) (p. 338)

Retrieves (queries) quotas and aggregated usage data for one or more accounts.

- [GetUsageTotals](#) (p. 348)

Retrieves (queries) aggregated usage data for an account.

- [ListClassificationJobs](#) (p. 81)

Retrieves a subset of information about one or more classification jobs.

- [ListCustomDataIdentifiers](#) (p. 115)

Retrieves a subset of information about all the custom data identifiers for an account.

- [ListFindings](#) (p. 240)

Retrieves a subset of information about one or more findings.

- [ListFindingsFilters](#) (p. 230)

Retrieves a subset of information about all the findings filters for an account.

- [ListInvitations](#) (p. 288)

Retrieves information about the Amazon Macie membership invitations that were received by an account.

- [ListManagedDataIdentifiers](#) (p. 296)

Retrieves information about all the managed data identifiers that Amazon Macie currently provides.

- [ListMembers](#) (p. 324)

Retrieves information about the accounts that are associated with an Amazon Macie administrator account.

- [ListOrganizationAdminAccounts](#) (p. 27)

Retrieves information about the delegated Amazon Macie administrator account for an AWS organization.

- [ListTagsForResource](#) (p. 333)

Retrieves the tags (keys and values) that are associated with a classification job, custom data identifier, findings filter, or member account.

- [PutClassificationExportConfiguration](#) (p. 173)

Creates or updates the configuration settings for storing data classification results.

- [PutFindingsPublicationConfiguration](#) (p. 249)

Updates the configuration settings for publishing findings to AWS Security Hub.

- [SearchResources](#) (p. 157)

Retrieves (queries) statistical data and other information about AWS resources that Amazon Macie monitors and analyzes.

- [TagResource](#) (p. 334)

Adds or updates one or more tags (keys and values) that are associated with a classification job, custom data identifier, findings filter, or member account.

- [TestCustomDataIdentifier](#) (p. 120)

Tests a custom data identifier.

- [UntagResource](#) (p. 334)

Removes one or more tags (keys and values) from a classification job, custom data identifier, findings filter, or member account.

- [UpdateClassificationJob](#) (p. 60)

Changes the status of a classification job.

- [UpdateFindingsFilter](#) (p. 220)

Updates the criteria and other settings for a findings filter.

- [UpdateMacieSession](#) (p. 10)

Suspends or re-enables an Amazon Macie account, or updates the configuration settings for a Macie account.

- [UpdateMemberSession](#) (p. 319)

Enables an Amazon Macie administrator to suspend or re-enable a member account.

- [UpdateOrganizationConfiguration](#) (p. 36)

Updates the Amazon Macie configuration settings for an AWS organization.

Resources

The Amazon Macie REST API includes the following resources.

Topics

- [Account Administration](#) (p. 8)
- [Administrator](#) (p. 18)
- [Administrator Disassociation](#) (p. 23)
- [AWS Organizations - Macie Administrator](#) (p. 27)
- [AWS Organizations - Macie Configuration](#) (p. 35)
- [Classification Job Creation](#) (p. 41)
- [Classification Job Description](#) (p. 58)
- [Classification Job List](#) (p. 81)
- [Custom Data Identifier](#) (p. 95)
- [Custom Data Identifier Creation](#) (p. 102)
- [Custom Data Identifier Descriptions](#) (p. 109)
- [Custom Data Identifier List](#) (p. 114)
- [Custom Data Identifier Testing](#) (p. 120)
- [Data Sources - Amazon S3](#) (p. 126)
- [Data Sources - Amazon S3 Statistics](#) (p. 145)
- [Data Sources - Search](#) (p. 156)
- [Export Configuration](#) (p. 171)
- [Findings Descriptions](#) (p. 178)
- [Findings Filter](#) (p. 218)
- [Findings Filters](#) (p. 229)
- [Findings List](#) (p. 240)
- [Findings Publication Configuration](#) (p. 247)
- [Findings Samples](#) (p. 254)
- [Findings Statistics](#) (p. 259)
- [Invitation Acceptance](#) (p. 267)
- [Invitation Count](#) (p. 272)
- [Invitation Decline](#) (p. 276)
- [Invitation Deletion](#) (p. 282)
- [Invitation List](#) (p. 287)
- [Managed Data Identifiers](#) (p. 296)
- [Master Account](#) (p. 298)
- [Master Disassociation](#) (p. 304)
- [Member](#) (p. 307)
- [Member Disassociation](#) (p. 315)

- [Member Status \(p. 319\)](#)
- [Members \(p. 324\)](#)
- [Tags \(p. 333\)](#)
- [Usage Statistics \(p. 338\)](#)
- [Usage Totals \(p. 347\)](#)

Account Administration

The Account Administration resource provides access to the status and configuration settings for your Amazon Macie account.

You can use this resource to enable and specify settings for your Macie account. When you enable Macie, the service generates a *session* for your AWS account in the current AWS Region, and it assigns a unique identifier to that session. A *session* is a resource that represents the Macie service for a specific account in a specific Region. It enables Macie to become operational. An account can have only one session in each Region.

After you enable Macie, you can use this resource to review and update the status and configuration settings for your account. This includes suspending (pausing) your account and subsequently re-enabling your account. If you suspend your Macie account, Macie stops performing all activities for your account. However, the service retains the session identifier, settings, and resources for your account. To suspend a Macie administrator account, you must first disassociate the account from all of its member accounts.

If you decide to disable your Macie account completely, you can use this resource to do so. If you disable your Macie account, the service stops performing all activities for your account. In addition, Macie permanently deletes all resources that it stores or maintains for you. This includes classification jobs, custom data identifiers, findings, and the session resource (and identifier) for your account. This doesn't include resources that Macie created and stored in another AWS service for you, such as data classification results in Amazon S3 and findings in AWS Security Hub. Before you disable your Macie account, you must disassociate your account from its Macie administrator account or, if it's an administrator account, all of its member accounts.

URI

/macie

HTTP methods

GET

Operation ID: GetMacieSession

Retrieves the current status and configuration settings for an Amazon Macie account.

Responses

Status code	Response model	Description
200	GetMacieSessionResponse (p. 12)	The request succeeded.
400	ValidationException (p. 12)	The request failed because it contains a syntax error.

Status code	Response model	Description
402	ServiceQuotaExceededException (p. 12)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 12)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 12)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 12)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 12)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 12)	The request failed due to an unknown internal server error, exception, or failure.

POST

Operation ID: EnableMacie

Enables Amazon Macie and specifies the configuration settings for a Macie account.

Responses

Status code	Response model	Description
200	Empty Schema (p. 12)	The request succeeded and there isn't any content to include in the body of the response (No Content).
400	ValidationException (p. 12)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 12)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 12)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 12)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 12)	The request failed because it conflicts with the current state of the specified resource.

Status code	Response model	Description
429	ThrottlingException (p. 12)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 13)	The request failed due to an unknown internal server error, exception, or failure.

DELETE

Operation ID: DisableMacie

Disables an Amazon Macie account and deletes Macie resources for the account.

Responses

Status code	Response model	Description
200	Empty Schema (p. 12)	The request succeeded and there isn't any content to include in the body of the response (No Content).
400	ValidationException (p. 12)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 12)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 13)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 13)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 12)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 12)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 13)	The request failed due to an unknown internal server error, exception, or failure.

PATCH

Operation ID: UpdateMacieSession

Suspends or re-enables an Amazon Macie account, or updates the configuration settings for a Macie account.

Responses

Status code	Response model	Description
200	Empty Schema (p. 12)	The request succeeded and there isn't any content to include in the body of the response (No Content).
400	ValidationException (p. 12)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 12)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 12)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 12)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 12)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 12)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 12)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

POST schema

```
{
  "clientToken": "string",
  "findingPublishingFrequency": enum,
  "status": enum
}
```

PATCH schema

```
{
  "findingPublishingFrequency": enum,
  "status": enum
}
```

Response bodies

GetMacieSessionResponse schema

```
{
  "createdAt": "string",
  "serviceRole": "string",
  "findingPublishingFrequency": enum,
  "status": enum,
  "updatedAt": "string"
}
```

Empty Schema schema

```
{
}
```

ValidationException schema

```
{
  "message": "string"
}
```

ServiceQuotaExceededException schema

```
{
  "message": "string"
}
```

AccessDeniedException schema

```
{
  "message": "string"
}
```

ResourceNotFoundException schema

```
{
  "message": "string"
}
```

ConflictException schema

```
{
  "message": "string"
}
```

ThrottlingException schema

```
{
  "message": "string"
}
```

InternalServerError schema

```
{  
  "message": "string"  
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

Empty

The request succeeded and there isn't any content to include in the body of the response (No Content).

EnableMacieRequest

Enables Amazon Macie and specifies the configuration settings for a Macie account.

clientToken

A unique, case-sensitive token that you provide to ensure the idempotency of the request.

Type: string

Required: False

findingPublishingFrequency

Specifies how often to publish updates to policy findings for the account. This includes publishing updates to AWS Security Hub and Amazon EventBridge (formerly called Amazon CloudWatch Events).

Type: [FindingPublishingFrequency](#) (p. 14)

Required: False

status

Specifies the new status for the account. To enable Amazon Macie and start all Macie activities for the account, set this value to `ENABLED`.

Type: [MacieStatus](#) (p. 15)

Required: False

FindingPublishingFrequency

The frequency with which Amazon Macie publishes updates to policy findings for an account. This includes publishing updates to AWS Security Hub and Amazon EventBridge (formerly called Amazon CloudWatch Events). For more information, see [Monitoring and processing findings](#) in the *Amazon Macie User Guide*. Valid values are:

`FIFTEEN_MINUTES`
`ONE_HOUR`
`SIX_HOURS`

GetMacieSessionResponse

Provides information about the current status and configuration settings for an Amazon Macie account.

createdAt

The date and time, in UTC and extended ISO 8601 format, when the Amazon Macie account was created.

Type: string

Required: False

Format: date-time

serviceRole

The Amazon Resource Name (ARN) of the service-linked role that allows Macie to monitor and analyze data in AWS resources for the account.

Type: string

Required: False

findingPublishingFrequency

The frequency with which Macie publishes updates to policy findings for the account. This includes publishing updates to AWS Security Hub and Amazon EventBridge (formerly called Amazon CloudWatch Events).

Type: [FindingPublishingFrequency](#) (p. 14)

Required: False

status

The current status of the Macie account. Possible values are: `PAUSED`, the account is enabled but all Macie activities are suspended (paused) for the account; and, `ENABLED`, the account is enabled and all Macie activities are enabled for the account.

Type: [MacieStatus](#) (p. 15)

Required: False

updatedAt

The date and time, in UTC and extended ISO 8601 format, of the most recent change to the status of the Macie account.

Type: string

Required: False

Format: date-time

[InternalServerErrorException](#)

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string

Required: False

[MacieStatus](#)

The status of an Amazon Macie account. Valid values are:

PAUSED

ENABLED

[ResourceNotFoundException](#)

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string

Required: False

[ServiceQuotaExceededException](#)

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string

Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string

Required: False

UpdateMacieSessionRequest

Changes the status or configuration settings for an Amazon Macie account.

findingPublishingFrequency

Specifies how often to publish updates to policy findings for the account. This includes publishing updates to AWS Security Hub and Amazon EventBridge (formerly called Amazon CloudWatch Events).

Type: [FindingPublishingFrequency](#) (p. 14)

Required: False

status

Specifies a new status for the account. Valid values are: `ENABLED`, resume all Amazon Macie activities for the account; and, `PAUSED`, suspend all Macie activities for the account.

Type: [MacieStatus](#) (p. 15)

Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string

Required: False

See also

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

GetMacieSession

- [AWS Command Line Interface](#)

- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

EnableMacie

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

DisableMacie

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

UpdateMacieSession

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)

- [AWS SDK for Ruby V3](#)

Administrator

The Administrator resource provides information about the Amazon Macie administrator account for your account. If you joined an organization by accepting a Macie membership invitation, this resource also provides information about that invitation. After you join an organization, the Macie administrator account can manage certain Macie settings and resources on your behalf and on behalf of other members of the organization.

You can use the Administrator resource to retrieve information about the Macie administrator account for your account.

URI

/administrator

HTTP methods

GET

Operation ID: GetAdministratorAccount

Retrieves information about the Amazon Macie administrator account for an account.

Responses

Status code	Response model	Description
200	GetAdministratorAccountResponse	The request succeeded.
400	ValidationException (p. 19)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 19)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 19)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 19)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 19)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 19)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 19)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Response bodies

GetAdministratorAccountResponse schema

```
{
  "administrator": {
    "accountId": "string",
    "relationshipStatus": enum,
    "invitationId": "string",
    "invitedAt": "string"
  }
}
```

ValidationException schema

```
{
  "message": "string"
}
```

ServiceQuotaExceededException schema

```
{
  "message": "string"
}
```

AccessDeniedException schema

```
{
  "message": "string"
}
```

ResourceNotFoundException schema

```
{
  "message": "string"
}
```

ConflictException schema

```
{
  "message": "string"
}
```

ThrottlingException schema

```
{
  "message": "string"
}
```

InternalServerError schema

```
{  
  "message": "string"  
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

GetAdministratorAccountResponse

Provides information about the Amazon Macie administrator account for an account. If the accounts are associated by a Macie membership invitation, the response also provides information about that invitation.

administrator

The AWS account ID for the administrator account. If the accounts are associated by a Macie membership invitation, this object also provides details about the invitation that was sent to establish the relationship between the accounts.

Type: [Invitation](#) (p. 21)

Required: False

InternalServerError

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string
Required: False

Invitation

Provides information about an Amazon Macie membership invitation that was received by an account.

accountId

The AWS account ID for the account that sent the invitation.

Type: string
Required: False

relationshipStatus

The status of the relationship between the account that sent the invitation (*inviter account*) and the account that received the invitation (*invitee account*).

Type: [RelationshipStatus](#) (p. 21)
Required: False

invitationId

The unique identifier for the invitation. Amazon Macie uses this identifier to validate the inviter account with the invitee account.

Type: string
Required: False

invitedAt

The date and time, in UTC and extended ISO 8601 format, when the invitation was sent.

Type: string
Required: False
Format: date-time

RelationshipStatus

The current status of the relationship between an account and an associated Amazon Macie administrator account (*inviter account*). Possible values are:

Enabled
Paused
Invited
Created
Removed
Resigned
EmailVerificationInProgress
EmailVerificationFailed
RegionDisabled
AccountSuspended

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string

Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string

Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string

Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string

Required: False

See also

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

GetAdministratorAccount

- [AWS Command Line Interface](#)

- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Administrator Disassociation

The Administrator Disassociation resource provides access to the association between your Amazon Macie account and its Macie administrator account. You can use this resource to disassociate your Macie account from its current Macie administrator account.

If you're a user of a Macie administrator account and you want to disassociate a member account from your account, use the [Member Disassociation \(p. 315\)](#) resource.

URI

/administrator/disassociate

HTTP methods

POST

Operation ID: DisassociateFromAdministratorAccount

Disassociates a member account from its Amazon Macie administrator account.

Responses

Status code	Response model	Description
200	Empty Schema (p. 24)	The request succeeded and there isn't any content to include in the body of the response (No Content).
400	ValidationException (p. 24)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 24)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 24)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 24)	The request failed because the specified resource wasn't found.

Status code	Response model	Description
409	ConflictException (p. 24)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 25)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerError (p. 25)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Response bodies

Empty Schema schema

```
{  
}
```

ValidationException schema

```
{  
  "message": "string"  
}
```

ServiceQuotaExceededException schema

```
{  
  "message": "string"  
}
```

AccessDeniedException schema

```
{  
  "message": "string"  
}
```

ResourceNotFoundException schema

```
{  
  "message": "string"  
}
```

ConflictException schema

```
{
```

```
"message": "string"
}
```

ThrottlingException schema

```
{
  "message": "string"
}
```

InternalServerError schema

```
{
  "message": "string"
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

Empty

The request succeeded and there isn't any content to include in the body of the response (No Content).

InternalServerError

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string
Required: False

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string
Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string
Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string
Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string
Required: False

See also

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

DisassociateFromAdministratorAccount

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

AWS Organizations - Macie Administrator

The Macie Administrator resource for AWS Organizations provides settings that specify which account is the delegated Amazon Macie administrator account for an AWS organization. An *AWS organization* is a set of AWS accounts that are managed as a group by using AWS Organizations. AWS Organizations is an account management service that enables administrators to consolidate and centrally manage multiple AWS accounts as a single organization. To learn more about this service, see the [AWS Organizations User Guide](#).

If you're a user of the management account for an AWS organization, you can use this resource to designate a delegated Macie administrator account for the organization. You can also use this resource to retrieve information about and change that designation. Note that an AWS organization can have only one delegated Macie administrator account. To use this resource, you must be a user of the management account for an AWS organization.

URI

/admin

HTTP methods

GET

Operation ID: ListOrganizationAdminAccounts

Retrieves information about the delegated Amazon Macie administrator account for an AWS organization.

Query parameters

Name	Type	Required	Description
nextToken	String	False	The <code>nextToken</code> string that specifies which page of results to return in a paginated response.

Name	Type	Required	Description
maxResults	String	False	The maximum number of items to include in each page of a paginated response.

Responses

Status code	Response model	Description
200	ListOrganizationAdminAccountsResponse (p. 30)	The request succeeded.
400	ValidationException (p. 30)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 30)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 31)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 31)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 31)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 31)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 31)	The request failed due to an unknown internal server error, exception, or failure.

POST

Operation ID: EnableOrganizationAdminAccount

Designates an account as the delegated Amazon Macie administrator account for an AWS organization.

Responses

Status code	Response model	Description
200	Empty Schema (p. 30)	The request succeeded and there isn't any content to include in the body of the response (No Content).
400	ValidationException (p. 30)	The request failed because it contains a syntax error.

Status code	Response model	Description
402	ServiceQuotaExceededException (p. 31)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 31)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 31)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 31)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 31)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 31)	The request failed due to an unknown internal server error, exception, or failure.

DELETE

Operation ID: DisableOrganizationAdminAccount

Disables an account as the delegated Amazon Macie administrator account for an AWS organization.

Query parameters

Name	Type	Required	Description
adminAccountId	String	True	The AWS account ID of the delegated Amazon Macie administrator account.

Responses

Status code	Response model	Description
200	Empty Schema (p. 30)	The request succeeded and there isn't any content to include in the body of the response (No Content).
400	ValidationException (p. 30)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 31)	The request failed because fulfilling the request would exceed one or more service quotas for your account.

Status code	Response model	Description
403	AccessDeniedException (p. 31)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 31)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 31)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 31)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 31)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

POST schema

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

Response bodies

ListOrganizationAdminAccountsResponse schema

```
{
  "nextToken": "string",
  "adminAccounts": [
    {
      "accountId": "string",
      "status": enum
    }
  ]
}
```

Empty Schema schema

```
{
}
```

ValidationException schema

```
{
```

```
"message": "string"
}
```

ServiceQuotaExceededException schema

```
{
  "message": "string"
}
```

AccessDeniedException schema

```
{
  "message": "string"
}
```

ResourceNotFoundException schema

```
{
  "message": "string"
}
```

ConflictException schema

```
{
  "message": "string"
}
```

ThrottlingException schema

```
{
  "message": "string"
}
```

InternalServerError schema

```
{
  "message": "string"
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

AdminAccount

Provides information about the delegated Amazon Macie administrator account for an AWS organization.

accountId

The AWS account ID for the account.

Type: string

Required: False

status

The current status of the account as the delegated administrator of Amazon Macie for the organization.

Type: [AdminStatus](#) (p. 32)

Required: False

AdminStatus

The current status of an account as the delegated Amazon Macie administrator account for an AWS organization. Possible values are:

ENABLED

DISABLING_IN_PROGRESS

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

Empty

The request succeeded and there isn't any content to include in the body of the response (No Content).

EnableOrganizationAdminAccountRequest

Specifies an account to designate as a delegated Amazon Macie administrator account for an AWS organization. To submit this request, you must be a user of the management account for the AWS organization.

clientToken

A unique, case-sensitive token that you provide to ensure the idempotency of the request.

Type: string

Required: False

adminAccountId

The AWS account ID for the account to designate as the delegated Amazon Macie administrator account for the organization.

Type: string
Required: True

InternalServerErrorException

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string
Required: False

ListOrganizationAdminAccountsResponse

Provides information about the delegated Amazon Macie administrator accounts for an AWS organization.

nextToken

The string to use in a subsequent request to get the next page of results in a paginated response. This value is null if there are no additional pages.

Type: string
Required: False

adminAccounts

An array of objects, one for each delegated Amazon Macie administrator account for the organization. Only one of these accounts can have a status of `ENABLED`.

Type: Array of type [AdminAccount](#) (p. 32)
Required: False

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string
Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string

Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string

Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string

Required: False

See also

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

ListOrganizationAdminAccounts

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

EnableOrganizationAdminAccount

- [AWS Command Line Interface](#)

- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

DisableOrganizationAdminAccount

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

AWS Organizations - Macie Configuration

The Macie Configuration resource for AWS Organizations provides access to the Amazon Macie configuration settings for accounts in an AWS organization. An *AWS organization* is a set of AWS accounts that are managed as a group by using AWS Organizations. AWS Organizations is an account management service that enables administrators to consolidate and centrally manage multiple AWS accounts as a single organization. To learn more about this service, see the [AWS Organizations User Guide](#).

If you're the delegated Macie administrator for an AWS organization, you can use this resource to retrieve information about and update the Macie configuration settings for the organization. This includes the setting that determines whether Macie is enabled automatically for accounts that are added to the organization. To use this resource, you must be the delegated Macie administrator for an AWS organization.

URI

/admin/configuration

HTTP methods

GET

Operation ID: DescribeOrganizationConfiguration

Retrieves the Amazon Macie configuration settings for an AWS organization.

Responses

Status code	Response model	Description
200	DescribeOrganizationConfiguration (p. 37)	The request succeeded.
400	ValidationException (p. 37)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 37)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 38)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 38)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 38)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 38)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 38)	The request failed due to an unknown internal server error, exception, or failure.

PATCH

Operation ID: UpdateOrganizationConfiguration

Updates the Amazon Macie configuration settings for an AWS organization.

Responses

Status code	Response model	Description
200	Empty Schema (p. 37)	The request succeeded and there isn't any content to include in the body of the response (No Content).
400	ValidationException (p. 37)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 37)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 38)	The request was denied because you don't have sufficient access to the specified resource.

Status code	Response model	Description
404	ResourceNotFoundException (p. 38)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 38)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 38)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 38)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

PATCH schema

```
{
  "autoEnable": boolean
}
```

Response bodies

DescribeOrganizationConfigurationResponse schema

```
{
  "autoEnable": boolean,
  "maxAccountLimitReached": boolean
}
```

Empty Schema schema

```
{
}
```

ValidationException schema

```
{
  "message": "string"
}
```

ServiceQuotaExceededException schema

```
{
  "message": "string"
}
```

AccessDeniedException schema

```
{  
  "message": "string"  
}
```

ResourceNotFoundException schema

```
{  
  "message": "string"  
}
```

ConflictException schema

```
{  
  "message": "string"  
}
```

ThrottlingException schema

```
{  
  "message": "string"  
}
```

InternalServerError schema

```
{  
  "message": "string"  
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string
Required: False

DescribeOrganizationConfigurationResponse

Provides information about the Amazon Macie configuration settings for an AWS organization.

autoEnable

Specifies whether Amazon Macie is enabled automatically for accounts that are added to the AWS organization.

Type: boolean
Required: False

maxAccountLimitReached

Specifies whether the maximum number of Amazon Macie member accounts are part of the AWS organization.

Type: boolean
Required: False

Empty

The request succeeded and there isn't any content to include in the body of the response (No Content).

InternalServerErrorException

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string
Required: False

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string
Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string

Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string

Required: False

UpdateOrganizationConfigurationRequest

Specifies whether to enable Amazon Macie automatically for accounts that are added to an AWS organization.

autoEnable

Specifies whether to enable Amazon Macie automatically for each account, when the account is added to the AWS organization.

Type: boolean

Required: True

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string

Required: False

See also

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

DescribeOrganizationConfiguration

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)

- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

UpdateOrganizationConfiguration

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Classification Job Creation

The Classification Job Creation resource represents the collection of settings that define the scope and schedule for a classification job. A *classification job*, also referred to as a *sensitive data discovery job*, is a job that analyzes objects in Amazon Simple Storage Service (Amazon S3) buckets to determine whether the objects contain sensitive data. To detect sensitive data, a job can use managed data identifiers that Amazon Macie provides, custom data identifiers that you define, or a combination of the two.

When you create a classification job, you can configure it to address specific scenarios. For example, you can use property- and tag-based conditions to perform targeted analysis of S3 buckets and objects that meet specific criteria. You can also define a schedule for running the job on a recurring basis, such as every day or a specific day of each week or month. This can be helpful if you want to monitor buckets for the presence of sensitive data or align your analysis with periodic updates to bucket objects.

You can use the Classification Job Creation resource to create and define the settings for a new classification job. Note that you can't change any settings for a job after you create it. This helps ensure that you have an immutable history of sensitive data findings and discovery results for data privacy and protection audits or investigations that you perform.

URI

/jobs

HTTP methods

POST

Operation ID: CreateClassificationJob

Creates and defines the settings for a classification job.

Responses

Status code	Response model	Description
200	CreateClassificationJobResponse	The request succeeded. The specified job was created.
400	ValidationException (p. 44)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 44)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 44)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 45)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 45)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerError (p. 45)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

POST schema

```
{
  "customDataIdentifierIds": [
    "string"
  ],
  "scheduleFrequency": {
    "dailySchedule": {
    },
    "weeklySchedule": {
      "dayOfWeek": enum
    },
    "monthlySchedule": {
      "dayOfMonth": integer
    }
  },
  "managedDataIdentifierIds": [
    "string"
  ],
  "samplingPercentage": integer,
  "clientToken": "string",
}
```

```

"name": "string",
"description": "string",
"initialRun": boolean,
"jobType": enum,
"s3JobDefinition": {
  "bucketDefinitions": [
    {
      "accountId": "string",
      "buckets": [
        "string"
      ]
    }
  ],
  "bucketCriteria": {
    "excludes": {
      "and": [
        {
          "tagCriterion": {
            "comparator": enum,
            "tagValues": [
              {
                "value": "string",
                "key": "string"
              }
            ]
          },
          "simpleCriterion": {
            "comparator": enum,
            "values": [
              "string"
            ],
            "key": enum
          }
        }
      ]
    },
    "includes": {
      "and": [
        {
          "tagCriterion": {
            "comparator": enum,
            "tagValues": [
              {
                "value": "string",
                "key": "string"
              }
            ]
          },
          "simpleCriterion": {
            "comparator": enum,
            "values": [
              "string"
            ],
            "key": enum
          }
        }
      ]
    }
  },
  "scoping": {
    "excludes": {
      "and": [
        {
          "simpleScopeTerm": {
            "comparator": enum,
            "values": [

```

```

        "string"
      ],
      "key": enum
    },
    "tagScopeTerm": {
      "comparator": enum,
      "tagValues": [
        {
          "value": "string",
          "key": "string"
        }
      ],
      "key": "string",
      "target": enum
    }
  }
]
},
"includes": {
  "and": [
    {
      "simpleScopeTerm": {
        "comparator": enum,
        "values": [
          "string"
        ],
        "key": enum
      },
      "tagScopeTerm": {
        "comparator": enum,
        "tagValues": [
          {
            "value": "string",
            "key": "string"
          }
        ],
        "key": "string",
        "target": enum
      }
    }
  ]
}
},
"tags": {
},
"managedDataIdentifierSelector": enum
}

```

Response bodies

CreateClassificationJobResponse schema

```

{
  "jobId": "string",
  "jobArn": "string"
}

```

ValidationException schema

```

{
  "message": "string"
}

```

```
}
```

ServiceQuotaExceededException schema

```
{  
  "message": "string"  
}
```

AccessDeniedException schema

```
{  
  "message": "string"  
}
```

ResourceNotFoundException schema

```
{  
  "message": "string"  
}
```

ConflictException schema

```
{  
  "message": "string"  
}
```

ThrottlingException schema

```
{  
  "message": "string"  
}
```

InternalServerError schema

```
{  
  "message": "string"  
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

CreateClassificationJobRequest

Specifies the scope, schedule, and other settings for a classification job. You can't change any settings for a classification job after you create it. This helps ensure that you have an immutable history of sensitive data findings and discovery results for data privacy and protection audits or investigations.

customDataIdentifierIds

An array of unique identifiers, one for each custom data identifier for the job to use when it analyzes data. To use only managed data identifiers, don't specify a value for this property and specify a value other than `NONE` for the `managedDataIdentifierSelector` property.

Type: Array of type string

Required: False

scheduleFrequency

The recurrence pattern for running the job. To run the job only once, don't specify a value for this property and set the value for the `jobType` property to `ONE_TIME`.

Type: [JobScheduleFrequency \(p. 50\)](#)

Required: False

managedDataIdentifierIds

An array of unique identifiers, one for each managed data identifier for the job to include (use) or exclude (not use) when it analyzes data. Inclusion or exclusion depends on the managed data identifier selection type that you specify for the job (`managedDataIdentifierSelector`).

To retrieve a list of valid values for this property, use the `ListManagedDataIdentifiers` operation.

Type: Array of type string

Required: False

samplingPercentage

The sampling depth, as a percentage, for the job to apply when processing objects. This value determines the percentage of eligible objects that the job analyzes. If this value is less than 100, Amazon Macie selects the objects to analyze at random, up to the specified percentage, and analyzes all the data in those objects.

Type: integer

Required: False
Format: int32

clientToken

A unique, case-sensitive token that you provide to ensure the idempotency of the request.

Type: string
Required: True

name

A custom name for the job. The name can contain as many as 500 characters.

Type: string
Required: True

description

A custom description of the job. The description can contain as many as 200 characters.

Type: string
Required: False

initialRun

For a recurring job, specifies whether to analyze all existing, eligible objects immediately after the job is created (`true`). To analyze only those objects that are created or changed after you create the job and before the job's first scheduled run, set this value to `false`.

If you configure the job to run only once, don't specify a value for this property.

Type: boolean
Required: False

jobType

The schedule for running the job. Valid values are:

- `ONE_TIME` - Run the job only once. If you specify this value, don't specify a value for the `scheduleFrequency` property.
- `SCHEDULED` - Run the job on a daily, weekly, or monthly basis. If you specify this value, use the `scheduleFrequency` property to define the recurrence pattern for the job.

Type: [JobType \(p. 51\)](#)
Required: True

s3JobDefinition

The S3 buckets that contain the objects to analyze, and the scope of that analysis.

Type: [S3JobDefinition \(p. 52\)](#)
Required: True

tags

A map of key-value pairs that specifies the tags to associate with the job.

A job can have a maximum of 50 tags. Each tag consists of a tag key and an associated tag value. The maximum length of a tag key is 128 characters. The maximum length of a tag value is 256 characters.

Type: [TagMap \(p. 56\)](#)

Required: False

managedDataIdentifierSelector

The selection type to apply when determining which managed data identifiers the job uses to analyze data. Valid values are:

- **ALL** - Use all the managed data identifiers that Amazon Macie provides. If you specify this value, don't specify any values for the `managedDataIdentifierIds` property.
- **EXCLUDE** - Use all the managed data identifiers that Macie provides except the managed data identifiers specified by the `managedDataIdentifierIds` property.
- **INCLUDE** - Use only the managed data identifiers specified by the `managedDataIdentifierIds` property.
- **NONE** - Don't use any managed data identifiers. If you specify this value, specify at least one custom data identifier for the job (`customDataIdentifierIds`) and don't specify any values for the `managedDataIdentifierIds` property.

If you don't specify a value for this property, the job uses all managed data identifiers. If you don't specify a value for this property or you specify **ALL** or **EXCLUDE** for a recurring job, the job also uses new managed data identifiers as they are released.

Type: [ManagedDataIdentifierSelector \(p. 51\)](#)

Required: False

CreateClassificationJobResponse

Provides information about a classification job that was created in response to a request.

jobId

The unique identifier for the job.

Type: string

Required: False

jobArn

The Amazon Resource Name (ARN) of the job.

Type: string

Required: False

CriteriaBlockForJob

Specifies one or more property- and tag-based conditions that define criteria for including or excluding S3 buckets from a classification job.

and

An array of conditions, one for each condition that determines which buckets to include or exclude from the job. If you specify more than one condition, Amazon Macie uses AND logic to join the conditions.

Type: Array of type [CriteriaForJob](#) (p. 49)

Required: False

CriteriaForJob

Specifies a property- or tag-based condition that defines criteria for including or excluding S3 buckets from a classification job.

tagCriterion

A tag-based condition that defines an operator and tag keys, tag values, or tag key and value pairs for including or excluding buckets from the job.

Type: [TagCriterionForJob](#) (p. 55)

Required: False

simpleCriterion

A property-based condition that defines a property, operator, and one or more values for including or excluding buckets from the job.

Type: [SimpleCriterionForJob](#) (p. 54)

Required: False

DailySchedule

Specifies that a classification job runs once a day, every day. This is an empty object.

InternalServerErrorException

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string

Required: False

JobComparator

The operator to use in a condition. Valid values are:

EQ
GT
GTE
LT
LTE
NE

CONTAINS
STARTS_WITH

JobScheduleFrequency

Specifies the recurrence pattern for running a classification job.

dailySchedule

Specifies a daily recurrence pattern for running the job.

Type: [DailySchedule](#) (p. 49)
Required: False

weeklySchedule

Specifies a weekly recurrence pattern for running the job.

Type: [WeeklySchedule](#) (p. 58)
Required: False

monthlySchedule

Specifies a monthly recurrence pattern for running the job.

Type: [MonthlySchedule](#) (p. 51)
Required: False

JobScopeTerm

Specifies a property- or tag-based condition that defines criteria for including or excluding S3 objects from a classification job. A `JobScopeTerm` object can contain only one `simpleScopeTerm` object or one `tagScopeTerm` object.

simpleScopeTerm

A property-based condition that defines a property, operator, and one or more values for including or excluding objects from the job.

Type: [SimpleScopeTerm](#) (p. 55)
Required: False

tagScopeTerm

A tag-based condition that defines the operator and tag keys or tag key and value pairs for including or excluding objects from the job.

Type: [TagScopeTerm](#) (p. 56)
Required: False

JobScopingBlock

Specifies one or more property- and tag-based conditions that define criteria for including or excluding S3 objects from a classification job.

and

An array of conditions, one for each property- or tag-based condition that determines which objects to include or exclude from the job. If you specify more than one condition, Amazon Macie uses AND logic to join the conditions.

Type: Array of type [JobScopeTerm](#) (p. 50)

Required: False

JobType

The schedule for running a classification job. Valid values are:

ONE_TIME
SCHEDULED

ManagedDataIdentifierSelector

The selection type that determines which managed data identifiers a classification job uses to analyze data. Valid values are:

ALL
EXCLUDE
INCLUDE
NONE

MonthlySchedule

Specifies a monthly recurrence pattern for running a classification job.

dayOfMonth

The numeric day of the month when Amazon Macie runs the job. This value can be an integer from 1 through 31.

If this value exceeds the number of days in a certain month, Macie doesn't run the job that month. Macie runs the job only during months that have the specified day. For example, if this value is 31 and a month has only 30 days, Macie doesn't run the job that month. To run the job every month, specify a value that's less than 29.

Type: integer

Required: False

Format: int32

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string

Required: False

S3BucketCriteriaForJob

Specifies property- and tag-based conditions that define criteria for including or excluding S3 buckets from a classification job. Exclude conditions take precedence over include conditions.

excludes

The property- and tag-based conditions that determine which buckets to exclude from the job.

Type: [CriteriaBlockForJob](#) (p. 48)

Required: False

includes

The property- and tag-based conditions that determine which buckets to include in the job.

Type: [CriteriaBlockForJob](#) (p. 48)

Required: False

S3BucketDefinitionForJob

Specifies an AWS account that owns S3 buckets for a classification job to analyze, and one or more specific buckets to analyze for that account.

accountId

The unique identifier for the AWS account that owns the buckets.

Type: string

Required: True

buckets

An array that lists the names of the buckets.

Type: Array of type string

Required: True

S3JobDefinition

Specifies which S3 buckets contain the objects that a classification job analyzes, and the scope of that analysis. The bucket specification can be static (`bucketDefinitions`) or dynamic (`bucketCriteria`). If it's static, the job analyzes objects in the same predefined set of buckets each time the job runs. If it's dynamic, the job analyzes objects in any buckets that match the specified criteria each time the job starts to run.

bucketDefinitions

An array of objects, one for each AWS account that owns specific S3 buckets to analyze. Each object specifies the account ID for an account and one or more buckets to analyze for that account. A job's definition can contain a `bucketDefinitions` array or a `bucketCriteria` object, not both.

Type: Array of type [S3BucketDefinitionForJob](#) (p. 52)
Required: False

bucketCriteria

The property- and tag-based conditions that determine which S3 buckets to include or exclude from the analysis. Each time the job runs, the job uses these criteria to determine which buckets contain objects to analyze. A job's definition can contain a `bucketCriteria` object or a `bucketDefinitions` array, not both.

Type: [S3BucketCriteriaForJob](#) (p. 52)
Required: False

scoping

The property- and tag-based conditions that determine which S3 objects to include or exclude from the analysis. Each time the job runs, the job uses these criteria to determine which objects to analyze.

Type: [Scoping](#) (p. 53)
Required: False

ScopeFilterKey

The property to use in a condition that determines whether an S3 object is included or excluded from a classification job. Valid values are:

```
OBJECT_EXTENSION  
OBJECT_LAST_MODIFIED_DATE  
OBJECT_SIZE  
OBJECT_KEY
```

Scoping

Specifies one or more property- and tag-based conditions that define criteria for including or excluding S3 objects from a classification job. Exclude conditions take precedence over include conditions.

excludes

The property- and tag-based conditions that determine which objects to exclude from the analysis.

Type: [JobScopingBlock](#) (p. 50)
Required: False

includes

The property- and tag-based conditions that determine which objects to include in the analysis.

Type: [JobScopingBlock](#) (p. 50)
Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string

Required: False

SimpleCriterionForJob

Specifies a property-based condition that determines whether an S3 bucket is included or excluded from a classification job.

comparator

The operator to use in the condition. Valid values are `EQ` (equals) and `NE` (not equals).

Type: [JobComparator](#) (p. 49)

Required: False

values

An array that lists one or more values to use in the condition. If you specify multiple values, Amazon Macie uses OR logic to join the values. Valid values for each supported property (key) are:

- `ACCOUNT_ID` - A string that represents the unique identifier for the AWS account that owns the bucket.
- `S3_BUCKET_EFFECTIVE_PERMISSION` - A string that represents an enumerated value that Macie defines for the [BucketPublicAccess.effectivePermission](#) property of a bucket.
- `S3_BUCKET_NAME` - A string that represents the name of a bucket.
- `S3_BUCKET_SHARED_ACCESS` - A string that represents an enumerated value that Macie defines for the [BucketMetadata.sharedAccess](#) property of a bucket.

Values are case sensitive. Also, Macie doesn't support use of partial values or wildcard characters in these values.

Type: Array of type string

Required: False

key

The property to use in the condition.

Type: [SimpleCriterionKeyForJob](#) (p. 54)

Required: False

SimpleCriterionKeyForJob

The property to use in a condition that determines whether an S3 bucket is included or excluded from a classification job. Valid values are:

`ACCOUNT_ID`
`S3_BUCKET_NAME`
`S3_BUCKET_EFFECTIVE_PERMISSION`

S3_BUCKET_SHARED_ACCESS

SimpleScopeTerm

Specifies a property-based condition that determines whether an S3 object is included or excluded from a classification job.

comparator

The operator to use in the condition. Valid values for each supported property (key) are:

- OBJECT_EXTENSION - EQ (equals) or NE (not equals)
- OBJECT_KEY - STARTS_WITH
- OBJECT_LAST_MODIFIED_DATE - Any operator except CONTAINS
- OBJECT_SIZE - Any operator except CONTAINS

Type: [JobComparator](#) (p. 49)

Required: False

values

An array that lists the values to use in the condition. If the value for the key property is OBJECT_EXTENSION or OBJECT_KEY, this array can specify multiple values and Amazon Macie uses OR logic to join the values. Otherwise, this array can specify only one value.

Valid values for each supported property (key) are:

- OBJECT_EXTENSION - A string that represents the file name extension of an object. For example: docx or pdf
- OBJECT_KEY - A string that represents the key prefix (folder name or path) of an object. For example: logs or awslogs/eventlogs. This value applies a condition to objects whose keys (names) begin with the specified value.
- OBJECT_LAST_MODIFIED_DATE - The date and time (in UTC and extended ISO 8601 format) when an object was created or last changed, whichever is latest. For example: 2020-09-28T14:31:13Z
- OBJECT_SIZE - An integer that represents the storage size (in bytes) of an object.

Macie doesn't support use of wildcard characters in these values. Also, string values are case sensitive.

Type: Array of type string

Required: False

key

The object property to use in the condition.

Type: [ScopeFilterKey](#) (p. 53)

Required: False

TagCriterionForJob

Specifies a tag-based condition that determines whether an S3 bucket is included or excluded from a classification job.

comparator

The operator to use in the condition. Valid values are `EQ` (equals) and `NE` (not equals).

Type: [JobComparator](#) (p. 49)

Required: False

tagValues

The tag keys, tag values, or tag key and value pairs to use in the condition.

Type: Array of type [TagCriterionPairForJob](#) (p. 56)

Required: False

TagCriterionPairForJob

Specifies a tag key, a tag value, or a tag key and value (as a pair) to use in a tag-based condition that determines whether an S3 bucket is included or excluded from a classification job. Tag keys and values are case sensitive. Also, Amazon Macie doesn't support use of partial values or wildcard characters in tag-based conditions.

value

The tag value to use in the condition.

Type: string

Required: False

key

The value for the tag key to use in the condition.

Type: string

Required: False

TagMap

A string-to-string map of key-value pairs that specifies the tags (keys and values) for a classification job, custom data identifier, findings filter, or member account.

key-value pairs

Type: string

TagScopeTerm

Specifies a tag-based condition that determines whether an S3 object is included or excluded from a classification job.

comparator

The operator to use in the condition. Valid values are `EQ` (equals) or `NE` (not equals).

Type: [JobComparator](#) (p. 49)

Required: False

tagValues

The tag keys or tag key and value pairs to use in the condition. To specify only tag keys in a condition, specify the keys in this array and set the value for each associated tag value to an empty string.

Type: Array of type [TagValuePair](#) (p. 57)

Required: False

key

The object property to use in the condition. The only valid value is `TAG`.

Type: string

Required: False

target

The type of object to apply the condition to.

Type: [TagTarget](#) (p. 57)

Required: False

TagTarget

The type of object to apply a tag-based condition to. Valid values are:

`S3_OBJECT`

TagValuePair

Specifies a tag key or tag key and value pair to use in a tag-based condition that determines whether an S3 object is included or excluded from a classification job. Tag keys and values are case sensitive. Also, Amazon Macie doesn't support use of partial values or wildcard characters in tag-based conditions.

value

The tag value, associated with the specified tag key (`key`), to use in the condition. To specify only a tag key for a condition, specify the tag key for the `key` property and set this value to an empty string.

Type: string

Required: False

key

The value for the tag key to use in the condition.

Type: string

Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string

Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string

Required: False

WeeklySchedule

Specifies a weekly recurrence pattern for running a classification job.

dayOfWeek

The day of the week when Amazon Macie runs the job.

Type: string

Required: False

Values: SUNDAY | MONDAY | TUESDAY | WEDNESDAY | THURSDAY | FRIDAY | SATURDAY

See also

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

CreateClassificationJob

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Classification Job Description

The Classification Job Description resource provides detailed information about the classification jobs for your account. It also provides access to the status of individual classification jobs. A *classification job*,

also referred to as a *sensitive data discovery job*, is a job that analyzes objects in Amazon Simple Storage Service (Amazon S3) buckets to determine whether the objects contain sensitive data.

You can use this resource to pause, resume, or cancel a classification job, or retrieve detailed information about a classification job. To retrieve information about more than one classification job, use the [Classification Job List \(p. 81\)](#) resource.

URI

/jobs/*jobId*

HTTP methods

GET

Operation ID: DescribeClassificationJob

Retrieves the status and settings for a classification job.

Path parameters

Name	Type	Required	Description
<i>jobId</i>	String	True	The unique identifier for the classification job.

Responses

Status code	Response model	Description
200	DescribeClassificationJobResponse	The request succeeded.
400	ValidationException (p. 63)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 63)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 63)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 63)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 64)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 64)	The request failed because you sent too many requests during a certain amount of time.

Status code	Response model	Description
500	InternalServerError (p. 64)	The request failed due to an unknown internal server error, exception, or failure.

PATCH

Operation ID: UpdateClassificationJob

Changes the status of a classification job.

Path parameters

Name	Type	Required	Description
<i>jobId</i>	String	True	The unique identifier for the classification job.

Responses

Status code	Response model	Description
200	Empty Schema (p. 63)	The request succeeded. The job's status was changed and there isn't any content to include in the body of the response (No Content).
400	ValidationException (p. 63)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 63)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 63)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 63)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 64)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 64)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerError (p. 64)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

PATCH schema

```
{
  "jobStatus": enum
}
```

Response bodies

DescribeClassificationJobResponse schema

```
{
  "userPausedDetails": {
    "jobImminentExpirationHealthEventArn": "string",
    "jobExpiresAt": "string",
    "jobPausedAt": "string"
  },
  "jobStatus": enum,
  "samplingPercentage": integer,
  "clientToken": "string",
  "managedDataIdentifierIds": [
    "string"
  ],
  "description": "string",
  "jobArn": "string",
  "initialRun": boolean,
  "lastRunErrorStatus": {
    "code": enum
  },
  "managedDataIdentifierSelector": enum,
  "tags": {
  },
  "customDataIdentifierIds": [
    "string"
  ],
  "scheduleFrequency": {
    "dailySchedule": {
    },
    "weeklySchedule": {
      "dayOfWeek": enum
    },
    "monthlySchedule": {
      "dayOfMonth": integer
    }
  },
  "jobId": "string",
  "createdAt": "string",
  "lastRunTime": "string",
  "name": "string",
  "jobType": enum,
  "s3JobDefinition": {
    "bucketDefinitions": [
      {
        "accountId": "string",
        "buckets": [
          "string"
        ]
      }
    ]
  }
}
```

```

],
"bucketCriteria": {
  "excludes": {
    "and": [
      {
        "tagCriterion": {
          "comparator": enum,
          "tagValues": [
            {
              "value": "string",
              "key": "string"
            }
          ]
        },
        "simpleCriterion": {
          "comparator": enum,
          "values": [
            "string"
          ],
          "key": enum
        }
      }
    ]
  },
  "includes": {
    "and": [
      {
        "tagCriterion": {
          "comparator": enum,
          "tagValues": [
            {
              "value": "string",
              "key": "string"
            }
          ]
        },
        "simpleCriterion": {
          "comparator": enum,
          "values": [
            "string"
          ],
          "key": enum
        }
      }
    ]
  }
},
"scoping": {
  "excludes": {
    "and": [
      {
        "simpleScopeTerm": {
          "comparator": enum,
          "values": [
            "string"
          ],
          "key": enum
        },
        "tagScopeTerm": {
          "comparator": enum,
          "tagValues": [
            {
              "value": "string",
              "key": "string"
            }
          ]
        }
      }
    ]
  }
}

```

```
        "key": "string",
        "target": enum
      }
    ]
  },
  "includes": {
    "and": [
      {
        "simpleScopeTerm": {
          "comparator": enum,
          "values": [
            "string"
          ],
          "key": enum
        },
        "tagScopeTerm": {
          "comparator": enum,
          "tagValues": [
            {
              "value": "string",
              "key": "string"
            }
          ],
          "key": "string",
          "target": enum
        }
      ]
    ]
  },
  "statistics": {
    "numberOfRuns": number,
    "approximateNumberOfObjectsToProcess": number
  }
}
```

Empty Schema schema

```
{
}
```

ValidationException schema

```
{
  "message": "string"
}
```

ServiceQuotaExceededException schema

```
{
  "message": "string"
}
```

AccessDeniedException schema

```
{
```

```
"message": "string"
}
```

ResourceNotFoundException schema

```
{
  "message": "string"
}
```

ConflictException schema

```
{
  "message": "string"
}
```

ThrottlingException schema

```
{
  "message": "string"
}
```

InternalServerError schema

```
{
  "message": "string"
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

CriteriaBlockForJob

Specifies one or more property- and tag-based conditions that define criteria for including or excluding S3 buckets from a classification job.

and

An array of conditions, one for each condition that determines which buckets to include or exclude from the job. If you specify more than one condition, Amazon Macie uses AND logic to join the conditions.

Type: Array of type [CriteriaForJob](#) (p. 65)

Required: False

CriteriaForJob

Specifies a property- or tag-based condition that defines criteria for including or excluding S3 buckets from a classification job.

tagCriterion

A tag-based condition that defines an operator and tag keys, tag values, or tag key and value pairs for including or excluding buckets from the job.

Type: [TagCriterionForJob](#) (p. 76)

Required: False

simpleCriterion

A property-based condition that defines a property, operator, and one or more values for including or excluding buckets from the job.

Type: [SimpleCriterionForJob](#) (p. 74)

Required: False

DailySchedule

Specifies that a classification job runs once a day, every day. This is an empty object.

DescribeClassificationJobResponse

Provides information about a classification job, including the current configuration settings and status of the job.

userPausedDetails

If the current status of the job is `USER_PAUSED`, specifies when the job was paused and when the job or job run will expire and be cancelled if it isn't resumed. This value is present only if the value for `jobStatus` is `USER_PAUSED`.

Type: [UserPausedDetails](#) (p. 79)

Required: False

jobStatus

The current status of the job. Possible values are:

- **CANCELLED** - You cancelled the job or, if it's a one-time job, you paused the job and didn't resume it within 30 days.
- **COMPLETE** - For a one-time job, Amazon Macie finished processing the data specified for the job. This value doesn't apply to recurring jobs.
- **IDLE** - For a recurring job, the previous scheduled run is complete and the next scheduled run is pending. This value doesn't apply to one-time jobs.
- **PAUSED** - Macie started running the job but additional processing would exceed the monthly sensitive data discovery quota for your account or one or more member accounts that the job analyzes data for.
- **RUNNING** - For a one-time job, the job is in progress. For a recurring job, a scheduled run is in progress.
- **USER_PAUSED** - You paused the job. If you paused the job while it had a status of **RUNNING** and you don't resume it within 30 days of pausing it, the job or job run will expire and be cancelled, depending on the job's type. To check the expiration date, refer to the `UserPausedDetails.jobExpiresAt` property.

Type: [JobStatus](#) (p. 70)

Required: False

samplingPercentage

The sampling depth, as a percentage, that determines the percentage of eligible objects that the job analyzes.

Type: integer

Required: False

Format: int32

clientToken

The token that was provided to ensure the idempotency of the request to create the job.

Type: string

Required: False

managedDataIdentifierIds

An array of unique identifiers, one for each managed data identifier that the job is explicitly configured to include (use) or exclude (not use) when it analyzes data. Inclusion or exclusion depends on the managed data identifier selection type specified for the job (`managedDataIdentifierSelector`). This value is null if the job's managed data identifier selection type is **ALL** or the job uses only custom data identifiers (`customDataIdentifierIds`) to analyze data.

Type: Array of type string

Required: False

description

The custom description of the job.

Type: string
Required: False

jobArn

The Amazon Resource Name (ARN) of the job.

Type: string
Required: False

initialRun

For a recurring job, specifies whether you configured the job to analyze all existing, eligible objects immediately after the job was created (`true`). If you configured the job to analyze only those objects that were created or changed after the job was created and before the job's first scheduled run, this value is `false`. This value is also `false` for a one-time job.

Type: boolean
Required: False

lastRunErrorStatus

Specifies whether any account- or bucket-level access errors occurred when the job ran. For a recurring job, this value indicates the error status of the job's most recent run.

Type: [LastRunErrorStatus](#) (p. 71)
Required: False

managedDataIdentifierSelector

The selection type that determines which managed data identifiers the job uses to analyze data. Possible values are:

- **ALL** - Use all the managed data identifiers that Amazon Macie provides.
- **EXCLUDE** - Use all the managed data identifiers that Macie provides except the managed data identifiers specified by the `managedDataIdentifierIds` property.
- **INCLUDE** - Use only the managed data identifiers specified by the `managedDataIdentifierIds` property.
- **NONE** - Don't use any managed data identifiers.

If this value is null, the job uses all managed data identifiers. If this value is null, **ALL**, or **EXCLUDE** for a recurring job, the job also uses new managed data identifiers as they are released.

Type: [ManagedDataIdentifierSelector](#) (p. 71)
Required: False

tags

A map of key-value pairs that specifies which tags (keys and values) are associated with the classification job.

Type: [TagMap](#) (p. 77)
Required: False

customDataIdentifierIds

An array of unique identifiers, one for each custom data identifier that the job uses to analyze data. This value is null if the job uses only managed data identifiers to analyze data.

Type: Array of type string

Required: False

scheduleFrequency

The recurrence pattern for running the job. This value is null if the job is configured to run only once.

Type: [JobScheduleFrequency \(p. 69\)](#)

Required: False

jobId

The unique identifier for the job.

Type: string

Required: False

createdAt

The date and time, in UTC and extended ISO 8601 format, when the job was created.

Type: string

Required: False

Format: date-time

lastRunTime

The date and time, in UTC and extended ISO 8601 format, when the job started. If the job is a recurring job, this value indicates when the most recent run started.

Type: string

Required: False

Format: date-time

name

The custom name of the job.

Type: string

Required: False

jobType

The schedule for running the job. Possible values are:

- `ONE_TIME` - The job runs only once.
- `SCHEDULED` - The job runs on a daily, weekly, or monthly basis. The `scheduleFrequency` property indicates the recurrence pattern for the job.

Type: [JobType \(p. 71\)](#)

Required: False

s3JobDefinition

The S3 buckets that contain the objects to analyze, and the scope of that analysis.

Type: [S3JobDefinition](#) (p. 73)

Required: False

statistics

The number of times that the job has run and processing statistics for the job's current run.

Type: [Statistics](#) (p. 76)

Required: False

Empty

The request succeeded and there isn't any content to include in the body of the response (No Content).

InternalServerErrorException

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string

Required: False

JobComparator

The operator to use in a condition. Valid values are:

EQ
GT
GTE
LT
LTE
NE
CONTAINS
STARTS_WITH

JobScheduleFrequency

Specifies the recurrence pattern for running a classification job.

dailySchedule

Specifies a daily recurrence pattern for running the job.

Type: [DailySchedule](#) (p. 65)

Required: False

weeklySchedule

Specifies a weekly recurrence pattern for running the job.

Type: [WeeklySchedule](#) (p. 80)

Required: False

monthlySchedule

Specifies a monthly recurrence pattern for running the job.

Type: [MonthlySchedule](#) (p. 71)

Required: False

JobScopeTerm

Specifies a property- or tag-based condition that defines criteria for including or excluding S3 objects from a classification job. A `JobScopeTerm` object can contain only one `simpleScopeTerm` object or one `tagScopeTerm` object.

simpleScopeTerm

A property-based condition that defines a property, operator, and one or more values for including or excluding objects from the job.

Type: [SimpleScopeTerm](#) (p. 75)

Required: False

tagScopeTerm

A tag-based condition that defines the operator and tag keys or tag key and value pairs for including or excluding objects from the job.

Type: [TagScopeTerm](#) (p. 77)

Required: False

JobScopingBlock

Specifies one or more property- and tag-based conditions that define criteria for including or excluding S3 objects from a classification job.

and

An array of conditions, one for each property- or tag-based condition that determines which objects to include or exclude from the job. If you specify more than one condition, Amazon Macie uses AND logic to join the conditions.

Type: Array of type [JobScopeTerm](#) (p. 70)

Required: False

JobStatus

The status of a classification job. Possible values are:

RUNNING
PAUSED
CANCELLED
COMPLETE
IDLE
USER_PAUSED

JobType

The schedule for running a classification job. Valid values are:

ONE_TIME
SCHEDULED

LastRunErrorStatus

Specifies whether any account- or bucket-level access errors occurred when a classification job ran. For information about using logging data to investigate these errors, see [Monitoring sensitive data discovery jobs](#) in the *Amazon Macie User Guide*.

code

Specifies whether any account- or bucket-level access errors occurred when the job ran. For a recurring job, this value indicates the error status of the job's most recent run. Possible values are:

- ERROR - One or more errors occurred. Amazon Macie didn't process all the data specified for the job.
- NONE - No errors occurred. Macie processed all the data specified for the job.

Type: [LastRunErrorStatusCode](#) (p. 71)

Required: False

LastRunErrorStatusCode

Specifies whether any account- or bucket-level access errors occurred during the run of a one-time classification job or the most recent run of a recurring classification job. Possible values are:

NONE
ERROR

ManagedDataIdentifierSelector

The selection type that determines which managed data identifiers a classification job uses to analyze data. Valid values are:

ALL
EXCLUDE
INCLUDE
NONE

MonthlySchedule

Specifies a monthly recurrence pattern for running a classification job.

dayOfMonth

The numeric day of the month when Amazon Macie runs the job. This value can be an integer from 1 through 31.

If this value exceeds the number of days in a certain month, Macie doesn't run the job that month. Macie runs the job only during months that have the specified day. For example, if this value is 31 and a month has only 30 days, Macie doesn't run the job that month. To run the job every month, specify a value that's less than 29.

Type: integer
Required: False
Format: int32

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string
Required: False

S3BucketCriteriaForJob

Specifies property- and tag-based conditions that define criteria for including or excluding S3 buckets from a classification job. Exclude conditions take precedence over include conditions.

excludes

The property- and tag-based conditions that determine which buckets to exclude from the job.

Type: [CriteriaBlockForJob](#) (p. 65)
Required: False

includes

The property- and tag-based conditions that determine which buckets to include in the job.

Type: [CriteriaBlockForJob](#) (p. 65)
Required: False

S3BucketDefinitionForJob

Specifies an AWS account that owns S3 buckets for a classification job to analyze, and one or more specific buckets to analyze for that account.

accountId

The unique identifier for the AWS account that owns the buckets.

Type: string

Required: True

buckets

An array that lists the names of the buckets.

Type: Array of type string

Required: True

S3JobDefinition

Specifies which S3 buckets contain the objects that a classification job analyzes, and the scope of that analysis. The bucket specification can be static (`bucketDefinitions`) or dynamic (`bucketCriteria`). If it's static, the job analyzes objects in the same predefined set of buckets each time the job runs. If it's dynamic, the job analyzes objects in any buckets that match the specified criteria each time the job starts to run.

bucketDefinitions

An array of objects, one for each AWS account that owns specific S3 buckets to analyze. Each object specifies the account ID for an account and one or more buckets to analyze for that account. A job's definition can contain a `bucketDefinitions` array or a `bucketCriteria` object, not both.

Type: Array of type [S3BucketDefinitionForJob](#) (p. 72)

Required: False

bucketCriteria

The property- and tag-based conditions that determine which S3 buckets to include or exclude from the analysis. Each time the job runs, the job uses these criteria to determine which buckets contain objects to analyze. A job's definition can contain a `bucketCriteria` object or a `bucketDefinitions` array, not both.

Type: [S3BucketCriteriaForJob](#) (p. 72)

Required: False

scoping

The property- and tag-based conditions that determine which S3 objects to include or exclude from the analysis. Each time the job runs, the job uses these criteria to determine which objects to analyze.

Type: [Scoping](#) (p. 74)

Required: False

ScopeFilterKey

The property to use in a condition that determines whether an S3 object is included or excluded from a classification job. Valid values are:

```
OBJECT_EXTENSION
OBJECT_LAST_MODIFIED_DATE
OBJECT_SIZE
OBJECT_KEY
```


Scoping

Specifies one or more property- and tag-based conditions that define criteria for including or excluding S3 objects from a classification job. Exclude conditions take precedence over include conditions.

excludes

The property- and tag-based conditions that determine which objects to exclude from the analysis.

Type: [JobScopingBlock](#) (p. 70)

Required: False

includes

The property- and tag-based conditions that determine which objects to include in the analysis.

Type: [JobScopingBlock](#) (p. 70)

Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string

Required: False

SimpleCriterionForJob

Specifies a property-based condition that determines whether an S3 bucket is included or excluded from a classification job.

comparator

The operator to use in the condition. Valid values are `EQ` (equals) and `NE` (not equals).

Type: [JobComparator](#) (p. 69)

Required: False

values

An array that lists one or more values to use in the condition. If you specify multiple values, Amazon Macie uses OR logic to join the values. Valid values for each supported property (key) are:

- `ACCOUNT_ID` - A string that represents the unique identifier for the AWS account that owns the bucket.
- `S3_BUCKET_EFFECTIVE_PERMISSION` - A string that represents an enumerated value that Macie defines for the [BucketPublicAccess.effectivePermission](#) property of a bucket.
- `S3_BUCKET_NAME` - A string that represents the name of a bucket.
- `S3_BUCKET_SHARED_ACCESS` - A string that represents an enumerated value that Macie defines for the [BucketMetadata.sharedAccess](#) property of a bucket.

Values are case sensitive. Also, Macie doesn't support use of partial values or wildcard characters in these values.

Type: Array of type string
Required: False

key

The property to use in the condition.

Type: [SimpleCriterionKeyForJob](#) (p. 75)
Required: False

SimpleCriterionKeyForJob

The property to use in a condition that determines whether an S3 bucket is included or excluded from a classification job. Valid values are:

```
ACCOUNT_ID
S3_BUCKET_NAME
S3_BUCKET_EFFECTIVE_PERMISSION
S3_BUCKET_SHARED_ACCESS
```

SimpleScopeTerm

Specifies a property-based condition that determines whether an S3 object is included or excluded from a classification job.

comparator

The operator to use in the condition. Valid values for each supported property (key) are:

- OBJECT_EXTENSION - EQ (equals) or NE (not equals)
- OBJECT_KEY - STARTS_WITH
- OBJECT_LAST_MODIFIED_DATE - Any operator except CONTAINS
- OBJECT_SIZE - Any operator except CONTAINS

Type: [JobComparator](#) (p. 69)
Required: False

values

An array that lists the values to use in the condition. If the value for the key property is OBJECT_EXTENSION or OBJECT_KEY, this array can specify multiple values and Amazon Macie uses OR logic to join the values. Otherwise, this array can specify only one value.

Valid values for each supported property (key) are:

- OBJECT_EXTENSION - A string that represents the file name extension of an object. For example: docx or pdf
- OBJECT_KEY - A string that represents the key prefix (folder name or path) of an object. For example: logs or awslogs/eventlogs. This value applies a condition to objects whose keys (names) begin with the specified value.

- `OBJECT_LAST_MODIFIED_DATE` - The date and time (in UTC and extended ISO 8601 format) when an object was created or last changed, whichever is latest. For example: 2020-09-28T14:31:13Z
- `OBJECT_SIZE` - An integer that represents the storage size (in bytes) of an object.

Macie doesn't support use of wildcard characters in these values. Also, string values are case sensitive.

Type: Array of type string
Required: False

key

The object property to use in the condition.

Type: [ScopeFilterKey](#) (p. 73)
Required: False

Statistics

Provides processing statistics for a classification job.

numberOfRuns

The number of times that the job has run.

Type: number
Required: False

approximateNumberOfObjectsToProcess

The approximate number of objects that the job has yet to process during its current run.

Type: number
Required: False

TagCriterionForJob

Specifies a tag-based condition that determines whether an S3 bucket is included or excluded from a classification job.

comparator

The operator to use in the condition. Valid values are `EQ` (equals) and `NE` (not equals).

Type: [JobComparator](#) (p. 69)
Required: False

tagValues

The tag keys, tag values, or tag key and value pairs to use in the condition.

Type: Array of type [TagCriterionPairForJob](#) (p. 77)
Required: False

TagCriterionPairForJob

Specifies a tag key, a tag value, or a tag key and value (as a pair) to use in a tag-based condition that determines whether an S3 bucket is included or excluded from a classification job. Tag keys and values are case sensitive. Also, Amazon Macie doesn't support use of partial values or wildcard characters in tag-based conditions.

value

The tag value to use in the condition.

Type: string
Required: False

key

The value for the tag key to use in the condition.

Type: string
Required: False

TagMap

A string-to-string map of key-value pairs that specifies the tags (keys and values) for a classification job, custom data identifier, findings filter, or member account.

key-value pairs

Type: string

TagScopeTerm

Specifies a tag-based condition that determines whether an S3 object is included or excluded from a classification job.

comparator

The operator to use in the condition. Valid values are `EQ` (equals) or `NE` (not equals).

Type: [JobComparator](#) (p. 69)
Required: False

tagValues

The tag keys or tag key and value pairs to use in the condition. To specify only tag keys in a condition, specify the keys in this array and set the value for each associated tag value to an empty string.

Type: Array of type [TagValuePair](#) (p. 78)
Required: False

key

The object property to use in the condition. The only valid value is `TAG`.

Type: string
Required: False

target

The type of object to apply the condition to.

Type: [TagTarget](#) (p. 78)

Required: False

TagTarget

The type of object to apply a tag-based condition to. Valid values are:

`S3_OBJECT`

TagValuePair

Specifies a tag key or tag key and value pair to use in a tag-based condition that determines whether an S3 object is included or excluded from a classification job. Tag keys and values are case sensitive. Also, Amazon Macie doesn't support use of partial values or wildcard characters in tag-based conditions.

value

The tag value, associated with the specified tag key (`key`), to use in the condition. To specify only a tag key for a condition, specify the tag key for the `key` property and set this value to an empty string.

Type: string

Required: False

key

The value for the tag key to use in the condition.

Type: string

Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string

Required: False

UpdateClassificationJobRequest

Changes the status of a classification job. For more information about pausing, resuming, or cancelling jobs, see [Managing sensitive data discovery jobs](#) in the *Amazon Macie User Guide*.

jobStatus

The new status for the job. Valid values are:

- **CANCELLED** - Stops the job permanently and cancels it. This value is valid only if the job's current status is `IDLE`, `PAUSED`, `RUNNING`, or `USER_PAUSED`.

If you specify this value and the job's current status is `RUNNING`, Amazon Macie immediately begins to stop all processing tasks for the job. You can't resume or restart a job after you cancel it.

- **RUNNING** - Resumes the job. This value is valid only if the job's current status is `USER_PAUSED`.

If you paused the job while it was actively running and you specify this value less than 30 days after you paused the job, Macie immediately resumes processing from the point where you paused the job. Otherwise, Macie resumes the job according to the schedule and other settings for the job.

- **USER_PAUSED** - Pauses the job temporarily. This value is valid only if the job's current status is `IDLE`, `PAUSED`, or `RUNNING`. If you specify this value and the job's current status is `RUNNING`, Macie immediately begins to pause all processing tasks for the job.

If you pause a one-time job and you don't resume it within 30 days, the job expires and Macie cancels the job. If you pause a recurring job when its status is `RUNNING` and you don't resume it within 30 days, the job run expires and Macie cancels the run. To check the expiration date, refer to the `UserPausedDetails.jobExpiresAt` property.

Type: [JobStatus](#) (p. 70)

Required: True

UserPausedDetails

Provides information about when a classification job was paused. For a one-time job, this object also specifies when the job will expire and be cancelled if it isn't resumed. For a recurring job, this object also specifies when the paused job run will expire and be cancelled if it isn't resumed. This object is present only if a job's current status (`jobStatus`) is `USER_PAUSED`. The information in this object applies only to a job that was paused while it had a status of `RUNNING`.

jobImminentExpirationHealthEventArn

The Amazon Resource Name (ARN) of the AWS Health event that Amazon Macie sent to notify you of the job or job run's pending expiration and cancellation. This value is null if a job has been paused for less than 23 days.

Type: string

Required: False

jobExpiresAt

The date and time, in UTC and extended ISO 8601 format, when the job or job run will expire and be cancelled if you don't resume it first.

Type: string

Required: False

Format: date-time

jobPausedAt

The date and time, in UTC and extended ISO 8601 format, when you paused the job.

Type: string

Required: False

Format: date-time

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string

Required: False

WeeklySchedule

Specifies a weekly recurrence pattern for running a classification job.

dayOfWeek

The day of the week when Amazon Macie runs the job.

Type: string

Required: False

Values: SUNDAY | MONDAY | TUESDAY | WEDNESDAY | THURSDAY | FRIDAY | SATURDAY

See also

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

DescribeClassificationJob

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

UpdateClassificationJob

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)

- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Classification Job List

The Classification Job List resource provides a subset of information about the classification jobs for your account. A *classification job*, also referred to as a *sensitive data discovery job*, is a job that analyzes objects in Amazon Simple Storage Service (Amazon S3) buckets to determine whether the objects contain sensitive data.

You can use the Classification Job List resource to retrieve a subset of information about your classification jobs. To customize and refine your request, you can use the supported parameters to specify whether and how to filter, sort, and paginate the results. To retrieve additional information about a particular classification job, use the [Classification Job Description \(p. 58\)](#) resource.

URI

/jobs/list

HTTP methods

POST

Operation ID: ListClassificationJobs

Retrieves a subset of information about one or more classification jobs.

Responses

Status code	Response model	Description
200	ListClassificationJobsResponse (p. 83)	The request succeeded.
400	ValidationException (p. 83)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 83)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 84)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 84)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 84)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 84)	The request failed because you sent too many requests during a certain amount of time.

Status code	Response model	Description
500	InternalServerErrorException (p.114)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

POST schema

```
{
  "filterCriteria": {
    "excludes": [
      {
        "comparator": enum,
        "values": [
          "string"
        ],
        "key": enum
      }
    ],
    "includes": [
      {
        "comparator": enum,
        "values": [
          "string"
        ],
        "key": enum
      }
    ]
  },
  "nextToken": "string",
  "maxResults": integer,
  "sortCriteria": {
    "orderBy": enum,
    "attributeName": enum
  }
}
```

Response bodies

ListClassificationJobsResponse schema

```
{
  "nextToken": "string",
  "items": [
    {
      "userPausedDetails": {
        "jobImminentExpirationHealthEventArn": "string",
        "jobExpiresAt": "string",
        "jobPausedAt": "string"
      },
      "bucketDefinitions": [
        {
          "accountId": "string",
          "buckets": [
            "string"
          ]
        }
      ]
    }
  ]
}
```

```

    ]
  }
],
"jobId": "string",
"createdAt": "string",
"jobStatus": enum,
"name": "string",
"bucketCriteria": {
  "excludes": {
    "and": [
      {
        "tagCriterion": {
          "comparator": enum,
          "tagValues": [
            {
              "value": "string",
              "key": "string"
            }
          ]
        },
        "simpleCriterion": {
          "comparator": enum,
          "values": [
            "string"
          ],
          "key": enum
        }
      }
    ]
  },
  "includes": {
    "and": [
      {
        "tagCriterion": {
          "comparator": enum,
          "tagValues": [
            {
              "value": "string",
              "key": "string"
            }
          ]
        },
        "simpleCriterion": {
          "comparator": enum,
          "values": [
            "string"
          ],
          "key": enum
        }
      }
    ]
  }
},
"jobType": enum,
"lastRunErrorStatus": {
  "code": enum
}
}
]
}

```

ValidationException schema

```

{

```

```
"message": "string"
}
```

ServiceQuotaExceededException schema

```
{
  "message": "string"
}
```

AccessDeniedException schema

```
{
  "message": "string"
}
```

ResourceNotFoundException schema

```
{
  "message": "string"
}
```

ConflictException schema

```
{
  "message": "string"
}
```

ThrottlingException schema

```
{
  "message": "string"
}
```

InternalServerError schema

```
{
  "message": "string"
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

CriteriaBlockForJob

Specifies one or more property- and tag-based conditions that define criteria for including or excluding S3 buckets from a classification job.

and

An array of conditions, one for each condition that determines which buckets to include or exclude from the job. If you specify more than one condition, Amazon Macie uses AND logic to join the conditions.

Type: Array of type [CriteriaForJob](#) (p. 85)

Required: False

CriteriaForJob

Specifies a property- or tag-based condition that defines criteria for including or excluding S3 buckets from a classification job.

tagCriterion

A tag-based condition that defines an operator and tag keys, tag values, or tag key and value pairs for including or excluding buckets from the job.

Type: [TagCriterionForJob](#) (p. 93)

Required: False

simpleCriterion

A property-based condition that defines a property, operator, and one or more values for including or excluding buckets from the job.

Type: [SimpleCriterionForJob](#) (p. 92)

Required: False

InternalServerError

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string
Required: False

JobComparator

The operator to use in a condition. Valid values are:

EQ
GT
GTE
LT
LTE
NE
CONTAINS
STARTS_WITH

JobStatus

The status of a classification job. Possible values are:

RUNNING
PAUSED
CANCELLED
COMPLETE
IDLE
USER_PAUSED

JobSummary

Provides information about a classification job, including the current status of the job.

userPausedDetails

If the current status of the job is `USER_PAUSED`, specifies when the job was paused and when the job or job run will expire and be cancelled if it isn't resumed. This value is present only if the value for `jobStatus` is `USER_PAUSED`.

Type: [UserPausedDetails](#) (p. 94)
Required: False

bucketDefinitions

An array of objects, one for each AWS account that owns specific S3 buckets for the job to analyze. Each object specifies the account ID for an account and one or more buckets to analyze for that account. A job's definition can contain a `bucketDefinitions` array or a `bucketCriteria` object, not both.

Type: Array of type [S3BucketDefinitionForJob](#) (p. 91)
Required: False

jobId

The unique identifier for the job.

Type: string
Required: False

createdAt

The date and time, in UTC and extended ISO 8601 format, when the job was created.

Type: string
Required: False
Format: date-time

jobStatus

The current status of the job. Possible values are:

- **CANCELLED** - You cancelled the job or, if it's a one-time job, you paused the job and didn't resume it within 30 days.
- **COMPLETE** - For a one-time job, Amazon Macie finished processing the data specified for the job. This value doesn't apply to recurring jobs.
- **IDLE** - For a recurring job, the previous scheduled run is complete and the next scheduled run is pending. This value doesn't apply to one-time jobs.
- **PAUSED** - Macie started running the job but additional processing would exceed the monthly sensitive data discovery quota for your account or one or more member accounts that the job analyzes data for.
- **RUNNING** - For a one-time job, the job is in progress. For a recurring job, a scheduled run is in progress.
- **USER_PAUSED** - You paused the job. If you paused the job while it had a status of **RUNNING** and you don't resume it within 30 days of pausing it, the job or job run will expire and be cancelled, depending on the job's type. To check the expiration date, refer to the `UserPausedDetails.jobExpiresAt` property.

Type: [JobStatus](#) (p. 86)
Required: False

name

The custom name of the job.

Type: string
Required: False

bucketCriteria

The property- and tag-based conditions that determine which S3 buckets are included or excluded from the job's analysis. Each time the job runs, the job uses these criteria to determine which buckets to analyze. A job's definition can contain a `bucketCriteria` object or a `bucketDefinitions` array, not both.

Type: [S3BucketCriteriaForJob](#) (p. 91)
Required: False

jobType

The schedule for running the job. Possible values are:

- `ONE_TIME` - The job runs only once.
- `SCHEDULED` - The job runs on a daily, weekly, or monthly basis.

Type: [JobType](#) (p. 88)

Required: False

lastRunErrorStatus

Specifies whether any account- or bucket-level access errors occurred when the job ran. For a recurring job, this value indicates the error status of the job's most recent run.

Type: [LastRunErrorStatus](#) (p. 88)

Required: False

JobType

The schedule for running a classification job. Valid values are:

`ONE_TIME`
`SCHEDULED`

LastRunErrorStatus

Specifies whether any account- or bucket-level access errors occurred when a classification job ran. For information about using logging data to investigate these errors, see [Monitoring sensitive data discovery jobs](#) in the *Amazon Macie User Guide*.

code

Specifies whether any account- or bucket-level access errors occurred when the job ran. For a recurring job, this value indicates the error status of the job's most recent run. Possible values are:

- `ERROR` - One or more errors occurred. Amazon Macie didn't process all the data specified for the job.
- `NONE` - No errors occurred. Macie processed all the data specified for the job.

Type: [LastRunErrorStatusCode](#) (p. 88)

Required: False

LastRunErrorStatusCode

Specifies whether any account- or bucket-level access errors occurred during the run of a one-time classification job or the most recent run of a recurring classification job. Possible values are:

`NONE`
`ERROR`

ListClassificationJobsRequest

Specifies criteria for filtering, sorting, and paginating the results of a request for information about classification jobs.

filterCriteria

The criteria to use to filter the results.

Type: [ListJobsFilterCriteria](#) (p. 89)

Required: False

nextToken

The `nextToken` string that specifies which page of results to return in a paginated response.

Type: string

Required: False

maxResults

The maximum number of items to include in each page of the response.

Type: integer

Required: False

Format: int32

sortCriteria

The criteria to use to sort the results.

Type: [ListJobsSortCriteria](#) (p. 91)

Required: False

ListClassificationJobsResponse

Provides the results of a request for information about one or more classification jobs.

nextToken

The string to use in a subsequent request to get the next page of results in a paginated response. This value is null if there are no additional pages.

Type: string

Required: False

items

An array of objects, one for each job that meets the filter criteria specified in the request.

Type: Array of type [JobSummary](#) (p. 86)

Required: False

ListJobsFilterCriteria

Specifies criteria for filtering the results of a request for information about classification jobs.

excludes

An array of objects, one for each condition that determines which jobs to exclude from the results.

Type: Array of type [ListJobsFilterTerm](#) (p. 90)
Required: False

includes

An array of objects, one for each condition that determines which jobs to include in the results.

Type: Array of type [ListJobsFilterTerm](#) (p. 90)
Required: False

ListJobsFilterKey

The property to use to filter the results. Valid values are:

jobType
jobStatus
createdAt
name

ListJobsFilterTerm

Specifies a condition that filters the results of a request for information about classification jobs. Each condition consists of a property, an operator, and one or more values.

comparator

The operator to use to filter the results.

Type: [JobComparator](#) (p. 86)
Required: False

values

An array that lists one or more values to use to filter the results.

Type: Array of type string
Required: False

key

The property to use to filter the results.

Type: [ListJobsFilterKey](#) (p. 90)
Required: False

ListJobsSortAttributeName

The property to sort the results by. Valid values are:

createdAt
jobStatus
name
jobType

ListJobsSortCriteria

Specifies criteria for sorting the results of a request for information about classification jobs.

orderBy

The sort order to apply to the results, based on the value for the property specified by the `attributeName` property. Valid values are: `ASC`, sort the results in ascending order; and, `DESC`, sort the results in descending order.

Type: string
Required: False
Values: `ASC` | `DESC`

attributeName

The property to sort the results by.

Type: [ListJobsSortAttributeName](#) (p. 90)
Required: False

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string
Required: False

S3BucketCriteriaForJob

Specifies property- and tag-based conditions that define criteria for including or excluding S3 buckets from a classification job. Exclude conditions take precedence over include conditions.

excludes

The property- and tag-based conditions that determine which buckets to exclude from the job.

Type: [CriteriaBlockForJob](#) (p. 85)
Required: False

includes

The property- and tag-based conditions that determine which buckets to include in the job.

Type: [CriteriaBlockForJob](#) (p. 85)
Required: False

S3BucketDefinitionForJob

Specifies an AWS account that owns S3 buckets for a classification job to analyze, and one or more specific buckets to analyze for that account.

accountId

The unique identifier for the AWS account that owns the buckets.

Type: string
Required: True

buckets

An array that lists the names of the buckets.

Type: Array of type string
Required: True

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string
Required: False

SimpleCriterionForJob

Specifies a property-based condition that determines whether an S3 bucket is included or excluded from a classification job.

comparator

The operator to use in the condition. Valid values are `EQ` (equals) and `NE` (not equals).

Type: [JobComparator](#) (p. 86)
Required: False

values

An array that lists one or more values to use in the condition. If you specify multiple values, Amazon Macie uses OR logic to join the values. Valid values for each supported property (key) are:

- `ACCOUNT_ID` - A string that represents the unique identifier for the AWS account that owns the bucket.
- `S3_BUCKET_EFFECTIVE_PERMISSION` - A string that represents an enumerated value that Macie defines for the [BucketPublicAccess.effectivePermission](#) property of a bucket.
- `S3_BUCKET_NAME` - A string that represents the name of a bucket.
- `S3_BUCKET_SHARED_ACCESS` - A string that represents an enumerated value that Macie defines for the [BucketMetadata.sharedAccess](#) property of a bucket.

Values are case sensitive. Also, Macie doesn't support use of partial values or wildcard characters in these values.

Type: Array of type string
Required: False

key

The property to use in the condition.

Type: [SimpleCriterionKeyForJob](#) (p. 93)

Required: False

SimpleCriterionKeyForJob

The property to use in a condition that determines whether an S3 bucket is included or excluded from a classification job. Valid values are:

```
ACCOUNT_ID
S3_BUCKET_NAME
S3_BUCKET_EFFECTIVE_PERMISSION
S3_BUCKET_SHARED_ACCESS
```

TagCriterionForJob

Specifies a tag-based condition that determines whether an S3 bucket is included or excluded from a classification job.

comparator

The operator to use in the condition. Valid values are `EQ` (equals) and `NE` (not equals).

Type: [JobComparator](#) (p. 86)

Required: False

tagValues

The tag keys, tag values, or tag key and value pairs to use in the condition.

Type: Array of type [TagCriterionPairForJob](#) (p. 93)

Required: False

TagCriterionPairForJob

Specifies a tag key, a tag value, or a tag key and value (as a pair) to use in a tag-based condition that determines whether an S3 bucket is included or excluded from a classification job. Tag keys and values are case sensitive. Also, Amazon Macie doesn't support use of partial values or wildcard characters in tag-based conditions.

value

The tag value to use in the condition.

Type: string

Required: False

key

The value for the tag key to use in the condition.

Type: string

Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string

Required: False

UserPausedDetails

Provides information about when a classification job was paused. For a one-time job, this object also specifies when the job will expire and be cancelled if it isn't resumed. For a recurring job, this object also specifies when the paused job run will expire and be cancelled if it isn't resumed. This object is present only if a job's current status (`jobStatus`) is `USER_PAUSED`. The information in this object applies only to a job that was paused while it had a status of `RUNNING`.

jobImminentExpirationHealthEventArn

The Amazon Resource Name (ARN) of the AWS Health event that Amazon Macie sent to notify you of the job or job run's pending expiration and cancellation. This value is null if a job has been paused for less than 23 days.

Type: string

Required: False

jobExpiresAt

The date and time, in UTC and extended ISO 8601 format, when the job or job run will expire and be cancelled if you don't resume it first.

Type: string

Required: False

Format: date-time

jobPausedAt

The date and time, in UTC and extended ISO 8601 format, when you paused the job.

Type: string

Required: False

Format: date-time

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string
Required: False

See also

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

ListClassificationJobs

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Custom Data Identifier

The Custom Data Identifier resource provides access to the repository of custom data identifiers for your account. A *custom data identifier* is a set of criteria that you define to detect sensitive data.

You can use this resource to retrieve detailed information about a custom data identifier, or delete a custom data identifier. When you use this resource, you have to specify the unique identifier for the custom data identifier that your request applies to. To find this identifier, use the [Custom Data Identifier List \(p. 114\)](#) resource.

URI

/custom-data-identifiers/*id*

HTTP methods

GET

Operation ID: GetCustomDataIdentifier

Retrieves the criteria and other settings for a custom data identifier.

Path parameters

Name	Type	Required	Description
<i>id</i>	String	True	The unique identifier for the Amazon Macie resource or account that the request applies to.

Responses

Status code	Response model	Description
200	GetCustomDataIdentifierResponse	The request succeeded.
400	ValidationException (p. 98)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 98)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 98)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 98)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 98)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 98)	The request failed due to an unknown internal server error, exception, or failure.

DELETE

Operation ID: DeleteCustomDataIdentifier

Soft deletes a custom data identifier.

Path parameters

Name	Type	Required	Description
<i>id</i>	String	True	The unique identifier for the Amazon Macie resource or account that the request applies to.

Responses

Status code	Response model	Description
200	Empty Schema (p. 97)	The request succeeded. The specified custom data identifier was deleted and there isn't any content to include in the body of the response (No Content).

Status code	Response model	Description
400	ValidationException (p. 98)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 98)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 98)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 98)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 98)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 98)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 98)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Response bodies

GetCustomDataIdentifierResponse schema

```
{
  "createdAt": "string",
  "regex": "string",
  "deleted": boolean,
  "keywords": [
    "string"
  ],
  "ignoreWords": [
    "string"
  ],
  "name": "string",
  "description": "string",
  "maximumMatchDistance": integer,
  "id": "string",
  "arn": "string",
  "tags": {
  }
}
```

Empty Schema schema

```
{
```



```
}
```

ValidationException schema

```
{  
  "message": "string"  
}
```

ServiceQuotaExceededException schema

```
{  
  "message": "string"  
}
```

AccessDeniedException schema

```
{  
  "message": "string"  
}
```

ResourceNotFoundException schema

```
{  
  "message": "string"  
}
```

ConflictException schema

```
{  
  "message": "string"  
}
```

ThrottlingException schema

```
{  
  "message": "string"  
}
```

InternalServerError schema

```
{  
  "message": "string"  
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

Empty

The request succeeded and there isn't any content to include in the body of the response (No Content).

GetCustomDataIdentifierResponse

Provides information about the criteria and other settings for a custom data identifier.

createdAt

The date and time, in UTC and extended ISO 8601 format, when the custom data identifier was created.

Type: string

Required: False

Format: date-time

regex

The regular expression (*regex*) that defines the pattern to match.

Type: string

Required: False

deleted

Specifies whether the custom data identifier was deleted. If you delete a custom data identifier, Amazon Macie doesn't delete it permanently. Instead, it soft deletes the identifier.

Type: boolean

Required: False

keywords

An array that lists specific character sequences (keywords), one of which must be within proximity (*maximumMatchDistance*) of the regular expression to match. Keywords aren't case sensitive.

Type: Array of type string
Required: False

ignoreWords

An array that lists specific character sequences (ignore words) to exclude from the results. If the text matched by the regular expression is the same as any string in this array, Amazon Macie ignores it. Ignore words are case sensitive.

Type: Array of type string
Required: False

name

The custom name of the custom data identifier.

Type: string
Required: False

description

The custom description of the custom data identifier.

Type: string
Required: False

maximumMatchDistance

The maximum number of characters that can exist between text that matches the regex pattern and the character sequences specified by the `keywords` array. Amazon Macie includes or excludes a result based on the proximity of a keyword to text that matches the regex pattern.

Type: integer
Required: False
Format: int32

id

The unique identifier for the custom data identifier.

Type: string
Required: False

arn

The Amazon Resource Name (ARN) of the custom data identifier.

Type: string
Required: False

tags

A map of key-value pairs that identifies the tags (keys and values) that are associated with the custom data identifier.

Type: [TagMap](#) (p. 101)
Required: False

InternalServerErrorException

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string
Required: False

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string
Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string
Required: False

TagMap

A string-to-string map of key-value pairs that specifies the tags (keys and values) for a classification job, custom data identifier, findings filter, or member account.

key-value pairs

Type: string

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string
Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string
Required: False

See also

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

GetCustomDataIdentifier

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

DeleteCustomDataIdentifier

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Custom Data Identifier Creation

A *custom data identifier* is a set of criteria that you define to detect sensitive data. Each custom data identifier specifies a regular expression (*regex*) that defines a text pattern to match in a data source. It

can also specify character sequences, such as words and phrases, and a proximity rule that refine the analysis of a data source. By using custom data identifiers, you can detect sensitive data that reflects your particular scenarios, intellectual property, or proprietary data, and supplement the managed data identifiers that Amazon Macie provides.

You can use the Custom Data Identifier Creation resource to create a new custom data identifier. Note that you can't change a custom data identifier after you create it. This helps ensure that you have an immutable history of sensitive data findings and discovery results for data privacy and protection audits or investigations. To test and refine a custom data identifier before you create it, use the [Custom Data Identifier Testing \(p. 120\)](#) resource.

URI

/custom-data-identifiers

HTTP methods

POST

Operation ID: CreateCustomDataIdentifier

Creates and defines the criteria and other settings for a custom data identifier.

Responses

Status code	Response model	Description
200	CreateCustomDataIdentifierResponse	The request succeeded. The specified custom data identifier was created.
400	ValidationException (p. 104)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 11)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 10)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 105)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 105)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerError (p. 106)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

POST schema

```
{
  "regex": "string",
  "keywords": [
    "string"
  ],
  "clientToken": "string",
  "ignoreWords": [
    "string"
  ],
  "name": "string",
  "description": "string",
  "maximumMatchDistance": integer,
  "tags": {
  }
}
```

Response bodies

CreateCustomDataIdentifierResponse schema

```
{
  "customDataIdentifierId": "string"
}
```

ValidationException schema

```
{
  "message": "string"
}
```

ServiceQuotaExceededException schema

```
{
  "message": "string"
}
```

AccessDeniedException schema

```
{
  "message": "string"
}
```

ResourceNotFoundException schema

```
{
```

```
"message": "string"
}
```

ConflictException schema

```
{
  "message": "string"
}
```

ThrottlingException schema

```
{
  "message": "string"
}
```

InternalServerError schema

```
{
  "message": "string"
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

CreateCustomDataIdentifierRequest

Specifies the criteria and other settings for a custom data identifier. You can't change a custom data identifier after you create it. This helps ensure that you have an immutable history of sensitive data findings and discovery results for data privacy and protection audits or investigations.

regex

The regular expression (*regex*) that defines the pattern to match. The expression can contain as many as 512 characters.

Type: string
Required: True

keywords

An array that lists specific character sequences (keywords), one of which must be within proximity (*maximumMatchDistance*) of the regular expression to match. The array can contain as many as 50 keywords. Each keyword can contain 3-90 UTF-8 characters. Keywords aren't case sensitive.

Type: Array of type string
Required: False

clientToken

A unique, case-sensitive token that you provide to ensure the idempotency of the request.

Type: string
Required: False

ignoreWords

An array that lists specific character sequences (ignore words) to exclude from the results. If the text matched by the regular expression is the same as any string in this array, Amazon Macie ignores it. The array can contain as many as 10 ignore words. Each ignore word can contain 4-90 UTF-8 characters. Ignore words are case sensitive.

Type: Array of type string
Required: False

name

A custom name for the custom data identifier. The name can contain as many as 128 characters.

We strongly recommend that you avoid including any sensitive data in the name of a custom data identifier. Other users of your account might be able to see the identifier's name, depending on the actions that they're allowed to perform in Amazon Macie.

Type: string
Required: True

description

A custom description of the custom data identifier. The description can contain as many as 512 characters.

We strongly recommend that you avoid including any sensitive data in the description of a custom data identifier. Other users of your account might be able to see the identifier's description, depending on the actions that they're allowed to perform in Amazon Macie.

Type: string
Required: False

maximumMatchDistance

The maximum number of characters that can exist between text that matches the regex pattern and the character sequences specified by the `keywords` array. Amazon Macie includes or excludes a result based on the proximity of a keyword to text that matches the regex pattern. The distance can be 1-300 characters. The default value is 50.

Type: integer
Required: False
Format: int32

tags

A map of key-value pairs that specifies the tags to associate with the custom data identifier.

A custom data identifier can have a maximum of 50 tags. Each tag consists of a tag key and an associated tag value. The maximum length of a tag key is 128 characters. The maximum length of a tag value is 256 characters.

Type: [TagMap \(p. 108\)](#)
Required: False

CreateCustomDataIdentifierResponse

Provides information about a custom data identifier that was created in response to a request.

customDataIdentifierId

The unique identifier for the custom data identifier that was created.

Type: string
Required: False

InternalServerErrorException

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string
Required: False

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string
Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string

Required: False

TagMap

A string-to-string map of key-value pairs that specifies the tags (keys and values) for a classification job, custom data identifier, findings filter, or member account.

key-value pairs

Type: string

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string

Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string

Required: False

See also

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

CreateCustomDataIdentifier

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)

- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Custom Data Identifier Descriptions

The Custom Data Identifier Descriptions resource provides information about the custom data identifiers for your account. A *custom data identifier* is a set of criteria that you define to detect sensitive data.

You can use this resource to retrieve information about one or more custom data identifiers for your account. To refine your request, you can use the supported request parameter to specify which custom data identifiers to retrieve information about. To retrieve detailed information about the criteria and other settings for an individual custom data identifier, use the [Custom Data Identifier \(p. 95\)](#) resource.

URI

`/custom-data-identifiers/get`

HTTP methods

POST

Operation ID: `BatchGetCustomDataIdentifiers`

Retrieves information about one or more custom data identifiers.

Responses

Status code	Response model	Description
200	BatchGetCustomDataIdentifiersResponse (p. 110)	The request succeeded.
400	ValidationException (p. 110)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 111)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 111)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 111)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 111)	The request failed because it conflicts with the current state of the specified resource.

Status code	Response model	Description
429	ThrottlingException (p. 111)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 111)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

POST schema

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

Response bodies

BatchGetCustomDataIdentifiersResponse schema

```
{
  "customDataIdentifiers": [
    {
      "createdAt": "string",
      "deleted": boolean,
      "name": "string",
      "description": "string",
      "id": "string",
      "arn": "string"
    }
  ],
  "notFoundIdentifierIds": [
    "string"
  ]
}
```

ValidationException schema

```
{
  "message": "string"
}
```

ServiceQuotaExceededException schema

```
{
  "message": "string"
}
```

AccessDeniedException schema

```
{  
  "message": "string"  
}
```

ResourceNotFoundException schema

```
{  
  "message": "string"  
}
```

ConflictException schema

```
{  
  "message": "string"  
}
```

ThrottlingException schema

```
{  
  "message": "string"  
}
```

InternalServerError schema

```
{  
  "message": "string"  
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

BatchGetCustomDataIdentifierSummary

Provides information about a custom data identifier.

createdAt

The date and time, in UTC and extended ISO 8601 format, when the custom data identifier was created.

Type: string

Required: False
Format: date-time

deleted

Specifies whether the custom data identifier was deleted. If you delete a custom data identifier, Amazon Macie doesn't delete it permanently. Instead, it soft deletes the identifier.

Type: boolean
Required: False

name

The custom name of the custom data identifier.

Type: string
Required: False

description

The custom description of the custom data identifier.

Type: string
Required: False

id

The unique identifier for the custom data identifier.

Type: string
Required: False

arn

The Amazon Resource Name (ARN) of the custom data identifier.

Type: string
Required: False

BatchGetCustomDataIdentifiersRequest

Specifies one or more custom data identifiers to retrieve information about.

ids

An array of custom data identifier IDs, one for each custom data identifier to retrieve information about.

Type: Array of type string
Required: False

BatchGetCustomDataIdentifiersResponse

Provides information about one or more custom data identifiers.

customDataIdentifiers

An array of objects, one for each custom data identifier that meets the criteria specified in the request.

Type: Array of type [BatchGetCustomDataIdentifierSummary](#) (p. 111)

Required: False

notFoundIdentifierIds

An array of custom data identifier IDs, one for each custom data identifier that was specified in the request but doesn't correlate to an existing custom data identifier.

Type: Array of type string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

InternalServerError

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string

Required: False

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string

Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string

Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string

Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string

Required: False

See also

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

BatchGetCustomDataIdentifiers

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Custom Data Identifier List

The Custom Data Identifier List resource represents the repository of custom data identifiers for your account. A *custom data identifier* is a set of criteria that you define to detect sensitive data.

You can use this resource to retrieve a subset of information about all the custom data identifiers for your account. To retrieve detailed information about the criteria and other settings for an individual custom data identifier, use the [Custom Data Identifier \(p. 95\)](#) resource.

URI

`/custom-data-identifiers/list`

HTTP methods

POST

Operation ID: `ListCustomDataIdentifiers`

Retrieves a subset of information about all the custom data identifiers for an account.

Responses

Status code	Response model	Description
200	ListCustomDataIdentifiersResponse (p. 116)	The request succeeded.
400	ValidationException (p. 116)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 116)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 116)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 116)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 116)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 117)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 117)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

POST schema

```
{
```

```
"nextToken": "string",  
"maxResults": integer  
}
```

Response bodies

ListCustomDataIdentifiersResponse schema

```
{  
  "nextToken": "string",  
  "items": [  
    {  
      "createdAt": "string",  
      "name": "string",  
      "description": "string",  
      "id": "string",  
      "arn": "string"  
    }  
  ]  
}
```

ValidationException schema

```
{  
  "message": "string"  
}
```

ServiceQuotaExceededException schema

```
{  
  "message": "string"  
}
```

AccessDeniedException schema

```
{  
  "message": "string"  
}
```

ResourceNotFoundException schema

```
{  
  "message": "string"  
}
```

ConflictException schema

```
{  
  "message": "string"  
}
```

ThrottlingException schema

```
{  
  "message": "string"  
}
```

InternalServerError schema

```
{  
  "message": "string"  
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

CustomDataIdentifierSummary

Provides information about a custom data identifier.

createdAt

The date and time, in UTC and extended ISO 8601 format, when the custom data identifier was created.

Type: string

Required: False

Format: date-time

name

The custom name of the custom data identifier.

Type: string

Required: False

description

The custom description of the custom data identifier.

Type: string

Required: False

id

The unique identifier for the custom data identifier.

Type: string

Required: False

arn

The Amazon Resource Name (ARN) of the custom data identifier.

Type: string

Required: False

InternalServerError

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string

Required: False

ListCustomDataIdentifiersRequest

Specifies criteria for paginating the results of a request for information about custom data identifiers.

nextToken

The `nextToken` string that specifies which page of results to return in a paginated response.

Type: string

Required: False

maxResults

The maximum number of items to include in each page of the response.

Type: integer

Required: False

Format: int32

ListCustomDataIdentifiersResponse

Provides the results of a request for information about custom data identifiers.

nextToken

The string to use in a subsequent request to get the next page of results in a paginated response. This value is null if there are no additional pages.

Type: string

Required: False

items

An array of objects, one for each custom data identifier.

Type: Array of type [CustomDataIdentifierSummary](#) (p. 117)

Required: False

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string

Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string

Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string

Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string

Required: False

See also

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

ListCustomDataIdentifiers

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Custom Data Identifier Testing

The Custom Data Identifier Testing resource provides an environment for developing, testing, and refining a custom data identifier. A *custom data identifier* is a set of criteria that you define to detect sensitive data. By using custom data identifiers, you can detect sensitive data that reflects your particular scenarios, intellectual property, or proprietary data, and supplement the managed data identifiers that Amazon Macie provides.

When you develop a customer data identifier, you specify a regular expression (*regex*) that defines a text pattern to match in a data source. You can also specify character sequences, such as words and phrases, and a proximity rule to refine the analysis of a data source.

You can use the Custom Data Identifier Testing resource to develop, test, and refine a custom data identifier. Note that this resource doesn't create a persistent custom data identifier that you can subsequently access and use in Macie. Instead, it provides a test environment that can help you optimize and refine a custom data identifier by using sample data. When you finish developing and testing a custom data identifier, use the [Custom Data Identifier Creation \(p. 102\)](#) resource to create it.

URI

/custom-data-identifiers/test

HTTP methods

POST

Operation ID: TestCustomDataIdentifier

Tests a custom data identifier.

Responses

Status code	Response model	Description
200	TestCustomDataIdentifierResponse (p. 122)	The request succeeded.
400	ValidationException (p. 122)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 122)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 122)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 122)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 122)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 122)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 122)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

POST schema

```
{
  "regex": "string",
  "keywords": [
    "string"
  ],
  "ignoreWords": [
    "string"
  ],
  "maximumMatchDistance": integer,
  "sampleText": "string"
}
```

POST schema

```
{
  "regex": "string",
```



```
"keywords": [
  "string"
],
"ignoreWords": [
  "string"
],
"maximumMatchDistance": integer,
"sampleText": "string"
}
```

Response bodies

TestCustomDataIdentifierResponse schema

```
{
  "matchCount": integer
}
```

ValidationException schema

```
{
  "message": "string"
}
```

ServiceQuotaExceededException schema

```
{
  "message": "string"
}
```

AccessDeniedException schema

```
{
  "message": "string"
}
```

ResourceNotFoundException schema

```
{
  "message": "string"
}
```

ConflictException schema

```
{
  "message": "string"
}
```

ThrottlingException schema

```
{
```

```
"message": "string"
}
```

InternalServerError schema

```
{
  "message": "string"
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

InternalServerError

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string

Required: False

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string
Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string
Required: False

TestCustomDataIdentifierRequest

Specifies the detection criteria of a custom data identifier to test.

regex

The regular expression (*regex*) that defines the pattern to match. The expression can contain as many as 512 characters.

Type: string
Required: True

keywords

An array that lists specific character sequences (keywords), one of which must be within proximity (*maximumMatchDistance*) of the regular expression to match. The array can contain as many as 50 keywords. Each keyword can contain 3-90 UTF-8 characters. Keywords aren't case sensitive.

Type: Array of type string
Required: False

ignoreWords

An array that lists specific character sequences (ignore words) to exclude from the results. If the text matched by the regular expression is the same as any string in this array, Amazon Macie ignores it. The array can contain as many as 10 ignore words. Each ignore word can contain 4-90 UTF-8 characters. Ignore words are case sensitive.

Type: Array of type string
Required: False

maximumMatchDistance

The maximum number of characters that can exist between text that matches the regex pattern and the character sequences specified by the *keywords* array. Amazon Macie includes or excludes a result based on the proximity of a keyword to text that matches the regex pattern. The distance can be 1-300 characters. The default value is 50.

Type: integer
Required: False
Format: int32

sampleText

The sample text to inspect by using the custom data identifier. The text can contain as many as 1,000 characters.

Type: string
Required: True

TestCustomDataIdentifierResponse

Provides test results for a custom data identifier.

matchCount

The number of instances of sample text that matched the detection criteria specified in the custom data identifier.

Type: integer
Required: False
Format: int32

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string
Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string
Required: False

See also

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

TestCustomDataIdentifier

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)

- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Data Sources - Amazon S3

The Amazon S3 Data Sources resource provides statistical data and other information about the Amazon Simple Storage Service (Amazon S3) buckets that Amazon Macie monitors and analyzes for your account. This includes a breakdown of each bucket's public access settings, and the size and number of objects that Macie can analyze to detect sensitive data in a bucket. This resource also indicates whether you configured any classification jobs to analyze objects in a bucket and, if you have, the date and time when one of those jobs most recently ran. The data is available for all the S3 buckets that Macie monitors and analyzes for your account.

Note that complete data is available for an S3 bucket only if Macie can retrieve and process information about the bucket. If a bucket's permissions settings or an error prevents Macie from retrieving and processing information about a bucket or a bucket's objects, statistical data and other information is limited to a subset of the bucket's properties, such as the bucket's name and the account ID for the AWS account that owns the bucket.

You can use the Amazon S3 Data Sources resource to retrieve (query) statistical data and other information about the settings and contents of one or more S3 buckets that Macie monitors and analyzes for your account. To customize and refine your query, you can use supported parameters to specify whether and how to filter, sort, and paginate the query results.

URI

/datasources/s3

HTTP methods

POST

Operation ID: DescribeBuckets

Retrieves (queries) statistical data and other information about one or more S3 buckets that Amazon Macie monitors and analyzes.

Responses

Status code	Response model	Description
200	DescribeBucketsResponse (p. 129)	The request succeeded.
400	ValidationException (p. 129)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 129)	The request failed because fulfilling the request would exceed one or more service quotas for your account.

Status code	Response model	Description
403	AccessDeniedException (p. 129)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 129)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 129)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 129)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerError (p. 129)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

POST schema

```
{
  "criteria": {
  },
  "nextToken": "string",
  "maxResults": integer,
  "sortCriteria": {
    "orderBy": enum,
    "attributeName": "string"
  }
}
```

Response bodies

DescribeBucketsResponse schema

```
{
  "nextToken": "string",
  "buckets": [
    {
      "bucketName": "string",
      "objectCount": integer,
      "sizeInBytes": integer,
      "serverSideEncryption": {
        "kmsMasterKeyId": "string",
        "type": enum
      },
      "versioning": boolean,
      "classifiableObjectCount": integer,
      "allowsUnencryptedObjectUploads": enum,
      "publicAccess": {
        "effectivePermission": enum,

```

```

"permissionConfiguration": {
  "accountLevelPermissions": {
    "blockPublicAccess": {
      "blockPublicPolicy": boolean,
      "restrictPublicBuckets": boolean,
      "blockPublicAcls": boolean,
      "ignorePublicAcls": boolean
    }
  },
  "bucketLevelPermissions": {
    "accessControlList": {
      "allowsPublicReadAccess": boolean,
      "allowsPublicWriteAccess": boolean
    },
    "blockPublicAccess": {
      "blockPublicPolicy": boolean,
      "restrictPublicBuckets": boolean,
      "blockPublicAcls": boolean,
      "ignorePublicAcls": boolean
    },
    "bucketPolicy": {
      "allowsPublicReadAccess": boolean,
      "allowsPublicWriteAccess": boolean
    }
  }
},
"objectCountByEncryptionType": {
  "kmsManaged": integer,
  "s3Managed": integer,
  "customerManaged": integer,
  "unencrypted": integer,
  "unknown": integer
},
"errorMessage": "string",
"errorCode": enum,
"classifiableSizeInBytes": integer,
"tags": [
  {
    "value": "string",
    "key": "string"
  }
],
"unclassifiableObjectCount": {
  "total": integer,
  "storageClass": integer,
  "fileType": integer
},
"accountId": "string",
"lastUpdated": "string",
"bucketArn": "string",
"bucketCreatedAt": "string",
"replicationDetails": {
  "replicationAccounts": [
    "string"
  ],
  "replicatedExternally": boolean,
  "replicated": boolean
},
"jobDetails": {
  "lastJobId": "string",
  "lastJobRunTime": "string",
  "isDefinedInJob": enum,
  "isMonitoredByJob": enum
},
"sharedAccess": enum,

```

```
    "unclassifiableObjectSizeInBytes": {
      "total": integer,
      "storageClass": integer,
      "fileType": integer
    },
    "region": "string",
    "sizeInBytesCompressed": integer
  }
]
```

ValidationException schema

```
{
  "message": "string"
}
```

ServiceQuotaExceededException schema

```
{
  "message": "string"
}
```

AccessDeniedException schema

```
{
  "message": "string"
}
```

ResourceNotFoundException schema

```
{
  "message": "string"
}
```

ConflictException schema

```
{
  "message": "string"
}
```

ThrottlingException schema

```
{
  "message": "string"
}
```

InternalServerError schema

```
{
  "message": "string"
}
```


Properties

AccessControlList

Provides information about the permissions settings of the bucket-level access control list (ACL) for an S3 bucket.

allowsPublicReadAccess

Specifies whether the ACL grants the general public with read access permissions for the bucket.

Type: boolean
Required: False

allowsPublicWriteAccess

Specifies whether the ACL grants the general public with write access permissions for the bucket.

Type: boolean
Required: False

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string
Required: False

AccountLevelPermissions

Provides information about the account-level permissions settings that apply to an S3 bucket.

blockPublicAccess

The block public access settings for the AWS account that owns the bucket.

Type: [BlockPublicAccess](#) (p. 130)
Required: False

BlockPublicAccess

Provides information about the block public access settings for an S3 bucket. These settings can apply to a bucket at the account level or bucket level. For detailed information about each setting, see [Blocking public access to your Amazon S3 storage](#) in the *Amazon Simple Storage Service User Guide*.

blockPublicPolicy

Specifies whether Amazon S3 blocks public bucket policies for the bucket.

Type: boolean
Required: False

restrictPublicBuckets

Specifies whether Amazon S3 restricts public bucket policies for the bucket.

Type: boolean
Required: False

blockPublicAcls

Specifies whether Amazon S3 blocks public access control lists (ACLs) for the bucket and objects in the bucket.

Type: boolean
Required: False

ignorePublicAcls

Specifies whether Amazon S3 ignores public ACLs for the bucket and objects in the bucket.

Type: boolean
Required: False

BucketCriteria

Specifies, as a map, one or more property-based conditions that filter the results of a query for information about S3 buckets.

key-value pairs

Type: object

BucketCriteriaAdditionalProperties

Specifies the operator to use in a property-based condition that filters the results of a query for information about S3 buckets.

prefix

The name of the bucket begins with the specified value.

Type: string
Required: False

lt

The value for the property is less than the specified value.

Type: integer
Required: False
Format: int64

gte

The value for the property is greater than or equal to the specified value.

Type: integer
Required: False
Format: int64

neq

The value for the property doesn't match (doesn't equal) the specified value. If you specify multiple values, Amazon Macie uses OR logic to join the values.

Type: Array of type string
Required: False

lte

The value for the property is less than or equal to the specified value.

Type: integer
Required: False
Format: int64

eq

The value for the property matches (equals) the specified value. If you specify multiple values, Amazon Macie uses OR logic to join the values.

Type: Array of type string
Required: False

gt

The value for the property is greater than the specified value.

Type: integer
Required: False
Format: int64

BucketLevelPermissions

Provides information about the bucket-level permissions settings for an S3 bucket.

accessControlList

The permissions settings of the access control list (ACL) for the bucket. This value is null if an ACL hasn't been defined for the bucket.

Type: [AccessControlList](#) (p. 130)
Required: False

blockPublicAccess

The block public access settings for the bucket.

Type: [BlockPublicAccess](#) (p. 130)
Required: False

bucketPolicy

The permissions settings of the bucket policy for the bucket. This value is null if a bucket policy hasn't been defined for the bucket.

Type: [BucketPolicy](#) (p. 137)

Required: False

BucketMetadata

Provides statistical data and other information about an S3 bucket that Amazon Macie monitors and analyzes for your account. If an error occurs when Macie attempts to retrieve and process information about the bucket or the bucket's objects, the value for the `versioning` property is `false` and the value for most other properties is null. Exceptions are `accountId`, `bucketArn`, `bucketCreatedAt`, `bucketName`, `lastUpdated`, and `region`. To identify the cause of the error, refer to the `errorCode` and `errorMessage` values.

bucketName

The name of the bucket.

Type: string

Required: False

objectCount

The total number of objects in the bucket.

Type: integer

Required: False

Format: int64

sizeInBytes

The total storage size, in bytes, of the bucket.

If versioning is enabled for the bucket, Amazon Macie calculates this value based on the size of the latest version of each object in the bucket. This value doesn't reflect the storage size of all versions of each object in the bucket.

Type: integer

Required: False

Format: int64

serverSideEncryption

Specifies whether the bucket encrypts new objects by default and, if so, the type of server-side encryption that's used.

Type: [BucketServerSideEncryption](#) (p. 138)

Required: False

versioning

Specifies whether versioning is enabled for the bucket.

Type: boolean
Required: False

classifiableObjectCount

The total number of objects that Amazon Macie can analyze in the bucket. These objects use a supported storage class and have a file name extension for a supported file or storage format.

Type: integer
Required: False
Format: int64

allowsUnencryptedObjectUploads

Specifies whether the bucket policy for the bucket requires server-side encryption of objects when objects are uploaded to the bucket. Possible values are:

- **FALSE** - The bucket policy requires server-side encryption of new objects. `PutObject` requests must include the `x-amz-server-side-encryption` header and the value for that header must be `AES256` or `aws:kms`.
- **TRUE** - The bucket doesn't have a bucket policy or it has a bucket policy that doesn't require server-side encryption of new objects. If a bucket policy exists, it doesn't require `PutObject` requests to include the `x-amz-server-side-encryption` header and it doesn't require the value for that header to be `AES256` or `aws:kms`.
- **UNKNOWN** - Amazon Macie can't determine whether the bucket policy requires server-side encryption of new objects.

Type: string
Required: False
Values: `TRUE` | `FALSE` | `UNKNOWN`

publicAccess

Specifies whether the bucket is publicly accessible due to the combination of permissions settings that apply to the bucket, and provides information about those settings.

Type: [BucketPublicAccess \(p. 138\)](#)
Required: False

objectCountByEncryptionType

The total number of objects that are in the bucket, grouped by server-side encryption type. This includes a grouping that reports the total number of objects that aren't encrypted or use client-side encryption.

Type: [ObjectCountByEncryptionType \(p. 142\)](#)
Required: False

errorMessage

A brief description of the error (`errorCode`) that prevented Amazon Macie from retrieving and processing information about the bucket and the bucket's objects. This value is null if Macie was able to retrieve and process the information.

Type: string

Required: False

errorCode

Specifies the error code for an error that prevented Amazon Macie from retrieving and processing information about the bucket and the bucket's objects. If this value is `ACCESS_DENIED`, Macie doesn't have permission to retrieve the information. For example, the bucket has a restrictive bucket policy and Amazon S3 denied the request. If this value is null, Macie was able to retrieve and process the information.

Type: [BucketMetadataErrorCode](#) (p. 137)

Required: False

classifiableSizeInBytes

The total storage size, in bytes, of the objects that Amazon Macie can analyze in the bucket. These objects use a supported storage class and have a file name extension for a supported file or storage format.

If versioning is enabled for the bucket, Macie calculates this value based on the size of the latest version of each applicable object in the bucket. This value doesn't reflect the storage size of all versions of each applicable object in the bucket.

Type: integer

Required: False

Format: int64

tags

An array that specifies the tags (keys and values) that are associated with the bucket.

Type: Array of type [KeyValuePair](#) (p. 142)

Required: False

unclassifiableObjectCount

The total number of objects that Amazon Macie can't analyze in the bucket. These objects don't use a supported storage class or don't have a file name extension for a supported file or storage format.

Type: [ObjectLevelStatistics](#) (p. 143)

Required: False

accountId

The unique identifier for the AWS account that owns the bucket.

Type: string

Required: False

lastUpdated

The date and time, in UTC and extended ISO 8601 format, when Amazon Macie most recently retrieved both bucket and object metadata from Amazon S3 for the bucket.

Type: string

Required: False
Format: date-time

bucketArn

The Amazon Resource Name (ARN) of the bucket.

Type: string
Required: False

bucketCreatedAt

The date and time, in UTC and extended ISO 8601 format, when the bucket was created.

Type: string
Required: False
Format: date-time

replicationDetails

Specifies whether the bucket is configured to replicate one or more objects to buckets for other AWS accounts and, if so, which accounts.

Type: [ReplicationDetails \(p. 144\)](#)
Required: False

jobDetails

Specifies whether any one-time or recurring classification jobs are configured to analyze data in the bucket, and, if so, the details of the job that ran most recently.

Type: [JobDetails \(p. 141\)](#)
Required: False

sharedAccess

Specifies whether the bucket is shared with another AWS account. Possible values are:

- **EXTERNAL** - The bucket is shared with an AWS account that isn't part of the same Amazon Macie organization.
- **INTERNAL** - The bucket is shared with an AWS account that's part of the same Amazon Macie organization.
- **NOT_SHARED** - The bucket isn't shared with other AWS accounts.
- **UNKNOWN** - Amazon Macie wasn't able to evaluate the shared access settings for the bucket.

Type: string
Required: False
Values: EXTERNAL | INTERNAL | NOT_SHARED | UNKNOWN

unclassifiableObjectSizeInBytes

The total storage size, in bytes, of the objects that Amazon Macie can't analyze in the bucket. These objects don't use a supported storage class or don't have a file name extension for a supported file or storage format.

Type: [ObjectLevelStatistics](#) (p. 143)
Required: False

region

The AWS Region that hosts the bucket.

Type: string
Required: False

sizeInBytesCompressed

The total storage size, in bytes, of the objects that are compressed (.gz, .gzip, .zip) files in the bucket.

If versioning is enabled for the bucket, Amazon Macie calculates this value based on the size of the latest version of each applicable object in the bucket. This value doesn't reflect the storage size of all versions of each applicable object in the bucket.

Type: integer
Required: False
Format: int64

BucketMetadataErrorCode

The error code for an error that prevented Amazon Macie from retrieving and processing information about an S3 bucket and the bucket's objects.

ACCESS_DENIED

BucketPermissionConfiguration

Provides information about the account-level and bucket-level permissions settings for an S3 bucket.

accountLevelPermissions

The account-level permissions settings that apply to the bucket.

Type: [AccountLevelPermissions](#) (p. 130)
Required: False

bucketLevelPermissions

The bucket-level permissions settings for the bucket.

Type: [BucketLevelPermissions](#) (p. 132)
Required: False

BucketPolicy

Provides information about the permissions settings of the bucket policy for an S3 bucket.

allowsPublicReadAccess

Specifies whether the bucket policy allows the general public to have read access to the bucket.

Type: boolean
Required: False

allowsPublicWriteAccess

Specifies whether the bucket policy allows the general public to have write access to the bucket.

Type: boolean
Required: False

BucketPublicAccess

Provides information about the permissions settings that determine whether an S3 bucket is publicly accessible.

effectivePermission

Specifies whether the bucket is publicly accessible due to the combination of permissions settings that apply to the bucket. Possible values are:

- `NOT_PUBLIC` - The bucket isn't publicly accessible.
- `PUBLIC` - The bucket is publicly accessible.
- `UNKNOWN` - Amazon Macie can't determine whether the bucket is publicly accessible.

Type: string
Required: False
Values: `PUBLIC` | `NOT_PUBLIC` | `UNKNOWN`

permissionConfiguration

The account-level and bucket-level permissions settings for the bucket.

Type: [BucketPermissionConfiguration](#) (p. 137)
Required: False

BucketServerSideEncryption

Provides information about the default server-side encryption settings for an S3 bucket. For detailed information about these settings, see [Setting default server-side encryption behavior for Amazon S3 buckets](#) in the *Amazon Simple Storage Service User Guide*.

kmsMasterKeyId

The Amazon Resource Name (ARN) or unique identifier (key ID) for the AWS KMS key that's used by default to encrypt objects that are added to the bucket. This value is null if the bucket uses an Amazon S3 managed key to encrypt new objects or the bucket doesn't encrypt new objects by default.

Type: string
Required: False

type

The type of server-side encryption that's used by default when storing new objects in the bucket. Possible values are:

- `AES256` - New objects are encrypted with an Amazon S3 managed key. They use SSE-S3 encryption.
- `aws:kms` - New objects are encrypted with an AWS KMS key (`kmsMasterKeyId`), either an AWS managed key or a customer managed key. They use SSE-KMS encryption.
- `NONE` - New objects aren't encrypted by default. Default encryption is disabled for the bucket.

Type: string

Required: False

Values: `NONE` | `AES256` | `aws:kms`

BucketSortCriteria

Specifies criteria for sorting the results of a query for information about S3 buckets.

orderBy

The sort order to apply to the results, based on the value specified by the `attributeName` property. Valid values are: `ASC`, sort the results in ascending order; and, `DESC`, sort the results in descending order.

Type: string

Required: False

Values: `ASC` | `DESC`

attributeName

The name of the bucket property to sort the results by. This value can be one of the following properties that Amazon Macie defines as bucket metadata: `accountId`, `bucketName`, `classifiableObjectCount`, `classifiableSizeInBytes`, `objectCount`, or `sizeInBytes`.

Type: string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

DescribeBucketsRequest

Specifies criteria for filtering, sorting, and paginating the results of a query for statistical data and other information about S3 buckets.

criteria

The criteria to use to filter the query results.

Type: [BucketCriteria](#) (p. 131)

Required: False

nextToken

The `nextToken` string that specifies which page of results to return in a paginated response.

Type: string

Required: False

maxResults

The maximum number of items to include in each page of the response. The default value is 50.

Type: integer

Required: False

Format: int32

sortCriteria

The criteria to use to sort the query results.

Type: [BucketSortCriteria](#) (p. 139)

Required: False

DescribeBucketsResponse

Provides the results of a query that retrieved statistical data and other information about one or more S3 buckets that Amazon Macie monitors and analyzes for your account.

nextToken

The string to use in a subsequent request to get the next page of results in a paginated response. This value is null if there are no additional pages.

Type: string

Required: False

buckets

An array of objects, one for each bucket that meets the filter criteria specified in the request.

Type: Array of type [BucketMetadata](#) (p. 133)

Required: False

InternalServerError

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string

Required: False

JobDetails

Specifies whether any one-time or recurring classification jobs are configured to analyze data in an S3 bucket, and, if so, the details of the job that ran most recently.

lastJobId

The unique identifier for the job that ran most recently and is configured to analyze data in the bucket, either the latest run of a recurring job or the only run of a one-time job.

This value is typically null if the value for the `isDefinedInJob` property is `FALSE` or `UNKNOWN`.

Type: string

Required: False

lastJobRunTime

The date and time, in UTC and extended ISO 8601 format, when the job (`lastJobId`) started. If the job is a recurring job, this value indicates when the most recent run started.

This value is typically null if the value for the `isDefinedInJob` property is `FALSE` or `UNKNOWN`.

Type: string

Required: False

Format: date-time

isDefinedInJob

Specifies whether any one-time or recurring jobs are configured to analyze data in the bucket. Possible values are:

- `TRUE` - The bucket is explicitly included in the bucket definition (`S3BucketDefinitionForJob`) for one or more jobs and at least one of those jobs has a status other than `CANCELLED`. Or the bucket matched the bucket criteria (`S3BucketCriteriaForJob`) for at least one job that previously ran.
- `FALSE` - The bucket isn't explicitly included in the bucket definition (`S3BucketDefinitionForJob`) for any jobs, all the jobs that explicitly include the bucket in their bucket definitions have a status of `CANCELLED`, or the bucket didn't match the bucket criteria (`S3BucketCriteriaForJob`) for any jobs that previously ran.
- `UNKNOWN` - An exception occurred when Amazon Macie attempted to retrieve job data for the bucket.

Type: string

Required: False

Values: `TRUE` | `FALSE` | `UNKNOWN`

isMonitoredByJob

Specifies whether any recurring jobs are configured to analyze data in the bucket. Possible values are:

- `TRUE` - The bucket is explicitly included in the bucket definition (`S3BucketDefinitionForJob`) for one or more recurring jobs or the bucket matches the bucket criteria (`S3BucketCriteriaForJob`) for one or more recurring jobs. At least one of those jobs has a status other than `CANCELLED`.
- `FALSE` - The bucket isn't explicitly included in the bucket definition (`S3BucketDefinitionForJob`) for any recurring jobs, the bucket doesn't match the bucket criteria (`S3BucketCriteriaForJob`) for any recurring jobs, or all the recurring jobs that are configured to analyze data in the bucket have a status of `CANCELLED`.

- UNKNOWN - An exception occurred when Amazon Macie attempted to retrieve job data for the bucket.

Type: string
Required: False
Values: TRUE | FALSE | UNKNOWN

KeyValuePair

Provides information about the tags that are associated with an S3 bucket or object. Each tag consists of a required tag key and an associated tag value.

value

One part of a key-value pair that comprises a tag. A tag value acts as a descriptor for a tag key. A tag value can be an empty string.

Type: string
Required: False

key

One part of a key-value pair that comprises a tag. A tag key is a general label that acts as a category for more specific tag values.

Type: string
Required: False

ObjectCountByEncryptionType

Provides information about the number of objects that are in an S3 bucket and use certain types of server-side encryption, use client-side encryption, or aren't encrypted.

kmsManaged

The total number of objects that are encrypted with an AWS KMS key, either an AWS managed key or a customer managed key. The objects use AWS KMS encryption (SSE-KMS).

Type: integer
Required: False
Format: int64

s3Managed

The total number of objects that are encrypted with an Amazon S3 managed key. The objects use Amazon S3 managed encryption (SSE-S3).

Type: integer
Required: False
Format: int64

customerManaged

The total number of objects that are encrypted with a customer-provided key. The objects use customer-provided server-side encryption (SSE-C).

Type: integer
Required: False
Format: int64

unencrypted

The total number of objects that aren't encrypted or use client-side encryption.

Type: integer
Required: False
Format: int64

unknown

The total number of objects that Amazon Macie doesn't have current encryption metadata for. Macie can't provide current data about the encryption settings for these objects.

Type: integer
Required: False
Format: int64

ObjectLevelStatistics

Provides information about the total storage size (in bytes) or number of objects that Amazon Macie can't analyze in one or more S3 buckets. In a `BucketMetadata` or `MatchingBucket` object, this data is for a specific bucket. In a `GetBucketStatisticsResponse` object, this data is aggregated for the buckets in the query results. If versioning is enabled for a bucket, total storage size values are based on the size of the latest version of each applicable object in the bucket.

total

The total storage size (in bytes) or number of objects that Amazon Macie can't analyze because the objects use an unsupported storage class or don't have a file name extension for a supported file or storage format.

Type: integer
Required: False
Format: int64

storageClass

The total storage size (in bytes) or number of objects that Amazon Macie can't analyze because the objects use an unsupported storage class.

Type: integer
Required: False
Format: int64

fileType

The total storage size (in bytes) or number of objects that Amazon Macie can't analyze because the objects don't have a file name extension for a supported file or storage format.

Type: integer

Required: False

Format: int64

ReplicationDetails

Provides information about settings that define whether one or more objects in an S3 bucket are replicated to S3 buckets for other AWS accounts and, if so, which accounts.

replicationAccounts

An array of AWS account IDs, one for each AWS account that the bucket is configured to replicate one or more objects to.

Type: Array of type string

Required: False

replicatedExternally

Specifies whether the bucket is configured to replicate one or more objects to an AWS account that isn't part of the same Amazon Macie organization.

Type: boolean

Required: False

replicated

Specifies whether the bucket is configured to replicate one or more objects to any destination.

Type: boolean

Required: False

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string

Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string

Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string

Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string

Required: False

See also

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

DescribeBuckets

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Data Sources - Amazon S3 Statistics

The Amazon S3 Data Source Statistics resource provides aggregated statistical data for all the Amazon Simple Storage Service (Amazon S3) buckets that Amazon Macie monitors and analyzes for your account. This includes data for key security metrics such as the number of buckets that are publicly accessible, don't encrypt new objects by default, or are shared with other AWS accounts.

You can use the Amazon S3 Data Source Statistics resource to retrieve (query) aggregated data for security metrics that apply to all the S3 buckets that Macie monitors and analyzes for your account. To retrieve additional data for these buckets, use the [Amazon S3 Data Sources \(p. 126\)](#) resource.

URI

/datasources/s3/statistics

HTTP methods

POST

Operation ID: GetBucketStatistics

Retrieves (queries) aggregated statistical data for all the S3 buckets that Amazon Macie monitors and analyzes.

Responses

Status code	Response model	Description
200	GetBucketStatisticsResponse (p. 147)	The request succeeded.
400	ValidationException (p. 147)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 147)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 147)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 147)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 148)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 148)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 148)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

POST schema

```
{
  "accountId": "string"
}
```

Response bodies

GetBucketStatisticsResponse schema

```
{
  "bucketCountByObjectEncryptionRequirement": {
    "deniesUnencryptedObjectUploads": integer,
    "allowsUnencryptedObjectUploads": integer,
    "unknown": integer
  },
  "objectCount": integer,
  "sizeInBytes": integer,
  "classifiableObjectCount": integer,
  "classifiableSizeInBytes": integer,
  "bucketCountBySharedAccessType": {
    "internal": integer,
    "external": integer,
    "notShared": integer,
    "unknown": integer
  },
  "unclassifiableObjectCount": {
    "total": integer,
    "storageClass": integer,
    "fileType": integer
  },
  "bucketCountByEffectivePermission": {
    "publiclyWritable": integer,
    "publiclyReadable": integer,
    "publiclyAccessible": integer,
    "unknown": integer
  },
  "lastUpdated": "string",
  "bucketCount": integer,
  "bucketCountByEncryptionType": {
    "kmsManaged": integer,
    "s3Managed": integer,
    "unencrypted": integer,
    "unknown": integer
  },
  "unclassifiableObjectSizeInBytes": {
    "total": integer,
    "storageClass": integer,
    "fileType": integer
  },
  "sizeInBytesCompressed": integer
}
```

ValidationException schema

```
{
  "message": "string"
}
```

ServiceQuotaExceededException schema

```
{
  "message": "string"
}
```

AccessDeniedException schema

```
{  
  "message": "string"  
}
```

ResourceNotFoundException schema

```
{  
  "message": "string"  
}
```

ConflictException schema

```
{  
  "message": "string"  
}
```

ThrottlingException schema

```
{  
  "message": "string"  
}
```

InternalServerError schema

```
{  
  "message": "string"  
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

BucketCountByEffectivePermission

Provides information about the number of S3 buckets that are publicly accessible based on a combination of permissions settings for each bucket.

publiclyWritable

The total number of buckets that allow the general public to have write access to the bucket.

Type: integer
Required: False
Format: int64

publiclyReadable

The total number of buckets that allow the general public to have read access to the bucket.

Type: integer
Required: False
Format: int64

publiclyAccessible

The total number of buckets that allow the general public to have read or write access to the bucket.

Type: integer
Required: False
Format: int64

unknown

The total number of buckets that Amazon Macie wasn't able to evaluate permissions settings for. Macie can't determine whether these buckets are publicly accessible.

Type: integer
Required: False
Format: int64

BucketCountByEncryptionType

Provides information about the number of S3 buckets that use certain types of server-side encryption by default or don't encrypt new objects by default. For detailed information about these settings, see [Setting default server-side encryption behavior for Amazon S3 buckets](#) in the *Amazon Simple Storage Service User Guide*.

kmsManaged

The total number of buckets that use an AWS KMS key to encrypt new objects by default, either an AWS managed key or a customer managed key. These buckets use AWS KMS encryption (SSE-KMS) by default.

Type: integer
Required: False
Format: int64

s3Managed

The total number of buckets that use an Amazon S3 managed key to encrypt new objects by default. These buckets use Amazon S3 managed encryption (SSE-S3) by default.

Type: integer
Required: False
Format: int64

unencrypted

The total number of buckets that don't encrypt new objects by default. Default encryption is disabled for these buckets.

Type: integer
Required: False
Format: int64

unknown

The total number of buckets that Amazon Macie doesn't have current encryption metadata for. Macie can't provide current data about the default encryption settings for these buckets.

Type: integer
Required: False
Format: int64

BucketCountBySharedAccessType

Provides information about the number of S3 buckets that are or aren't shared with other AWS accounts.

internal

The total number of buckets that are shared with an AWS account that's part of the same Amazon Macie organization.

Type: integer
Required: False
Format: int64

external

The total number of buckets that are shared with an AWS account that isn't part of the same Amazon Macie organization.

Type: integer
Required: False
Format: int64

notShared

The total number of buckets that aren't shared with other AWS accounts.

Type: integer
Required: False
Format: int64

unknown

The total number of buckets that Amazon Macie wasn't able to evaluate shared access settings for. Macie can't determine whether these buckets are shared with other AWS accounts.

Type: integer

Required: False
Format: int64

BucketCountPolicyAllowsUnencryptedObjectUploads

Provides information about the number of S3 buckets whose bucket policies do or don't require server-side encryption of objects when objects are uploaded to the buckets.

deniesUnencryptedObjectUploads

The total number of buckets whose bucket policies require server-side encryption of new objects. `PutObject` requests for these buckets must include the `x-amz-server-side-encryption` header and the value for that header must be `AES256` or `aws:kms`.

Type: integer
Required: False
Format: int64

allowsUnencryptedObjectUploads

The total number of buckets that don't have a bucket policy or have a bucket policy that doesn't require server-side encryption of new objects. If a bucket policy exists, the policy doesn't require `PutObject` requests to include the `x-amz-server-side-encryption` header and it doesn't require the value for that header to be `AES256` or `aws:kms`.

Type: integer
Required: False
Format: int64

unknown

The total number of buckets that Amazon Macie wasn't able to evaluate server-side encryption requirements for. Macie can't determine whether the bucket policies for these buckets require server-side encryption of new objects.

Type: integer
Required: False
Format: int64

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string
Required: False

GetBucketStatisticsRequest

Specifies the account that owns the S3 buckets to retrieve aggregated statistical data for.

accountId

The unique identifier for the AWS account.

Type: string

Required: False

GetBucketStatisticsResponse

Provides the results of a query that retrieved aggregated statistical data for all the S3 buckets that Amazon Macie monitors and analyzes for your account.

bucketCountByObjectEncryptionRequirement

The total number of buckets whose bucket policies do or don't require server-side encryption of objects when objects are uploaded to the buckets.

Type: [BucketCountPolicyAllowsUnencryptedObjectUploads \(p. 151\)](#)

Required: False

objectCount

The total number of objects in the buckets.

Type: integer

Required: False

Format: int64

sizeInBytes

The total storage size, in bytes, of the buckets.

If versioning is enabled for any of the buckets, Amazon Macie calculates this value based on the size of the latest version of each object in those buckets. This value doesn't reflect the storage size of all versions of the objects in the buckets.

Type: integer

Required: False

Format: int64

classifiableObjectCount

The total number of objects that Amazon Macie can analyze in the buckets. These objects use a supported storage class and have a file name extension for a supported file or storage format.

Type: integer

Required: False

Format: int64

classifiableSizeInBytes

The total storage size, in bytes, of all the objects that Amazon Macie can analyze in the buckets. These objects use a supported storage class and have a file name extension for a supported file or storage format.

If versioning is enabled for any of the buckets, Macie calculates this value based on the size of the latest version of each applicable object in those buckets. This value doesn't reflect the storage size of all versions of all applicable objects in the buckets.

Type: integer
Required: False
Format: int64

bucketCountBySharedAccessType

The total number of buckets that are or aren't shared with another AWS account.

Type: [BucketCountBySharedAccessType](#) (p. 150)
Required: False

unclassifiableObjectCount

The total number of objects that Amazon Macie can't analyze in the buckets. These objects don't use a supported storage class or don't have a file name extension for a supported file or storage format.

Type: [ObjectLevelStatistics](#) (p. 154)
Required: False

bucketCountByEffectivePermission

The total number of buckets that are publicly accessible based on a combination of permissions settings for each bucket.

Type: [BucketCountByEffectivePermission](#) (p. 148)
Required: False

lastUpdated

The date and time, in UTC and extended ISO 8601 format, when Amazon Macie most recently retrieved both bucket and object metadata from Amazon S3 for the buckets.

Type: string
Required: False
Format: date-time

bucketCount

The total number of buckets.

Type: integer
Required: False
Format: int64

bucketCountByEncryptionType

The total number of buckets that use certain types of server-side encryption to encrypt new objects by default. This object also reports the total number of buckets that don't encrypt new objects by default.

Type: [BucketCountByEncryptionType](#) (p. 149)
Required: False

unclassifiableObjectSizeInBytes

The total storage size, in bytes, of the objects that Amazon Macie can't analyze in the buckets. These objects don't use a supported storage class or don't have a file name extension for a supported file or storage format.

Type: [ObjectLevelStatistics](#) (p. 154)

Required: False

sizeInBytesCompressed

The total storage size, in bytes, of the objects that are compressed (.gz, .gzip, .zip) files in the buckets.

If versioning is enabled for any of the buckets, Amazon Macie calculates this value based on the size of the latest version of each applicable object in those buckets. This value doesn't reflect the storage size of all versions of the applicable objects in the buckets.

Type: integer

Required: False

Format: int64

InternalServerErrorException

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string

Required: False

ObjectLevelStatistics

Provides information about the total storage size (in bytes) or number of objects that Amazon Macie can't analyze in one or more S3 buckets. In a `BucketMetadata` or `MatchingBucket` object, this data is for a specific bucket. In a `GetBucketStatisticsResponse` object, this data is aggregated for the buckets in the query results. If versioning is enabled for a bucket, total storage size values are based on the size of the latest version of each applicable object in the bucket.

total

The total storage size (in bytes) or number of objects that Amazon Macie can't analyze because the objects use an unsupported storage class or don't have a file name extension for a supported file or storage format.

Type: integer

Required: False

Format: int64

storageClass

The total storage size (in bytes) or number of objects that Amazon Macie can't analyze because the objects use an unsupported storage class.

Type: integer
Required: False
Format: int64

fileType

The total storage size (in bytes) or number of objects that Amazon Macie can't analyze because the objects don't have a file name extension for a supported file or storage format.

Type: integer
Required: False
Format: int64

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string
Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string
Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string
Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string
Required: False

See also

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

GetBucketStatistics

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Data Sources - Search

The Search Data Sources resource provides statistical data and other information about AWS resources that Amazon Macie monitors and analyzes for your account. The information includes quantitative breakdowns that indicate how much data Macie can analyze to detect sensitive data in a resource. It also indicates whether you configured any classification jobs to analyze data in a resource and, if so, the date and time when one of those jobs most recently ran. The data is available for all the AWS resources that Macie monitors and analyzes for your account.

Note that complete data is available for a resource only if Macie can retrieve and process information about the resource. If a resource's permissions settings or an error prevents Macie from retrieving and processing information about a resource, statistical data and other information is limited to a subset of the resource's properties, such as the name of the resource and the account ID for the AWS account that owns the resource.

In addition to querying data, you can use this resource to build, test, and refine Amazon Simple Storage Service (Amazon S3) bucket criteria that you want to use for new classification jobs. For existing classification jobs, you can use this resource to create a snapshot of the S3 buckets that a job would analyze if the job ran at a certain time—the same time that you query this resource using the bucket criteria for the job. The `SearchResourcesBucketCriteria` structure for the Search Data Sources resource is the same as the `S3BucketCriteriaForJob` structure for classification jobs.

You can use the Search Data Sources resource to query (retrieve) statistical data and other information about AWS resources that Macie monitors and analyzes for your account. To customize and refine your query, you can use supported parameters to specify whether and how to filter, sort, and paginate the query results. You can also use this resource to build and test S3 bucket criteria for classification jobs.

URI

`/datasources/search-resources`

HTTP methods

POST

Operation ID: SearchResources

Retrieves (queries) statistical data and other information about AWS resources that Amazon Macie monitors and analyzes.

Responses

Status code	Response model	Description
200	SearchResourcesResponse (p. 158)	The request succeeded.
400	ValidationException (p. 159)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 158)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 158)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 158)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 159)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 160)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 158)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

POST schema

```
{
  "nextToken": "string",
  "maxResults": integer,
  "bucketCriteria": {
    "excludes": {
      "and": [
        {
          "tagCriterion": {
            "comparator": enum,
```

```

        "tagValues": [
            {
                "value": "string",
                "key": "string"
            }
        ]
    },
    "simpleCriterion": {
        "comparator": enum,
        "values": [
            "string"
        ],
        "key": enum
    }
}
]
},
"includes": {
    "and": [
        {
            "tagCriterion": {
                "comparator": enum,
                "tagValues": [
                    {
                        "value": "string",
                        "key": "string"
                    }
                ]
            },
            "simpleCriterion": {
                "comparator": enum,
                "values": [
                    "string"
                ],
                "key": enum
            }
        }
    ]
}
},
"sortCriteria": {
    "orderBy": enum,
    "attributeName": enum
}
}

```

Response bodies

SearchResourcesResponse schema

```

{
    "nextToken": "string",
    "matchingResources": [
        {
            "matchingBucket": {
                "bucketName": "string",
                "objectCount": integer,
                "sizeInBytes": integer,
                "classifiableObjectCount": integer,
                "objectCountByEncryptionType": {
                    "kmsManaged": integer,
                    "s3Managed": integer,
                    "customerManaged": integer,
                    "unencrypted": integer,

```

```
        "unknown": integer
      },
      "errorMessage": "string",
      "errorCode": enum,
      "classifiableSizeInBytes": integer,
      "unclassifiableObjectCount": {
        "total": integer,
        "storageClass": integer,
        "fileType": integer
      },
      "accountId": "string",
      "unclassifiableObjectSizeInBytes": {
        "total": integer,
        "storageClass": integer,
        "fileType": integer
      },
      "jobDetails": {
        "lastJobId": "string",
        "lastJobRunTime": "string",
        "isDefinedInJob": enum,
        "isMonitoredByJob": enum
      },
      "sizeInBytesCompressed": integer
    }
  }
]
```

ValidationException schema

```
{
  "message": "string"
}
```

ServiceQuotaExceededException schema

```
{
  "message": "string"
}
```

AccessDeniedException schema

```
{
  "message": "string"
}
```

ResourceNotFoundException schema

```
{
  "message": "string"
}
```

ConflictException schema

```
{
```

```
"message": "string"
}
```

ThrottlingException schema

```
{
  "message": "string"
}
```

InternalServerError schema

```
{
  "message": "string"
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

BucketMetadataErrorCode

The error code for an error that prevented Amazon Macie from retrieving and processing information about an S3 bucket and the bucket's objects.

ACCESS_DENIED

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

InternalServerError

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string

Required: False

JobDetails

Specifies whether any one-time or recurring classification jobs are configured to analyze data in an S3 bucket, and, if so, the details of the job that ran most recently.

lastJobId

The unique identifier for the job that ran most recently and is configured to analyze data in the bucket, either the latest run of a recurring job or the only run of a one-time job.

This value is typically null if the value for the `isDefinedInJob` property is `FALSE` or `UNKNOWN`.

Type: string

Required: False

lastJobRunTime

The date and time, in UTC and extended ISO 8601 format, when the job (`lastJobId`) started. If the job is a recurring job, this value indicates when the most recent run started.

This value is typically null if the value for the `isDefinedInJob` property is `FALSE` or `UNKNOWN`.

Type: string

Required: False

Format: date-time

isDefinedInJob

Specifies whether any one-time or recurring jobs are configured to analyze data in the bucket. Possible values are:

- `TRUE` - The bucket is explicitly included in the bucket definition (`S3BucketDefinitionForJob`) for one or more jobs and at least one of those jobs has a status other than `CANCELLED`. Or the bucket matched the bucket criteria (`S3BucketCriteriaForJob`) for at least one job that previously ran.
- `FALSE` - The bucket isn't explicitly included in the bucket definition (`S3BucketDefinitionForJob`) for any jobs, all the jobs that explicitly include the bucket in their bucket definitions have a status of `CANCELLED`, or the bucket didn't match the bucket criteria (`S3BucketCriteriaForJob`) for any jobs that previously ran.
- `UNKNOWN` - An exception occurred when Amazon Macie attempted to retrieve job data for the bucket.

Type: string

Required: False

Values: `TRUE` | `FALSE` | `UNKNOWN`

isMonitoredByJob

Specifies whether any recurring jobs are configured to analyze data in the bucket. Possible values are:

- **TRUE** - The bucket is explicitly included in the bucket definition (`S3BucketDefinitionForJob`) for one or more recurring jobs or the bucket matches the bucket criteria (`S3BucketCriteriaForJob`) for one or more recurring jobs. At least one of those jobs has a status other than `CANCELLED`.
- **FALSE** - The bucket isn't explicitly included in the bucket definition (`S3BucketDefinitionForJob`) for any recurring jobs, the bucket doesn't match the bucket criteria (`S3BucketCriteriaForJob`) for any recurring jobs, or all the recurring jobs that are configured to analyze data in the bucket have a status of `CANCELLED`.
- **UNKNOWN** - An exception occurred when Amazon Macie attempted to retrieve job data for the bucket.

Type: string

Required: False

Values: TRUE | FALSE | UNKNOWN

MatchingBucket

Provides statistical data and other information about an S3 bucket that Amazon Macie monitors and analyzes for your account. If an error occurs when Macie attempts to retrieve and process information about the bucket or the bucket's objects, the value for most of these properties is null. Exceptions are `accountId` and `bucketName`. To identify the cause of the error, refer to the `errorCode` and `errorMessage` values.

bucketName

The name of the bucket.

Type: string

Required: False

objectCount

The total number of objects in the bucket.

Type: integer

Required: False

Format: int64

sizeInBytes

The total storage size, in bytes, of the bucket.

If versioning is enabled for the bucket, Amazon Macie calculates this value based on the size of the latest version of each object in the bucket. This value doesn't reflect the storage size of all versions of each object in the bucket.

Type: integer

Required: False

Format: int64

classifiableObjectCount

The total number of objects that Amazon Macie can analyze in the bucket. These objects use a supported storage class and have a file name extension for a supported file or storage format.

Type: integer

Required: False

Format: int64

objectCountByEncryptionType

The total number of objects that are in the bucket, grouped by server-side encryption type. This includes a grouping that reports the total number of objects that aren't encrypted or use client-side encryption.

Type: [ObjectCountByEncryptionType](#) (p. 164)

Required: False

errorMessage

A brief description of the error (`errorCode`) that prevented Amazon Macie from retrieving and processing information about the bucket and the bucket's objects. This value is null if Macie was able to retrieve and process the information.

Type: string

Required: False

errorCode

Specifies the error code for an error that prevented Amazon Macie from retrieving and processing information about the bucket and the bucket's objects. If this value is `ACCESS_DENIED`, Macie doesn't have permission to retrieve the information. For example, the bucket has a restrictive bucket policy and Amazon S3 denied the request. If this value is null, Macie was able to retrieve and process the information.

Type: [BucketMetadataErrorCode](#) (p. 160)

Required: False

classifiableSizeInBytes

The total storage size, in bytes, of the objects that Amazon Macie can analyze in the bucket. These objects use a supported storage class and have a file name extension for a supported file or storage format.

If versioning is enabled for the bucket, Macie calculates this value based on the size of the latest version of each applicable object in the bucket. This value doesn't reflect the storage size of all versions of each applicable object in the bucket.

Type: integer

Required: False

Format: int64

unclassifiableObjectCount

The total number of objects that Amazon Macie can't analyze in the bucket. These objects don't use a supported storage class or don't have a file name extension for a supported file or storage format.

Type: [ObjectLevelStatistics](#) (p. 165)

Required: False

accountId

The unique identifier for the AWS account that owns the bucket.

Type: string
Required: False

unclassifiableObjectSizeInBytes

The total storage size, in bytes, of the objects that Amazon Macie can't analyze in the bucket. These objects don't use a supported storage class or don't have a file name extension for a supported file or storage format.

Type: [ObjectLevelStatistics](#) (p. 165)
Required: False

jobDetails

Specifies whether any one-time or recurring classification jobs are configured to analyze objects in the bucket, and, if so, the details of the job that ran most recently.

Type: [JobDetails](#) (p. 161)
Required: False

sizeInBytesCompressed

The total storage size, in bytes, of the objects that are compressed (.gz, .gzip, .zip) files in the bucket.

If versioning is enabled for the bucket, Amazon Macie calculates this value based on the size of the latest version of each applicable object in the bucket. This value doesn't reflect the storage size of all versions of each applicable object in the bucket.

Type: integer
Required: False
Format: int64

MatchingResource

Provides statistical data and other information about an AWS resource that Amazon Macie monitors and analyzes for your account.

matchingBucket

The details of an S3 bucket that Amazon Macie monitors and analyzes.

Type: [MatchingBucket](#) (p. 162)
Required: False

ObjectCountByEncryptionType

Provides information about the number of objects that are in an S3 bucket and use certain types of server-side encryption, use client-side encryption, or aren't encrypted.

kmsManaged

The total number of objects that are encrypted with an AWS KMS key, either an AWS managed key or a customer managed key. The objects use AWS KMS encryption (SSE-KMS).

Type: integer

Required: False
Format: int64

s3Managed

The total number of objects that are encrypted with an Amazon S3 managed key. The objects use Amazon S3 managed encryption (SSE-S3).

Type: integer
Required: False
Format: int64

customerManaged

The total number of objects that are encrypted with a customer-provided key. The objects use customer-provided server-side encryption (SSE-C).

Type: integer
Required: False
Format: int64

unencrypted

The total number of objects that aren't encrypted or use client-side encryption.

Type: integer
Required: False
Format: int64

unknown

The total number of objects that Amazon Macie doesn't have current encryption metadata for. Macie can't provide current data about the encryption settings for these objects.

Type: integer
Required: False
Format: int64

ObjectLevelStatistics

Provides information about the total storage size (in bytes) or number of objects that Amazon Macie can't analyze in one or more S3 buckets. In a `BucketMetadata` or `MatchingBucket` object, this data is for a specific bucket. In a `GetBucketStatisticsResponse` object, this data is aggregated for the buckets in the query results. If versioning is enabled for a bucket, total storage size values are based on the size of the latest version of each applicable object in the bucket.

total

The total storage size (in bytes) or number of objects that Amazon Macie can't analyze because the objects use an unsupported storage class or don't have a file name extension for a supported file or storage format.

Type: integer
Required: False

Format: int64

storageClass

The total storage size (in bytes) or number of objects that Amazon Macie can't analyze because the objects use an unsupported storage class.

Type: integer

Required: False

Format: int64

fileType

The total storage size (in bytes) or number of objects that Amazon Macie can't analyze because the objects don't have a file name extension for a supported file or storage format.

Type: integer

Required: False

Format: int64

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string

Required: False

SearchResourcesBucketCriteria

Specifies property- and tag-based conditions that define filter criteria for including or excluding S3 buckets from the query results. Exclude conditions take precedence over include conditions.

excludes

The property- and tag-based conditions that determine which buckets to exclude from the results.

Type: [SearchResourcesCriteriaBlock](#) (p. 167)

Required: False

includes

The property- and tag-based conditions that determine which buckets to include in the results.

Type: [SearchResourcesCriteriaBlock](#) (p. 167)

Required: False

SearchResourcesComparator

The operator to use in a condition that filters the results of a query. Valid values are:

EQ
NE

SearchResourcesCriteria

Specifies a property- or tag-based filter condition for including or excluding AWS resources from the query results.

tagCriterion

A tag-based condition that defines an operator and tag keys, tag values, or tag key and value pairs for including or excluding resources from the results.

Type: [SearchResourcesTagCriterion](#) (p. 170)
Required: False

simpleCriterion

A property-based condition that defines a property, operator, and one or more values for including or excluding resources from the results.

Type: [SearchResourcesSimpleCriterion](#) (p. 168)
Required: False

SearchResourcesCriteriaBlock

Specifies property- and tag-based conditions that define filter criteria for including or excluding AWS resources from the query results.

and

An array of objects, one for each property- or tag-based condition that includes or excludes resources from the query results. If you specify more than one condition, Amazon Macie uses AND logic to join the conditions.

Type: Array of type [SearchResourcesCriteria](#) (p. 167)
Required: False

SearchResourcesRequest

Specifies criteria for filtering, sorting, and paginating the results of a query for statistical data and other information about AWS resources that Amazon Macie monitors and analyzes.

nextToken

The `nextToken` string that specifies which page of results to return in a paginated response.

Type: string
Required: False

maxResults

The maximum number of items to include in each page of the response. The default value is 50.

Type: integer
Required: False
Format: int32

bucketCriteria

The filter conditions that determine which S3 buckets to include or exclude from the query results.

Type: [SearchResourcesBucketCriteria](#) (p. 166)
Required: False

sortCriteria

The criteria to use to sort the results.

Type: [SearchResourcesSortCriteria](#) (p. 169)
Required: False

SearchResourcesResponse

Provides the results of a query that retrieved statistical data and other information about AWS resources that Amazon Macie monitors and analyzes for your account.

nextToken

The string to use in a subsequent request to get the next page of results in a paginated response. This value is null if there are no additional pages.

Type: string
Required: False

matchingResources

An array of objects, one for each resource that meets the filter criteria specified in the request.

Type: Array of type [MatchingResource](#) (p. 164)
Required: False

SearchResourcesSimpleCriterion

Specifies a property-based filter condition that determines which AWS resources are included or excluded from the query results.

comparator

The operator to use in the condition. Valid values are `EQ` (equals) and `NE` (not equals).

Type: [SearchResourcesComparator](#) (p. 166)
Required: False

values

An array that lists one or more values to use in the condition. If you specify multiple values, Amazon Macie uses OR logic to join the values. Valid values for each supported property (`key`) are:

- `ACCOUNT_ID` - A string that represents the unique identifier for the AWS account that owns the resource.
- `S3_BUCKET_EFFECTIVE_PERMISSION` - A string that represents an enumerated value that Macie defines for the [BucketPublicAccess.effectivePermission](#) property of an S3 bucket.
- `S3_BUCKET_NAME` - A string that represents the name of an S3 bucket.
- `S3_BUCKET_SHARED_ACCESS` - A string that represents an enumerated value that Macie defines for the [BucketMetadata.sharedAccess](#) property of an S3 bucket.

Values are case sensitive. Also, Macie doesn't support use of partial values or wildcard characters in values.

Type: Array of type string
Required: False

key

The property to use in the condition.

Type: [SearchResourcesSimpleCriterionKey](#) (p. 169)
Required: False

SearchResourcesSimpleCriterionKey

The property to use in a condition that filters the query results. Valid values are:

```
ACCOUNT_ID
S3_BUCKET_NAME
S3_BUCKET_EFFECTIVE_PERMISSION
S3_BUCKET_SHARED_ACCESS
```

SearchResourcesSortAttributeName

The property to sort the query results by. Valid values are:

```
ACCOUNT_ID
RESOURCE_NAME
S3_CLASSIFIABLE_OBJECT_COUNT
S3_CLASSIFIABLE_SIZE_IN_BYTES
```

SearchResourcesSortCriteria

Specifies criteria for sorting the results of a query for information about AWS resources that Amazon Macie monitors and analyzes.

orderBy

The sort order to apply to the results, based on the value for the property specified by the `attributeName` property. Valid values are: `ASC`, sort the results in ascending order; and, `DESC`, sort the results in descending order.

Type: string
Required: False
Values: `ASC` | `DESC`

attributeName

The property to sort the results by.

Type: [SearchResourcesSortAttributeName](#) (p. 169)

Required: False

SearchResourcesTagCriterion

Specifies a tag-based filter condition that determines which AWS resources are included or excluded from the query results.

comparator

The operator to use in the condition. Valid values are `EQ` (equals) and `NE` (not equals).

Type: [SearchResourcesComparator](#) (p. 166)

Required: False

tagValues

The tag keys, tag values, or tag key and value pairs to use in the condition.

Type: Array of type [SearchResourcesTagCriterionPair](#) (p. 170)

Required: False

SearchResourcesTagCriterionPair

Specifies a tag key, a tag value, or a tag key and value (as a pair) to use in a tag-based filter condition for a query. Tag keys and values are case sensitive. Also, Amazon Macie doesn't support use of partial values or wildcard characters in tag-based filter conditions.

value

The tag value to use in the condition.

Type: string

Required: False

key

The value for the tag key to use in the condition.

Type: string

Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string
Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string
Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string
Required: False

See also

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

SearchResources

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Export Configuration

The Export Configuration resource provides settings for storing data classification results in an Amazon Simple Storage Service (Amazon S3) bucket. A *data classification result*, also referred to as a *sensitive data discovery result*, is a record that logs details about the analysis of each Amazon S3 object that you configure a classification job to analyze. This includes objects that don't contain sensitive data, and

therefore don't produce a finding, and objects that Amazon Macie can't analyze due to issues such as permissions settings. Macie automatically creates these records for each (and every) classification job that you create and run. You can configure Macie to store these records in an S3 bucket that you specify, and encrypt them using an AWS Key Management Service (AWS KMS) key that you also specify. For more information, see [Storing and retaining sensitive data discovery results](#) in the *Amazon Macie User Guide*.

If you use Macie in multiple AWS Regions, you need to configure these settings for each Region in which you use Macie. If you prefer to store all classification results for all Regions in one S3 bucket, you can do this by specifying the same bucket, located in one specific Region, for each Region in which you use Macie.

You can use the Export Configuration resource to create, retrieve information about, or update settings for storing data classification results in an S3 bucket.

URI

/classification-export-configuration

HTTP methods

GET

Operation ID: GetClassificationExportConfiguration

Retrieves the configuration settings for storing data classification results.

Responses

Status code	Response model	Description
200	GetClassificationExportConfiguration (p. 174)	The request succeeded.
400	ValidationException (p. 174)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 174)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 174)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 174)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 174)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 175)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 175)	The request failed due to an unknown internal server error, exception, or failure.

PUT

Operation ID: PutClassificationExportConfiguration

Creates or updates the configuration settings for storing data classification results.

Responses

Status code	Response model	Description
200	PutClassificationExportConfiguration (p. 174)	The request succeeded.
400	ValidationException (p. 174)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 174)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 174)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 174)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 174)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 175)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 175)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

PUT schema

```
{
  "configuration": {
    "s3Destination": {
      "bucketName": "string",
      "kmsKeyArn": "string",
      "keyPrefix": "string"
    }
  }
}
```

Response bodies

GetClassificationExportConfigurationResponse schema

```
{
  "configuration": {
    "s3Destination": {
      "bucketName": "string",
      "kmsKeyArn": "string",
      "keyPrefix": "string"
    }
  }
}
```

PutClassificationExportConfigurationResponse schema

```
{
  "configuration": {
    "s3Destination": {
      "bucketName": "string",
      "kmsKeyArn": "string",
      "keyPrefix": "string"
    }
  }
}
```

ValidationException schema

```
{
  "message": "string"
}
```

ServiceQuotaExceededException schema

```
{
  "message": "string"
}
```

AccessDeniedException schema

```
{
  "message": "string"
}
```

ResourceNotFoundException schema

```
{
  "message": "string"
}
```

ConflictException schema

```
{
```

```
"message": "string"
}
```

ThrottlingException schema

```
{
  "message": "string"
}
```

InternalServerError schema

```
{
  "message": "string"
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

ClassificationExportConfiguration

Specifies where to store data classification results, and the encryption settings to use when storing results in that location. Currently, you can store classification results only in an S3 bucket.

s3Destination

The S3 bucket to store data classification results in, and the encryption settings to use when storing results in that bucket.

Type: [S3Destination](#) (p. 177)

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

GetClassificationExportConfigurationResponse

Provides information about the current configuration settings for storing data classification results.

configuration

The location where data classification results are stored, and the encryption settings that are used when storing results in that location.

Type: [ClassificationExportConfiguration](#) (p. 175)

Required: False

InternalServerErrorException

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string

Required: False

PutClassificationExportConfigurationRequest

Specifies where to store data classification results, and the encryption settings to use when storing results in that location. Currently, you can store classification results only in an S3 bucket.

configuration

The location to store data classification results in, and the encryption settings to use when storing results in that location.

Type: [ClassificationExportConfiguration](#) (p. 175)

Required: True

PutClassificationExportConfigurationResponse

Provides information about updated settings for storing data classification results.

configuration

The location where the data classification results are stored, and the encryption settings that are used when storing results in that location.

Type: [ClassificationExportConfiguration](#) (p. 175)

Required: False

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string

Required: False

S3Destination

Specifies an S3 bucket to store data classification results in, and the encryption settings to use when storing results in that bucket.

bucketName

The name of the bucket.

Type: string

Required: True

kmsKeyArn

The Amazon Resource Name (ARN) of the AWS KMS key to use for encryption of the results. This must be the ARN of an existing, symmetric, customer managed KMS key that's in the same AWS Region as the bucket.

Type: string

Required: True

keyPrefix

The path prefix to use in the path to the location in the bucket. This prefix specifies where to store classification results in the bucket.

Type: string

Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string

Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string
Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string
Required: False

See also

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

GetClassificationExportConfiguration

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

PutClassificationExportConfiguration

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Findings Descriptions

The Findings Descriptions resource represents the repository of findings for your Amazon Macie account. A *finding* is a detailed report of a potential policy violation for an Amazon Simple Storage Service (Amazon S3) bucket or sensitive data in an S3 object. Each finding provides a severity rating, information

about the affected resources, and additional details, such as when and how Macie found the issue. For information about the types of findings that Macie can report, see [Types of Amazon Macie findings](#) in the *Amazon Macie User Guide*.

You can use this resource to retrieve the details of one or more findings. To customize and refine your query, you can use supported parameters to specify which findings to retrieve and how to sort the results.

URI

/findings/describe

HTTP methods

POST

Operation ID: GetFindings

Retrieves the details of one or more findings.

Responses

Status code	Response model	Description
200	GetFindingsResponse (p. 180)	The request succeeded.
400	ValidationException (p. 185)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 185)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 185)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 185)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 185)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 185)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 185)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

POST schema

```
{
  "findingIds": [
    "string"
  ],
  "sortCriteria": {
    "orderBy": enum,
    "attributeName": "string"
  }
}
```

Response bodies

GetFindingsResponse schema

```
{
  "findings": [
    {
      "severity": {
        "score": integer,
        "description": enum
      },
      "schemaVersion": "string",
      "count": integer,
      "description": "string",
      "title": "string",
      "type": enum,
      "sample": boolean,
      "archived": boolean,
      "accountId": "string",
      "createdAt": "string",
      "partition": "string",
      "classificationDetails": {
        "result": {
          "customDataIdentifiers": {
            "totalCount": integer,
            "detections": [
              {
                "occurrences": {
                  "lineRanges": [
                    {
                      "startColumn": integer,
                      "start": integer,
                      "end": integer
                    }
                  ],
                  "offsetRanges": [
                    {
                      "startColumn": integer,
                      "start": integer,
                      "end": integer
                    }
                  ]
                },
                "cells": [
                  {
                    "column": integer,
                    "row": integer,
                    "columnName": "string",
                    "cellReference": "string"
                  }
                ]
              }
            ],
            "pages": [
```

```

        {
            "pageNumber": integer,
            "offsetRange": {
                "startColumn": integer,
                "start": integer,
                "end": integer
            },
            "lineRange": {
                "startColumn": integer,
                "start": integer,
                "end": integer
            }
        }
    ],
    "records": [
        {
            "jsonPath": "string",
            "recordIndex": integer
        }
    ]
},
"count": integer,
"name": "string",
"arn": "string"
}
]
},
"sensitiveData": [
    {
        "category": enum,
        "totalCount": integer,
        "detections": [
            {
                "occurrences": {
                    "lineRanges": [
                        {
                            "startColumn": integer,
                            "start": integer,
                            "end": integer
                        }
                    ],
                    "offsetRanges": [
                        {
                            "startColumn": integer,
                            "start": integer,
                            "end": integer
                        }
                    ]
                },
                "cells": [
                    {
                        "column": integer,
                        "row": integer,
                        "columnName": "string",
                        "cellReference": "string"
                    }
                ],
                "pages": [
                    {
                        "pageNumber": integer,
                        "offsetRange": {
                            "startColumn": integer,
                            "start": integer,
                            "end": integer
                        },
                        "lineRange": {
                            "startColumn": integer,

```

```

        "start": integer,
        "end": integer
    }
},
"records": [
    {
        "jsonPath": "string",
        "recordIndex": integer
    }
],
"count": integer,
"type": "string"
}
]
}
],
"sizeClassified": integer,
"mimeType": "string",
"additionalOccurrences": boolean,
"status": {
    "reason": "string",
    "code": "string"
}
},
"jobId": "string",
"detailedResultsLocation": "string",
"jobArn": "string"
},
"policyDetails": {
    "actor": {
        "domainDetails": {
            "domainName": "string"
        },
        "ipAddressDetails": {
            "ipOwner": {
                "org": "string",
                "asnOrg": "string",
                "isp": "string",
                "asn": "string"
            },
            "ipCity": {
                "name": "string"
            },
            "ipAddressV4": "string",
            "ipCountry": {
                "code": "string",
                "name": "string"
            },
            "ipGeoLocation": {
                "lon": number,
                "lat": number
            }
        },
        "userIdentity": {
            "federatedUser": {
                "accessKeyId": "string",
                "sessionContext": {
                    "sessionIssuer": {
                        "accountId": "string",
                        "principalId": "string",
                        "userName": "string",
                        "type": "string",
                        "arn": "string"
                    }
                }
            }
        }
    }
}

```

```
        "attributes": {
            "mfaAuthenticated": boolean,
            "creationDate": "string"
        }
    },
    "accountId": "string",
    "principalId": "string",
    "arn": "string"
},
"awsAccount": {
    "accountId": "string",
    "principalId": "string"
},
"root": {
    "accountId": "string",
    "principalId": "string",
    "arn": "string"
},
"assumedRole": {
    "accessKeyId": "string",
    "sessionContext": {
        "sessionIssuer": {
            "accountId": "string",
            "principalId": "string",
            "userName": "string",
            "type": "string",
            "arn": "string"
        },
        "attributes": {
            "mfaAuthenticated": boolean,
            "creationDate": "string"
        }
    },
    "accountId": "string",
    "principalId": "string",
    "arn": "string"
},
"type": enum,
"iamUser": {
    "accountId": "string",
    "principalId": "string",
    "userName": "string",
    "arn": "string"
},
"awsService": {
    "invokedBy": "string"
}
}
},
"action": {
    "actionType": enum,
    "apiCallDetails": {
        "lastSeen": "string",
        "firstSeen": "string",
        "apiServiceName": "string",
        "api": "string"
    }
}
},
"id": "string",
"category": enum,
"region": "string",
"resourcesAffected": {
    "s3Object": {
        "path": "string",
        "extension": "string",
```

```

"versionId": "string",
"storageClass": enum,
"bucketArn": "string",
"serverSideEncryption": {
  "encryptionType": enum,
  "kmsMasterKeyId": "string"
},
"size": integer,
"publicAccess": boolean,
"eTag": "string",
"lastModified": "string",
"key": "string",
"tags": [
  {
    "value": "string",
    "key": "string"
  }
]
},
"s3Bucket": {
  "owner": {
    "displayName": "string",
    "id": "string"
  },
  "createdAt": "string",
  "allowsUnencryptedObjectUploads": enum,
  "publicAccess": {
    "effectivePermission": enum,
    "permissionConfiguration": {
      "accountLevelPermissions": {
        "blockPublicAccess": {
          "blockPublicPolicy": boolean,
          "restrictPublicBuckets": boolean,
          "blockPublicAcls": boolean,
          "ignorePublicAcls": boolean
        }
      },
      "bucketLevelPermissions": {
        "accessControlList": {
          "allowsPublicReadAccess": boolean,
          "allowsPublicWriteAccess": boolean
        },
        "blockPublicAccess": {
          "blockPublicPolicy": boolean,
          "restrictPublicBuckets": boolean,
          "blockPublicAcls": boolean,
          "ignorePublicAcls": boolean
        },
        "bucketPolicy": {
          "allowsPublicReadAccess": boolean,
          "allowsPublicWriteAccess": boolean
        }
      }
    }
  },
  "name": "string",
  "defaultServerSideEncryption": {
    "encryptionType": enum,
    "kmsMasterKeyId": "string"
  },
  "arn": "string",
  "tags": [
    {
      "value": "string",
      "key": "string"
    }
  ]
}

```

```
    ]
  },
  "updatedAt": "string"
}
]
```

ValidationException schema

```
{
  "message": "string"
}
```

ServiceQuotaExceededException schema

```
{
  "message": "string"
}
```

AccessDeniedException schema

```
{
  "message": "string"
}
```

ResourceNotFoundException schema

```
{
  "message": "string"
}
```

ConflictException schema

```
{
  "message": "string"
}
```

ThrottlingException schema

```
{
  "message": "string"
}
```

InternalServerError schema

```
{
  "message": "string"
}
```



```
}
```

Properties

AccessControlList

Provides information about the permissions settings of the bucket-level access control list (ACL) for an S3 bucket.

allowsPublicReadAccess

Specifies whether the ACL grants the general public with read access permissions for the bucket.

Type: boolean
Required: False

allowsPublicWriteAccess

Specifies whether the ACL grants the general public with write access permissions for the bucket.

Type: boolean
Required: False

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string
Required: False

AccountLevelPermissions

Provides information about the account-level permissions settings that apply to an S3 bucket.

blockPublicAccess

The block public access settings for the AWS account that owns the bucket.

Type: [BlockPublicAccess](#) (p. 188)
Required: False

ApiCallDetails

Provides information about an API operation that an entity invoked for an affected resource.

lastSeen

The most recent date and time, in UTC and extended ISO 8601 format, when the specified operation (`api`) was invoked and produced the finding.

Type: string
Required: False
Format: date-time

firstSeen

The first date and time, in UTC and extended ISO 8601 format, when any operation was invoked and produced the finding.

Type: string
Required: False
Format: date-time

apiServiceName

The URL of the AWS service that provides the operation, for example: `s3.amazonaws.com`.

Type: string
Required: False

api

The name of the operation that was invoked most recently and produced the finding.

Type: string
Required: False

AssumedRole

Provides information about an identity that performed an action on an affected resource by using temporary security credentials. The credentials were obtained using the `AssumeRole` operation of the AWS Security Token Service (AWS STS) API.

accessKeyId

The AWS access key ID that identifies the credentials.

Type: string
Required: False

sessionContext

The details of the session that was created for the credentials, including the entity that issued the session.

Type: [SessionContext](#) (p. 213)
Required: False

accountId

The unique identifier for the AWS account that owns the entity that was used to get the credentials.

Type: string

Required: False

principalId

The unique identifier for the entity that was used to get the credentials.

Type: string

Required: False

arn

The Amazon Resource Name (ARN) of the entity that was used to get the credentials.

Type: string

Required: False

AwsAccount

Provides information about an AWS account and entity that performed an action on an affected resource. The action was performed using the credentials for an AWS account other than your own account.

accountId

The unique identifier for the AWS account.

Type: string

Required: False

principalId

The unique identifier for the entity that performed the action.

Type: string

Required: False

AwsService

Provides information about an AWS service that performed an action on an affected resource.

invokedBy

The name of the AWS service that performed the action.

Type: string

Required: False

BlockPublicAccess

Provides information about the block public access settings for an S3 bucket. These settings can apply to a bucket at the account level or bucket level. For detailed information about each setting, see [Blocking public access to your Amazon S3 storage](#) in the *Amazon Simple Storage Service User Guide*.

blockPublicPolicy

Specifies whether Amazon S3 blocks public bucket policies for the bucket.

Type: boolean
Required: False

restrictPublicBuckets

Specifies whether Amazon S3 restricts public bucket policies for the bucket.

Type: boolean
Required: False

blockPublicAcls

Specifies whether Amazon S3 blocks public access control lists (ACLs) for the bucket and objects in the bucket.

Type: boolean
Required: False

ignorePublicAcls

Specifies whether Amazon S3 ignores public ACLs for the bucket and objects in the bucket.

Type: boolean
Required: False

BucketLevelPermissions

Provides information about the bucket-level permissions settings for an S3 bucket.

accessControlList

The permissions settings of the access control list (ACL) for the bucket. This value is null if an ACL hasn't been defined for the bucket.

Type: [AccessControlList](#) (p. 186)
Required: False

blockPublicAccess

The block public access settings for the bucket.

Type: [BlockPublicAccess](#) (p. 188)
Required: False

bucketPolicy

The permissions settings of the bucket policy for the bucket. This value is null if a bucket policy hasn't been defined for the bucket.

Type: [BucketPolicy](#) (p. 190)
Required: False

BucketPermissionConfiguration

Provides information about the account-level and bucket-level permissions settings for an S3 bucket.

accountLevelPermissions

The account-level permissions settings that apply to the bucket.

Type: [AccountLevelPermissions](#) (p. 186)

Required: False

bucketLevelPermissions

The bucket-level permissions settings for the bucket.

Type: [BucketLevelPermissions](#) (p. 189)

Required: False

BucketPolicy

Provides information about the permissions settings of the bucket policy for an S3 bucket.

allowsPublicReadAccess

Specifies whether the bucket policy allows the general public to have read access to the bucket.

Type: boolean

Required: False

allowsPublicWriteAccess

Specifies whether the bucket policy allows the general public to have write access to the bucket.

Type: boolean

Required: False

BucketPublicAccess

Provides information about the permissions settings that determine whether an S3 bucket is publicly accessible.

effectivePermission

Specifies whether the bucket is publicly accessible due to the combination of permissions settings that apply to the bucket. Possible values are:

- `NOT_PUBLIC` - The bucket isn't publicly accessible.
- `PUBLIC` - The bucket is publicly accessible.
- `UNKNOWN` - Amazon Macie can't determine whether the bucket is publicly accessible.

Type: string

Required: False

Values: `PUBLIC` | `NOT_PUBLIC` | `UNKNOWN`

permissionConfiguration

The account-level and bucket-level permissions settings for the bucket.

Type: [BucketPermissionConfiguration](#) (p. 190)

Required: False

Cell

Specifies the location of an occurrence of sensitive data in a Microsoft Excel workbook, CSV file, or TSV file.

column

The column number of the column that contains the sensitive data. For a Microsoft Excel workbook, this value correlates to the alphabetical character(s) for a column identifier, for example: 1 for column A, 2 for column B, and so on.

Type: integer

Required: False

Format: int64

row

The row number of the row that contains the sensitive data.

Type: integer

Required: False

Format: int64

columnName

The name of the column that contains the sensitive data, if available.

Type: string

Required: False

cellReference

The location of the cell, as an absolute cell reference, that contains the sensitive data, for example `Sheet2!C5` for cell C5 on Sheet2 in a Microsoft Excel workbook. This value is null for CSV and TSV files.

Type: string

Required: False

ClassificationDetails

Provides information about a sensitive data finding, including the classification job that produced the finding.

result

The status and other details of the finding.

Type: [ClassificationResult](#) (p. 192)

Required: False

jobId

The unique identifier for the classification job that produced the finding.

Type: string

Required: False

detailedResultsLocation

The path to the folder or file (in Amazon S3) that contains the corresponding sensitive data discovery result for the finding. If a finding applies to a large archive or compressed file, this value is the path to a folder. Otherwise, this value is the path to a file.

Type: string

Required: False

jobArn

The Amazon Resource Name (ARN) of the classification job that produced the finding.

Type: string

Required: False

ClassificationResult

Provides the details of a sensitive data finding, including the types, number of occurrences, and locations of the sensitive data that was detected.

customDataIdentifiers

The custom data identifiers that detected the sensitive data and the number of occurrences of the data that they detected.

Type: [CustomDataIdentifiers](#) (p. 194)

Required: False

sensitiveData

The category, types, and number of occurrences of the sensitive data that produced the finding.

Type: Array of type [SensitiveDataItem](#) (p. 211)

Required: False

sizeClassified

The total size, in bytes, of the data that the finding applies to.

Type: integer

Required: False

Format: int64

contentType

The type of content, as a MIME type, that the finding applies to. For example, `application/gzip`, for a GNU Gzip compressed archive file, or `application/pdf`, for an Adobe Portable Document Format file.

Type: string
Required: False

additionalOccurrences

Specifies whether Amazon Macie detected additional occurrences of sensitive data in the S3 object. A finding includes location data for a maximum of 15 occurrences of sensitive data.

This value can help you determine whether to investigate additional occurrences of sensitive data in an object. You can do this by referring to the corresponding sensitive data discovery result for the finding (`ClassificationDetails.detailedResultsLocation`).

Type: boolean
Required: False

status

The status of the finding.

Type: [ClassificationResultStatus](#) (p. 193)
Required: False

ClassificationResultStatus

Provides information about the status of a sensitive data finding.

reason

A brief description of the status of the finding. Amazon Macie uses this value to notify you of any errors, warnings, or considerations that might impact your analysis of the finding.

Type: string
Required: False

code

The status of the finding. Possible values are:

- **COMPLETE** - Amazon Macie successfully completed its analysis of the S3 object that the finding applies to.
- **PARTIAL** - Macie analyzed only a subset of the data in the S3 object that the finding applies to. For example, the object is an archive file that contains files in an unsupported format.
- **SKIPPED** - Macie wasn't able to analyze the S3 object that the finding applies to. For example, the object is a file in an unsupported format.

Type: string
Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

CustomDataIdentifiers

Provides information about custom data identifiers that produced a sensitive data finding, and the number of occurrences of the data that they detected for the finding.

totalCount

The total number of occurrences of the data that was detected by the custom data identifiers and produced the finding.

Type: integer

Required: False

Format: int64

detections

The custom data identifiers that detected the data, and the number of occurrences of the data that each identifier detected.

Type: Array of type [CustomDetection](#) (p. 194)

Required: False

CustomDetection

Provides information about a custom data identifier that produced a sensitive data finding, and the sensitive data that it detected for the finding.

occurrences

The location of 1-15 occurrences of the sensitive data that the custom data identifier detected. A finding includes location data for a maximum of 15 occurrences of sensitive data.

Type: [Occurrences](#) (p. 204)

Required: False

count

The total number of occurrences of the sensitive data that the custom data identifier detected.

Type: integer

Required: False

Format: int64

name

The name of the custom data identifier.

Type: string

Required: False

arn

The Amazon Resource Name (ARN) of the custom data identifier.

Type: string

Required: False

DefaultDetection

Provides information about a type of sensitive data that was detected by a managed data identifier and produced a sensitive data finding.

occurrences

The location of 1-15 occurrences of the sensitive data that was detected. A finding includes location data for a maximum of 15 occurrences of sensitive data.

Type: [Occurrences](#) (p. 204)

Required: False

count

The total number of occurrences of the type of sensitive data that was detected.

Type: integer

Required: False

Format: int64

type

The type of sensitive data that was detected. For example, `AWS_CREDENTIALS`, `PHONE_NUMBER`, or `ADDRESS`.

Type: string

Required: False

DomainDetails

Provides information about the domain name of the device that an entity used to perform an action on an affected resource.

domainName

The name of the domain.

Type: string

Required: False

EncryptionType

The type of server-side encryption that's used to encrypt an S3 object or objects in an S3 bucket. Valid values are:

NONE
AES256
aws:kms
UNKNOWN

FederatedUser

Provides information about an identity that performed an action on an affected resource by using temporary security credentials. The credentials were obtained using the `GetFederationToken` operation of the AWS Security Token Service (AWS STS) API.

accessKeyId

The AWS access key ID that identifies the credentials.

Type: string
Required: False

sessionContext

The details of the session that was created for the credentials, including the entity that issued the session.

Type: [SessionContext](#) (p. 213)
Required: False

accountId

The unique identifier for the AWS account that owns the entity that was used to get the credentials.

Type: string
Required: False

principalId

The unique identifier for the entity that was used to get the credentials.

Type: string
Required: False

arn

The Amazon Resource Name (ARN) of the entity that was used to get the credentials.

Type: string
Required: False

Finding

Provides the details of a finding.

severity

The severity level and score for the finding.

Type: [Severity](#) (p. 214)

Required: False

schemaVersion

The version of the schema that was used to define the data structures in the finding.

Type: string

Required: False

count

The total number of occurrences of the finding. For sensitive data findings, this value is always 1. All sensitive data findings are considered new (unique) because they derive from individual classification jobs.

Type: integer

Required: False

Format: int64

description

The description of the finding.

Type: string

Required: False

title

The brief description of the finding.

Type: string

Required: False

type

The type of the finding.

Type: [FindingType](#) (p. 200)

Required: False

sample

Specifies whether the finding is a sample finding. A *sample finding* is a finding that uses example data to demonstrate what a finding might contain.

Type: boolean

Required: False

archived

Specifies whether the finding is archived (suppressed).

Type: boolean

Required: False

accountId

The unique identifier for the AWS account that the finding applies to. This is typically the account that owns the affected resource.

Type: string

Required: False

createdAt

The date and time, in UTC and extended ISO 8601 format, when the finding was created.

Type: string

Required: False

Format: date-time

partition

The AWS partition that Amazon Macie created the finding in.

Type: string

Required: False

classificationDetails

The details of a sensitive data finding. This value is null for a policy finding.

Type: [ClassificationDetails \(p. 191\)](#)

Required: False

policyDetails

The details of a policy finding. This value is null for a sensitive data finding.

Type: [PolicyDetails \(p. 206\)](#)

Required: False

id

The unique identifier for the finding. This is a random string that Amazon Macie generates and assigns to a finding when it creates the finding.

Type: string

Required: False

category

The category of the finding. Possible values are: `CLASSIFICATION`, for a sensitive data finding; and, `POLICY`, for a policy finding.

Type: [FindingCategory \(p. 200\)](#)

Required: False

region

The AWS Region that Amazon Macie created the finding in.

Type: string

Required: False

resourcesAffected

The resources that the finding applies to.

Type: [ResourcesAffected](#) (p. 207)

Required: False

updatedAt

The date and time, in UTC and extended ISO 8601 format, when the finding was last updated. For sensitive data findings, this value is the same as the value for the `createdAt` property. All sensitive data findings are considered new (unique) because they derive from individual classification jobs.

Type: string

Required: False

Format: date-time

FindingAction

Provides information about an action that occurred for a resource and produced a policy finding.

actionType

The type of action that occurred for the affected resource. This value is typically `AWS_API_CALL`, which indicates that an entity invoked an API operation for the resource.

Type: [FindingActionType](#) (p. 199)

Required: False

apiCallDetails

The invocation details of the API operation that an entity invoked for the affected resource, if the value for the `actionType` property is `AWS_API_CALL`.

Type: [ApiCallDetails](#) (p. 186)

Required: False

FindingActionType

The type of action that occurred for the resource and produced the policy finding:

`AWS_API_CALL`

FindingActor

Provides information about an entity that performed an action that produced a policy finding for a resource.

domainDetails

The domain name of the device that the entity used to perform the action on the affected resource.

Type: [DomainDetails](#) (p. 195)

Required: False

ipAddressDetails

The IP address of the device that the entity used to perform the action on the affected resource. This object also provides information such as the owner and geographic location for the IP address.

Type: [IpAddressDetails](#) (p. 202)

Required: False

userIdentity

The type and other characteristics of the entity that performed the action on the affected resource.

Type: [UserIdentity](#) (p. 215)

Required: False

FindingCategory

The category of the finding. Valid values are:

CLASSIFICATION
POLICY

FindingType

The type of finding. For details about each type, see [Types of Amazon Macie findings](#) in the *Amazon Macie User Guide*. Valid values are:

SensitiveData:S3Object/Multiple
SensitiveData:S3Object/Financial
SensitiveData:S3Object/Personal
SensitiveData:S3Object/Credentials
SensitiveData:S3Object/CustomIdentifier
Policy:IAMUser/S3BucketPublic
Policy:IAMUser/S3BucketSharedExternally
Policy:IAMUser/S3BucketReplicatedExternally
Policy:IAMUser/S3BucketEncryptionDisabled
Policy:IAMUser/S3BlockPublicAccessDisabled

GetFindingsRequest

Specifies one or more findings to retrieve.

findingIds

An array of strings that lists the unique identifiers for the findings to retrieve.

Type: Array of type string

Required: True

sortCriteria

The criteria for sorting the results of the request.

Type: [SortCriteria](#) (p. 215)

Required: False

GetFindingsResponse

Provides the results of a request for one or more findings.

findings

An array of objects, one for each finding that meets the criteria specified in the request.

Type: Array of type [Finding](#) (p. 196)

Required: False

IamUser

Provides information about an AWS Identity and Access Management (IAM) user who performed an action on an affected resource.

accountId

The unique identifier for the AWS account that's associated with the IAM user who performed the action.

Type: string

Required: False

principalId

The unique identifier for the IAM user who performed the action.

Type: string

Required: False

userName

The user name of the IAM user who performed the action.

Type: string

Required: False

arn

The Amazon Resource Name (ARN) of the principal that performed the action. The last section of the ARN contains the name of the user who performed the action.

Type: string

Required: False

InternalServerErrorException

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string
Required: False

IpAddressDetails

Provides information about the IP address of the device that an entity used to perform an action on an affected resource.

ipOwner

The registered owner of the IP address.

Type: [IpOwner \(p. 203\)](#)
Required: False

ipCity

The city that the IP address originated from.

Type: [IpCity \(p. 202\)](#)
Required: False

ipAddressV4

The Internet Protocol version 4 (IPv4) address of the device.

Type: string
Required: False

ipCountry

The country that the IP address originated from.

Type: [IpCountry \(p. 203\)](#)
Required: False

ipGeoLocation

The geographic coordinates of the location that the IP address originated from.

Type: [IpGeoLocation \(p. 203\)](#)
Required: False

IpCity

Provides information about the city that an IP address originated from.

name

The name of the city.

Type: string

Required: False

IpCountry

Provides information about the country that an IP address originated from.

code

The two-character code, in ISO 3166-1 alpha-2 format, for the country that the IP address originated from. For example, `US` for the United States.

Type: string

Required: False

name

The name of the country that the IP address originated from.

Type: string

Required: False

IpGeoLocation

Provides geographic coordinates that indicate where a specified IP address originated from.

lon

The longitude coordinate of the location, rounded to four decimal places.

Type: number

Required: False

lat

The latitude coordinate of the location, rounded to four decimal places.

Type: number

Required: False

IpOwner

Provides information about the registered owner of an IP address.

org

The name of the organization that owned the IP address.

Type: string

Required: False

asnOrg

The organization identifier that's associated with the autonomous system number (ASN) for the autonomous system that included the IP address.

Type: string
Required: False

isp

The name of the internet service provider (ISP) that owned the IP address.

Type: string
Required: False

asn

The autonomous system number (ASN) for the autonomous system that included the IP address.

Type: string
Required: False

KeyValuePair

Provides information about the tags that are associated with an S3 bucket or object. Each tag consists of a required tag key and an associated tag value.

value

One part of a key-value pair that comprises a tag. A tag value acts as a descriptor for a tag key. A tag value can be an empty string.

Type: string
Required: False

key

One part of a key-value pair that comprises a tag. A tag key is a general label that acts as a category for more specific tag values.

Type: string
Required: False

Occurrences

Specifies the location of 1-15 occurrences of sensitive data that was detected by a managed data identifier or a custom data identifier and produced a sensitive data finding.

lineRanges

An array of objects, one for each occurrence of sensitive data in a non-binary text file, such as an HTML, TXT, or XML file. Each Range object specifies a line or inclusive range of lines that contains the sensitive data, and the position of the data on the specified line or lines.

This value is often null for file types that are supported by `Cell`, `Page`, or `Record` objects. Exceptions are the location of sensitive data in: unstructured sections of an otherwise structured file, such as a

comment in a file; a malformed file that Amazon Macie analyzes as plain text; and, a CSV or TSV file that has any column names that contain sensitive data.

Type: Array of type [Range \(p. 206\)](#)
Required: False

offsetRanges

Reserved for future use.

Type: Array of type [Range \(p. 206\)](#)
Required: False

cells

An array of objects, one for each occurrence of sensitive data in a Microsoft Excel workbook, CSV file, or TSV file. This value is null for all other types of files.

Each `Cell` object specifies a cell or field that contains the sensitive data.

Type: Array of type [Cell \(p. 191\)](#)
Required: False

pages

An array of objects, one for each occurrence of sensitive data in an Adobe Portable Document Format file. This value is null for all other types of files.

Each `Page` object specifies a page that contains the sensitive data.

Type: Array of type [Page \(p. 205\)](#)
Required: False

records

An array of objects, one for each occurrence of sensitive data in an Apache Avro object container, Apache Parquet file, JSON file, or JSON Lines file. This value is null for all other types of files.

For an Avro object container or Parquet file, each `Record` object specifies a record index and the path to a field in a record that contains the sensitive data. For a JSON or JSON Lines file, each `Record` object specifies the path to a field or array that contains the sensitive data. For a JSON Lines file, it also specifies the index of the line that contains the data.

Type: Array of type [Record \(p. 207\)](#)
Required: False

Page

Specifies the location of an occurrence of sensitive data in an Adobe Portable Document Format file.

pageNumber

The page number of the page that contains the sensitive data.

Type: integer
Required: False

Format: int64

offsetRange

Reserved for future use.

Type: [Range \(p. 206\)](#)

Required: False

lineRange

Reserved for future use.

Type: [Range \(p. 206\)](#)

Required: False

PolicyDetails

Provides the details of a policy finding.

actor

The entity that performed the action that produced the finding.

Type: [FindingActor \(p. 199\)](#)

Required: False

action

The action that produced the finding.

Type: [FindingAction \(p. 199\)](#)

Required: False

Range

Specifies the location of an occurrence of sensitive data in a non-binary text file, such as an HTML, TXT, or XML file.

startColumn

The number of characters, with spaces and starting from 1, from the beginning of the first line that contains the sensitive data (`start`) to the beginning of the sensitive data.

Type: integer

Required: False

Format: int64

start

The number of lines from the beginning of the file to the beginning of the sensitive data.

Type: integer

Required: False

Format: int64

end

The number of lines from the beginning of the file to the end of the sensitive data.

Type: integer
Required: False
Format: int64

Record

Specifies the location of an occurrence of sensitive data in an Apache Avro object container, Apache Parquet file, JSON file, or JSON Lines file.

jsonPath

The path, as a JSONPath expression, to the sensitive data. For an Avro object container or Parquet file, this is the path to the field in the record (`recordIndex`) that contains the data. For a JSON or JSON Lines file, this is the path to the field or array that contains the data. If the data is a value in an array, the path also indicates which value contains the data.

If Amazon Macie detects sensitive data in the name of any element in the path, Macie omits this field. If the name of an element exceeds 20 characters, Macie truncates the name by removing characters from the beginning of the name. If the resulting full path exceeds 250 characters, Macie also truncates the path, starting with the first element in the path, until the path contains 250 or fewer characters.

Type: string
Required: False

recordIndex

For an Avro object container or Parquet file, the record index, starting from 0, for the record that contains the sensitive data. For a JSON Lines file, the line index, starting from 0, for the line that contains the sensitive data. This value is always 0 for JSON files.

Type: integer
Required: False
Format: int64

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string
Required: False

ResourcesAffected

Provides information about the resources that a finding applies to.

s3Object

The details of the S3 object that the finding applies to.

Type: [S3Object](#) (p. 209)

Required: False

s3Bucket

The details of the S3 bucket that the finding applies to.

Type: [S3Bucket](#) (p. 208)

Required: False

S3Bucket

Provides information about the S3 bucket that a finding applies to.

owner

The display name and canonical user ID for the AWS account that owns the bucket.

Type: [S3BucketOwner](#) (p. 209)

Required: False

createdAt

The date and time, in UTC and extended ISO 8601 format, when the bucket was created.

Type: string

Required: False

Format: date-time

allowsUnencryptedObjectUploads

Specifies whether the bucket policy for the bucket requires server-side encryption of objects when objects are uploaded to the bucket. Possible values are:

- **FALSE** - The bucket policy requires server-side encryption of new objects. `PutObject` requests must include the `x-amz-server-side-encryption` header and the value for that header must be `AES256` or `aws:kms`.
- **TRUE** - The bucket doesn't have a bucket policy or it has a bucket policy that doesn't require server-side encryption of new objects. If a bucket policy exists, it doesn't require `PutObject` requests to include the `x-amz-server-side-encryption` header and it doesn't require the value for that header to be `AES256` or `aws:kms`.
- **UNKNOWN** - Amazon Macie can't determine whether the bucket policy requires server-side encryption of objects.

Type: string

Required: False

Values: `TRUE` | `FALSE` | `UNKNOWN`

publicAccess

The permissions settings that determine whether the bucket is publicly accessible.

Type: [BucketPublicAccess](#) (p. 190)

Required: False

name

The name of the bucket.

Type: string

Required: False

defaultServerSideEncryption

The type of server-side encryption that's used by default to encrypt objects in the bucket.

Type: [ServerSideEncryption](#) (p. 212)

Required: False

arn

The Amazon Resource Name (ARN) of the bucket.

Type: string

Required: False

tags

The tags that are associated with the bucket.

Type: Array of type [KeyValuePair](#) (p. 204)

Required: False

S3BucketOwner

Provides information about the AWS account that owns an S3 bucket.

displayName

The display name of the account that owns the bucket.

Type: string

Required: False

id

The canonical user ID for the account that owns the bucket.

Type: string

Required: False

S3Object

Provides information about the S3 object that a finding applies to.

path

The path to the object, including the full key (name).

Type: string

Required: False

extension

The file name extension of the object. If the object doesn't have a file name extension, this value is "".

Type: string

Required: False

versionId

The identifier for the affected version of the object.

Type: string

Required: False

storageClass

The storage class of the object.

Type: [StorageClass](#) (p. 215)

Required: False

bucketArn

The Amazon Resource Name (ARN) of the bucket that contains the object.

Type: string

Required: False

serverSideEncryption

The type of server-side encryption that's used to encrypt the object.

Type: [ServerSideEncryption](#) (p. 212)

Required: False

size

The total storage size, in bytes, of the object.

Type: integer

Required: False

Format: int64

publicAccess

Specifies whether the object is publicly accessible due to the combination of permissions settings that apply to the object.

Type: boolean
Required: False

eTag

The entity tag (ETag) that identifies the affected version of the object. If the object was overwritten or changed after Amazon Macie produced the finding, this value might be different from the current ETag for the object.

Type: string
Required: False

lastModified

The date and time, in UTC and extended ISO 8601 format, when the object was last modified.

Type: string
Required: False
Format: date-time

key

The full key (name) that's assigned to the object.

Type: string
Required: False

tags

The tags that are associated with the object.

Type: Array of type [KeyValuePair](#) (p. 204)
Required: False

SensitiveDataItem

Provides information about the category, types, and occurrences of sensitive data that produced a sensitive data finding.

category

The category of sensitive data that was detected. For example: `CREDENTIALS`, for credentials data such as private keys or AWS secret keys; `FINANCIAL_INFORMATION`, for financial data such as credit card numbers; or, `PERSONAL_INFORMATION`, for personal health information, such as health insurance identification numbers, or personally identifiable information, such as passport numbers.

Type: [SensitiveDataItemCategory](#) (p. 212)
Required: False

totalCount

The total number of occurrences of the sensitive data that was detected.

Type: integer
Required: False

Format: int64

detections

An array of objects, one for each type of sensitive data that was detected. Each object reports the number of occurrences of a specific type of sensitive data that was detected, and the location of up to 15 of those occurrences.

Type: Array of type [DefaultDetection](#) (p. 195)

Required: False

SensitiveDataItemCategory

For a finding, the category of sensitive data that was detected and produced the finding. For a managed data identifier, the category of sensitive data that the managed data identifier detects. Possible values are:

```
FINANCIAL_INFORMATION  
PERSONAL_INFORMATION  
CREDENTIALS  
CUSTOM_IDENTIFIER
```

ServerSideEncryption

Provides information about the server-side encryption settings for an S3 bucket or S3 object.

encryptionType

The server-side encryption algorithm that's used when storing data in the bucket or object. If default encryption is disabled for the bucket or the object isn't encrypted using server-side encryption, this value is NONE.

Type: [EncryptionType](#) (p. 195)

Required: False

kmsMasterKeyId

The Amazon Resource Name (ARN) or unique identifier (key ID) for the AWS KMS key that's used to encrypt data in the bucket or the object. This value is null if an AWS KMS key isn't used to encrypt the data.

Type: string

Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string

Required: False

SessionContext

Provides information about a session that was created for an entity that performed an action by using temporary security credentials.

sessionIssuer

The source and type of credentials that were issued to the entity.

Type: [SessionIssuer](#) (p. 213)

Required: False

attributes

The date and time when the credentials were issued, and whether the credentials were authenticated with a multi-factor authentication (MFA) device.

Type: [SessionContextAttributes](#) (p. 213)

Required: False

SessionContextAttributes

Provides information about the context in which temporary security credentials were issued to an entity.

mfaAuthenticated

Specifies whether the credentials were authenticated with a multi-factor authentication (MFA) device.

Type: boolean

Required: False

creationDate

The date and time, in UTC and ISO 8601 format, when the credentials were issued.

Type: string

Required: False

Format: date-time

SessionIssuer

Provides information about the source and type of temporary security credentials that were issued to an entity.

accountId

The unique identifier for the AWS account that owns the entity that was used to get the credentials.

Type: string

Required: False

principalId

The unique identifier for the entity that was used to get the credentials.

Type: string
Required: False

userName

The name or alias of the user or role that issued the session. This value is null if the credentials were obtained from a root account that doesn't have an alias.

Type: string
Required: False

type

The source of the temporary security credentials, such as `Root`, `IAMUser`, or `Role`.

Type: string
Required: False

arn

The Amazon Resource Name (ARN) of the source account, IAM user, or role that was used to get the credentials.

Type: string
Required: False

Severity

Provides the numerical and qualitative representations of a finding's severity.

score

The numerical representation of the finding's severity, ranging from 1 (least severe) to 3 (most severe).

Type: integer
Required: False
Format: int64

description

The qualitative representation of the finding's severity, ranging from `Low` (least severe) to `High` (most severe).

Type: [SeverityDescription](#) (p. 214)
Required: False

SeverityDescription

The qualitative representation of the finding's severity. Possible values are:

`Low`
`Medium`
`High`

SortCriteria

Specifies criteria for sorting the results of a request for findings.

orderBy

The sort order to apply to the results, based on the value for the property specified by the `attributeName` property. Valid values are: `ASC`, sort the results in ascending order; and, `DESC`, sort the results in descending order.

Type: string
Required: False
Values: `ASC` | `DESC`

attributeName

The name of the property to sort the results by. This value can be the name of any property that Amazon Macie defines for a finding.

Type: string
Required: False

StorageClass

The storage class of the S3 object. Possible values are:

`STANDARD`
`REDUCED_REDUNDANCY`
`STANDARD_IA`
`INTELLIGENT_TIERING`
`DEEP_ARCHIVE`
`ONEZONE_IA`
`GLACIER`

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string
Required: False

UserIdentity

Provides information about the type and other characteristics of an entity that performed an action on an affected resource.

federatedUser

If the action was performed with temporary security credentials that were obtained using the `GetFederationToken` operation of the AWS Security Token Service (AWS STS) API, the identifiers, session context, and other details about the identity.

Type: [FederatedUser](#) (p. 196)

Required: False

awsAccount

If the action was performed using the credentials for another AWS account, the details of that account.

Type: [AwsAccount](#) (p. 188)

Required: False

root

If the action was performed using the credentials for your AWS account, the details of your account.

Type: [UserIdentityRoot](#) (p. 216)

Required: False

assumedRole

If the action was performed with temporary security credentials that were obtained using the `AssumeRole` operation of the AWS Security Token Service (AWS STS) API, the identifiers, session context, and other details about the identity.

Type: [AssumedRole](#) (p. 187)

Required: False

type

The type of entity that performed the action.

Type: [UserIdentityType](#) (p. 217)

Required: False

iamUser

If the action was performed using the credentials for an AWS Identity and Access Management (IAM) user, the name and other details about the user.

Type: [IamUser](#) (p. 201)

Required: False

awsService

If the action was performed by an AWS account that belongs to an AWS service, the name of the service.

Type: [AwsService](#) (p. 188)

Required: False

UserIdentityRoot

Provides information about an AWS account and entity that performed an action on an affected resource. The action was performed using the credentials for your AWS account.

accountId

The unique identifier for the AWS account.

Type: string
Required: False

principalId

The unique identifier for the entity that performed the action.

Type: string
Required: False

arn

The Amazon Resource Name (ARN) of the principal that performed the action. The last section of the ARN contains the name of the user or role that performed the action.

Type: string
Required: False

UserIdentityType

The type of entity that performed the action on the affected resource. Possible values are:

AssumedRole
IAMUser
FederatedUser
Root
AWSAccount
AWSService

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string
Required: False

See also

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

GetFindings

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)

- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Findings Filter

The Findings Filter resource represents an individual filter that you created and saved to view, analyze, and manage findings. A *findings filter*, also referred to as a *filter*, is a set of criteria that specifies which findings to include in the results of a query for findings. A findings filter can also perform specific actions on findings that meet the filter's criteria. For example, you can configure a filter to suppress (automatically archive) findings that meet the filter's criteria. For more information about creating and using filters, see [Filtering findings](#) in the *Amazon Macie User Guide*.

You can use the Findings Filter resource to update, delete, or retrieve detailed information about a findings filter. To create a new filter, use the [Findings Filters](#) (p. 229) resource.

URI

/findingsfilters/*id*

HTTP methods

GET

Operation ID: GetFindingsFilter

Retrieves the criteria and other settings for a findings filter.

Path parameters

Name	Type	Required	Description
<i>id</i>	String	True	The unique identifier for the Amazon Macie resource or account that the request applies to.

Responses

Status code	Response model	Description
200	GetFindingsFilterResponse (p. 222)	The request succeeded.
400	ValidationException (p. 222)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 222)	The request failed because fulfilling the request would exceed one or more service quotas for your account.

Status code	Response model	Description
403	AccessDeniedException (p. 222)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 222)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 222)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 222)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 222)	The request failed due to an unknown internal server error, exception, or failure.

DELETE

Operation ID: DeleteFindingsFilter

Deletes a findings filter.

Path parameters

Name	Type	Required	Description
<i>id</i>	String	True	The unique identifier for the Amazon Macie resource or account that the request applies to.

Responses

Status code	Response model	Description
200	Empty Schema (p. 221)	The request succeeded. The specified findings filter was deleted and there isn't any content to include in the body of the response (No Content).
400	ValidationException (p. 222)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 222)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 222)	The request was denied because you don't have sufficient access to the specified resource.

Status code	Response model	Description
404	ResourceNotFoundException (p. 222)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 222)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 222)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 222)	The request failed due to an unknown internal server error, exception, or failure.

PATCH

Operation ID: UpdateFindingsFilter

Updates the criteria and other settings for a findings filter.

Path parameters

Name	Type	Required	Description
<code>id</code>	String	True	The unique identifier for the Amazon Macie resource or account that the request applies to.

Responses

Status code	Response model	Description
200	UpdateFindingsFilterResponse (p. 222)	The request succeeded. The specified findings filter was updated.
400	ValidationException (p. 222)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 222)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 222)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 222)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 222)	The request failed because it conflicts with the current state of the specified resource.

Status code	Response model	Description
429	ThrottlingException (p. 222)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerError (p. 222)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

PATCH schema

```
{
  "findingCriteria": {
    "criterion": {
    }
  },
  "clientToken": "string",
  "name": "string",
  "description": "string",
  "action": enum,
  "position": integer
}
```

Response bodies

GetFindingsFilterResponse schema

```
{
  "findingCriteria": {
    "criterion": {
    }
  },
  "name": "string",
  "action": enum,
  "description": "string",
  "position": integer,
  "id": "string",
  "arn": "string",
  "tags": {
  }
}
```

Empty Schema schema

```
{
}
```

UpdateFindingsFilterResponse schema

```
{
```

```
{  
  "id": "string",  
  "arn": "string"  
}
```

ValidationException schema

```
{  
  "message": "string"  
}
```

ServiceQuotaExceededException schema

```
{  
  "message": "string"  
}
```

AccessDeniedException schema

```
{  
  "message": "string"  
}
```

ResourceNotFoundException schema

```
{  
  "message": "string"  
}
```

ConflictException schema

```
{  
  "message": "string"  
}
```

ThrottlingException schema

```
{  
  "message": "string"  
}
```

InternalServerErrorException schema

```
{  
  "message": "string"  
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

Criterion

Specifies a condition that defines a property, operator, and one or more values to filter the results of a query for findings. The number of values depends on the property and operator specified by the condition. For information about defining filter conditions, see [Fundamentals of filtering findings](#) in the *Amazon Macie User Guide*.

key-value pairs

Type: object

CriterionAdditionalProperties

Specifies the operator to use in a property-based condition that filters the results of a query for findings. For detailed information and examples of each operator, see [Fundamentals of filtering findings](#) in the *Amazon Macie User Guide*.

eqExactMatch

The value for the property exclusively matches (equals an exact match for) all the specified values. If you specify multiple values, Amazon Macie uses AND logic to join the values.

You can use this operator with the following properties: `customDataIdentifiers.detections.arn`, `customDataIdentifiers.detections.name`, `resourcesAffected.s3Bucket.tags.key`, `resourcesAffected.s3Bucket.tags.value`, `resourcesAffected.s3Object.tags.key`, `resourcesAffected.s3Object.tags.value`, `sensitiveData.category`, and `sensitiveData.detections.type`.

Type: Array of type string

Required: False

lt

The value for the property is less than the specified value.

Type: integer

Required: False

Format: int64

gte

The value for the property is greater than or equal to the specified value.

Type: integer

Required: False

Format: int64

neq

The value for the property doesn't match (doesn't equal) the specified value. If you specify multiple values, Macie uses OR logic to join the values.

Type: Array of type string

Required: False

lte

The value for the property is less than or equal to the specified value.

Type: integer

Required: False

Format: int64

eq

The value for the property matches (equals) the specified value. If you specify multiple values, Macie uses OR logic to join the values.

Type: Array of type string

Required: False

gt

The value for the property is greater than the specified value.

Type: integer

Required: False

Format: int64

Empty

The request succeeded and there isn't any content to include in the body of the response (No Content).

FindingCriteria

Specifies, as a map, one or more property-based conditions that filter the results of a query for findings.

criterion

A condition that specifies the property, operator, and one or more values to use to filter the results.

Type: [Criterion](#) (p. 223)
Required: False

FindingsFilterAction

The action to perform on findings that meet the filter criteria. To suppress (automatically archive) findings that meet the criteria, set this value to `ARCHIVE`. Valid values are:

`ARCHIVE`
`NOOP`

GetFindingsFilterResponse

Provides information about the criteria and other settings for a findings filter.

findingCriteria

The criteria that's used to filter findings.

Type: [FindingCriteria](#) (p. 224)
Required: False

name

The custom name of the filter.

Type: string
Required: False

action

The action that's performed on findings that meet the filter criteria (`findingCriteria`). Possible values are: `ARCHIVE`, suppress (automatically archive) the findings; and, `NOOP`, don't perform any action on the findings.

Type: [FindingsFilterAction](#) (p. 225)
Required: False

description

The custom description of the filter.

Type: string
Required: False

position

The position of the filter in the list of saved filters on the Amazon Macie console. This value also determines the order in which the filter is applied to findings, relative to other filters that are also applied to the findings.

Type: integer
Required: False
Format: int32

id

The unique identifier for the filter.

Type: string

Required: False

arn

The Amazon Resource Name (ARN) of the filter.

Type: string

Required: False

tags

A map of key-value pairs that identifies the tags (keys and values) that are associated with the filter.

Type: [TagMap \(p. 227\)](#)

Required: False

InternalServerErrorException

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string

Required: False

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string

Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string

Required: False

TagMap

A string-to-string map of key-value pairs that specifies the tags (keys and values) for a classification job, custom data identifier, findings filter, or member account.

key-value pairs

Type: string

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string

Required: False

UpdateFindingsFilterRequest

Specifies the criteria and other settings for a findings filter.

findingCriteria

The criteria to use to filter findings.

Type: [FindingCriteria](#) (p. 224)

Required: False

clientToken

A unique, case-sensitive token that you provide to ensure the idempotency of the request.

Type: string

Required: False

name

A custom name for the filter. The name must contain at least 3 characters and can contain as many as 64 characters.

We strongly recommend that you avoid including any sensitive data in the name of a filter. Other users might be able to see the filter's name, depending on the actions that they're allowed to perform in Amazon Macie.

Type: string

Required: False

description

A custom description of the filter. The description can contain as many as 512 characters.

We strongly recommend that you avoid including any sensitive data in the description of a filter. Other users might be able to see the filter's description, depending on the actions that they're allowed to perform in Amazon Macie.

Type: string
Required: False

action

The action to perform on findings that meet the filter criteria (`findingCriteria`). Valid values are: `ARCHIVE`, suppress (automatically archive) the findings; and, `NOOP`, don't perform any action on the findings.

Type: [FindingsFilterAction](#) (p. 225)
Required: False

position

The position of the filter in the list of saved filters on the Amazon Macie console. This value also determines the order in which the filter is applied to findings, relative to other filters that are also applied to the findings.

Type: integer
Required: False
Format: int32

UpdateFindingsFilterResponse

Provides information about a findings filter that was updated in response to a request.

id

The unique identifier for the filter that was updated.

Type: string
Required: False

arn

The Amazon Resource Name (ARN) of the filter that was updated.

Type: string
Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string
Required: False

See also

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

GetFindingsFilter

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

DeleteFindingsFilter

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

UpdateFindingsFilter

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Findings Filters

The Findings Filters resource represents the repository of filters that you create and save to view, analyze, and manage findings. A *findings filter*, also referred to as a *filter*, is a set of criteria that specifies

which findings to include in the results of a query for findings. A findings filter can also perform specific actions on findings that meet the filter's criteria. For example, you can configure a filter to suppress (automatically archive) findings that meet the filter's criteria. For more information about creating and using filters, see [Filtering findings](#) in the *Amazon Macie User Guide*.

You can use the Findings Filters resource to create a new filter or retrieve information about all the existing filters for your account. To update, delete, or retrieve detailed information about an individual filter, use the [Findings Filter \(p. 218\)](#) resource.

URI

`/findingsfilters`

HTTP methods

GET

Operation ID: `ListFindingsFilters`

Retrieves a subset of information about all the findings filters for an account.

Query parameters

Name	Type	Required	Description
<code>nextToken</code>	String	False	The <code>nextToken</code> string that specifies which page of results to return in a paginated response.
<code>maxResults</code>	String	False	The maximum number of items to include in each page of a paginated response.

Responses

Status code	Response model	Description
200	ListFindingsFiltersResponse (p. 232)	The request succeeded.
400	ValidationException (p. 232)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 232)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 232)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 232)	The request failed because the specified resource wasn't found.

Status code	Response model	Description
409	ConflictException (p. 233)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 233)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 233)	The request failed due to an unknown internal server error, exception, or failure.

POST

Operation ID: CreateFindingsFilter

Creates and defines the criteria and other settings for a findings filter.

Responses

Status code	Response model	Description
200	CreateFindingsFilterResponse (p. 232)	The request succeeded.
400	ValidationException (p. 232)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 232)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 232)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 232)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 233)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 233)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 233)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

POST schema

```
{
  "findingCriteria": {
    "criterion": {
    }
  },
  "clientToken": "string",
  "name": "string",
  "description": "string",
  "action": enum,
  "position": integer,
  "tags": {
  }
}
```

Response bodies

ListFindingsFiltersResponse schema

```
{
  "nextToken": "string",
  "findingsFilterListItems": [
    {
      "name": "string",
      "action": enum,
      "id": "string",
      "arn": "string",
      "tags": {
      }
    }
  ]
}
```

CreateFindingsFilterResponse schema

```
{
  "id": "string",
  "arn": "string"
}
```

ValidationException schema

```
{
  "message": "string"
}
```

ServiceQuotaExceededException schema

```
{
  "message": "string"
}
```

AccessDeniedException schema

```
{
```

```
"message": "string"
}
```

ResourceNotFoundException schema

```
{
  "message": "string"
}
```

ConflictException schema

```
{
  "message": "string"
}
```

ThrottlingException schema

```
{
  "message": "string"
}
```

InternalServerError schema

```
{
  "message": "string"
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

CreateFindingsFilterRequest

Specifies the criteria and other settings for a new findings filter.

findingCriteria

The criteria to use to filter findings.

Type: [FindingCriteria](#) (p. 237)

Required: True

clientToken

A unique, case-sensitive token that you provide to ensure the idempotency of the request.

Type: string

Required: False

name

A custom name for the filter. The name must contain at least 3 characters and can contain as many as 64 characters.

We strongly recommend that you avoid including any sensitive data in the name of a filter. Other users of your account might be able to see the filter's name, depending on the actions that they're allowed to perform in Amazon Macie.

Type: string

Required: True

description

A custom description of the filter. The description can contain as many as 512 characters.

We strongly recommend that you avoid including any sensitive data in the description of a filter. Other users of your account might be able to see the filter's description, depending on the actions that they're allowed to perform in Amazon Macie.

Type: string

Required: False

action

The action to perform on findings that meet the filter criteria (*findingCriteria*). Valid values are: `ARCHIVE`, suppress (automatically archive) the findings; and, `NOOP`, don't perform any action on the findings.

Type: [FindingsFilterAction](#) (p. 237)

Required: True

position

The position of the filter in the list of saved filters on the Amazon Macie console. This value also determines the order in which the filter is applied to findings, relative to other filters that are also applied to the findings.

Type: integer
Required: False
Format: int32

tags

A map of key-value pairs that specifies the tags to associate with the filter.

A findings filter can have a maximum of 50 tags. Each tag consists of a tag key and an associated tag value. The maximum length of a tag key is 128 characters. The maximum length of a tag value is 256 characters.

Type: [TagMap \(p. 239\)](#)
Required: False

CreateFindingsFilterResponse

Provides information about a findings filter that was created in response to a request.

id

The unique identifier for the filter that was created.

Type: string
Required: False

arn

The Amazon Resource Name (ARN) of the filter that was created.

Type: string
Required: False

Criterion

Specifies a condition that defines a property, operator, and one or more values to filter the results of a query for findings. The number of values depends on the property and operator specified by the condition. For information about defining filter conditions, see [Fundamentals of filtering findings](#) in the *Amazon Macie User Guide*.

key-value pairs

Type: object

CriterionAdditionalProperties

Specifies the operator to use in a property-based condition that filters the results of a query for findings. For detailed information and examples of each operator, see [Fundamentals of filtering findings](#) in the *Amazon Macie User Guide*.

eqExactMatch

The value for the property exclusively matches (equals an exact match for) all the specified values. If you specify multiple values, Amazon Macie uses AND logic to join the values.

You can use this operator with the following properties: `customDataIdentifiers.detections.arn`, `customDataIdentifiers.detections.name`, `resourcesAffected.s3Bucket.tags.key`, `resourcesAffected.s3Bucket.tags.value`, `resourcesAffected.s3Object.tags.key`, `resourcesAffected.s3Object.tags.value`, `sensitiveData.category`, and `sensitiveData.detections.type`.

Type: Array of type string

Required: False

lt

The value for the property is less than the specified value.

Type: integer

Required: False

Format: int64

gte

The value for the property is greater than or equal to the specified value.

Type: integer

Required: False

Format: int64

neq

The value for the property doesn't match (doesn't equal) the specified value. If you specify multiple values, Macie uses OR logic to join the values.

Type: Array of type string

Required: False

lte

The value for the property is less than or equal to the specified value.

Type: integer

Required: False

Format: int64

eq

The value for the property matches (equals) the specified value. If you specify multiple values, Macie uses OR logic to join the values.

Type: Array of type string

Required: False

gt

The value for the property is greater than the specified value.

Type: integer

Required: False
Format: int64

FindingCriteria

Specifies, as a map, one or more property-based conditions that filter the results of a query for findings.

criterion

A condition that specifies the property, operator, and one or more values to use to filter the results.

Type: [Criterion](#) (p. 235)
Required: False

FindingsFilterAction

The action to perform on findings that meet the filter criteria. To suppress (automatically archive) findings that meet the criteria, set this value to `ARCHIVE`. Valid values are:

`ARCHIVE`
`NOOP`

FindingsFilterListItem

Provides information about a findings filter.

name

The custom name of the filter.

Type: string
Required: False

action

The action that's performed on findings that meet the filter criteria. Possible values are: `ARCHIVE`, suppress (automatically archive) the findings; and, `NOOP`, don't perform any action on the findings.

Type: [FindingsFilterAction](#) (p. 237)
Required: False

id

The unique identifier for the filter.

Type: string
Required: False

arn

The Amazon Resource Name (ARN) of the filter.

Type: string

Required: False

tags

A map of key-value pairs that identifies the tags (keys and values) that are associated with the filter.

Type: [TagMap](#) (p. 239)

Required: False

InternalServerError

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string

Required: False

ListFindingsFiltersResponse

Provides information about all the findings filters for an account.

nextToken

The string to use in a subsequent request to get the next page of results in a paginated response. This value is null if there are no additional pages.

Type: string

Required: False

findingsFilterListItems

An array of objects, one for each filter that's associated with the account.

Type: Array of type [FindingsFilterListItem](#) (p. 237)

Required: False

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string

Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string

Required: False

TagMap

A string-to-string map of key-value pairs that specifies the tags (keys and values) for a classification job, custom data identifier, findings filter, or member account.

key-value pairs

Type: string

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string

Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string

Required: False

See also

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

ListFindingsFilters

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

CreateFindingsFilter

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Findings List

The Findings List resource provides a subset of information about the findings for your Amazon Macie account. A *finding* is a detailed report of a potential policy violation for an Amazon Simple Storage Service (Amazon S3) bucket or sensitive data in an S3 object.

Note that this resource doesn't provide access to all the data for a finding. Instead, it provides only a subset of metadata, such as the finding identifier. To retrieve all the data for one or more findings, use the [Findings Descriptions](#) (p. 178) resource.

You can use the Findings List resource to retrieve a subset of information about one or more findings. To customize and refine your query, you can use supported parameters to specify whether and how to filter, sort, and paginate the results.

URI

/findings

HTTP methods

POST

Operation ID: ListFindings

Retrieves a subset of information about one or more findings.

Responses

Status code	Response model	Description
200	ListFindingsResponse (p. 240)	The request succeeded.

Status code	Response model	Description
400	ValidationException (p. 242)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 242)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 242)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 242)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 242)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 242)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 242)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

POST schema

```
{
  "nextToken": "string",
  "maxResults": integer,
  "findingCriteria": {
    "criterion": {
    }
  },
  "sortCriteria": {
    "orderBy": enum,
    "attributeName": "string"
  }
}
```

Response bodies

ListFindingsResponse schema

```
{
  "findingIds": [
    "string"
  ],
  "nextToken": "string"
}
```



```
}
```

ValidationException schema

```
{  
  "message": "string"  
}
```

ServiceQuotaExceededException schema

```
{  
  "message": "string"  
}
```

AccessDeniedException schema

```
{  
  "message": "string"  
}
```

ResourceNotFoundException schema

```
{  
  "message": "string"  
}
```

ConflictException schema

```
{  
  "message": "string"  
}
```

ThrottlingException schema

```
{  
  "message": "string"  
}
```

InternalServerError schema

```
{  
  "message": "string"  
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

Criterion

Specifies a condition that defines a property, operator, and one or more values to filter the results of a query for findings. The number of values depends on the property and operator specified by the condition. For information about defining filter conditions, see [Fundamentals of filtering findings](#) in the *Amazon Macie User Guide*.

key-value pairs

Type: object

CriterionAdditionalProperties

Specifies the operator to use in a property-based condition that filters the results of a query for findings. For detailed information and examples of each operator, see [Fundamentals of filtering findings](#) in the *Amazon Macie User Guide*.

eqExactMatch

The value for the property exclusively matches (equals an exact match for) all the specified values. If you specify multiple values, Amazon Macie uses AND logic to join the values.

You can use this operator with the following properties: `customDataIdentifiers.detections.arn`, `customDataIdentifiers.detections.name`, `resourcesAffected.s3Bucket.tags.key`, `resourcesAffected.s3Bucket.tags.value`, `resourcesAffected.s3Object.tags.key`, `resourcesAffected.s3Object.tags.value`, `sensitiveData.category`, and `sensitiveData.detections.type`.

Type: Array of type string

Required: False

lt

The value for the property is less than the specified value.

Type: integer

Required: False
Format: int64

gte

The value for the property is greater than or equal to the specified value.

Type: integer
Required: False
Format: int64

neq

The value for the property doesn't match (doesn't equal) the specified value. If you specify multiple values, Macie uses OR logic to join the values.

Type: Array of type string
Required: False

lte

The value for the property is less than or equal to the specified value.

Type: integer
Required: False
Format: int64

eq

The value for the property matches (equals) the specified value. If you specify multiple values, Macie uses OR logic to join the values.

Type: Array of type string
Required: False

gt

The value for the property is greater than the specified value.

Type: integer
Required: False
Format: int64

FindingCriteria

Specifies, as a map, one or more property-based conditions that filter the results of a query for findings.

criterion

A condition that specifies the property, operator, and one or more values to use to filter the results.

Type: [Criterion](#) (p. 243)
Required: False

InternalServerErrorException

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string

Required: False

ListFindingsRequest

Specifies criteria for filtering, sorting, and paginating the results of a request for information about findings.

nextToken

The `nextToken` string that specifies which page of results to return in a paginated response.

Type: string

Required: False

maxResults

The maximum number of items to include in each page of the response.

Type: integer

Required: False

Format: int32

findingCriteria

The criteria to use to filter the results.

Type: [FindingCriteria](#) (p. 244)

Required: False

sortCriteria

The criteria to use to sort the results.

Type: [SortCriteria](#) (p. 246)

Required: False

ListFindingsResponse

Provides the results of a request for information about one or more findings.

findingIds

An array of strings, where each string is the unique identifier for a finding that meets the filter criteria specified in the request.

Type: Array of type string
Required: False

nextToken

The string to use in a subsequent request to get the next page of results in a paginated response. This value is null if there are no additional pages.

Type: string
Required: False

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string
Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string
Required: False

SortCriteria

Specifies criteria for sorting the results of a request for findings.

orderBy

The sort order to apply to the results, based on the value for the property specified by the `attributeName` property. Valid values are: `ASC`, sort the results in ascending order; and, `DESC`, sort the results in descending order.

Type: string
Required: False
Values: `ASC` | `DESC`

attributeName

The name of the property to sort the results by. This value can be the name of any property that Amazon Macie defines for a finding.

Type: string

Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string

Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string

Required: False

See also

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

ListFindings

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Findings Publication Configuration

The Findings Publication Configuration resource provides settings for publishing findings to AWS Security Hub. With these settings, you can configure Macie to automatically publish all policy findings, all sensitive data findings, or both policy and sensitive data findings to Security Hub. This doesn't include findings that were suppressed (automatically archived) by a findings filter. You can also use

these settings to stop publishing any findings to Security Hub. To learn more about how Macie publishes findings to Security Hub, see [Amazon Macie integration with Security Hub](#) in the *Amazon Macie User Guide*.

Security Hub is a service that provides you with a comprehensive view of your security state across your AWS environment and helps you check your environment against security industry standards and best practices. It does this partly by consuming, aggregating, organizing, and prioritizing findings from multiple AWS services and supported AWS Partner Network (APN) Partner security solutions. It helps you analyze your security trends and identify the highest priority security issues. To learn more about Security Hub, see the [AWS Security Hub User Guide](#).

You can use the Findings Publication Configuration resource to retrieve information about or update your configuration settings for publishing findings to Security Hub automatically. If you configure Macie to publish policy findings to Security Hub, Macie publishes updates to those findings on a recurring basis, using a publication frequency that you specify. To specify this frequency, use the [Account Administration \(p. 8\)](#) resource.

URI

/findings-publication-configuration

HTTP methods

GET

Operation ID: GetFindingsPublicationConfiguration

Retrieves the configuration settings for publishing findings to AWS Security Hub.

Responses

Status code	Response model	Description
200	GetFindingsPublicationConfigurationResponse (p. 250)	The request succeeded.
400	ValidationException (p. 250)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 250)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 250)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 250)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 250)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 250)	The request failed because you sent too many requests during a certain amount of time.

Status code	Response model	Description
500	InternalServerError (p. 250)	The request failed due to an unknown internal server error, exception, or failure.

PUT

Operation ID: PutFindingsPublicationConfiguration

Updates the configuration settings for publishing findings to AWS Security Hub.

Responses

Status code	Response model	Description
200	None	The request succeeded and there isn't any content to include in the body of the response (No Content).
400	ValidationException (p. 250)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 250)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 250)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 250)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 250)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 250)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerError (p. 250)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

PUT schema

```
{
  "securityHubConfiguration": {
```



```
"publishPolicyFindings": boolean,
"publishClassificationFindings": boolean
},
"clientToken": "string"
}
```

Response bodies

GetFindingsPublicationConfigurationResponse schema

```
{
  "securityHubConfiguration": {
    "publishPolicyFindings": boolean,
    "publishClassificationFindings": boolean
  }
}
```

ValidationException schema

```
{
  "message": "string"
}
```

ServiceQuotaExceededException schema

```
{
  "message": "string"
}
```

AccessDeniedException schema

```
{
  "message": "string"
}
```

ResourceNotFoundException schema

```
{
  "message": "string"
}
```

ConflictException schema

```
{
  "message": "string"
}
```

ThrottlingException schema

```
{
```

```
"message": "string"
}
```

InternalServerError schema

```
{
  "message": "string"
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

GetFindingsPublicationConfigurationResponse

Provides information about the current configuration settings for publishing findings to AWS Security Hub automatically.

securityHubConfiguration

The configuration settings that determine which findings are published to AWS Security Hub.

Type: [SecurityHubConfiguration](#) (p. 252)

Required: False

InternalServerError

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string
Required: False

PutFindingsPublicationConfigurationRequest

Specifies configuration settings for publishing findings to AWS Security Hub automatically.

securityHubConfiguration

The configuration settings that determine which findings to publish to AWS Security Hub.

Type: [SecurityHubConfiguration](#) (p. 252)
Required: False

clientToken

A unique, case-sensitive token that you provide to ensure the idempotency of the request.

Type: string
Required: False

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string
Required: False

SecurityHubConfiguration

Specifies configuration settings that determine which findings are published to AWS Security Hub automatically. For information about how Macie publishes findings to Security Hub, see [Amazon Macie integration with Security Hub](#) in the *Amazon Macie User Guide*.

publishPolicyFindings

Specifies whether to publish policy findings to AWS Security Hub. If you set this value to `true`, Amazon Macie automatically publishes all new and updated policy findings that weren't suppressed by a findings filter. The default value is `true`.

Type: boolean
Required: True

publishClassificationFindings

Specifies whether to publish sensitive data findings to AWS Security Hub. If you set this value to `true`, Amazon Macie automatically publishes all sensitive data findings that weren't suppressed by a findings filter. The default value is `false`.

Type: boolean

Required: True

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string

Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string

Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string

Required: False

See also

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

GetFindingsPublicationConfiguration

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)

- [AWS SDK for Ruby V3](#)

PutFindingsPublicationConfiguration

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Findings Samples

The Findings Samples resource provides a set of findings that use example data to help you understand and analyze the various types of findings that Amazon Macie can report. A *finding* is a detailed report of a potential policy violation for an Amazon Simple Storage Service (Amazon S3) bucket or sensitive data in an S3 object. For information about the types of findings that Macie can report, see [Types of Amazon Macie findings](#) in the *Amazon Macie User Guide*.

If you use this resource to create sample findings, Macie generates one sample finding for each supported finding type that you choose to include in the set of samples. You can then view and work with these sample findings by using the Amazon Macie API or the Amazon Macie console. To help you identify a sample finding, Macie adds the [SAMPLE] prefix to the value for the `FindingType` property of each sample finding. It also sets the value for the `sample` property to `true`.

You can use the Findings Samples resource to create one or more sample findings. To create only certain types of sample findings, you can use the supported request parameter to specify each type of sample that you want Macie to create.

URI

/findings/sample

HTTP methods

POST

Operation ID: CreateSampleFindings

Creates sample findings.

Responses

Status code	Response model	Description
200	Empty Schema (p. 255)	The request succeeded and there isn't any content to include in the body of the response (No Content).

Status code	Response model	Description
400	ValidationException (p. 255)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 255)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 255)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 255)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 256)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 256)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 256)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

POST schema

```
{
  "findingTypes": [
    enum
  ]
}
```

Response bodies

Empty Schema schema

```
{
}
```

ValidationException schema

```
{
  "message": "string"
}
```

ServiceQuotaExceededException schema

```
{  
  "message": "string"  
}
```

AccessDeniedException schema

```
{  
  "message": "string"  
}
```

ResourceNotFoundException schema

```
{  
  "message": "string"  
}
```

ConflictException schema

```
{  
  "message": "string"  
}
```

ThrottlingException schema

```
{  
  "message": "string"  
}
```

InternalServerErrorException schema

```
{  
  "message": "string"  
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

CreateSampleFindingsRequest

Specifies the types of findings to include in a set of sample findings that Amazon Macie creates.

findingTypes

An array that lists one or more types of findings to include in the set of sample findings. Currently, the only supported value is `Policy:IAMUser/S3BucketEncryptionDisabled`.

Type: Array of type [FindingType](#) (p. 257)

Required: False

Empty

The request succeeded and there isn't any content to include in the body of the response (No Content).

FindingType

The type of finding. For details about each type, see [Types of Amazon Macie findings](#) in the *Amazon Macie User Guide*. Valid values are:

```
SensitiveData:S3Object/Multiple
SensitiveData:S3Object/Financial
SensitiveData:S3Object/Personal
SensitiveData:S3Object/Credentials
SensitiveData:S3Object/CustomIdentifier
Policy:IAMUser/S3BucketPublic
Policy:IAMUser/S3BucketSharedExternally
Policy:IAMUser/S3BucketReplicatedExternally
Policy:IAMUser/S3BucketEncryptionDisabled
Policy:IAMUser/S3BlockPublicAccessDisabled
```

InternalServerError

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string

Required: False

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string

Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string

Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string

Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string

Required: False

See also

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

CreateSampleFindings

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Findings Statistics

The Findings Statistics resource provides aggregated statistical data about the findings for your Amazon Macie account. This primarily includes data about the total number of findings, grouped by a key value such as severity, finding type, or affected resource. The data is available for all the findings that Macie stores for your account.

You can use this resource to retrieve (query) aggregated statistical data about findings for your account. To customize and refine your query, you can use supported parameters to specify how to filter, group, and sort the query results.

URI

/findings/statistics

HTTP methods

POST

Operation ID: GetFindingStatistics

Retrieves (queries) aggregated statistical data about findings.

Responses

Status code	Response model	Description
200	GetFindingStatisticsResponse (p. 260)	The request succeeded.
400	ValidationException (p. 260)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 260)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 260)	The request was denied because you don't have sufficient access to the specified resource.

Status code	Response model	Description
404	ResourceNotFoundException (p. 261)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 261)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 261)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 261)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

POST schema

```
{
  "size": integer,
  "findingCriteria": {
    "criterion": {
    }
  },
  "groupBy": enum,
  "sortCriteria": {
    "orderBy": enum,
    "attributeName": enum
  }
}
```

Response bodies

GetFindingStatisticsResponse schema

```
{
  "countsByGroup": [
    {
      "count": integer,
      "groupKey": "string"
    }
  ]
}
```

ValidationException schema

```
{
  "message": "string"
}
```

ServiceQuotaExceededException schema

```
{  
  "message": "string"  
}
```

AccessDeniedException schema

```
{  
  "message": "string"  
}
```

ResourceNotFoundException schema

```
{  
  "message": "string"  
}
```

ConflictException schema

```
{  
  "message": "string"  
}
```

ThrottlingException schema

```
{  
  "message": "string"  
}
```

InternalServerErrorException schema

```
{  
  "message": "string"  
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

Criterion

Specifies a condition that defines a property, operator, and one or more values to filter the results of a query for findings. The number of values depends on the property and operator specified by the condition. For information about defining filter conditions, see [Fundamentals of filtering findings](#) in the *Amazon Macie User Guide*.

key-value pairs

Type: object

CriterionAdditionalProperties

Specifies the operator to use in a property-based condition that filters the results of a query for findings. For detailed information and examples of each operator, see [Fundamentals of filtering findings](#) in the *Amazon Macie User Guide*.

eqExactMatch

The value for the property exclusively matches (equals an exact match for) all the specified values. If you specify multiple values, Amazon Macie uses AND logic to join the values.

You can use this operator with the following properties: `customDataIdentifiers.detections.arn`, `customDataIdentifiers.detections.name`, `resourcesAffected.s3Bucket.tags.key`, `resourcesAffected.s3Bucket.tags.value`, `resourcesAffected.s3Object.tags.key`, `resourcesAffected.s3Object.tags.value`, `sensitiveData.category`, and `sensitiveData.detections.type`.

Type: Array of type string

Required: False

lt

The value for the property is less than the specified value.

Type: integer

Required: False

Format: int64

gte

The value for the property is greater than or equal to the specified value.

Type: integer
Required: False
Format: int64

neq

The value for the property doesn't match (doesn't equal) the specified value. If you specify multiple values, Macie uses OR logic to join the values.

Type: Array of type string
Required: False

lte

The value for the property is less than or equal to the specified value.

Type: integer
Required: False
Format: int64

eq

The value for the property matches (equals) the specified value. If you specify multiple values, Macie uses OR logic to join the values.

Type: Array of type string
Required: False

gt

The value for the property is greater than the specified value.

Type: integer
Required: False
Format: int64

FindingCriteria

Specifies, as a map, one or more property-based conditions that filter the results of a query for findings.

criterion

A condition that specifies the property, operator, and one or more values to use to filter the results.

Type: [Criterion](#) (p. 262)
Required: False

FindingStatisticsSortAttributeName

The grouping to sort the results by. Valid values are:

groupKey
count

FindingStatisticsSortCriteria

Specifies criteria for sorting the results of a query that retrieves aggregated statistical data about findings.

orderBy

The sort order to apply to the results, based on the value for the property specified by the `attributeName` property. Valid values are: `ASC`, sort the results in ascending order; and, `DESC`, sort the results in descending order.

Type: string

Required: False

Values: `ASC` | `DESC`

attributeName

The grouping to sort the results by. Valid values are: `count`, sort the results by the number of findings in each group of results; and, `groupBy`, sort the results by the name of each group of results.

Type: [FindingStatisticsSortAttributeName](#) (p. 263)

Required: False

GetFindingStatisticsRequest

Specifies criteria for filtering, grouping, sorting, and paginating the results of a query that retrieves aggregated statistical data about findings.

size

The maximum number of items to include in each page of the response.

Type: integer

Required: False

Format: int32

findingCriteria

The criteria to use to filter the query results.

Type: [FindingCriteria](#) (p. 263)

Required: False

groupBy

The finding property to use to group the query results. Valid values are:

- `classificationDetails.jobId` - The unique identifier for the classification job that produced the finding.
- `resourcesAffected.s3Bucket.name` - The name of the S3 bucket that the finding applies to.
- `severity.description` - The severity level of the finding, such as `High` or `Medium`.
- `type` - The type of finding, such as `Policy:IAMUser/S3BucketPublic` and `SensitiveData:S3Object/Personal`.

Type: string

Required: True

Values: `resourcesAffected.s3Bucket.name` | `type` | `classificationDetails.jobId` | `severity.description`

sortCriteria

The criteria to use to sort the query results.

Type: [FindingStatisticsSortCriteria](#) (p. 264)

Required: False

GetFindingStatisticsResponse

Provides the results of a query that retrieved aggregated statistical data about findings.

countsByGroup

An array of objects, one for each group of findings that meet the filter criteria specified in the request.

Type: Array of type [GroupCount](#) (p. 265)

Required: False

GroupCount

Provides a group of results for a query that retrieved aggregated statistical data about findings.

count

The total number of findings in the group of query results.

Type: integer

Required: False

Format: int64

groupKey

The name of the property that defines the group in the query results, as specified by the `groupBy` property in the query request.

Type: string

Required: False

InternalServerErrorException

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string

Required: False

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string

Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string

Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string

Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string

Required: False

See also

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

GetFindingStatistics

- [AWS Command Line Interface](#)

- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Invitation Acceptance

In Amazon Macie, an *invitation*, also referred to as a *membership invitation*, is a request to become a member of a Macie organization. A *Macie organization* is a set of Amazon Macie accounts that are created and managed as a group by using Macie.

The Invitation Acceptance resource provides access to membership invitations that you've received and haven't responded to, and it enables you to accept one of those invitations. Note that this resource doesn't provide access to invitations for AWS organizations. It provides access only to invitations that were sent using Macie. An *AWS organization* is a set of AWS accounts that are managed as a group by using AWS Organizations. AWS Organizations is an account management service that enables administrators to consolidate and centrally manage multiple AWS accounts as a single organization. To learn more about this service, see the [AWS Organizations User Guide](#).

You can use the Invitation Acceptance resource to accept a Macie membership invitation that you received. If you do this, you have to specify the AWS account ID for the account that sent the invitation, and the unique identifier for the invitation. To find these IDs, you can use the [Invitation List \(p. 287\)](#) resource.

URI

`/invitations/accept`

HTTP methods

POST

Operation ID: AcceptInvitation

Accepts an Amazon Macie membership invitation that was received from a specific account.

Responses

Status code	Response model	Description
200	Empty Schema (p. 268)	The request succeeded and there isn't any content to include in the body of the response (No Content).
400	ValidationException (p. 268)	The request failed because it contains a syntax error.

Status code	Response model	Description
402	ServiceQuotaExceededException (p. 268)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 268)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 268)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 269)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 269)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 269)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

POST schema

```
{
  "masterAccount": "string",
  "invitationId": "string",
  "administratorAccountId": "string"
}
```

Response bodies

Empty Schema schema

```
{
}
```

ValidationException schema

```
{
  "message": "string"
}
```

ServiceQuotaExceededException schema

```
{
```

```
"message": "string"
}
```

AccessDeniedException schema

```
{
  "message": "string"
}
```

ResourceNotFoundException schema

```
{
  "message": "string"
}
```

ConflictException schema

```
{
  "message": "string"
}
```

ThrottlingException schema

```
{
  "message": "string"
}
```

InternalServerError schema

```
{
  "message": "string"
}
```

Properties

AcceptInvitationRequest

Specifies an Amazon Macie membership invitation to accept. In the request, you have to specify the ID for the AWS account that sent the invitation. Otherwise, a validation error occurs. To specify this ID, we recommend that you use the `administratorAccountId` property instead of the `masterAccount` property. The `masterAccount` property has been deprecated and is retained only for backward compatibility.

masterAccount

(Deprecated) The AWS account ID for the account that sent the invitation. This property has been replaced by the `administratorAccountId` property and is retained only for backward compatibility.

Type: string

Required: False

invitationId

The unique identifier for the invitation to accept.

Type: string

Required: True

administratorAccountId

The AWS account ID for the account that sent the invitation.

Type: string

Required: False

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

Empty

The request succeeded and there isn't any content to include in the body of the response (No Content).

InternalServerErrorException

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string

Required: False

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string

Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string

Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string

Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string

Required: False

See also

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

AcceptInvitation

- [AWS Command Line Interface](#)

- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Invitation Count

In Amazon Macie, an *invitation*, also referred to as a *membership invitation*, is a request to become a member of a Macie organization. A *Macie organization* is a set of Amazon Macie accounts that are created and managed as a group by using Macie.

The Invitation Count resource reports the total number of membership invitations that you've received. If you accepted an invitation and your account is currently part of an organization, this number doesn't include that invitation. In addition, this number doesn't include invitations that you've received for AWS organizations. It's limited to invitations that were sent using Macie. An *AWS organization* is a set of AWS accounts that are managed as a group by using AWS Organizations. AWS Organizations is an account management service that enables administrators to consolidate and centrally manage multiple AWS accounts as a single organization. To learn more about this service, see the [AWS Organizations User Guide](#).

You can use the Invitation Count resource to retrieve the number of Macie membership invitations that you've received, not including the currently accepted invitation.

URI

/invitations/count

HTTP methods

GET

Operation ID: GetInvitationsCount

Retrieves the count of Amazon Macie membership invitations that were received by an account.

Responses

Status code	Response model	Description
200	GetInvitationsCountResponse (p. 273)	The request succeeded.
400	ValidationException (p. 273)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 273)	The request failed because fulfilling the request would exceed one or more service quotas for your account.

Status code	Response model	Description
403	AccessDeniedException (p. 274)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 274)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 274)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 274)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerError (p. 274)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Response bodies

GetInvitationsCountResponse schema

```
{
  "invitationsCount": integer
}
```

ValidationException schema

```
{
  "message": "string"
}
```

ServiceQuotaExceededException schema

```
{
  "message": "string"
}
```

AccessDeniedException schema

```
{
  "message": "string"
}
```

ResourceNotFoundException schema

```
{
```



```
"message": "string"
}
```

ConflictException schema

```
{
  "message": "string"
}
```

ThrottlingException schema

```
{
  "message": "string"
}
```

InternalServerError schema

```
{
  "message": "string"
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

GetInvitationsCountResponse

Provides the count of all the Amazon Macie membership invitations that were received by an account, not including the currently accepted invitation.

invitationsCount

The total number of invitations that were received by the account, not including the currently accepted invitation.

Type: integer
Required: False
Format: int64

InternalServerErrorException

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string
Required: False

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string
Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string
Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string

Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string

Required: False

See also

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

GetInvitationsCount

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Invitation Decline

In Amazon Macie, an *invitation*, also referred to as a *membership invitation*, is a request to become a member of a Macie organization. A *Macie organization* is a set of Amazon Macie accounts that are created and managed as a group by using Macie.

The Invitation Decline resource provides access to membership invitations that you've received and haven't responded to, and it enables you to decline one or more of those invitations. After you decline an invitation, you can optionally delete the invitation.

Note that this resource doesn't provide access to invitations for AWS organizations. It provides access only to invitations that were sent using Macie. An *AWS organization* is a set of AWS accounts that are managed as a group by using AWS Organizations. AWS Organizations is an account management service that enables administrators to consolidate and centrally manage multiple AWS accounts as a single organization. To learn more about this service, see the [AWS Organizations User Guide](#).

You can use the Invitation Decline resource to decline Macie membership invitations that you received from specific accounts. If you do this, you have to specify the AWS account ID for each account that sent an invitation to decline. To find these IDs, you can use the [Invitation List \(p. 287\)](#) resource.

URI

/invitations/decline

HTTP methods

POST

Operation ID: DeclineInvitations

Declines Amazon Macie membership invitations that were received from specific accounts.

Responses

Status code	Response model	Description
200	DeclineInvitationsResponse (p. 278)	The request succeeded. Processing might not be complete.
400	ValidationException (p. 278)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 278)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 278)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 278)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 278)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 278)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 278)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

POST schema

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

```
]
}
```

Response bodies

DeclineInvitationsResponse schema

```
{
  "unprocessedAccounts": [
    {
      "accountId": "string",
      "errorMessage": "string",
      "errorCode": enum
    }
  ]
}
```

ValidationException schema

```
{
  "message": "string"
}
```

ServiceQuotaExceededException schema

```
{
  "message": "string"
}
```

AccessDeniedException schema

```
{
  "message": "string"
}
```

ResourceNotFoundException schema

```
{
  "message": "string"
}
```

ConflictException schema

```
{
  "message": "string"
}
```

ThrottlingException schema

```
{
```

```
"message": "string"  
}
```

InternalServerError schema

```
{  
  "message": "string"  
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

DeclineInvitationsRequest

Specifies one or more accounts that sent Amazon Macie membership invitations to decline.

accountIds

An array that lists AWS account IDs, one for each account that sent an invitation to decline.

Type: Array of type string

Required: True

DeclineInvitationsResponse

Provides information about unprocessed requests to decline Amazon Macie membership invitations that were received from specific accounts.

unprocessedAccounts

An array of objects, one for each account whose invitation hasn't been declined. Each object identifies the account and explains why the request hasn't been processed for that account.

Type: Array of type [UnprocessedAccount](#) (p. 281)
Required: False

ErrorCode

The source of an issue or delay. Possible values are:

`ClientError`
`InternalError`

InternalServerError

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string
Required: False

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string
Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string
Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string
Required: False

UnprocessedAccount

Provides information about an account-related request that hasn't been processed.

accountId

The AWS account ID for the account that the request applies to.

Type: string
Required: False

errorMessage

The reason why the request hasn't been processed.

Type: string
Required: False

errorCode

The source of the issue or delay in processing the request.

Type: [ErrorCode](#) (p. 280)
Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string
Required: False

See also

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

DeclineInvitations

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)

- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Invitation Deletion

In Amazon Macie, an *invitation*, also referred to as a *membership invitation*, is a request to become a member of a Macie organization. A *Macie organization* is a set of Amazon Macie accounts that are created and managed as a group by using Macie.

The Invitation Deletion resource provides access to membership invitations that you received and declined, and it enables you to delete one or more of those invitations. Note that this resource doesn't provide access to invitations for AWS organizations. It provides access only to invitations that were sent using Macie. An *AWS organization* is a set of AWS accounts that are managed as a group by using AWS Organizations. AWS Organizations is an account management service that enables administrators to consolidate and centrally manage multiple AWS accounts as a single organization. To learn more about this service, see the [AWS Organizations User Guide](#).

You can use the Invitation Deletion resource to delete Macie membership invitations that you received from specific accounts and previously declined. If you do this, you have to specify the AWS account ID for each account that sent an invitation to delete. To find these IDs, you can use the [Invitation List \(p. 287\)](#) resource.

URI

/invitations/delete

HTTP methods

POST

Operation ID: DeleteInvitations

Deletes Amazon Macie membership invitations that were received from specific accounts.

Responses

Status code	Response model	Description
200	DeleteInvitationsResponse (p. 283)	The request succeeded. Processing might not be complete.
400	ValidationException (p. 283)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 283)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 283)	The request was denied because you don't have sufficient access to the specified resource.

Status code	Response model	Description
404	ResourceNotFoundException (p. 284)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 284)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 284)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 284)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

POST schema

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

Response bodies

DeleteInvitationsResponse schema

```
{
  "unprocessedAccounts": [
    {
      "accountId": "string",
      "errorMessage": "string",
      "errorCode": enum
    }
  ]
}
```

ValidationException schema

```
{
  "message": "string"
}
```

ServiceQuotaExceededException schema

```
{
  "message": "string"
}
```

```
}
```

AccessDeniedException schema

```
{  
  "message": "string"  
}
```

ResourceNotFoundException schema

```
{  
  "message": "string"  
}
```

ConflictException schema

```
{  
  "message": "string"  
}
```

ThrottlingException schema

```
{  
  "message": "string"  
}
```

InternalServerError schema

```
{  
  "message": "string"  
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

DeleteInvitationsRequest

Specifies one or more accounts that sent Amazon Macie membership invitations to delete.

accountIds

An array that lists AWS account IDs, one for each account that sent an invitation to delete.

Type: Array of type string

Required: True

DeleteInvitationsResponse

Provides information about unprocessed requests to delete Amazon Macie membership invitations that were received from specific accounts.

unprocessedAccounts

An array of objects, one for each account whose invitation hasn't been deleted. Each object identifies the account and explains why the request hasn't been processed for that account.

Type: Array of type [UnprocessedAccount](#) (p. 286)

Required: False

ErrorCode

The source of an issue or delay. Possible values are:

`ClientError`

`InternalError`

InternalServerError

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string

Required: False

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string

Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string

Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string

Required: False

UnprocessedAccount

Provides information about an account-related request that hasn't been processed.

accountId

The AWS account ID for the account that the request applies to.

Type: string

Required: False

errorMessage

The reason why the request hasn't been processed.

Type: string

Required: False

errorCode

The source of the issue or delay in processing the request.

Type: [ErrorCode](#) (p. 285)

Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string

Required: False

See also

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

DeleteInvitations

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Invitation List

In Amazon Macie, an *invitation*, also referred to as a *membership invitation*, is a request to become a member of a Macie organization. A *Macie organization* is a set of Amazon Macie accounts that are created and managed as a group by using Macie.

The Invitation List resource provides information about all the membership invitations that you've received. For each invitation, this includes the unique identifier for the invitation, the AWS account ID for the account that sent it, and the current status of the relationship between your account and the account that sent it. This resource also enables you to send invitations to other accounts.

Note that this resource doesn't provide information about invitations for AWS organizations. It's limited to invitations that were sent using Macie. An *AWS organization* is a set of AWS accounts that are managed as a group by using AWS Organizations. AWS Organizations is an account management service that enables administrators to consolidate and centrally manage multiple AWS accounts as a single organization. To learn more about this service, see the [AWS Organizations User Guide](#).

You can use the Invitation List resource to retrieve information about all the Macie membership invitations that you've received. You can also use this resource to send a membership invitation to another account.

URI

/invitations

HTTP methods

GET

Operation ID: ListInvitations

Retrieves information about the Amazon Macie membership invitations that were received by an account.

Query parameters

Name	Type	Required	Description
nextToken	String	False	The nextToken string that specifies which page of results to return in a paginated response.
maxResults	String	False	The maximum number of items to include in each page of a paginated response.

Responses

Status code	Response model	Description
200	ListInvitationsResponse (p. 290)	The request succeeded.
400	ValidationException (p. 290)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 290)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 291)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 291)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 291)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 291)	The request failed because you sent too many requests during a certain amount of time.

Status code	Response model	Description
500	InternalServerError (p. 290)	The request failed due to an unknown internal server error, exception, or failure.

POST

Operation ID: CreateInvitations

Sends an Amazon Macie membership invitation to one or more accounts.

Responses

Status code	Response model	Description
200	CreateInvitationsResponse (p. 290)	The request succeeded. Processing might not be complete.
400	ValidationException (p. 290)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 290)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 290)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 290)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 291)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 291)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerError (p. 290)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

POST schema

```
{
  "disableEmailNotification": boolean,
  "accountIds": [
```



```
    "string"
  ],
  "message": "string"
}
```

Response bodies

ListInvitationsResponse schema

```
{
  "invitations": [
    {
      "accountId": "string",
      "relationshipStatus": enum,
      "invitationId": "string",
      "invitedAt": "string"
    }
  ],
  "nextToken": "string"
}
```

CreateInvitationsResponse schema

```
{
  "unprocessedAccounts": [
    {
      "accountId": "string",
      "errorMessage": "string",
      "errorCode": enum
    }
  ]
}
```

ValidationException schema

```
{
  "message": "string"
}
```

ServiceQuotaExceededException schema

```
{
  "message": "string"
}
```

AccessDeniedException schema

```
{
  "message": "string"
}
```

ResourceNotFoundException schema

```
{
  "message": "string"
}
```

```
}
```

ConflictException schema

```
{  
  "message": "string"  
}
```

ThrottlingException schema

```
{  
  "message": "string"  
}
```

InternalServerError schema

```
{  
  "message": "string"  
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

CreateInvitationsRequest

Specifies the settings for an Amazon Macie membership invitation.

disableEmailNotification

Specifies whether to send an email notification to the root user of each account that the invitation will be sent to. This notification is in addition to an alert that the root user receives in AWS Personal Health Dashboard. To send an email notification to the root user of each account, set this value to `true`.

Type: boolean
Required: False

accountIds

An array that lists AWS account IDs, one for each account to send the invitation to.

Type: Array of type string
Required: True

message

A custom message to include in the invitation. Amazon Macie adds this message to the standard content that it sends for an invitation.

Type: string
Required: False

CreateInvitationsResponse

Provides information about an unprocessed request to send an Amazon Macie membership invitation to a specific account.

unprocessedAccounts

An array of objects, one for each account whose invitation hasn't been processed. Each object identifies the account and explains why the invitation hasn't been processed for the account.

Type: Array of type [UnprocessedAccount](#) (p. 294)
Required: False

ErrorCode

The source of an issue or delay. Possible values are:

ClientError
InternalError

InternalServerError

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string
Required: False

Invitation

Provides information about an Amazon Macie membership invitation that was received by an account.

accountId

The AWS account ID for the account that sent the invitation.

Type: string
Required: False

relationshipStatus

The status of the relationship between the account that sent the invitation (*inviter account*) and the account that received the invitation (*invitee account*).

Type: [RelationshipStatus](#) (p. 293)
Required: False

invitationId

The unique identifier for the invitation. Amazon Macie uses this identifier to validate the inviter account with the invitee account.

Type: string
Required: False

invitedAt

The date and time, in UTC and extended ISO 8601 format, when the invitation was sent.

Type: string
Required: False
Format: date-time

ListInvitationsResponse

Provides information about the Amazon Macie membership invitations that were received by an account.

invitations

An array of objects, one for each invitation that was received by the account.

Type: Array of type [Invitation](#) (p. 292)
Required: False

nextToken

The string to use in a subsequent request to get the next page of results in a paginated response. This value is null if there are no additional pages.

Type: string
Required: False

RelationshipStatus

The current status of the relationship between an account and an associated Amazon Macie administrator account (*inviter account*). Possible values are:

Enabled
Paused
Invited
Created
Removed
Resigned
EmailVerificationInProgress
EmailVerificationFailed
RegionDisabled
AccountSuspended

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string
Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string
Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string
Required: False

UnprocessedAccount

Provides information about an account-related request that hasn't been processed.

accountId

The AWS account ID for the account that the request applies to.

Type: string
Required: False

errorMessage

The reason why the request hasn't been processed.

Type: string

Required: False

errorCode

The source of the issue or delay in processing the request.

Type: [ErrorCode](#) (p. 292)

Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string

Required: False

See also

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

ListInvitations

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

CreateInvitations

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)

- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Managed Data Identifiers

The Managed Data Identifiers resource represents the repository of managed data identifiers that Amazon Macie currently provides. A *managed data identifier* is a set of built-in criteria and techniques that detect a specific type of sensitive data, such as credit card numbers, AWS secret keys, or passport numbers for a particular country or region. These identifiers can detect a large and growing list of sensitive data types for many countries and regions, including multiple types of financial data, personal health information (PHI), and personally identifiable information (PII). For information about the categories and types of sensitive data that they can detect, see [Using managed data identifiers](#) in the *Amazon Macie User Guide*.

To detect sensitive data with managed data identifiers, you create and run classification jobs. When you create a job, you can configure it to use all, some, or none of the managed data identifiers that Macie provides. If you want the job to use only some managed data identifiers, you specify the unique identifier for each managed data identifier that you want to explicitly include or exclude from the job's analysis. To find these unique identifiers, you can use this resource.

You can use the Managed Data Identifiers resource to retrieve information about the managed data identifiers that Macie currently provides.

URI

/managed-data-identifiers/list

HTTP methods

POST

Operation ID: ListManagedDataIdentifiers

Retrieves information about all the managed data identifiers that Amazon Macie currently provides.

Responses

Status code	Response model	Description
200	ListManagedDataIdentifiersResponse	The request succeeded.

Schemas

Request bodies

POST schema

```
{
  "nextToken": "string"
}
```

Response bodies

ListManagedDataIdentifiersResponse schema

```
{
  "nextToken": "string",
  "items": [
    {
      "id": "string",
      "category": enum
    }
  ]
}
```

Properties

ListManagedDataIdentifiersRequest

Specifies criteria for paginating the results of a request for information about managed data identifiers.

nextToken

The `nextToken` string that specifies which page of results to return in a paginated response.

Type: string

Required: False

ListManagedDataIdentifiersResponse

Provides information about the managed data identifiers that Amazon Macie currently provides.

nextToken

The string to use in a subsequent request to get the next page of results in a paginated response. This value is null if there are no additional pages.

Type: string

Required: False

items

An array of objects, one for each managed data identifier.

Type: Array of type [ManagedDataIdentifierSummary](#) (p. 297)

Required: False

ManagedDataIdentifierSummary

Provides information about a managed data identifier. For additional information, see [Using managed data identifiers](#) in the *Amazon Macie User Guide*.

id

The unique identifier for the managed data identifier. This is a string that describes the type of sensitive data that the managed data identifier detects. For example: `OPENSSH_PRIVATE_KEY` for OpenSSH

private keys, `CREDIT_CARD_NUMBER` for credit card numbers, or `USA_PASSPORT_NUMBER` for US passport numbers.

Type: string

Required: False

category

The category of sensitive data that the managed data identifier detects: `CREDENTIALS`, for credentials data such as private keys or AWS secret keys; `FINANCIAL_INFORMATION`, for financial data such as credit card numbers; or, `PERSONAL_INFORMATION`, for personal health information, such as health insurance identification numbers, or personally identifiable information, such as passport numbers.

Type: [SensitiveDataItemCategory](#) (p. 298)

Required: False

SensitiveDataItemCategory

For a finding, the category of sensitive data that was detected and produced the finding. For a managed data identifier, the category of sensitive data that the managed data identifier detects. Possible values are:

```
FINANCIAL_INFORMATION
PERSONAL_INFORMATION
CREDENTIALS
CUSTOM_IDENTIFIER
```

See also

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

ListManagedDataIdentifiers

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Master Account

This resource has been deprecated. It provides information about the Amazon Macie administrator account for your account but is retained only for backward compatibility. To retrieve information about

the Macie administrator account for your account, use the [Administrator \(p. 18\)](#) resource instead of this resource.

URI

`/master`

HTTP methods

GET

Operation ID: GetMasterAccount

(Deprecated) Retrieves information about the Amazon Macie administrator account for an account. This operation has been replaced by the [GetAdministratorAccount \(p. 18\)](#) operation.

Responses

Status code	Response model	Description
200	GetMasterAccountResponse (p. 200)	The request succeeded.
400	ValidationException (p. 300)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 300)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 300)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 300)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 300)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 300)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 300)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Response bodies

[GetMasterAccountResponse schema](#)

```
{
```

```
"master": {  
  "accountId": "string",  
  "relationshipStatus": enum,  
  "invitationId": "string",  
  "invitedAt": "string"  
}  
}
```

ValidationException schema

```
{  
  "message": "string"  
}
```

ServiceQuotaExceededException schema

```
{  
  "message": "string"  
}
```

AccessDeniedException schema

```
{  
  "message": "string"  
}
```

ResourceNotFoundException schema

```
{  
  "message": "string"  
}
```

ConflictException schema

```
{  
  "message": "string"  
}
```

ThrottlingException schema

```
{  
  "message": "string"  
}
```

InternalServerErrorException schema

```
{  
  "message": "string"  
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

GetMasterAccountResponse

(Deprecated) Provides information about the Amazon Macie administrator account for an account. If the accounts are associated by a Macie membership invitation, the response also provides information about that invitation.

master

(Deprecated) The AWS account ID for the administrator account. If the accounts are associated by a Macie membership invitation, this object also provides details about the invitation that was sent to establish the relationship between the accounts.

Type: [Invitation](#) (p. 301)

Required: False

InternalServerError

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string

Required: False

Invitation

Provides information about an Amazon Macie membership invitation that was received by an account.

accountId

The AWS account ID for the account that sent the invitation.

Type: string

Required: False

relationshipStatus

The status of the relationship between the account that sent the invitation (*inviter account*) and the account that received the invitation (*invitee account*).

Type: [RelationshipStatus](#) (p. 302)

Required: False

invitationId

The unique identifier for the invitation. Amazon Macie uses this identifier to validate the inviter account with the invitee account.

Type: string

Required: False

invitedAt

The date and time, in UTC and extended ISO 8601 format, when the invitation was sent.

Type: string

Required: False

Format: date-time

RelationshipStatus

The current status of the relationship between an account and an associated Amazon Macie administrator account (*inviter account*). Possible values are:

Enabled
Paused
Invited
Created
Removed
Resigned
EmailVerificationInProgress
EmailVerificationFailed
RegionDisabled
AccountSuspended

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string
Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string
Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string
Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string
Required: False

See also

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

GetMasterAccount

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)

- [AWS SDK for Ruby V3](#)

Master Disassociation

This resource has been deprecated. It enables you to disassociate your Amazon Macie account from its Macie administrator account but is retained only for backward compatibility. To disassociate your account from its Macie administrator account, use the [Administrator Disassociation \(p. 23\)](#) resource instead of this resource.

URI

/master/disassociate

HTTP methods

POST

Operation ID: DisassociateFromMasterAccount

(Deprecated) Disassociates a member account from its Amazon Macie administrator account. This operation has been replaced by the [DisassociateFromAdministratorAccount \(p. 23\)](#) operation.

Responses

Status code	Response model	Description
200	Empty Schema (p. 305)	The request succeeded and there isn't any content to include in the body of the response (No Content).
400	ValidationException (p. 305)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 305)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 305)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 305)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 305)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 305)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 305)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Response bodies

Empty Schema schema

```
{  
}
```

ValidationException schema

```
{  
  "message": "string"  
}
```

ServiceQuotaExceededException schema

```
{  
  "message": "string"  
}
```

AccessDeniedException schema

```
{  
  "message": "string"  
}
```

ResourceNotFoundException schema

```
{  
  "message": "string"  
}
```

ConflictException schema

```
{  
  "message": "string"  
}
```

ThrottlingException schema

```
{  
  "message": "string"  
}
```

InternalServerError schema

```
{  
  "message": "string"  
}
```


Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

Empty

The request succeeded and there isn't any content to include in the body of the response (No Content).

InternalServerErrorException

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string

Required: False

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string

Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string

Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string

Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string

Required: False

See also

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

DisassociateFromMasterAccount

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Member

The Member resource provides information about an individual account that's associated with your Amazon Macie account, typically a Macie administrator account. This information includes details such

as the AWS account ID for the account, and the current status of the relationship between your accounts. If you sent a Macie membership invitation to an account, this resource also indicates when you sent that invitation.

You can use the Member resource to retrieve information about an account that's associated with your Macie account. You can also use this resource to delete an existing association between your Macie account and another account. To use this resource, you have to specify the AWS account ID for the account that your request applies to. To find this ID, you can use the [Members \(p. 324\)](#) resource.

URI

`/members/id`

HTTP methods

GET

Operation ID: GetMember

Retrieves information about an account that's associated with an Amazon Macie administrator account.

Path parameters

Name	Type	Required	Description
<i>id</i>	String	True	The unique identifier for the Amazon Macie resource or account that the request applies to.

Responses

Status code	Response model	Description
200	GetMemberResponse (p. 310)	The request succeeded.
400	ValidationException (p. 310)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 310)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 310)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 310)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 310)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 310)	The request failed because you sent too many requests during a certain amount of time.

Status code	Response model	Description
500	InternalServerError (p. 310)	The request failed due to an unknown internal server error, exception, or failure.

DELETE

Operation ID: DeleteMember

Deletes the association between an Amazon Macie administrator account and an account.

Path parameters

Name	Type	Required	Description
<i>id</i>	String	True	The unique identifier for the Amazon Macie resource or account that the request applies to.

Responses

Status code	Response model	Description
200	Empty Schema (p. 310)	The request succeeded. The association was deleted and there isn't any content to include in the body of the response (No Content).
400	ValidationException (p. 310)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 310)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 310)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 310)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 310)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 311)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerError (p. 310)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Response bodies

GetMemberResponse schema

```
{
  "accountId": "string",
  "relationshipStatus": enum,
  "arn": "string",
  "masterAccountId": "string",
  "administratorAccountId": "string",
  "email": "string",
  "tags": {
  },
  "invitedAt": "string",
  "updatedAt": "string"
}
```

Empty Schema schema

```
{
}
```

ValidationException schema

```
{
  "message": "string"
}
```

ServiceQuotaExceededException schema

```
{
  "message": "string"
}
```

AccessDeniedException schema

```
{
  "message": "string"
}
```

ResourceNotFoundException schema

```
{
  "message": "string"
}
```

ConflictException schema

```
{
```

```
"message": "string"
}
```

ThrottlingException schema

```
{
  "message": "string"
}
```

InternalServerError schema

```
{
  "message": "string"
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string
Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string
Required: False

Empty

The request succeeded and there isn't any content to include in the body of the response (No Content).

GetMemberResponse

Provides information about an account that's associated with an Amazon Macie administrator account.

accountId

The AWS account ID for the account.

Type: string

Required: False

relationshipStatus

The current status of the relationship between the account and the administrator account.

Type: [RelationshipStatus](#) (p. 313)

Required: False

arn

The Amazon Resource Name (ARN) of the account.

Type: string

Required: False

masterAccountId

(Deprecated) The AWS account ID for the administrator account. This property has been replaced by the `administratorAccountId` property and is retained only for backward compatibility.

Type: string

Required: False

administratorAccountId

The AWS account ID for the administrator account.

Type: string

Required: False

email

The email address for the account.

Type: string

Required: False

tags

A map of key-value pairs that identifies the tags (keys and values) that are associated with the member account in Amazon Macie.

Type: [TagMap](#) (p. 314)

Required: False

invitedAt

The date and time, in UTC and extended ISO 8601 format, when an Amazon Macie membership invitation was last sent to the account. This value is null if a Macie invitation hasn't been sent to the account.

Type: string

Required: False

Format: date-time

updatedAt

The date and time, in UTC and extended ISO 8601 format, of the most recent change to the status of the relationship between the account and the administrator account.

Type: string
Required: False
Format: date-time

InternalServerErrorException

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string
Required: False

RelationshipStatus

The current status of the relationship between an account and an associated Amazon Macie administrator account (*inviter account*). Possible values are:

Enabled
Paused
Invited
Created
Removed
Resigned
EmailVerificationInProgress
EmailVerificationFailed
RegionDisabled
AccountSuspended

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string
Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string
Required: False

TagMap

A string-to-string map of key-value pairs that specifies the tags (keys and values) for a classification job, custom data identifier, findings filter, or member account.

key-value pairs

Type: string

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string
Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string
Required: False

See also

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

GetMember

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

DeleteMember

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Member Disassociation

The Member Disassociation resource provides access to associations between an Amazon Macie administrator account and its member accounts. If you're a user of a Macie administrator account, you can use this resource to disassociate a member account from your account. To use this resource, you have to specify the AWS account ID for the member account to disassociate. To find this ID, you can use the [Members \(p. 324\)](#) resource.

If you're a user of a member account and you want to disassociate your account from its Macie administrator account, use the [Administrator Disassociation \(p. 23\)](#) resource.

URI

/members/disassociate/*id*

HTTP methods

POST

Operation ID: DisassociateMember

Disassociates an Amazon Macie administrator account from a member account.

Path parameters

Name	Type	Required	Description
<i>id</i>	String	True	The unique identifier for the Amazon Macie resource or account that the request applies to.

Responses

Status code	Response model	Description
200	Empty Schema (p. 316)	The request succeeded.
400	ValidationException (p. 316)	The request failed because it contains a syntax error.

Status code	Response model	Description
402	ServiceQuotaExceededException (p. 316)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 317)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 317)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 317)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 317)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 317)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Response bodies

Empty Schema schema

```
{
}
```

ValidationException schema

```
{
  "message": "string"
}
```

ServiceQuotaExceededException schema

```
{
  "message": "string"
}
```

AccessDeniedException schema

```
{
  "message": "string"
}
```

ResourceNotFoundException schema

```
{  
  "message": "string"  
}
```

ConflictException schema

```
{  
  "message": "string"  
}
```

ThrottlingException schema

```
{  
  "message": "string"  
}
```

InternalServerError schema

```
{  
  "message": "string"  
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

Empty

The request succeeded and there isn't any content to include in the body of the response (No Content).

InternalServerErrorException

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string

Required: False

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string

Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string

Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string

Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string

Required: False

See also

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

DisassociateMember

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Member Status

The Member Status resource provides access to the status of an Amazon Macie member account in your organization. If you're a user of a Macie administrator account, you can use this resource to suspend (pause) a member account. If you suspend an account, Macie stops performing all activities for the account. However, it retains the session identifier, settings, and resources for the account.

As a user of a Macie administrator account, you can also use this resource to re-enable a member account that you previously suspended. When you re-enable an account, Macie resumes all activities for the account.

URI

`/macie/members/id`

HTTP methods

PATCH

Operation ID: UpdateMemberSession

Enables an Amazon Macie administrator to suspend or re-enable a member account.

Path parameters

Name	Type	Required	Description
<i>id</i>	String	True	The unique identifier for the Amazon Macie resource or account that the request applies to.

Responses

Status code	Response model	Description
200	Empty Schema (p. 320)	The request succeeded and there isn't any content to include in the body of the response (No Content).
400	ValidationException (p. 320)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 320)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 320)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 320)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 321)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 321)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 321)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

PATCH schema

```
{
  "status": enum
}
```

Response bodies

Empty Schema schema

```
{
}
```

ValidationException schema

```
{
```

```
{  
  "message": "string"  
}
```

ServiceQuotaExceededException schema

```
{  
  "message": "string"  
}
```

AccessDeniedException schema

```
{  
  "message": "string"  
}
```

ResourceNotFoundException schema

```
{  
  "message": "string"  
}
```

ConflictException schema

```
{  
  "message": "string"  
}
```

ThrottlingException schema

```
{  
  "message": "string"  
}
```

InternalServerErrorException schema

```
{  
  "message": "string"  
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string
Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string
Required: False

Empty

The request succeeded and there isn't any content to include in the body of the response (No Content).

InternalServerError

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string
Required: False

MacieStatus

The status of an Amazon Macie account. Valid values are:

PAUSED
ENABLED

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string
Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string

Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string

Required: False

UpdateMemberSessionRequest

Suspends (pauses) or re-enables an Amazon Macie member account.

status

Specifies the new status for the account. Valid values are: `ENABLED`, resume all Amazon Macie activities for the account; and, `PAUSED`, suspend all Macie activities for the account.

Type: [MacieStatus](#) (p. 322)

Required: True

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string

Required: False

See also

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

UpdateMemberSession

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)

- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Members

The Members resource provides information about all the accounts that are associated with your Amazon Macie account, typically a Macie administrator account. This includes member accounts, which are accounts that are part of your organization, and non-member accounts. For each account, this resource provides details such as the AWS account ID for the account and the current status of the relationship between your accounts. If you sent a Macie membership invitation to an account, this resource also indicates when you sent that invitation.

The Members resource also enables you to associate additional accounts with your Macie account. You can then invite those accounts to enable Macie and allow you to administer and manage certain Macie settings and resources on their behalf. If an invitation is accepted, your account is designated as the *administrator account*. The account that accepted the invitation is designated as a *member account*.

You can use the Members resource to associate one or more accounts with your Macie account. You can also use this resource to retrieve information about the accounts that are currently associated with your Macie account.

URI

`/members`

HTTP methods

GET

Operation ID: ListMembers

Retrieves information about the accounts that are associated with an Amazon Macie administrator account.

Query parameters

Name	Type	Required	Description
onlyAssociated	String	False	Specifies which accounts to include in the response, based on the status of an account's relationship with the administrator account. By default, the response includes only current member accounts. To include all accounts, set this value to <code>false</code> .

Name	Type	Required	Description
<code>nextToken</code>	String	False	The <code>nextToken</code> string that specifies which page of results to return in a paginated response.
<code>maxResults</code>	String	False	The maximum number of items to include in each page of a paginated response.

Responses

Status code	Response model	Description
200	ListMembersResponse (p. 326)	The request succeeded.
400	ValidationException (p. 327)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 327)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 327)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 327)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 327)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 327)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 327)	The request failed due to an unknown internal server error, exception, or failure.

POST

Operation ID: `CreateMember`

Associates an account with an Amazon Macie administrator account.

Responses

Status code	Response model	Description
200	CreateMemberResponse (p. 327)	The request succeeded.

Status code	Response model	Description
400	ValidationException (p. 327)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 327)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 327)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 327)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 327)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 327)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerErrorException (p. 328)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

POST schema

```
{
  "account": {
    "accountId": "string",
    "email": "string"
  },
  "tags": {
  }
}
```

Response bodies

ListMembersResponse schema

```
{
  "nextToken": "string",
  "members": [
    {
      "accountId": "string",
      "relationshipStatus": enum,
      "arn": "string",
      "masterAccountId": "string",
      "administratorAccountId": "string",
    }
  ]
}
```

```
    "email": "string",
    "tags": {
    },
    "invitedAt": "string",
    "updatedAt": "string"
  }
]
```

CreateMemberResponse schema

```
{
  "arn": "string"
}
```

ValidationException schema

```
{
  "message": "string"
}
```

ServiceQuotaExceededException schema

```
{
  "message": "string"
}
```

AccessDeniedException schema

```
{
  "message": "string"
}
```

ResourceNotFoundException schema

```
{
  "message": "string"
}
```

ConflictException schema

```
{
  "message": "string"
}
```

ThrottlingException schema

```
{
  "message": "string"
}
```

InternalServerError schema

```
{  
  "message": "string"  
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

AccountDetail

Specifies the details of an account to associate with an Amazon Macie administrator account.

accountId

The AWS account ID for the account.

Type: string

Required: True

email

The email address for the account.

Type: string

Required: True

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

CreateMemberRequest

Specifies an AWS account to associate with an Amazon Macie administrator account.

account

The details of the account to associate with the administrator account.

Type: [AccountDetail](#) (p. 328)

Required: True

tags

A map of key-value pairs that specifies the tags to associate with the account in Amazon Macie.

An account can have a maximum of 50 tags. Each tag consists of a tag key and an associated tag value. The maximum length of a tag key is 128 characters. The maximum length of a tag value is 256 characters.

Type: [TagMap](#) (p. 332)

Required: False

CreateMemberResponse

Provides information about a request to associate an account with an Amazon Macie administrator account.

arn

The Amazon Resource Name (ARN) of the account that was associated with the administrator account.

Type: string

Required: False

InternalServerError

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string

Required: False

ListMembersResponse

Provides information about the accounts that are associated with an Amazon Macie administrator account.

nextToken

The string to use in a subsequent request to get the next page of results in a paginated response. This value is null if there are no additional pages.

Type: string

Required: False

members

An array of objects, one for each account that's associated with the administrator account and meets the criteria specified by the `onlyAssociated` request parameter.

Type: Array of type [Member](#) (p. 330)
Required: False

Member

Provides information about an account that's associated with an Amazon Macie administrator account.

accountId

The AWS account ID for the account.

Type: string
Required: False

relationshipStatus

The current status of the relationship between the account and the administrator account.

Type: [RelationshipStatus](#) (p. 331)
Required: False

arn

The Amazon Resource Name (ARN) of the account.

Type: string
Required: False

masterAccountId

(Deprecated) The AWS account ID for the administrator account. This property has been replaced by the `administratorAccountId` property and is retained only for backward compatibility.

Type: string
Required: False

administratorAccountId

The AWS account ID for the administrator account.

Type: string
Required: False

email

The email address for the account.

Type: string
Required: False

tags

A map of key-value pairs that identifies the tags (keys and values) that are associated with the account in Amazon Macie.

Type: [TagMap](#) (p. 332)

Required: False

invitedAt

The date and time, in UTC and extended ISO 8601 format, when an Amazon Macie membership invitation was last sent to the account. This value is null if a Macie invitation hasn't been sent to the account.

Type: string

Required: False

Format: date-time

updatedAt

The date and time, in UTC and extended ISO 8601 format, of the most recent change to the status of the relationship between the account and the administrator account.

Type: string

Required: False

Format: date-time

RelationshipStatus

The current status of the relationship between an account and an associated Amazon Macie administrator account (*inviter account*). Possible values are:

Enabled
Paused
Invited
Created
Removed
Resigned
EmailVerificationInProgress
EmailVerificationFailed
RegionDisabled
AccountSuspended

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string

Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string

Required: False

TagMap

A string-to-string map of key-value pairs that specifies the tags (keys and values) for a classification job, custom data identifier, findings filter, or member account.

key-value pairs

Type: string

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string

Required: False

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string

Required: False

See also

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

ListMembers

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)

- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

CreateMember

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Tags

A *tag* is a label that you optionally define and associate with AWS resources, including certain types of Amazon Macie resources. Tags can help you identify, organize, and manage resources in different ways, such as by purpose, owner, environment, or other criteria. You can associate tags with the following types of Amazon Macie resources:

- Classification jobs
- Custom data identifiers
- Findings filters
- Member accounts

A resource can have as many as 50 tags. Each tag consists of a *tag key* and an associated *tag value*, both of which you define. A *tag key* is a general label that acts as a category for more specific tag values. A *tag value* acts as a descriptor for a tag key. For example, you might assign an `Owner` tag key to each classification job for your organization. The value for the key might be the name of the person or team to contact about the classification job.

You can use the Tags resource to add, retrieve, update, or remove tags from a classification job, custom data identifier, findings filter, or member account.

URI

/tags/*resourceArn*

HTTP methods

GET

Operation ID: `ListTagsForResource`

Retrieves the tags (keys and values) that are associated with a classification job, custom data identifier, findings filter, or member account.

Path parameters

Name	Type	Required	Description
<i>resourceArn</i>	String	True	The Amazon Resource Name (ARN) of the classification job, custom data identifier, findings filter, or member account.

Responses

Status code	Response model	Description
200	ListTagsForResourceResponse (p. 334)	The request succeeded.

POST

Operation ID: TagResource

Adds or updates one or more tags (keys and values) that are associated with a classification job, custom data identifier, findings filter, or member account.

Path parameters

Name	Type	Required	Description
<i>resourceArn</i>	String	True	The Amazon Resource Name (ARN) of the classification job, custom data identifier, findings filter, or member account.

Responses

Status code	Response model	Description
204	TagResourceResponse (p. 334)	The request succeeded and there isn't any content to include in the body of the response (No Content).

DELETE

Operation ID: UntagResource

Removes one or more tags (keys and values) from a classification job, custom data identifier, findings filter, or member account.

Path parameters

Name	Type	Required	Description
<i>resourceArn</i>	String	True	The Amazon Resource Name (ARN) of the classification job, custom data identifier, findings filter, or member account.

Query parameters

Name	Type	Required	Description
tagKeys	String	True	The key of the tag to remove from the resource. To remove multiple tags, append the tagKeys parameter and argument for each additional tag to remove, separated by an ampersand (&).

Responses

Status code	Response model	Description
204	UntagResourceResponse (p. 315)	The request succeeded and there isn't any content to include in the body of the response (No Content).

Schemas

Request bodies

POST schema

<pre>{ "tags": { } }</pre>

Response bodies

ListTagsForResourceResponse schema

<pre>{ "tags": { } }</pre>

```
}
```

TagResourceResponse schema

```
{  
}
```

UntagResourceResponse schema

```
{  
}
```

Properties

ListTagsForResourceResponse

Provides information about the tags (keys and values) that are associated with a classification job, custom data identifier, findings filter, or member account.

tags

A map of key-value pairs that identifies the tags (keys and values) that are associated with the resource.

Type: [TagMap](#) (p. 336)

Required: False

TagMap

A string-to-string map of key-value pairs that specifies the tags (keys and values) for a classification job, custom data identifier, findings filter, or member account.

key-value pairs

Type: string

TagResourceRequest

Specifies the tags (keys and values) to associate with a classification job, custom data identifier, findings filter, or member account.

tags

A map of key-value pairs that specifies the tags to associate with the resource.

A resource can have a maximum of 50 tags. Each tag consists of a tag key and an associated tag value. The maximum length of a tag key is 128 characters. The maximum length of a tag value is 256 characters.

Type: [TagMap](#) (p. 336)

Required: True

TagResourceResponse

The request succeeded. The specified tags were added to the resource.

UntagResourceResponse

The request succeeded. The specified tags were removed from the resource.

See also

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

ListTagsForResource

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

TagResource

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

UntagResource

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Usage Statistics

The Usage Statistics resource provides information about current quotas and usage statistics for your Amazon Macie account. This includes data for metrics that report the estimated cost of using Macie to perform specific types of tasks, and the current account quotas for those tasks. The data can help you track your use of the service and determine whether to adjust your quotas or use of the service. If you're participating in the Macie free trial, this resource also provides information about your free trial.

You can use the Usage Statistics resource to retrieve (query) aggregated data for usage metrics that apply to your Macie account and the quotas that correspond to those metrics. To customize your query, you can use supported parameters to filter and sort the data, and to specify a time range for the data. The time range can be the preceding 30 days or the current calendar month to date. If you're a user of a Macie administrator account, you can use this resource to get a breakdown of the quotas and usage data for each member account in your organization.

For information about how Macie calculates usage statistics for your account, see [Monitoring and forecasting costs](#) in the *Amazon Macie User Guide*.

URI

/usage/statistics

HTTP methods

POST

Operation ID: GetUsageStatistics

Retrieves (queries) quotas and aggregated usage data for one or more accounts.

Responses

Status code	Response model	Description
200	GetUsageStatisticsResponse	The request succeeded.
400	ValidationException (p. 340)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 340)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 340)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 340)	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException (p. 340)	The request failed because you sent too many requests during a certain amount of time.

Status code	Response model	Description
500	InternalServerError (p. 146)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

POST schema

```
{
  "nextToken": "string",
  "maxResults": integer,
  "sortBy": {
    "orderBy": enum,
    "key": enum
  },
  "filterBy": [
    {
      "comparator": enum,
      "values": [
        "string"
      ],
      "key": enum
    }
  ],
  "timeRange": enum
}
```

Response bodies

GetUsageStatisticsResponse schema

```
{
  "records": [
    {
      "accountId": "string",
      "freeTrialStartDate": "string",
      "usage": [
        {
          "serviceLimit": {
            "unit": enum,
            "isServiceLimited": boolean,
            "value": integer
          },
          "currency": enum,
          "estimatedCost": "string",
          "type": enum
        }
      ]
    }
  ],
  "nextToken": "string",
  "timeRange": enum
}
```

ValidationException schema

```
{  
  "message": "string"  
}
```

ServiceQuotaExceededException schema

```
{  
  "message": "string"  
}
```

AccessDeniedException schema

```
{  
  "message": "string"  
}
```

ResourceNotFoundException schema

```
{  
  "message": "string"  
}
```

ConflictException schema

```
{  
  "message": "string"  
}
```

ThrottlingException schema

```
{  
  "message": "string"  
}
```

InternalServerError schema

```
{  
  "message": "string"  
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string
Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string
Required: False

Currency

The type of currency that the data for an Amazon Macie usage metric is reported in. Possible values are:

USD

GetUsageStatisticsRequest

Specifies criteria for filtering, sorting, and paginating the results of a query for quotas and aggregated usage data for one or more Amazon Macie accounts.

nextToken

The `nextToken` string that specifies which page of results to return in a paginated response.

Type: string
Required: False

maxResults

The maximum number of items to include in each page of the response.

Type: integer
Required: False
Format: int32

sortBy

The criteria to use to sort the query results.

Type: [UsageStatisticsSortBy](#) (p. 346)
Required: False

filterBy

An array of objects, one for each condition to use to filter the query results. If you specify more than one condition, Amazon Macie uses an AND operator to join the conditions.

Type: Array of type [UsageStatisticsFilter](#) (p. 345)
Required: False

timeRange

The inclusive time period to query usage data for. Valid values are: `MONTH_TO_DATE`, for the current calendar month to date; and, `PAST_30_DAYS`, for the preceding 30 days. If you don't specify a value, Amazon Macie provides usage data for the preceding 30 days.

Type: [TimeRange](#) (p. 344)

Required: False

GetUsageStatisticsResponse

Provides the results of a query that retrieved quotas and aggregated usage data for one or more Amazon Macie accounts.

records

An array of objects that contains the results of the query. Each object contains the data for an account that meets the filter criteria specified in the request.

Type: Array of type [UsageRecord](#) (p. 344)

Required: False

nextToken

The string to use in a subsequent request to get the next page of results in a paginated response. This value is null if there are no additional pages.

Type: string

Required: False

timeRange

The inclusive time period that the usage data applies to. Possible values are: `MONTH_TO_DATE`, for the current calendar month to date; and, `PAST_30_DAYS`, for the preceding 30 days.

Type: [TimeRange](#) (p. 344)

Required: False

InternalServerErrorException

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string

Required: False

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string

Required: False

ServiceLimit

Specifies a current quota for an Amazon Macie account.

unit

The unit of measurement for the value specified by the `value` field.

Type: string

Required: False

Values: TERABYTES

isServiceLimited

Specifies whether the account has met the quota that corresponds to the metric specified by the `UsageByAccount.type` field in the response.

Type: boolean

Required: False

value

The value for the metric specified by the `UsageByAccount.type` field in the response.

Type: integer

Required: False

Format: int64

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string

Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string
Required: False

TimeRange

An inclusive time period that Amazon Macie usage data applies to. Possible values are:

MONTH_TO_DATE
PAST_30_DAYS

UsageByAccount

Provides data for a specific usage metric and the corresponding quota for an Amazon Macie account.

serviceLimit

The current value for the quota that corresponds to the metric specified by the `type` field.

Type: [ServiceLimit](#) (p. 343)
Required: False

currency

The type of currency that the value for the metric (`estimatedCost`) is reported in.

Type: [Currency](#) (p. 341)
Required: False

estimatedCost

The estimated value for the metric.

Type: string
Required: False

type

The name of the metric. Possible values are: `DATA_INVENTORY_EVALUATION`, for monitoring S3 buckets; and, `SENSITIVE_DATA_DISCOVERY`, for analyzing S3 objects to detect sensitive data.

Type: [UsageType](#) (p. 347)
Required: False

UsageRecord

Provides quota and aggregated usage data for an Amazon Macie account.

accountId

The unique identifier for the AWS account that the data applies to.

Type: string
Required: False

freeTrialStartDate

The date and time, in UTC and extended ISO 8601 format, when the free trial started for the account.

Type: string

Required: False

Format: date-time

usage

An array of objects that contains usage data and quotas for the account. Each object contains the data for a specific usage metric and the corresponding quota.

Type: Array of type [UsageByAccount](#) (p. 344)

Required: False

UsageStatisticsFilter

Specifies a condition for filtering the results of a query for quota and usage data for one or more Amazon Macie accounts.

comparator

The operator to use in the condition. If the value for the key property is `accountId`, this value must be `CONTAINS`. If the value for the key property is any other supported field, this value can be `EQ`, `GT`, `GTE`, `LT`, `LTE`, or `NE`.

Type: [UsageStatisticsFilterComparator](#) (p. 346)

Required: False

values

An array that lists values to use in the condition, based on the value for the field specified by the key property. If the value for the key property is `accountId`, this array can specify multiple values. Otherwise, this array can specify only one value.

Valid values for each supported field are:

- `accountId` - The unique identifier for an AWS account.
- `freeTrialStartDate` - The date and time, in UTC and extended ISO 8601 format, when the free trial started for an account.
- `serviceLimit` - A Boolean (`true` or `false`) value that indicates whether an account has reached its monthly quota.
- `total` - A string that represents the current estimated cost for an account.

Type: Array of type string

Required: False

key

The field to use in the condition.

Type: [UsageStatisticsFilterKey](#) (p. 346)

Required: False

UsageStatisticsFilterComparator

The operator to use in a condition that filters the results of a query for Amazon Macie account quotas and usage data. Valid values are:

GT
GTE
LT
LTE
EQ
NE
CONTAINS

UsageStatisticsFilterKey

The field to use in a condition that filters the results of a query for Amazon Macie account quotas and usage data. Valid values are:

accountId
serviceLimit
freeTrialStartDate
total

UsageStatisticsSortBy

Specifies criteria for sorting the results of a query for Amazon Macie account quotas and usage data.

orderBy

The sort order to apply to the results, based on the value for the field specified by the key property. Valid values are: `ASC`, sort the results in ascending order; and, `DESC`, sort the results in descending order.

Type: string
Required: False
Values: `ASC` | `DESC`

key

The field to sort the results by.

Type: [UsageStatisticsSortKey](#) (p. 346)
Required: False

UsageStatisticsSortKey

The field to use to sort the results of a query for Amazon Macie account quotas and usage data. Valid values are:

accountId
total
serviceLimitValue

`freeTrialStartDate`

UsageType

The name of an Amazon Macie usage metric for an account. Possible values are:

`DATA_INVENTORY_EVALUATION`
`SENSITIVE_DATA_DISCOVERY`

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string
Required: False

See also

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

GetUsageStatistics

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Usage Totals

The Usage Totals resource provides aggregated usage data for your Amazon Macie account. This data can provide insight into the estimated cost of using Macie to monitor and analyze your Amazon Simple Storage Service (Amazon S3) data.

You can use this resource to retrieve (query) aggregated usage data for your Macie account for the preceding 30 days or the current calendar month to date. If you're a user of a Macie administrator account, the data reports cumulative usage for all the member accounts in your organization. To query additional usage-related data or build a custom query for a select set of accounts, use the [Usage Statistics](#) (p. 338) resource.

For information about how Macie calculates usage data for your account, see [Monitoring and forecasting costs](#) in the *Amazon Macie User Guide*.

URI

/usage

HTTP methods

GET

Operation ID: GetUsageTotals

Retrieves (queries) aggregated usage data for an account.

Query parameters

Name	Type	Required	Description
timeRange	String	False	The inclusive time period to retrieve the data for. Valid values are: MONTH_TO_DATE, for the current calendar month to date; and, PAST_30_DAYS, for the preceding 30 days. If you don't specify a value for this parameter, Amazon Macie provides aggregated usage data for the preceding 30 days.

Responses

Status code	Response model	Description
200	GetUsageTotalsResponse (p. 349)	The request succeeded.
400	ValidationException (p. 349)	The request failed because it contains a syntax error.
402	ServiceQuotaExceededException (p. 349)	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException (p. 349)	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException (p. 349)	The request failed because the specified resource wasn't found.
409	ConflictException (p. 350)	The request failed because it conflicts with the current state of the specified resource.

Status code	Response model	Description
429	ThrottlingException (p. 350)	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerError (p. 350)	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Response bodies

[GetUsageTotalsResponse](#) schema

```
{
  "usageTotals": [
    {
      "currency": enum,
      "estimatedCost": "string",
      "type": enum
    }
  ],
  "timeRange": enum
}
```

[ValidationException](#) schema

```
{
  "message": "string"
}
```

[ServiceQuotaExceededException](#) schema

```
{
  "message": "string"
}
```

[AccessDeniedException](#) schema

```
{
  "message": "string"
}
```

[ResourceNotFoundException](#) schema

```
{
  "message": "string"
}
```

ConflictException schema

```
{  
  "message": "string"  
}
```

ThrottlingException schema

```
{  
  "message": "string"  
}
```

InternalServerError schema

```
{  
  "message": "string"  
}
```

Properties

AccessDeniedException

Provides information about an error that occurred due to insufficient access to a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

ConflictException

Provides information about an error that occurred due to a versioning conflict for a specified resource.

message

The explanation of the error that occurred.

Type: string

Required: False

Currency

The type of currency that the data for an Amazon Macie usage metric is reported in. Possible values are:

USD

GetUsageTotalsResponse

Provides the results of a query that retrieved aggregated usage data for an Amazon Macie account.

usageTotals

An array of objects that contains the results of the query. Each object contains the data for a specific usage metric.

Type: Array of type [UsageTotal](#) (p. 352)

Required: False

timeRange

The inclusive time period that the usage data applies to. Possible values are: `MONTH_TO_DATE`, for the current calendar month to date; and, `PAST_30_DAYS`, for the preceding 30 days.

Type: [TimeRange](#) (p. 352)

Required: False

InternalServerError

Provides information about an error that occurred due to an unknown internal server error, exception, or failure.

message

The explanation of the error that occurred.

Type: string

Required: False

ResourceNotFoundException

Provides information about an error that occurred because a specified resource wasn't found.

message

The explanation of the error that occurred.

Type: string

Required: False

ServiceQuotaExceededException

Provides information about an error that occurred due to one or more service quotas for an account.

message

The explanation of the error that occurred.

Type: string

Required: False

ThrottlingException

Provides information about an error that occurred because too many requests were sent during a certain amount of time.

message

The explanation of the error that occurred.

Type: string

Required: False

TimeRange

An inclusive time period that Amazon Macie usage data applies to. Possible values are:

MONTH_TO_DATE

PAST_30_DAYS

UsageTotal

Provides aggregated data for an Amazon Macie usage metric. The value for the metric reports estimated usage data for an account for the preceding 30 days or the current calendar month to date, depending on the time period (`timeRange`) specified in the request.

currency

The type of currency that the value for the metric (`estimatedCost`) is reported in.

Type: [Currency](#) (p. 350)

Required: False

estimatedCost

The estimated value for the metric.

Type: string

Required: False

type

The name of the metric. Possible values are: `DATA_INVENTORY_EVALUATION`, for monitoring S3 buckets; and, `SENSITIVE_DATA_DISCOVERY`, for analyzing S3 objects to detect sensitive data.

Type: [UsageType](#) (p. 352)

Required: False

UsageType

The name of an Amazon Macie usage metric for an account. Possible values are:

DATA_INVENTORY_EVALUATION

SENSITIVE_DATA_DISCOVERY

ValidationException

Provides information about an error that occurred due to a syntax error in a request.

message

The explanation of the error that occurred.

Type: string

Required: False

See also

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

GetUsageTotals

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

AWS glossary

For the latest AWS terminology, see the [AWS glossary](#) in the *AWS General Reference*.

Document history

The following table describes the important changes to the documentation since the last release of Amazon Macie. For notification about updates to this documentation, you can subscribe to an RSS feed.

- **API version:** 2020-01-01 (latest)
- **Latest documentation update:** September 30, 2021

update-history-change	update-history-description	update-history-date
Added APIs (p. 355)	Added Amazon Simple Storage Service (Amazon S3) bucket metadata that indicates whether a bucket's permissions settings or an error prevented Macie from retrieving and processing information about a bucket or a bucket's objects. Also updated references to AWS KMS keys and customer managed keys to reflect current terminology.	September 30, 2021
Added APIs (p. 355)	Added support for specifying which managed data identifiers are used by a classification job to detect sensitive data. Also added the Managed Data Identifiers resource for retrieving a list of the managed data identifiers that are currently available.	September 16, 2021
Added APIs (p. 355)	Added support for defining runtime criteria that determine which S3 buckets a classification job analyzes. Also added the Search Data Sources resource for querying data about the AWS resources that Macie monitors and analyzes for an account.	May 14, 2021
Added APIs (p. 355)	Added support for publishing sensitive data findings to AWS Security Hub and specifying which categories of findings to publish to Security Hub.	March 22, 2021
Added and deprecated APIs (p. 355)	Replaced the term <i>master account</i> with the term <i>administrator account</i> . This includes adding APIs that use the new term and deprecating APIs that use the previous term. The new APIs provide the same	February 12, 2021

	functionality as the deprecated APIs. An <i>administrator account</i> is used to centrally manage multiple accounts.	
Added APIs (p. 355)	Added support for using Amazon S3 object prefixes in property-based conditions that refine the scope of a classification job .	January 29, 2021
Added APIs (p. 355)	Added Amazon S3 bucket metadata that indicates whether any one-time or recurring classification jobs are configured to analyze data in a bucket.	November 20, 2020
Added APIs (p. 355)	Added support for pausing and resuming classification jobs by using the UpdateClassificationJob operation. Also, sensitive data findings now include location data for up to 15 occurrences of sensitive data in an affected Amazon S3 object.	October 15, 2020
Added APIs (p. 355)	Added Amazon S3 bucket metadata and statistics that indicate the size and count of objects that Macie can analyze as part of a classification job.	September 2, 2020
Added APIs (p. 355)	Added criteria for sorting and filtering query results for account quotas and usage statistics .	July 24, 2020
Removed APIs (p. 355)	Removed support for the ArchiveFindings and UnarchiveFindings operations. To suppress findings, use the <code>action</code> parameter of the CreateFindingsFilterRequest and UpdateFindingsFilterRequest operations.	June 11, 2020
General availability (p. 355)	This release introduces version 2020-01-01 of the Amazon Macie API.	May 13, 2020