REST API Reference

Amazon Macie

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Macie: REST API Reference

Copyright © 2024 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 2
Managing multiple accounts 2
Signing requests 3
Logging API calls 3
Operations **4**
Resources **12**
Account Administration 14
URI 15
HTTP methods 15
Schemas 20
Properties 22
See also 27
Administrator 29
URI 29
HTTP methods 29
Schemas 30
Properties 32
See also 36
Administrator Disassociation 36
URI 36
HTTP methods 37
Schemas 38
Properties 39
See also 41
Allow List 42
URI 43
HTTP methods 43
Schemas 47
Properties 50
See also 58
Allow Lists 60
URI 60
HTTP methods 61

Schemas ... 63
Properties ... 65
See also ... 73
AWS Organizations - Macie Administrator ... 74
URI ... 74
HTTP methods ... 74
Schemas ... 79
Properties ... 81
See also ... 85
AWS Organizations - Macie Configuration ... 86
URI ... 86
HTTP methods ... 87
Schemas ... 89
Properties ... 91
See also ... 94
Automated Sensitive Data Discovery - Accounts ... 95
URI ... 96
HTTP methods ... 96
Schemas ... 99
Properties ... 101
See also ... 106
Automated Sensitive Data Discovery - Configuration ... 107
URI ... 109
HTTP methods ... 109
Schemas ... 111
Properties ... 112
See also ... 117
Classification Job ... 118
URI ... 118
HTTP methods ... 118
Schemas ... 121
Properties ... 126
See also ... 150
Classification Job Creation ... 151
URI ... 151
HTTP methods ... 152

Schemas ... 153
Properties ... 157
See also ... 176
Classification Job List ... 177
URI ... 177
HTTP methods ... 177
Schemas ... 178
Properties ... 182
See also ... 197
Classification Results - Export Configuration ... 197
URI ... 198
HTTP methods ... 199
Schemas ... 201
Properties ... 203
See also ... 207
Classification Scope ... 208
URI ... 209
HTTP methods ... 209
Schemas ... 212
Properties ... 214
See also ... 218
Classification Scopes ... 219
URI ... 220
HTTP methods ... 220
Schemas ... 221
Properties ... 222
See also ... 224
Custom Data Identifier ... 225
URI ... 226
HTTP methods ... 226
Schemas ... 229
Properties ... 231
See also ... 237
Custom Data Identifier Creation ... 238
URI ... 238
HTTP methods ... 239

Schemas ... 240
Properties ... 242
See also ... 248
Custom Data Identifier Descriptions ... 249
URI ... 249
HTTP methods ... 249
Schemas ... 250
Properties ... 252
See also ... 256
Custom Data Identifier List ... 257
URI ... 257
HTTP methods ... 257
Schemas ... 258
Properties ... 260
See also ... 264
Custom Data Identifier Testing ... 265
URI ... 265
HTTP methods ... 266
Schemas ... 267
Properties ... 269
See also ... 273
Data Sources - Amazon S3 ... 273
URI ... 274
HTTP methods ... 274
Schemas ... 275
Properties ... 279
See also ... 303
Data Sources - Amazon S3 Statistics ... 303
URI ... 304
HTTP methods ... 304
Schemas ... 305
Properties ... 308
See also ... 322
Data Sources - Search ... 322
URI ... 323
HTTP methods ... 323

Schemas ... 324
Properties ... 328
See also ... 345
Finding List ... 346
URI ... 346
HTTP methods ... 346
Schemas ... 348
Properties ... 349
See also ... 356
Finding Samples ... 356
URI ... 357
HTTP methods ... 357
Schemas ... 358
Properties ... 360
See also ... 363
Finding Statistics ... 363
URI ... 364
HTTP methods ... 364
Schemas ... 365
Properties ... 367
See also ... 374
Findings ... 375
URI ... 375
HTTP methods ... 375
Schemas ... 376
Properties ... 385
See also ... 433
Findings - Publication Configuration ... 433
URI ... 434
HTTP methods ... 434
Schemas ... 436
Properties ... 438
See also ... 442
Findings - Reveal Sensitive Data Occurrences ... 443
URI ... 444
HTTP methods ... 444

Schemas ... 445
Properties ... 446
See also ... 451
Findings - Reveal Sensitive Data Occurrences Availability ... 452
URI ... 452
HTTP methods ... 452
Schemas ... 453
Properties ... 454
See also ... 458
Findings - Reveal Sensitive Data Occurrences Configuration ... 458
URI ... 460
HTTP methods ... 460
Schemas ... 461
Properties ... 463
See also ... 470
Findings Filter ... 471
URI ... 471
HTTP methods ... 471
Schemas ... 476
Properties ... 478
See also ... 487
Findings Filters ... 488
URI ... 488
HTTP methods ... 489
Schemas ... 492
Properties ... 494
See also ... 502
Invitation Acceptance ... 503
URI ... 504
HTTP methods ... 504
Schemas ... 505
Properties ... 507
See also ... 510
Invitation Count ... 510
URI ... 510
HTTP methods ... 510

Schemas ... 512
Properties ... 513
See also ... 516
Invitation Decline ... 516
URI ... 516
HTTP methods ... 517
Schemas ... 518
Properties ... 520
See also ... 523
Invitation Deletion ... 524
URI ... 524
HTTP methods ... 524
Schemas ... 525
Properties ... 527
See also ... 530
Invitation List ... 531
URI ... 531
HTTP methods ... 532
Schemas ... 535
Properties ... 537
See also ... 543
Managed Data Identifiers ... 544
URI ... 544
HTTP methods ... 544
Schemas ... 545
Properties ... 545
See also ... 547
Master Account ... 548
URI ... 548
HTTP methods ... 548
Schemas ... 549
Properties ... 551
See also ... 555
Master Disassociation ... 555
URI ... 555
HTTP methods ... 555

Schemas ... 557
Properties ... 558
See also ... 560
Member ... 561
URI ... 561
HTTP methods ... 561
Schemas ... 564
Properties ... 566
See also ... 571
Member Disassociation ... 572
URI ... 572
HTTP methods ... 572
Schemas ... 574
Properties ... 575
See also ... 577
Member Status ... 578
URI ... 578
HTTP methods ... 578
Schemas ... 580
Properties ... 582
See also ... 584
Members ... 585
URI ... 585
HTTP methods ... 585
Schemas ... 589
Properties ... 591
See also ... 597
Resource Sensitivity Profile ... 598
URI ... 599
HTTP methods ... 599
Schemas ... 602
Properties ... 604
See also ... 610
Resource Sensitivity Profile - Artifacts ... 611
URI ... 611
HTTP methods ... 611

Schemas ... 613
Properties ... 614
See also ... 617
Resource Sensitivity Profile - Detections ... 618
URI ... 618
HTTP methods ... 619
Schemas ... 622
Properties ... 624
See also ... 629
Sensitivity Inspection Template ... 630
URI ... 630
HTTP methods ... 631
Schemas ... 633
Properties ... 635
See also ... 640
Sensitivity Inspection Templates ... 641
URI ... 641
HTTP methods ... 642
Schemas ... 643
Properties ... 644
See also ... 647
Tags ... 647
URI ... 648
HTTP methods ... 648
Schemas ... 650
Properties ... 651
See also ... 652
Usage Statistics ... 654
URI ... 654
HTTP methods ... 654
Schemas ... 655
Properties ... 658
See also ... 667
Usage Totals ... 668
URI ... 668
HTTP methods ... 668

Schemas 670
Properties 672
See also 676
Document history 677

Welcome

Amazon Macie is a data security service that discovers sensitive data by using machine learning and pattern matching, provides visibility into data security risks, and enables automated protection against those risks.

To help you manage the security posture of your organization's Amazon Simple Storage Service (Amazon S3) data estate, Macie provides you with an inventory of your S3 general purpose buckets, and automatically evaluates and monitors the buckets for security and access control. If Macie detects a potential issue with the security or privacy of your data, such as a bucket that becomes publicly accessible, Macie generates a finding for you to review and remediate as necessary.

Macie also automates discovery and reporting of sensitive data to provide you with a better understanding of the data that your organization stores in Amazon S3. To detect sensitive data, you can use built-in criteria and techniques that Macie provides, custom criteria that you define, or a combination of the two. If Macie detects sensitive data in an S3 object, Macie generates a finding to notify you of the sensitive data that it found.

In addition to findings, Macie provides statistics and information that offer insight into the security posture of your Amazon S3 data and where sensitive data might reside in your data estate. The statistics and information can guide your decisions to perform deeper investigations of specific S3 buckets and objects. You can analyze and process findings, statistics, and other information by using the Amazon Macie API. You can also leverage Macie integration with Amazon EventBridge and AWS Security Hub to monitor, process, and remediate findings by using other services, applications, and systems.

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 *AWS General Reference*. To learn about managing AWS Regions for your AWS account, see Enable or disable AWS Regions in your account in the *AWS Account Management Reference Guide*.

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 in each additional Region that you want to apply the changes to.

Managing multiple accounts

If your AWS environment has multiple accounts, you can associate the Amazon Macie accounts in your environment and centrally manage them as an organization in Macie. To do this, designate a single account as the delegated Macie administrator account and associate other accounts with it as Macie member accounts. You can do this in two ways: by integrating Macie with AWS Organizations, or by sending and accepting membership invitations in Macie. We recommend that you integrate Macie with AWS Organizations.

With this configuration, a designated Macie administrator can assess and monitor the overall security posture of the organization's Amazon Simple Storage Service (Amazon S3) data estate. The Macie administrator can: access certain Macie settings, data, and resources for member accounts; perform automated sensitive data discovery and run classification jobs to detect sensitive data in S3 buckets that member accounts own; and, perform various account management and administration tasks at scale, such as monitoring estimated usage costs and assessing account quotas.

If you have a member account in an organization, you can access Macie settings, data, and resources only for your own account. For this reason, you might not be able to use certain operations of the Amazon Macie API.

For information about the tasks that administrator and member accounts can perform, see Managing multiple accounts as an organization 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 access key for your root AWS account. Instead, use the access key ID and secret access key for an AWS Identity and Access Management (IAM) identity. 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 information about using credentials and signing requests, refer to the following resources in the *IAM User Guide*:

- AWS security credentials – Provides information about the types of credentials that can be used to access AWS.
- IAM identities – Provides information about the types of identities that can be used to access an AWS account.
- Temporary security credentials in IAM – Provides information about creating and using temporary security credentials.
- AWS Signature Version 4 for API requests – Provides information about signing an API request.

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 operations.

By using the information collected by CloudTrail, you can determine which requests were sent to Macie successfully. For each request, you can identify when it was made, the IP address from which it was made, who made it, and additional details. For more information, see Logging API calls with AWS CloudTrail in the *Amazon Macie User Guide*.

Operations

The Amazon Macie REST API includes the following operations.

- AcceptInvitation

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

  Retrieves information about one or more custom data identifiers.
- BatchUpdateAutomatedDiscoveryAccounts

  Changes the status of automated sensitive data discovery for one or more accounts.
- CreateAllowList

  Creates and defines the settings for an allow list.
- CreateClassificationJob

  Creates and defines the settings for a classification job.
- CreateCustomDataIdentifier

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

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

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

  Associates an account with an Amazon Macie administrator account.
- CreateSampleFindings

  Creates sample findings.
- DeclineInvitations

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

Deletes an allow list.

- DeleteCustomDataIdentifier

  Soft deletes a custom data identifier.

- DeleteFindingsFilter

  Deletes a findings filter.

- DeleteInvitations

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

- DeleteMember

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

- DescribeBuckets

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

- DescribeClassificationJob

  Retrieves the status and settings for a classification job.

- DescribeOrganizationConfiguration

  Retrieves the Amazon Macie configuration settings for an organization in AWS Organizations.

- DisableMacie

  Disables Amazon Macie and deletes all settings and resources for a Macie account.

- DisableOrganizationAdminAccount

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

- DisassociateFromAdministratorAccount

  Disassociates a member account from its Amazon Macie administrator account.

- DisassociateFromMasterAccount

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

- DisassociateMember

  Disassociates an Amazon Macie administrator account from a member account.

- EnableMacie

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

- EnableOrganizationAdminAccount

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

- GetAdministratorAccount

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

- GetAllowList

  Retrieves the settings and status of an allow list.

- GetAutomatedDiscoveryConfiguration

  Retrieves the configuration settings and status of automated sensitive data discovery for an organization or standalone account.

- GetBucketStatistics

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

- GetClassificationExportConfiguration

  Retrieves the configuration settings for storing data classification results.

- GetClassificationScope

  Retrieves the classification scope settings for an account.

- GetCustomDataIdentifier

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

- GetFindings

  Retrieves the details of one or more findings.

- GetFindingsFilter

Retrieves the criteria and other settings for a findings filter.

- GetFindingsPublicationConfiguration

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

- GetFindingStatistics

  Retrieves (queries) aggregated statistical data about findings.

- GetInvitationsCount

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

- GetMacieSession

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

- GetMasterAccount

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

- GetMember

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

- GetResourceProfile

  Retrieves (queries) sensitive data discovery statistics and the sensitivity score for an S3 bucket.

- GetRevealConfiguration

  Retrieves the status and configuration settings for retrieving occurrences of sensitive data reported by findings.

- GetSensitiveDataOccurrences

  Retrieves occurrences of sensitive data reported by a finding.

- GetSensitiveDataOccurrencesAvailability

  Checks whether occurrences of sensitive data can be retrieved for a finding.

- GetSensitivityInspectionTemplate

  Retrieves the settings for the sensitivity inspection template for an account.

- GetUsageStatistics

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

- GetUsageTotals

  Retrieves (queries) aggregated usage data for an account.

- ListAllowLists

  Retrieves a subset of information about all the allow lists for an account.

- ListAutomatedDiscoveryAccounts

  Retrieves the status of automated sensitive data discovery for one or more accounts.

- ListClassificationJobs

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

- ListClassificationScopes

  Retrieves a subset of information about the classification scope for an account.

- ListCustomDataIdentifiers

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

- ListFindings

  Retrieves a subset of information about one or more findings.

- ListFindingsFilters

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

- ListInvitations

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

- ListManagedDataIdentifiers

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

- ListMembers

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

- ListOrganizationAdminAccounts

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

- ListResourceProfileArtifacts

  Retrieves information about objects that Amazon Macie selected from an S3 bucket for automated sensitive data discovery.

- ListResourceProfileDetections

  Retrieves information about the types and amount of sensitive data that Amazon Macie found in an S3 bucket.

- ListSensitivityInspectionTemplates

  Retrieves a subset of information about the sensitivity inspection template for an account.

- ListTagsForResource

  Retrieves the tags (keys and values) that are associated with an Amazon Macie resource.

- PutClassificationExportConfiguration

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

- PutFindingsPublicationConfiguration

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

- SearchResources

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

- TagResource

  Adds or updates one or more tags (keys and values) that are associated with an Amazon Macie resource.

- TestCustomDataIdentifier

  Tests criteria for a custom data identifier.

- UntagResource

  Removes one or more tags (keys and values) from an Amazon Macie resource.

- UpdateAllowList

  Updates the settings for an allow list.

- UpdateAutomatedDiscoveryConfiguration

  Changes the configuration settings and status of automated sensitive data discovery for an organization or standalone account.

- UpdateClassificationJob

  Changes the status of a classification job.

- UpdateClassificationScope

  Updates the classification scope settings for an account.

- UpdateFindingsFilter

  Updates the criteria and other settings for a findings filter.

- UpdateMacieSession

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

- UpdateMemberSession

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

- UpdateOrganizationConfiguration

  Updates the Amazon Macie configuration settings for an organization in AWS Organizations.

- UpdateResourceProfile

  Updates the sensitivity score for an S3 bucket.

- UpdateResourceProfileDetections

  Updates the sensitivity scoring settings for an S3 bucket.

- UpdateRevealConfiguration

Updates the status and configuration settings for retrieving occurrences of sensitive data reported by findings.

- UpdateSensitivityInspectionTemplate

  Updates the settings for the sensitivity inspection template for an account.

Resources

The Amazon Macie REST API includes the following resources.

Topics

- Account Administration
- Administrator
- Administrator Disassociation
- Allow List
- Allow Lists
- AWS Organizations - Macie Administrator
- AWS Organizations - Macie Configuration
- Automated Sensitive Data Discovery - Accounts
- Automated Sensitive Data Discovery - Configuration
- Classification Job
- Classification Job Creation
- Classification Job List
- Classification Results - Export Configuration
- Classification Scope
- Classification Scopes
- Custom Data Identifier
- Custom Data Identifier Creation
- Custom Data Identifier Descriptions
- Custom Data Identifier List
- Custom Data Identifier Testing
- Data Sources - Amazon S3
- Data Sources - Amazon S3 Statistics
- Data Sources - Search
- Finding List

- Finding Samples
- Finding Statistics
- Findings
- Findings - Publication Configuration
- Findings - Reveal Sensitive Data Occurrences
- Findings - Reveal Sensitive Data Occurrences Availability
- Findings - Reveal Sensitive Data Occurrences Configuration
- Findings Filter
- Findings Filters
- Invitation Acceptance
- Invitation Count
- Invitation Decline
- Invitation Deletion
- Invitation List
- Managed Data Identifiers
- Master Account
- Master Disassociation
- Member
- Member Disassociation
- Member Status
- Members
- Resource Sensitivity Profile
- Resource Sensitivity Profile - Artifacts
- Resource Sensitivity Profile - Detections
- Sensitivity Inspection Template
- Sensitivity Inspection Templates
- Tags
- Usage Statistics
- Usage Totals

Account Administration

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

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

After you enable Macie, you can use this resource to review and update the status and certain configuration settings for your Macie account. This includes suspending (pausing) and later re-enabling Macie. If you suspend Macie, the service stops performing all activities for your account and it cancels all of your classification jobs. However, the service retains the session identifier, settings, data, and resources for your account. If your account is the Macie administrator account for an organization, you must remove all member accounts that are associated with your account before you suspend Macie for your account.

If you want to disable Macie completely, you can use this resource to do so. If you disable Macie, the service stops performing all activities for your account. In addition, Macie permanently deletes all settings, data, and 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 other AWS services for you. These might include sensitive data discovery results in Amazon Simple Storage Service (Amazon S3), finding events in Amazon EventBridge, and findings in AWS Security Hub.

If you want to disable Macie and your account is the Macie administrator account for an organization, you must first:

- Remove all member accounts that are associated with your administrator account.
- Delete the associations between your administrator account and its member accounts.

If you want to disable Macie and your account is a Macie member account in an organization, you must first disassociate your account from its Macie administrator account.

For more information, see Suspending Macie and Disabling Macie in the *Amazon Macie User Guide*.

URI

`/macie`

HTTP methods

DELETE

Operation ID: `DisableMacie`

Disables Amazon Macie and deletes all settings and resources for a Macie account.

Responses

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

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

GET

Operation ID: `GetMacieSession`

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

Responses

Status code	Response model	Description
200	GetMacieSessionResponse	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.

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

PATCH

Operation ID: `UpdateMacieSession`

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

Responses

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

Status code	Response model	Description
500	InternalServerException	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

PATCH schema

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

POST schema

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

Response bodies

Empty Schema schema

```
{
}
```

GetMacieSessionResponse schema

```
{
  "createdAt": "string",
  "findingPublishingFrequency": enum,
  "serviceRole": "string",
```

```
  "status": enum,
  "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"
}
```

InternalServerException 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 Amazon CloudWatch Events).

Type: FindingPublishingFrequency
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
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 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 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

findingPublishingFrequency

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

Type: FindingPublishingFrequency
Required: False

serviceRole

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

Type: string
Required: False

status

The current status of the Amazon 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
Required: False

updatedAt

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

Type: string
Required: False
Format: date-time

InternalServerException

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 Amazon CloudWatch Events).

Type: FindingPublishingFrequency
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
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:

DisableMacie

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

GetMacieSession

- AWS Command Line Interface
- AWS SDK for .NET

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

UpdateMacieSession

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

EnableMacie

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

Administrator

If your account is an Amazon Macie member account in an organization, the Administrator resource provides information about the Macie administrator account for your account. If you joined the organization by accepting a Macie membership invitation, this resource also provides information about that invitation. For information about the relationship between your account and its Macie administrator account, see Managing multiple accounts in the *Amazon Macie User Guide*.

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	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.

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

Schemas

Response bodies

GetAdministratorAccountResponse schema

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

```
}
```

InternalServerException 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 an Amazon Macie membership invitation, this object also provides details about the invitation that was sent to establish the relationship between the accounts.

Type: Invitation
Required: False

InternalServerException

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.

accountId

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

Type: string
Required: False

invitationId

The unique identifier for the invitation.

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 status of the relationship between the account that sent the invitation and the account that received the invitation.

Type: RelationshipStatus
Required: False

RelationshipStatus

The current status of the relationship between an account and an associated Amazon Macie administrator 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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Administrator Disassociation

The Administrator Disassociation resource provides access to the association between your Amazon Macie account and its Macie administrator account. If you joined an organization by accepting a Macie membership invitation, you can use this resource to disassociate your Macie account from its current Macie administrator account. For more information, see Managing your membership in an organization in the *Amazon Macie User Guide*.

If you're the Macie administrator for an organization and you want to disassociate (remove) a member account from your organization, use the Member Disassociation resource instead of this 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	The request succeeded and there isn't any content to include in the body of the response (No Content).
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
409	ConflictException	The request failed because it conflicts with the current state of the specified resource.

Status code	Response model	Description
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	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"
}
```

InternalServerException 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).

InternalServerException

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Allow List

The Allow List resource provides access to existing allow lists for your Amazon Macie account. In Macie, an allow list defines specific text or a text pattern that you want Macie to ignore when it inspects a data source for sensitive data. If data matches text or a text pattern in an allow list, Macie doesn't report the data. This is the case even if the data matches the criteria of a managed data identifier or a custom data identifier. You can create and use allow lists in all the AWS Regions where Macie is currently available except the Asia Pacific (Osaka) Region.

Macie supports two types of allow lists. An allow list can be a line-delimited plaintext file that lists specific text to ignore. For this type of list (`s3WordsList`), you create the list by using a text editor, store the list in an Amazon Simple Storage Service (Amazon S3) general purpose bucket, and then configure settings for Macie to access the list in the bucket. Alternatively, an allow list can specify a regular expression (*regex*) that defines a text pattern to ignore. For this type of list (`regex`), you create and store the regex and all other list settings in Macie. For more information, see Defining sensitive data exceptions with allow lists in the *Amazon Macie User Guide*.

You can use the Allow List resource to retrieve detailed information about an allow list, including the current status of the list. If a list is stored in an S3 bucket, the list's status indicates whether Macie can retrieve and parse the list. You can also use the Allow List resource to update the settings for an allow list or to delete an allow list from Macie.

To use this resource, you have to specify the unique identifier for the allow list that your request applies to. To find this identifier, use the Allow Lists resource.

URI

`/allow-lists/id`

HTTP methods

DELETE

Operation ID: `DeleteAllowList`

Deletes an allow list.

Path parameters

Name	Type	Required	Description
id	String	True	The unique identifier for the Amazon Macie resource that the request applies to.

Query parameters

Name	Type	Required	Description
ignoreJobChecks	String	False	Specifies whether to force deletion of the allow list, even if active classification jobs are configured to use the list. When you try to delete an allow list, Amazon Macie checks for classification jobs that use the list and have a status other than COMPLETE or

Name	Type	Required	Description
			`CANCELLED` . By default, Macie rejects your request if any jobs meet these criteria. To skip these checks and delete the list, set this value to `true`. To delete the list only if no active jobs are configured to use it, set this value to `false`.

Responses

Status code	Response model	Description
`200`	`Empty Schema`	The request succeeded. The allow list was deleted and there isn't any content to include in the body of the response (No Content).
`400`	`ValidationException`	The request failed because the input doesn't satisfy the constraints specified by the service.
`403`	`AccessDeniedException`	The request was denied because you don't have sufficient access to the specified resource.

Status code	Response model	Description
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	The request failed due to an unknown internal server error, exception, or failure.

GET

Operation ID: `GetAllowList`

Retrieves the settings and status of an allow list.

Path parameters

Name	Type	Required	Description
id	String	True	The unique identifier for the Amazon Macie resource that the request applies to.

Responses

Status code	Response model	Description
200	GetAllowListResponse	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the

Status code	Response model	Description
		constraints specified by the service.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	The request failed due to an unknown internal server error, exception, or failure.

PUT

Operation ID: `UpdateAllowList`

Updates the settings for an allow list.

Path parameters

Name	Type	Required	Description
id	String	True	The unique identifier for the Amazon Macie resource that the request applies to.

Responses

Status code	Response model	Description
200	UpdateAllowListResponse	The request succeeded. The settings for the allow list were updated.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

PUT schema

```
{
  "criteria": {
```

```
    "regex": "string",
    "s3WordsList": {
      "bucketName": "string",
      "objectKey": "string"
    }
  },
  "description": "string",
  "name": "string"
}
```

Response bodies

Empty Schema schema

```
{
}
```

GetAllowListResponse schema

```
{
  "arn": "string",
  "createdAt": "string",
  "criteria": {
    "regex": "string",
    "s3WordsList": {
      "bucketName": "string",
      "objectKey": "string"
    }
  },
  "description": "string",
  "id": "string",
  "name": "string",
  "status": {
    "code": enum,
    "description": "string"
  },
  "tags": {
  },
  "updatedAt": "string"
}
```

UpdateAllowListResponse schema

```
{
  "arn": "string",
  "id": "string"
}
```

ValidationException schema

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

AccessDeniedException schema

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

ResourceNotFoundException schema

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

ThrottlingException schema

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

InternalServerException 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

AllowListCriteria

Specifies the criteria for an allow list. The criteria must specify a regular expression (`regex`) or an S3 object (`s3WordsList`). It can't specify both.

regex

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

Type: string
Required: False
Pattern: `^[\s\S]+$`
MinLength: 1
MaxLength: 512

s3WordsList

The location and name of the S3 object that lists specific text to ignore.

Type: S3WordsList
Required: False

AllowListStatus

Provides information about the current status of an allow list, which indicates whether Amazon Macie can access and use the list's criteria.

code

The current status of the allow list. If the list's criteria specify a regular expression (`regex`), this value is typically `OK`. Amazon Macie can compile the expression.

If the list's criteria specify an S3 object, possible values are:

- `OK` - Macie can retrieve and parse the contents of the object.
- `S3_OBJECT_ACCESS_DENIED` - Macie isn't allowed to access the object or the object is encrypted with a customer managed AWS KMS key that Macie isn't allowed to use. Check the bucket policy and other permissions settings for the bucket and the object. If the object is encrypted, also ensure that it's encrypted with a key that Macie is allowed to use.
- `S3_OBJECT_EMPTY` - Macie can retrieve the object but the object doesn't contain any content. Ensure that the object contains the correct entries. Also ensure that the list's criteria specify the correct bucket and object names.
- `S3_OBJECT_NOT_FOUND` - The object doesn't exist in Amazon S3. Ensure that the list's criteria specify the correct bucket and object names.
- `S3_OBJECT_OVERSIZE` - Macie can retrieve the object. However, the object contains too many entries or its storage size exceeds the quota for an allow list. Try breaking the list into multiple files and ensure that each file doesn't exceed any quotas. Then configure list settings in Macie for each file.
- `S3_THROTTLED` - Amazon S3 throttled the request to retrieve the object. Wait a few minutes and then try again.
- `S3_USER_ACCESS_DENIED` - Amazon S3 denied the request to retrieve the object. If the specified object exists, you're not allowed to access it or it's encrypted with an AWS KMS key that you're not allowed to use. Work with your AWS administrator to ensure that the list's criteria specify the correct bucket and object names, and you have read access to the bucket and the object. If the object is encrypted, also ensure that it's encrypted with a key that you're allowed to use.
- `UNKNOWN_ERROR` - A transient or internal error occurred when Macie attempted to retrieve or parse the object. Wait a few minutes and then try again. A list can also have this status if it's encrypted with a key that Amazon S3 and Macie can't access or use.

Type: AllowListStatusCode

Required: True

description

A brief description of the status of the allow list. Amazon Macie uses this value to provide additional information about an error that occurred when Macie tried to access and use the list's criteria.

Type: string
Required: False
Pattern: ^[\s\S]+$
MinLength: 1
MaxLength: 1024

AllowListStatusCode

Indicates the current status of an allow list. Depending on the type of criteria that the list specifies, possible values are:

OK
S3_OBJECT_NOT_FOUND
S3_USER_ACCESS_DENIED
S3_OBJECT_ACCESS_DENIED
S3_THROTTLED
S3_OBJECT_OVERSIZE
S3_OBJECT_EMPTY
UNKNOWN_ERROR

Empty

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

GetAllowListResponse

Provides information about the settings and status of an allow list.

arn

The Amazon Resource Name (ARN) of the allow list.

Type: string
Required: True
Pattern: `^arn:(aws|aws-cn|aws-us-gov):macie2:[a-z1-9-]{9,20}:\d{12}:allow-list\/[a-z0-9]{22}$`
MinLength: 71
MaxLength: 89

createdAt

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

Type: string
Required: True
Format: date-time

criteria

The criteria that specify the text or text pattern to ignore. The criteria can be the location and name of an S3 object that lists specific text to ignore (`s3WordsList`), or a regular expression (`regex`) that defines a text pattern to ignore.

Type: AllowListCriteria
Required: False

description

The custom description of the allow list.

Type: string
Required: False
Pattern: `^[\s\S]+$`
MinLength: 1
MaxLength: 512

id

The unique identifier for the allow list.

Type: string
Required: True
Pattern: ^[a-z0-9]{22}$
MinLength: 22
MaxLength: 22

name

The custom name of the allow list.

Type: string
Required: True
Pattern: ^.+$
MinLength: 1
MaxLength: 128

status

The current status of the allow list, which indicates whether Amazon Macie can access and use the list's criteria.

Type: AllowListStatus
Required: False

tags

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

Type: TagMap
Required: False

updatedAt

The date and time, in UTC and extended ISO 8601 format, when the allow list's settings were most recently changed in Amazon Macie.

Type: string

Required: True
Format: date-time

InternalServerException

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

S3WordsList

Provides information about an S3 object that lists specific text to ignore.

bucketName

The full name of the S3 bucket that contains the object.

Type: string
Required: True
Pattern: `^[A-Za-z0-9.\-_]{3,255}$`
MinLength: 3

MaxLength: 255

objectKey

The full name (key) of the object.

Type: string
Required: True
Pattern: ^[\s\S]+$
MinLength: 1
MaxLength: 1024

TagMap

A string-to-string map of key-value pairs that specifies the tags (keys and values) for an Amazon Macie resource.

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

UpdateAllowListRequest

Changes the settings for an allow list. If you change the list's criteria, Amazon Macie tests the new criteria when it processes your request. If the criteria specify a regular expression that Macie can't compile or an S3 object that Macie can't retrieve or parse, an error occurs.

criteria

The criteria that specify the text or text pattern to ignore. The criteria can be the location and name of an S3 object that lists specific text to ignore (`s3WordsList`), or a regular expression that defines a text pattern to ignore (`regex`).

You can change a list's underlying criteria, such as the name of the S3 object or the regular expression to use. However, you can't change the type from `s3WordsList` to `regex` or the other way around.

Type: AllowListCriteria
Required: True

description

A custom description of the allow list. The description can contain as many as 512 characters.

Type: string
Required: False
Pattern: `^[\s\S]+$`
MinLength: 1
MaxLength: 512

name

A custom name for the allow list. The name can contain as many as 128 characters.

Type: string
Required: True
Pattern: `^.+$`
MinLength: 1
MaxLength: 128

UpdateAllowListResponse

Provides information about an allow list whose settings were changed in response to a request.

arn

The Amazon Resource Name (ARN) of the allow list.

Type: string
Required: True
Pattern: `^arn:(aws|aws-cn|aws-us-gov):macie2:[a-z1-9-]{9,20}:\d{12}:allow-list\/[a-z0-9]{22}$`
MinLength: 71
MaxLength: 89

id

The unique identifier for the allow list.

Type: string
Required: True
Pattern: `^[a-z0-9]{22}$`
MinLength: 22
MaxLength: 22

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:

DeleteAllowList

- AWS Command Line Interface
- AWS SDK for .NET

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

GetAllowList

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

UpdateAllowList

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

Allow Lists

In Amazon Macie, an allow list defines specific text or a text pattern that you want Macie to ignore when it inspects a data source for sensitive data. If data matches text or a text pattern in an allow list, Macie doesn't report the data. This is the case even if the data matches the criteria of a managed data identifier or a custom data identifier. You can create and use allow lists in all the AWS Regions where Macie is currently available except the Asia Pacific (Osaka) Region.

Macie supports two types of allow lists:

- **Predefined text** - For this type of list (`s3WordsList`), you create a line-delimited plaintext file that lists specific text to ignore. You store the file in an Amazon Simple Storage Service (Amazon S3) general purpose bucket and then configure settings for Macie to access the list in the bucket.

  This type of list typically contains specific words, phrases, and other kinds of character sequences that aren't sensitive, aren't likely to change, and don't necessarily adhere to a common pattern. If you use this type of list, Macie doesn't report occurrences of text that exactly match a complete entry in the list. Macie treats each entry in the list as a string literal value. Matches aren't case sensitive.
- **Regular expression** - For this type of list (`regex`), you specify a regular expression that defines a text pattern to ignore. Unlike an allow list with predefined text, you create and store the regex and all other list settings in Macie.

  This type of list is helpful if you want to specify text that isn't sensitive but varies or is likely to change while also adhering to a common pattern. If you use this type of list, Macie doesn't report occurrences of text that completely match the pattern defined by the list.

For more information, see Defining sensitive data exceptions with allow lists in the *Amazon Macie User Guide*.

You can use the Allow Lists resource to create an allow list or to retrieve a subset of information about all the existing allow lists for your account. To retrieve detailed information about the settings and status of an individual allow list, use the Allow List resource.

URI

```
/allow-lists
```

HTTP methods

GET

Operation ID: `ListAllowLists`

Retrieves a subset of information about all the allow lists for 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`	`ListAllowListsResponse`	The request succeeded.
`400`	`ValidationException`	The request failed because the input doesn't satisfy the constraints specified by the service.
`403`	`AccessDeniedException`	The request was denied because you don't have

Status code	Response model	Description
		sufficient access to the specified resource.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	The request failed due to an unknown internal server error, exception, or failure.

POST

Operation ID: `CreateAllowList`

Creates and defines the settings for an allow list.

Responses

Status code	Response model	Description
200	CreateAllowListResponse	The request succeeded. The specified allow list was created.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have

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

Schemas

Request bodies

POST schema

```
{
  "clientToken": "string",
  "criteria": {
    "regex": "string",
    "s3WordsList": {
      "bucketName": "string",
      "objectKey": "string"
    }
  },
  "description": "string",
  "name": "string",
```

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

Response bodies

ListAllowListsResponse schema

```
{
  "allowLists": [
    {
      "arn": "string",
      "createdAt": "string",
      "description": "string",
      "id": "string",
      "name": "string",
      "updatedAt": "string"
    }
  ],
  "nextToken": "string"
}
```

CreateAllowListResponse schema

```
{
  "arn": "string",
  "id": "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"
}
```

InternalServerException 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

AllowListCriteria

Specifies the criteria for an allow list. The criteria must specify a regular expression (`regex`) or an S3 object (`s3WordsList`). It can't specify both.

regex

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

Type: string
Required: False
Pattern: `^[\s\S]+$`
MinLength: 1
MaxLength: 512

s3WordsList

The location and name of the S3 object that lists specific text to ignore.

Type: S3WordsList
Required: False

AllowListSummary

Provides a subset of information about an allow list.

arn

The Amazon Resource Name (ARN) of the allow list.

Type: string

Required: False
Pattern: `^arn:(aws|aws-cn|aws-us-gov):macie2:[a-z1-9-]{9,20}:\d{12}:allow-list\/[a-z0-9]{22}$`
MinLength: 71
MaxLength: 89

createdAt

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

Type: string
Required: False
Format: date-time

description

The custom description of the allow list.

Type: string
Required: False
Pattern: `^[\s\S]+$`
MinLength: 1
MaxLength: 512

id

The unique identifier for the allow list.

Type: string
Required: False
Pattern: `^[a-z0-9]{22}$`
MinLength: 22
MaxLength: 22

name

The custom name of the allow list.

Type: string
Required: False
Pattern: ^.+$
MinLength: 1
MaxLength: 128

updatedAt

The date and time, in UTC and extended ISO 8601 format, when the allow list's settings were most recently changed in Amazon Macie.

Type: string
Required: False
Format: date-time

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

CreateAllowListRequest

Specifies the settings for an allow list. When Amazon Macie processes the request, Macie tests the list's criteria. If the criteria specify a regular expression that Macie can't compile or an S3 object that Macie can't retrieve or parse, an error occurs.

clientToken

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

Type: string
Required: True

criteria

The criteria that specify the text or text pattern to ignore. The criteria can be the location and name of an S3 object that lists specific text to ignore (`s3WordsList`), or a regular expression (`regex`) that defines a text pattern to ignore.

Type: AllowListCriteria
Required: True

description

A custom description of the allow list. The description can contain as many as 512 characters.

Type: string
Required: False
Pattern: `^[\s\S]+$`
MinLength: 1
MaxLength: 512

name

A custom name for the allow list. The name can contain as many as 128 characters.

Type: string
Required: True
Pattern: `^.+$`
MinLength: 1
MaxLength: 128

tags

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

An allow list 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
Required: False

CreateAllowListResponse

Provides information about an allow list that was created in response to a request.

arn

The Amazon Resource Name (ARN) of the allow list.

Type: string
Required: True
Pattern: `^arn:(aws|aws-cn|aws-us-gov):macie2:[a-z1-9-]{9,20}:\d{12}:allow-list\/[a-z0-9]{22}$`
MinLength: 71
MaxLength: 89

id

The unique identifier for the allow list.

Type: string
Required: True
Pattern: `^[a-z0-9]{22}$`
MinLength: 22
MaxLength: 22

InternalServerException

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

ListAllowListsResponse

Provides the results of a request for information about allow lists.

allowLists

An array of objects, one for each allow list.

Type: Array of type AllowListSummary
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

S3WordsList

Provides information about an S3 object that lists specific text to ignore.

bucketName

The full name of the S3 bucket that contains the object.

Type: string
Required: True
Pattern: `^[A-Za-z0-9.\-_]{3,255}$`
MinLength: 3
MaxLength: 255

objectKey

The full name (key) of the object.

Type: string
Required: True
Pattern: ^[\s\S]+$
MinLength: 1
MaxLength: 1024

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 an Amazon Macie resource.

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:

ListAllowLists

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

CreateAllowList

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

AWS Organizations - Macie Administrator

The Macie Administrator resource for AWS Organizations provides settings for designating the delegated Amazon Macie administrator account for an organization in AWS Organizations. AWS Organizations is a global account management service that enables AWS administrators to consolidate and centrally manage multiple AWS accounts. For more information about this service, see the AWS Organizations User Guide. For information about integrating Macie with AWS Organizations, see Managing multiple accounts with AWS Organizations in the *Amazon Macie User Guide*.

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

To use this resource, you must be a user of the AWS Organizations management account for your organization.

URI

`/admin`

HTTP methods

DELETE

Operation ID: `DisableOrganizationAdminAccount`

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

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	The request succeeded and there isn't any content to include in the body of the response (No Content).
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.

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

GET

Operation ID: `ListOrganizationAdminAccounts`

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

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	ListOrganizationAdminAccountsResponse	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
409	ConflictException	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	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 organization in AWS Organizations.

Responses

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

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

Schemas

Request bodies

POST schema

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

Response bodies

Empty Schema schema

```
{
}
```

ListOrganizationAdminAccountsResponse schema

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

```
  "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"
}
```

InternalServerException 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 organization in AWS Organizations.

accountId

The AWS account ID for the account.

Type: string
Required: False

status

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

Type: AdminStatus

Required: False

AdminStatus

The current status of an account as the delegated Amazon Macie administrator account for an organization in AWS Organizations. 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 the delegated Amazon Macie administrator account for an organization in AWS Organizations. To submit this request, you must be a user of the AWS Organizations management account.

adminAccountId

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

Type: string

Required: True

clientToken

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

Type: string
Required: False

InternalServerException

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 organization in AWS Organizations.

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
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

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:

DisableOrganizationAdminAccount

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

ListOrganizationAdminAccounts

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

- AWS SDK for Ruby V3

EnableOrganizationAdminAccount

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

AWS Organizations - Macie Configuration

The Macie Configuration resource for AWS Organizations provides access to certain Amazon Macie configuration settings for an organization in AWS Organizations. AWS Organizations is a global account management service that enables AWS administrators to consolidate and centrally manage multiple AWS accounts. For more information about this service, see the AWS Organizations User Guide. For information about integrating Macie with AWS Organizations, see Managing multiple accounts with AWS Organizations in the *Amazon Macie User Guide*.

If you're the delegated Macie administrator for an organization in AWS Organizations, you can use this resource to retrieve or change the setting that determines whether Macie is enabled automatically for accounts that are added to your organization in AWS Organizations. To retrieve or change the setting that determines whether automated sensitive data discovery is also enabled automatically for new accounts, use the Configuration resource for automated sensitive data discovery.

To use this resource, you must be the delegated Macie administrator for an organization in AWS Organizations.

URI

`/admin/configuration`

HTTP methods

GET

Operation ID: `DescribeOrganizationConfiguration`

Retrieves the Amazon Macie configuration settings for an organization in AWS Organizations.

Responses

Status code	Response model	Description
200	DescribeOrganizationConfigurationResponse	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
409	ConflictException	The request failed because it conflicts with the current state of the specified resource.

Status code	Response model	Description
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	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 organization in AWS Organizations.

Responses

Status code	Response model	Description
200	Empty Schema	The request succeeded and there isn't any content to include in the body of the response (No Content).
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have

Status code	Response model	Description
		sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
409	ConflictException	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	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"
}
```

InternalServerException 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 for an organization in AWS Organizations.

autoEnable

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

Type: boolean
Required: False

maxAccountLimitReached

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

InternalServerException

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 organization in AWS Organizations, when the accounts are added to the organization.

autoEnable

Specifies whether to enable Amazon Macie automatically for accounts that are added to the organization in AWS Organizations.

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateOrganizationConfiguration

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

Automated Sensitive Data Discovery - Accounts

The Accounts resource for automated sensitive data discovery provides access to the status of automated sensitive data discovery for accounts that are centrally managed as an organization in Amazon Macie. If you're the Macie administrator for an organization, you can use this resource to check or change the status of automated sensitive data discovery for individual accounts in your organization. If you have a member account, you can use this resource to check the status of automated sensitive data discovery for your account. Contact your Macie administrator if you want to change the status.

If you're a Macie administrator, start by enabling automated sensitive data discovery for your organization. To enable it for your organization, use the Configuration resource for automated sensitive data discovery. By using that resource, you can also enable it automatically for all existing accounts and new member accounts, only new member accounts, or no accounts. After you enable it for your organization, you can manage the status of automated sensitive data discovery for individual accounts in your organization.

If automated sensitive data discovery is enabled for an account in an organization, Macie analyzes the account's Amazon Simple Storage Service (Amazon S3) data by using the configuration settings specified by the Macie administrator account for the organization:

- **Classification scope** - This specifies S3 buckets to exclude from the analyses. To exclude particular buckets that an account owns, add the buckets to the classification scope for the administrator account.

- **Sensitivity inspection template** - This specifies which allow lists, custom data identifiers, and managed data identifiers to use when analyzing data. To customize the analyses, update the sensitivity inspection template for the administrator account.

As the analyses progress, Macie produces records of the sensitive data that it finds and the analysis that it performs: *sensitive data findings*, which report sensitive data that Macie finds in individual S3 objects, and *sensitive data discovery results*, which log details about the analysis of individual S3 objects. Macie also updates statistics, inventory data, and other information that it provides about Amazon S3 data. For more information, see Performing automated sensitive data discovery in the *Amazon Macie User Guide*.

As a Macie administrator, you can disable automated sensitive data discovery for an account at any time. If you disable it, Macie stops analyzing the account's Amazon S3 data. Instead of disabling it for an account completely, consider excluding only particular S3 buckets that the account owns. If you exclude a bucket, existing sensitive data discovery statistics and details for the bucket persist. For example, the bucket's current sensitivity score remains unchanged. However, Macie skips the bucket when it subsequently performs automated sensitive data discovery for the account. If you exclude a bucket, you can include it again later. To exclude or include a bucket, update the classification scope for your administrator account.

If you're the Macie administrator for an organization, you can use the Accounts resource to check or change the status of automated sensitive data discovery for individual accounts in your organization. If you have a member account, you can use this resource to check the status of automated sensitive data discovery for your account.

URI

`/automated-discovery/accounts`

HTTP methods

GET

Operation ID: `ListAutomatedDiscoveryAccounts`

Retrieves the status of automated sensitive data discovery for one or more accounts.

Query parameters

Name	Type	Required	Description
nextToken	String	False	The nextToken string that specifies which page of results to return in a paginated response.
accountIds	String	False	The AWS account ID for each account, for as many as 50 accounts. To retrieve the status for multiple accounts, append the accountIds parameter and argument for each account, separated by an ampersand (&). To retrieve the status for all the accounts in an organization, omit this parameter.
maxResults	String	False	The maximum number of items to include in each page of a paginated response.

Responses

Status code	Response model	Description
200	ListAutomatedDiscoveryAccountsResponse	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	The request failed due to an unknown internal server error, exception, or failure.

PATCH

Operation ID: `BatchUpdateAutomatedDiscoveryAccounts`

Changes the status of automated sensitive data discovery for one or more accounts.

Responses

Status code	Response model	Description
200	BatchUpdateAutomatedDiscoveryAccountsResponse	The request succeeded. However, the update might have failed for one or more accounts.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
409	ConflictException	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

PATCH schema

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

Response bodies

ListAutomatedDiscoveryAccountsResponse schema

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

BatchUpdateAutomatedDiscoveryAccountsResponse schema

```
{
  "errors": [
    {
      "accountId": "string",
      "errorCode": enum
    }
  ]
}
```

ValidationException schema

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

AccessDeniedException schema

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

ResourceNotFoundException schema

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

ConflictException schema

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

ThrottlingException schema

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

InternalServerException 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

AutomatedDiscoveryAccount

Provides information about the status of automated sensitive data discovery for an Amazon Macie account.

accountId

The AWS account ID for the account.

Type: string
Required: False

status

The current status of automated sensitive data discovery for the account. Possible values are: `ENABLED`, perform automated sensitive data discovery activities for the account; and, `DISABLED`, don't perform automated sensitive data discovery activities for the account.

Type: AutomatedDiscoveryAccountStatus
Required: False

AutomatedDiscoveryAccountStatus

The status of automated sensitive data discovery for an Amazon Macie account. Valid values are:

```
ENABLED
DISABLED
```

AutomatedDiscoveryAccountUpdate

Changes the status of automated sensitive data discovery for an Amazon Macie account.

accountId

The AWS account ID for the account.

Type: string

Required: False

status

The new status of automated sensitive data discovery for the account. Valid values are: `ENABLED`, perform automated sensitive data discovery activities for the account; and, `DISABLED`, don't perform automated sensitive data discovery activities for the account.

Type: AutomatedDiscoveryAccountStatus
Required: False

AutomatedDiscoveryAccountUpdateError

Provides information about a request that failed to change the status of automated sensitive data discovery for an Amazon Macie account.

accountId

The AWS account ID for the account that the request applied to.

Type: string
Required: False

errorCode

The error code for the error that caused the request to fail for the account (`accountId`). Possible values are: `ACCOUNT_NOT_FOUND`, the account doesn't exist or you're not the Amazon Macie administrator for the account; and, `ACCOUNT_PAUSED`, Macie isn't enabled for the account in the current AWS Region.

Type: AutomatedDiscoveryAccountUpdateErrorCode
Required: False

AutomatedDiscoveryAccountUpdateErrorCode

The error code that indicates why a request failed to change the status of automated sensitive data discovery for an Amazon Macie account. Possible values are:

`ACCOUNT_PAUSED`

ACCOUNT_NOT_FOUND

BatchUpdateAutomatedDiscoveryAccountsRequest

Changes the status of automated sensitive data discovery for one or more Amazon Macie accounts.

accounts

An array of objects, one for each account to change the status of automated sensitive data discovery for. Each object specifies the AWS account ID for an account and a new status for that account.

Type: Array of type AutomatedDiscoveryAccountUpdate
Required: False

BatchUpdateAutomatedDiscoveryAccountsResponse

Provides the results of a request to change the status of automated sensitive data discovery for one or more Amazon Macie accounts.

errors

An array of objects, one for each account whose status wasn't changed. Each object identifies the account and explains why the status of automated sensitive data discovery wasn't changed for the account. This value is null if the request succeeded for all specified accounts.

Type: Array of type AutomatedDiscoveryAccountUpdateError
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

InternalServerException

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

ListAutomatedDiscoveryAccountsResponse

Provides information about the status of automated sensitive data discovery for one or more Amazon Macie accounts.

items

An array of objects, one for each account specified in the request. Each object specifies the AWS account ID for an account and the current status of automated sensitive data discovery for that account.

Type: Array of type AutomatedDiscoveryAccount
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

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:

ListAutomatedDiscoveryAccounts

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2

- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

BatchUpdateAutomatedDiscoveryAccounts

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

Automated Sensitive Data Discovery - Configuration

The Configuration resource for automated sensitive data discovery provides access to configuration settings for performing automated sensitive data discovery, and the status of the configuration. To manage the configuration settings and status of automated sensitive data discovery, your account must be the Amazon Macie administrator account for an organization or a standalone Macie account.

If you enable automated sensitive data discovery, Macie continually evaluates your inventory of Amazon Simple Storage Service (Amazon S3) general purpose buckets and uses sampling techniques to identify and select representative objects in the buckets. Macie then retrieves and analyzes the selected objects, inspecting them for sensitive data. If you're the Macie administrator for an organization, this can include objects in buckets that your member accounts own.

You can monitor and review analyses' results in resource sensitivity profiles, statistical data, and other information that Macie produces and provides about your Amazon S3 data. These results are in addition to *sensitive data findings*, which report sensitive data that Macie finds in individual S3

objects, and *sensitive data discovery results*, which log details about the analysis of individual S3 objects. For more information, see Performing automated sensitive data discovery in the *Amazon Macie User Guide*.

To customize the analyses, change the configuration settings for your account. The settings include a *classification scope* and a *sensitivity inspection template*. The *classification scope* specifies S3 buckets that you want to exclude from analyses, such as buckets that typically store AWS logging data. The *sensitivity inspection template* specifies the allow lists, custom data identifiers, and managed data identifiers that you want Macie to use when it analyzes S3 objects. To change these settings, use the Classification Scope and Sensitivity Inspection Template resources.

If you're the Macie administrator for an organization, Macie uses the classification scope and sensitivity inspection template for your account when it analyzes data for other accounts in your organization. To refine the scope of the analyses, you have several options:

- **Automatically include or exclude accounts** - When you enable automated sensitive data discovery, you also specify whether to enable it automatically for all existing accounts and new member accounts, only new member accounts, or no accounts. If it's enabled for an account, Macie includes S3 buckets that the account owns. If it's disabled for an account, Macie excludes buckets that the account owns.
- **Include or exclude specific accounts** - After you enable automated sensitive data discovery, you can enable or disable it for individual accounts on a case-by-case basis. To do this, use the Accounts resource for automated sensitive data discovery. If you enable it for an account, Macie includes S3 buckets that the account owns. If you disable it for an account, Macie excludes buckets that the account owns.
- **Exclude specific S3 buckets** - If you enable automated sensitive data discovery for one or more accounts, you can exclude particular buckets that the accounts own. Macie then skips those buckets when it analyzes data for your organization. To exclude particular buckets, update the classification scope for your administrator account. You can do this by using the Classification Scope resource.

If you disable automated sensitive data discovery for your organization or standalone account, Macie retains your configuration settings. However, Macie stops performing all automated sensitive data discovery activities for your organization or account. In addition, you lose access to all resource sensitivity profiles, statistical data, and other information that Macie produced and directly provided about your Amazon S3 data while performing those activities. This doesn't include sensitive data findings. Macie stores findings for 90 days.

After you disable automated sensitive data discovery for your organization or standalone account, you can enable it again. Macie then resumes all automated sensitive data discovery activities for your organization or account. If you re-enable it within 30 days, you regain access to resource sensitivity profiles, statistical data, and other information that Macie previously produced and directly provided while performing those activities. If you don't re-enable it within 30 days, Macie permanently deletes these profiles and the statistical data and other information that it produced and directly provided.

If you're the Macie administrator for an organization or you have a standalone Macie account, you can use the Configuration resource to retrieve your current configuration settings for automated sensitive data discovery. You can also enable or disable automated sensitive data discovery for your organization or account.

URI

`/automated-discovery/configuration`

HTTP methods

GET

Operation ID: `GetAutomatedDiscoveryConfiguration`

Retrieves the configuration settings and status of automated sensitive data discovery for an organization or standalone account.

Responses

Status code	Response model	Description
200	GetAutomatedDiscoveryConfigurationResponse	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
403	AccessDeniedException	The request was denied because you don't have

Status code	Response model	Description
		sufficient access to the specified resource.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	The request failed due to an unknown internal server error, exception, or failure.

PUT

Operation ID: `UpdateAutomatedDiscoveryConfiguration`

Changes the configuration settings and status of automated sensitive data discovery for an organization or standalone account.

Responses

Status code	Response model	Description
200	Empty Schema	The request succeeded. The status was updated and there isn't any content to include in the body of the response (No Content).
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
403	AccessDeniedException	The request was denied because you don't have

Status code	Response model	Description
		sufficient access to the specified resource.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

PUT schema

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

Response bodies

GetAutomatedDiscoveryConfigurationResponse schema

```
{
  "autoEnableOrganizationMembers": enum,
  "classificationScopeId": "string",
  "disabledAt": "string",
  "firstEnabledAt": "string",
  "lastUpdatedAt": "string",
  "sensitivityInspectionTemplateId": "string",
  "status": enum
}
```

Empty Schema schema

```
{
}
```

ValidationException schema

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

AccessDeniedException schema

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

ThrottlingException schema

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

InternalServerException 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

AutoEnableMode

Specifies whether to automatically enable automated sensitive data discovery for accounts that are part of an organization in Amazon Macie. Valid values are:

```
ALL
NEW
NONE
```

AutomatedDiscoveryStatus

The status of the automated sensitive data discovery configuration for an organization in Amazon Macie or a standalone Macie account. Valid values are:

```
ENABLED
DISABLED
```

Empty

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

GetAutomatedDiscoveryConfigurationResponse

Provides information about the configuration settings and status of automated sensitive data discovery for an organization in Amazon Macie or a standalone Macie account.

autoEnableOrganizationMembers

Specifies whether automated sensitive data discovery is enabled automatically for accounts in the organization. Possible values are: `ALL`, enable it for all existing accounts and new member accounts; `NEW`, enable it only for new member accounts; and, `NONE`, don't enable it for any accounts.

Type: AutoEnableMode
Required: False

classificationScopeId

The unique identifier for the classification scope that's used when performing automated sensitive data discovery. The classification scope specifies S3 buckets to exclude from analyses.

Type: string
Required: False

disabledAt

The date and time, in UTC and extended ISO 8601 format, when automated sensitive data discovery was most recently disabled. This value is null if automated sensitive data discovery is currently enabled.

Type: string
Required: False

firstEnabledAt

The date and time, in UTC and extended ISO 8601 format, when automated sensitive data discovery was initially enabled. This value is null if automated sensitive data discovery has never been enabled.

Type: string
Required: False

lastUpdatedAt

The date and time, in UTC and extended ISO 8601 format, when the configuration settings or status of automated sensitive data discovery was most recently changed.

Type: string
Required: False

sensitivityInspectionTemplateId

The unique identifier for the sensitivity inspection template that's used when performing automated sensitive data discovery. The template specifies which allow lists, custom data identifiers, and managed data identifiers to use when analyzing data.

Type: string
Required: False

status

The current status of automated sensitive data discovery for the organization or account. Possible values are: `ENABLED`, use the specified settings to perform automated sensitive data discovery activities; and, `DISABLED`, don't perform automated sensitive data discovery activities.

Type: AutomatedDiscoveryStatus
Required: False

InternalServerException

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

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

UpdateAutomatedDiscoveryConfigurationRequest

Changes the configuration settings and status of automated sensitive data discovery for an organization in Amazon Macie or a standalone Macie account. To change additional settings, such as the managed data identifiers to use when analyzing data, update the sensitivity inspection template and classification scope for the organization's Macie administrator account or the standalone account.

autoEnableOrganizationMembers

Specifies whether to automatically enable automated sensitive data discovery for accounts in the organization. Valid values are: `ALL` (default), enable it for all existing accounts and new member accounts; `NEW`, enable it only for new member accounts; and, `NONE`, don't enable it for any accounts.

If you specify `NEW` or `NONE`, automated sensitive data discovery continues to be enabled for any existing accounts that it's currently enabled for. To enable or disable it for individual member accounts, specify `NEW` or `NONE`, and then enable or disable it for each account by using the `BatchUpdateAutomatedDiscoveryAccounts` operation.

Type: AutoEnableMode
Required: False

status

The new status of automated sensitive data discovery for the organization or account. Valid values are: `ENABLED`, start or resume all automated sensitive data discovery activities; and, `DISABLED`, stop performing all automated sensitive data discovery activities.

If you specify `DISABLED` for an administrator account, you also disable automated sensitive data discovery for all member accounts in the organization.

Type: AutomatedDiscoveryStatus
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:

GetAutomatedDiscoveryConfiguration

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

UpdateAutomatedDiscoveryConfiguration

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

- AWS SDK for Ruby V3

Classification Job

The Classification Job resource provides detailed information about individual classification jobs for your Amazon Macie account. It also provides access to the status of each job. A *classification job*, also referred to as a *sensitive data discovery job*, is a job that you create to analyze objects in Amazon Simple Storage Service (Amazon S3) general purpose buckets, and determine whether the objects contain sensitive data. For more information, see Running sensitive data discovery jobs in the *Amazon Macie User Guide*.

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 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
jobId	String	True	The unique identifier for the classification job.

Responses

Status code	Response model	Description
200	DescribeClassificationJobResponse	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
409	ConflictException	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	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
jobId	String	True	The unique identifier for the classification job.

Responses

Status code	Response model	Description
200	Empty Schema	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	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.

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

Schemas

Request bodies

PATCH schema

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

Response bodies

DescribeClassificationJobResponse schema

```
{
  "allowListIds": [
    "string"
  ],
  "clientToken": "string",
```

```
  "createdAt": "string",
  "customDataIdentifierIds": [
    "string"
  ],
  "description": "string",
  "initialRun": boolean,
  "jobArn": "string",
  "jobId": "string",
  "jobStatus": enum,
  "jobType": enum,
  "lastRunErrorStatus": {
    "code": enum
  },
  "lastRunTime": "string",
  "managedDataIdentifierIds": [
    "string"
  ],
  "managedDataIdentifierSelector": enum,
  "name": "string",
  "s3JobDefinition": {
    "bucketCriteria": {
      "excludes": {
        "and": [
          {
            "simpleCriterion": {
              "comparator": enum,
              "key": enum,
              "values": [
                "string"
              ]
            },
            "tagCriterion": {
              "comparator": enum,
              "tagValues": [
                {
                  "key": "string",
                  "value": "string"
                }
              ]
            }
          }
        ]
      },
      "includes": {
```

```
        "and": [
          {
            "simpleCriterion": {
              "comparator": enum,
              "key": enum,
              "values": [
                "string"
              ]
            },
            "tagCriterion": {
              "comparator": enum,
              "tagValues": [
                {
                  "key": "string",
                  "value": "string"
                }
              ]
            }
          }
        ]
      }
    },
    "bucketDefinitions": [
      {
        "accountId": "string",
        "buckets": [
          "string"
        ]
      }
    ],
    "scoping": {
      "excludes": {
        "and": [
          {
            "simpleScopeTerm": {
              "comparator": enum,
              "key": enum,
              "values": [
                "string"
              ]
            },
            "tagScopeTerm": {
              "comparator": enum,
              "key": "string",
```

```
            "tagValues": [
              {
                "key": "string",
                "value": "string"
              }
            ],
            "target": enum
          }
        }
      ]
    },
    "includes": {
      "and": [
        {
          "simpleScopeTerm": {
            "comparator": enum,
            "key": enum,
            "values": [
              "string"
            ]
          },
          "tagScopeTerm": {
            "comparator": enum,
            "key": "string",
            "tagValues": [
              {
                "key": "string",
                "value": "string"
              }
            ],
            "target": enum
          }
        }
      ]
    }
  }
},
"samplingPercentage": integer,
"scheduleFrequency": {
  "dailySchedule": {
  },
  "monthlySchedule": {
    "dayOfMonth": integer
  },
```

```
    "weeklySchedule": {
      "dayOfWeek": enum
    }
  },
  "statistics": {
    "approximateNumberOfObjectsToProcess": number,
    "numberOfRuns": number
  },
  "tags": {
  },
  "userPausedDetails": {
    "jobExpiresAt": "string",
    "jobImminentExpirationHealthEventArn": "string",
    "jobPausedAt": "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"
}
```

InternalServerException 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
Required: False

CriteriaForJob

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

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
Required: False

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
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.

allowListIds

An array of unique identifiers, one for each allow list that the job is configured to use when it analyzes data.

Type: Array of type string
Required: False

clientToken

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

customDataIdentifierIds

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

Type: Array of type string
Required: False

description

The custom description 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

jobArn

The Amazon Resource Name (ARN) of the job.

Type: string
Required: False

jobId

The unique identifier for the job.

Type: string

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
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
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
Required: False

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 or, if the job hasn't run yet, when the job was created.

Type: string
Required: False
Format: date-time

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`, `NONE`, or `RECOMMENDED`.

Type: Array of type string
Required: False

managedDataIdentifierSelector

The selection type that determines which managed data identifiers the job uses when it analyzes data. Possible values are:

- `ALL` - Use all managed data identifiers.
- `EXCLUDE` - Use all managed data identifiers except the ones 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. Use only custom data identifiers (`customDataIdentifierIds`).
- `RECOMMENDED` (default) - Use the recommended set of managed data identifiers.

If this value is null, the job uses the recommended set of managed data identifiers.

If the job is a recurring job and this value is `ALL` or `EXCLUDE`, each job run automatically uses new managed data identifiers that are released. If this value is null or `RECOMMENDED` for a recurring job, each job run uses all the managed data identifiers that are in the recommended set when the run starts.

To learn about individual managed data identifiers or determine which ones are in the recommended set, see Using managed data identifiers or Recommended managed data identifiers in the *Amazon Macie User Guide*.

Type: ManagedDataIdentifierSelector
Required: False

name

The custom name of the job.

Type: string
Required: False

s3JobDefinition

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

Type: S3JobDefinition
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

scheduleFrequency

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

Type: JobScheduleFrequency
Required: False

statistics

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

Type: Statistics
Required: False

tags

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

Type: TagMap
Required: False

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
Required: False

Empty

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

InternalServerException

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. Depending on the type of condition, possible 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
Required: False

monthlySchedule

Specifies a monthly recurrence pattern for running the job.

Type: MonthlySchedule
Required: False

weeklySchedule

Specifies a weekly recurrence pattern for running the job.

Type: WeeklySchedule
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
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
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
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

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

RECOMMENDED

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
Required: False

includes

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

Type: CriteriaBlockForJob
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.

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
Required: False

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
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
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
Required: False

includes

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

Type: JobScopingBlock
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
Required: False

key

The property to use in the condition.

Type: SimpleCriterionKeyForJob
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

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 - EQ (equals), GT (greater than), GTE (greater than or equals), LT (less than), LTE (less than or equals), or NE (not equals)
- OBJECT_SIZE - EQ (equals), GT (greater than), GTE (greater than or equals), LT (less than), LTE (less than or equals), or NE (not equals)

Type: JobComparator
Required: False

key

The object property to use in the condition.

Type: ScopeFilterKey
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: 2023-09-24T14:31:13Z
- 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

Statistics

Provides processing statistics for a classification job.

approximateNumberOfObjectsToProcess

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

Type: number
Required: False

numberOfRuns

The number of times that the job has 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
Required: False

tagValues

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

Type: Array of type TagCriterionPairForJob

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.

key

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

Type: string

Required: False

value

The tag value 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 an Amazon Macie resource.

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
Required: False

key

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

Type: string
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
Required: False

target

The type of object to apply the condition to.

Type: TagTarget
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.

key

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

Type: string
Required: False

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

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 Changing the status of a job 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
  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`.

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

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

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateClassificationJob

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

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 you create to analyze objects in Amazon Simple Storage Service (Amazon S3) general purpose buckets, and 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 match 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 align your analysis with periodic updates to bucket objects or monitor buckets for the presence of sensitive data. In addition to these settings, you can configure a job to use one or more allow lists. Allow lists define specific text or text patterns that you want Macie to ignore when it analyzes objects. You can create and use allow lists in all the AWS Regions where Macie is currently available except the Asia Pacific (Osaka) Region. For more information about creating and configuring jobs, see Running sensitive data discovery jobs in the *Amazon Macie User Guide*.

You can use the Classification Job Creation resource to create and define the settings for a classification job. Note that you can't change any settings for a job after you create it. This helps to 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	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
409	ConflictException	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException	The request failed because you sent too many requests

Status code	Response model	Description
		during a certain amount of time.
500	InternalServerException	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

POST schema

```
{
  "allowListIds": [
    "string"
  ],
  "clientToken": "string",
  "customDataIdentifierIds": [
    "string"
  ],
  "description": "string",
  "initialRun": boolean,
  "jobType": enum,
  "managedDataIdentifierIds": [
    "string"
  ],
  "managedDataIdentifierSelector": enum,
  "name": "string",
  "s3JobDefinition": {
    "bucketCriteria": {
      "excludes": {
        "and": [
          {
            "simpleCriterion": {
              "comparator": enum,
              "key": enum,
              "values": [
                "string"
```

```
            ]
          },
          "tagCriterion": {
            "comparator": enum,
            "tagValues": [
              {
                "key": "string",
                "value": "string"
              }
            ]
          }
        }
      ]
    },
    "includes": {
      "and": [
        {
          "simpleCriterion": {
            "comparator": enum,
            "key": enum,
            "values": [
              "string"
            ]
          },
          "tagCriterion": {
            "comparator": enum,
            "tagValues": [
              {
                "key": "string",
                "value": "string"
              }
            ]
          }
        }
      ]
    }
  },
  "bucketDefinitions": [
    {
      "accountId": "string",
      "buckets": [
        "string"
      ]
    }
```

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

```
              ],
              "target": enum
            }
          }
        ]
      }
    }
  },
  "samplingPercentage": integer,
  "scheduleFrequency": {
    "dailySchedule": {
    },
    "monthlySchedule": {
      "dayOfMonth": integer
    },
    "weeklySchedule": {
      "dayOfWeek": enum
    }
  },
  "tags": {
  }
}
```

Response bodies

CreateClassificationJobResponse schema

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

InternalServerException 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 to ensure that you have an immutable history of sensitive data findings and discovery results for data privacy and protection audits or investigations.

allowListIds

An array of unique identifiers, one for each allow list for the job to use when it analyzes data.

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: True

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

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 specify the recurrence pattern for the job.

Type: JobType
Required: True

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

managedDataIdentifierSelector

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

- `ALL` - Use all managed data identifiers. If you specify this value, don't specify any values for the `managedDataIdentifierIds` property.
- `EXCLUDE` - Use all managed data identifiers except the ones 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 value for the `customDataIdentifierIds` property and don't specify any values for the `managedDataIdentifierIds` property.
- `RECOMMENDED` (default) - Use the recommended set of managed data identifiers. If you specify this value, don't specify any values for the `managedDataIdentifierIds` property.

If you don't specify a value for this property, the job uses the recommended set of managed data identifiers.

If the job is a recurring job and you specify `ALL` or `EXCLUDE`, each job run automatically uses new managed data identifiers that are released. If you don't specify a value for this property or you specify `RECOMMENDED` for a recurring job, each job run automatically uses all the managed data identifiers that are in the recommended set when the run starts.

To learn about individual managed data identifiers or determine which ones are in the recommended set, see Using managed data identifiers or Recommended managed data identifiers in the *Amazon Macie User Guide*.

Type: ManagedDataIdentifierSelector
Required: False

name

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

Type: string
Required: True

s3JobDefinition

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

Type: S3JobDefinition
Required: True

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

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
Required: False

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
Required: False

CreateClassificationJobResponse

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

jobArn

The Amazon Resource Name (ARN) of the job.

Type: string
Required: False

jobId

The unique identifier for 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
Required: False

CriteriaForJob

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

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
Required: False

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
Required: False

DailySchedule

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

InternalServerException

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. Depending on the type of condition, possible 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
Required: False

monthlySchedule

Specifies a monthly recurrence pattern for running the job.

Type: MonthlySchedule
Required: False

weeklySchedule

Specifies a weekly recurrence pattern for running the job.

Type: WeeklySchedule
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
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
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
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
RECOMMENDED

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
Required: False

includes

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

Type: CriteriaBlockForJob
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.

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
Required: False

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
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
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
Required: False

includes

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

Type: JobScopingBlock
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
Required: False

key

The property to use in the condition.

Type: SimpleCriterionKeyForJob
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

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` - `EQ` (equals), `GT` (greater than), `GTE` (greater than or equals), `LT` (less than), `LTE` (less than or equals), or `NE` (not equals)
- `OBJECT_SIZE` - `EQ` (equals), `GT` (greater than), `GTE` (greater than or equals), `LT` (less than), `LTE` (less than or equals), or `NE` (not equals)

Type: JobComparator
Required: False

key

The object property to use in the condition.

Type: ScopeFilterKey

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: `2023-09-24T14:31:13Z`
- `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

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
Required: False

tagValues

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

Type: Array of type TagCriterionPairForJob
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.

key

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

Type: string
Required: False

value

The tag value 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 an Amazon Macie resource.

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
Required: False

key

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

Type: string
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
Required: False

target

The type of object to apply the condition to.

Type: TagTarget
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.

key

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

Type: string
Required: False

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

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Classification Job List

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

You can use this 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 how to filter, sort, and paginate the results. To retrieve additional information about a particular classification job, use the Classification Job 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	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.

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

Schemas

Request bodies

POST schema

```
{
  "filterCriteria": {
    "excludes": [
      {
        "comparator": enum,
        "key": enum,
        "values": [
          "string"
```

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

Response bodies

ListClassificationJobsResponse schema

```
{
  "items": [
    {
      "bucketCriteria": {
        "excludes": {
          "and": [
            {
              "simpleCriterion": {
                "comparator": enum,
                "key": enum,
                "values": [
                  "string"
                ]
              },
              "tagCriterion": {
                "comparator": enum,
                "tagValues": [
                  {
```

```
                    "key": "string",
                    "value": "string"
                  }
                ]
              }
            }
          ]
        },
        "includes": {
          "and": [
            {
              "simpleCriterion": {
                "comparator": enum,
                "key": enum,
                "values": [
                  "string"
                ]
              },
              "tagCriterion": {
                "comparator": enum,
                "tagValues": [
                  {
                    "key": "string",
                    "value": "string"
                  }
                ]
              }
            }
          ]
        }
      },
      "bucketDefinitions": [
        {
          "accountId": "string",
          "buckets": [
            "string"
          ]
        }
      ],
      "createdAt": "string",
      "jobId": "string",
      "jobStatus": enum,
      "jobType": enum,
      "lastRunErrorStatus": {
```

```
        "code": enum
      },
      "name": "string",
      "userPausedDetails": {
        "jobExpiresAt": "string",
        "jobImminentExpirationHealthEventArn": "string",
        "jobPausedAt": "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"
}
```

InternalServerException 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

Required: False

CriteriaForJob

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

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

Required: False

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

Required: False

InternalServerException

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. Depending on the type of condition, possible 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.

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
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
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

jobId

The unique identifier for the job.

Type: string
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
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
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
Required: False

name

The custom name of the job.

Type: string
Required: False

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
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
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
Required: False

maxResults

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

Type: integer
Required: False

Format: int32

nextToken

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

Type: string
Required: False

sortCriteria

The criteria to use to sort the results.

Type: ListJobsSortCriteria
Required: False

ListClassificationJobsResponse

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

items

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

Type: Array of type JobSummary
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

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
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
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
Required: False

key

The property to use to filter the results.

Type: ListJobsFilterKey
Required: False

values

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

Type: Array of type string
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.

attributeName

The property to sort the results by.

Type: ListJobsSortAttributeName
Required: False

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`

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
Required: False

includes

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

Type: CriteriaBlockForJob
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
Required: False

key

The property to use in the condition.

Type: SimpleCriterionKeyForJob
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

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
Required: False

tagValues

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

Type: Array of type TagCriterionPairForJob
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.

key

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

Type: string
Required: False

value

The tag value 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`.

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

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

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Classification Results - Export Configuration

The Export Configuration resource for classification results provides access to 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 that Amazon Macie performed on an Amazon S3 object to determine whether the object contains sensitive data.

When you run a classification job or Macie performs automated sensitive data discovery, Macie automatically creates a data classification result for each S3 object that's included in the scope of the analysis. This includes objects that Macie doesn't find sensitive data in, and therefore don't produce findings, and objects that Macie can't analyze due to issues such as permissions settings. Data classification results provide you with analysis records that can be helpful for data privacy and protection audits or investigations. You can configure Macie to store these records in an S3 general purpose bucket and encrypt them with an AWS Key Management Service (AWS KMS) key. 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, configure these settings for each Region in which you use Macie. You can optionally store data classification results for multiple Regions in the same S3 bucket. However, note the following requirements:

- To store the results for a Region that AWS enables by default for AWS accounts, such as the US East (N. Virginia) Region, you have to specify a bucket in a Region that's enabled by default. The results can't be stored in a bucket in an opt-in Region (Region that's disabled by default).
- To store the results for an opt-in Region, such as the Middle East (Bahrain) Region, you have to specify a bucket in that same Region or a Region that's enabled by default. The results can't be stored in a bucket in a different opt-in Region.

To determine whether a Region is enabled by default, see Enable or disable AWS Regions in your account in the *AWS Account Management Reference Guide*. In addition to the preceding requirements, also consider whether you want to retrieve samples of sensitive data that Macie reports in individual findings. To retrieve sensitive data samples from an affected S3 object, all of the following resources and data must be stored in the same Region: the affected object, the applicable finding, and the corresponding sensitive data discovery result.

You can use the Export Configuration resource to specify or retrieve information about your configuration 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	GetClassificationExportConfigurationResponse	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
409	ConflictException	The request failed because it conflicts with the current state of the specified resource.

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

PUT

Operation ID: `PutClassificationExportConfiguration`

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

Responses

Status code	Response model	Description
200	PutClassificationExportConfigurationResponse	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.

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

Schemas

Request bodies

PUT schema

```
{
  "configuration": {
    "s3Destination": {
      "bucketName": "string",
      "keyPrefix": "string",
      "kmsKeyArn": "string"
    }
  }
}
```

Response bodies

GetClassificationExportConfigurationResponse schema

```
{
  "configuration": {
    "s3Destination": {
      "bucketName": "string",
      "keyPrefix": "string",
      "kmsKeyArn": "string"
    }
  }
}
```

PutClassificationExportConfigurationResponse schema

```
{
  "configuration": {
    "s3Destination": {
      "bucketName": "string",
      "keyPrefix": "string",
      "kmsKeyArn": "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"
}
```

InternalServerException 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. The location must be an S3 general purpose 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

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

Required: False

InternalServerException

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.

configuration

The location to store data classification results in, and the encryption settings to use when storing results in that location.

Type: ClassificationExportConfiguration
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
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. This must be the name of an existing general purpose 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

kmsKeyArn

The Amazon Resource Name (ARN) of the customer managed AWS KMS key to use for encryption of the results. This must be the ARN of an existing, symmetric encryption AWS KMS key that's enabled in the same AWS Region as the bucket.

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

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutClassificationExportConfiguration

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

Classification Scope

The Classification Scope resource provides access to the classification scope settings for your Amazon Macie account. The classification scope specifies Amazon Simple Storage Service (Amazon S3) buckets that you don't want Macie to analyze when it performs automated sensitive data discovery. It defines an S3 bucket exclusion list for automated sensitive data discovery. For more information, see Performing automated sensitive data discovery in the *Amazon Macie User Guide*.

The first time you or your Macie administrator enables automated sensitive data discovery for your account, Macie automatically creates the classification scope for your account. If you have a standalone Macie account, Macie then uses the scope's settings to determine which S3 buckets to exclude from analyses. If your account is part of an organization that centrally manages multiple Macie accounts, Macie uses the scope settings for your Macie administrator's account to determine which buckets to exclude. Contact your Macie administrator for information about the settings for your organization.

By default, Macie analyzes data in all the S3 general purpose buckets for an account. If you're the Macie administrator for an organization, this includes buckets that your member accounts own. If you're a Macie administrator or you have a standalone Macie account, you can adjust the scope of the analyses by adding buckets to and removing buckets from the list of buckets to exclude. For example, you might exclude buckets that typically store AWS logging data, such as a bucket that stores AWS CloudTrail event logs. To exclude all buckets for a particular account in an organization, you can disable automated sensitive data discovery for the account. To do this, use the Accounts resource for automated sensitive data discovery.

If you're a Macie administrator or you have a standalone Macie account, you can use the Classification Scope resource to retrieve or update the classification scope settings for your organization or account. When you use this resource, you have to specify the unique identifier for the classification scope that specifies the settings. To obtain this identifier, use the Classification Scopes resource.

URI

`/classification-scopes/id`

HTTP methods

GET

Operation ID: `GetClassificationScope`

Retrieves the classification scope settings for an account.

Path parameters

Name	Type	Required	Description
id	String	True	The unique identifier for the Amazon Macie

Name	Type	Required	Description
			resource that the request applies to.

Responses

Status code	Response model	Description
200	GetClassificationScopeResponse	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	The request failed due to an unknown internal server error, exception, or failure.

PATCH

Operation ID: `UpdateClassificationScope`

Updates the classification scope settings for an account.

Path parameters

Name	Type	Required	Description
id	String	True	The unique identifier for the Amazon Macie resource that the request applies to.

Responses

Status code	Response model	Description
200	Empty Schema	The request succeeded. The specified settings were updated and there isn't any content to include in the body of the response (No Content).
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.

Status code	Response model	Description
500	InternalServerException	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

PATCH schema

```
{
  "s3": {
    "excludes": {
      "bucketNames": [
        "string"
      ],
      "operation": enum
    }
  }
}
```

Response bodies

GetClassificationScopeResponse schema

```
{
  "id": "string",
  "name": "string",
  "s3": {
    "excludes": {
      "bucketNames": [
        "string"
      ]
    }
  }
}
```

Empty Schema schema

```
{
}
```

ValidationException schema

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

AccessDeniedException schema

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

ResourceNotFoundException schema

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

ThrottlingException schema

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

InternalServerException 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

ClassificationScopeUpdateOperation

Specifies how to apply changes to the S3 bucket exclusion list defined by the classification scope for an Amazon Macie account. Valid values are:

```
ADD
REPLACE
REMOVE
```

Empty

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

GetClassificationScopeResponse

Provides information about the classification scope settings for an Amazon Macie account. Macie uses these settings when it performs automated sensitive data discovery for the account.

id

The unique identifier for the classification scope.

Type: string
Required: False

name

The name of the classification scope: `automated-sensitive-data-discovery`.

Type: string
Required: False

s3

The S3 buckets that are excluded from automated sensitive data discovery.

Type: S3ClassificationScope
Required: False

InternalServerException

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

S3ClassificationScope

Specifies the S3 buckets that are excluded from automated sensitive data discovery for an Amazon Macie account.

excludes

The S3 buckets that are excluded.

Type: S3ClassificationScopeExclusion
Required: True

S3ClassificationScopeExclusion

Specifies the names of the S3 buckets that are excluded from automated sensitive data discovery.

bucketNames

An array of strings, one for each S3 bucket that is excluded. Each string is the full name of an excluded bucket.

Type: Array of type string
Required: True

S3ClassificationScopeExclusionUpdate

Specifies S3 buckets to add or remove from the exclusion list defined by the classification scope for an Amazon Macie account.

bucketNames

Depending on the value specified for the update operation (`ClassificationScopeUpdateOperation`), an array of strings that: lists the names of buckets to add or remove from the list, or specifies a new set of bucket names that overwrites all existing names in the list. Each string must be the full name of an S3 bucket. Values are case sensitive.

Type: Array of type string
Required: True

operation

Specifies how to apply the changes to the exclusion list. Valid values are:

- ADD - Append the specified bucket names to the current list.
- REMOVE - Remove the specified bucket names from the current list.
- REPLACE - Overwrite the current list with the specified list of bucket names. If you specify this value, Amazon Macie removes all existing names from the list and adds all the specified names to the list.

Type: ClassificationScopeUpdateOperation
Required: True

S3ClassificationScopeUpdate

Specifies changes to the list of S3 buckets that are excluded from automated sensitive data discovery for an Amazon Macie account.

excludes

The names of the S3 buckets to add or remove from the list.

Type: S3ClassificationScopeExclusionUpdate
Required: True

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

UpdateClassificationScopeRequest

Specifies new classification scope settings for an Amazon Macie account. Macie uses these settings when it performs automated sensitive data discovery for the account. To update the settings, automated sensitive data discovery must be enabled for the account.

s3

The S3 buckets to add or remove from the exclusion list defined by the classification scope.

Type: S3ClassificationScopeUpdate
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:

GetClassificationScope

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

- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateClassificationScope

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

Classification Scopes

The Classification Scopes resource provides a subset of information about the classification scope for your Amazon Macie account. The classification scope specifies Amazon Simple Storage Service (Amazon S3) buckets that you don't want Macie to analyze when it performs automated sensitive data discovery. It defines an S3 bucket exclusion list for automated sensitive data discovery.

The first time you or your Macie administrator enables automated sensitive data discovery for your account, Macie automatically creates the classification scope for your account. If you have a standalone Macie account, Macie then uses the scope's settings to determine which S3 buckets to exclude from analyses. If your account is part of an organization that centrally manages multiple Macie accounts, Macie uses the scope settings for your Macie administrator's account to determine which buckets to exclude. Contact your Macie administrator for information about the settings for your organization.

If you're the Macie administrator for an organization or you have a standalone Macie account, you can use this resource to retrieve the unique identifier and name of the classification scope that Macie created for your account. You can then use the unique identifier to retrieve or update the scope's settings by using the Classification Scope resource.

URI

`/classification-scopes`

HTTP methods

GET

Operation ID: `ListClassificationScopes`

Retrieves a subset of information about the classification scope for an account.

Query parameters

Name	Type	Required	Description
`name`	String	False	The name of the classification scope to retrieve the unique identifier for.
`nextToken`	String	False	The `nextToken` string that specifies which page of results to return in a paginated response.

Responses

Status code	Response model	Description
`200`	`ListClassificationScopesResponse`	The request succeeded.
`400`	`ValidationException`	The request failed because the input doesn't satisfy the constraints specified by the service.

Status code	Response model	Description
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Response bodies

ListClassificationScopesResponse schema

```
{
  "classificationScopes": [
    {
      "id": "string",
      "name": "string"
    }
  ],
  "nextToken": "string"
}
```

ValidationException schema

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

AccessDeniedException schema

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

ThrottlingException schema

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

InternalServerException 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

ClassificationScopeSummary

Provides information about the classification scope for an Amazon Macie account. Macie uses the scope's settings when it performs automated sensitive data discovery for the account.

id

The unique identifier for the classification scope.

Type: string
Required: False

name

The name of the classification scope: `automated-sensitive-data-discovery`.

Type: string
Required: False

InternalServerException

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

ListClassificationScopesResponse

Provides the results of a request for information about the classification scope for an Amazon Macie account. Macie uses the scope's settings when it performs automated sensitive data discovery for the account.

classificationScopes

An array that specifies the unique identifier and name of the classification scope for the account.

Type: Array of type ClassificationScopeSummary
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

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:

ListClassificationScopes

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2

- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Custom Data Identifier

The Custom Data Identifier resource provides access to the repository of custom data identifiers for your Amazon Macie account. A *custom data identifier* is a set of criteria that you define to detect sensitive data in a data source. The criteria consist of a regular expression (*regex*) that defines a text pattern to match and, optionally, character sequences and a proximity rule that refine the analysis of data. In addition to detection criteria, you can optionally define severity levels for findings that a custom data identifier produces. Severity levels are based on the number of occurrences of text that match the custom data identifier's detection criteria. For more information, see Building custom data identifiers in the *Amazon Macie User Guide*.

You can use this resource to retrieve detailed information about the detection criteria and other settings for a custom data identifier. You can also use this resource to delete a custom data identifier. If you delete a custom data identifier, Macie soft deletes it. This means that a record of the custom data identifier remains for your account, but it's marked as deleted. If a custom data identifier has this status, you can't configure new classification jobs to use it or add it to your settings for automated sensitive data discovery. In addition, you can't access it by using the Amazon Macie console. You can, however, retrieve its details programmatically.

If you delete a custom data identifier that you configured classification jobs or automated sensitive data discovery to use, the jobs and automated discovery will continue to use it. This means that sensitive data findings, statistics, and other types of results will continue to report text that matches the identifier's criteria. To prevent this, do the following before you delete the custom data identifier:

- Remove it from your automated discovery settings. To remove it, use the Sensitivity Inspection Template resource.
- Identify existing jobs that use it and are scheduled to run in the future. You can cancel these jobs. Then create copies of the jobs and adjust their settings to exclude the custom data identifier. To cancel a job or retrieve its settings, use the Classification Job resource.

To use the Custom Data Identifier 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 resource.

URI

`/custom-data-identifiers/id`

HTTP methods

DELETE

Operation ID: `DeleteCustomDataIdentifier`

Soft deletes a custom data identifier.

Path parameters

Name	Type	Required	Description
id	String	True	The unique identifier for the Amazon Macie resource that the request applies to.

Responses

Status code	Response model	Description
200	Empty Schema	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).
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.

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

GET

Operation ID: `GetCustomDataIdentifier`

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

Path parameters

Name	Type	Required	Description
id	String	True	The unique identifier for the Amazon Macie resource that the request applies to.

Responses

Status code	Response model	Description
200	GetCustomDataIdentifierResponse	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
409	ConflictException	The request failed because it conflicts with the current state of the specified resource.

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

Schemas

Response bodies

Empty Schema schema

```
{
}
```

GetCustomDataIdentifierResponse schema

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

```
      "occurrencesThreshold": integer,
      "severity": enum
    }
  ],
  "tags": {
  }
}
```

ValidationException schema

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

ServiceQuotaExceededException schema

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

AccessDeniedException schema

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

ResourceNotFoundException schema

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

ConflictException schema

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

```
}
```

ThrottlingException schema

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

InternalServerException 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

DataIdentifierSeverity

The severity of a finding, ranging from `LOW`, for least severe, to `HIGH`, for most severe. Valid values are:

`LOW`
`MEDIUM`
`HIGH`

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 detection criteria and other settings for a custom data identifier.

arn

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

Type: string
Required: False

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

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

ignoreWords

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

Type: Array of type string
Required: False

keywords

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

Type: Array of type string
Required: False

maximumMatchDistance

The maximum number of characters that can exist between the end of at least one complete character sequence specified by the `keywords` array and the end of the text that matches the

regex pattern. If a complete keyword precedes all the text that matches the pattern and the keyword is within the specified distance, Amazon Macie includes the result. Otherwise, Macie excludes the result.

Type: integer
Required: False
Format: int32

name

The custom name of the custom data identifier.

Type: string
Required: False

regex

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

Type: string
Required: False

severityLevels

Specifies the severity that's assigned to findings that the custom data identifier produces, based on the number of occurrences of text that match the custom data identifier's detection criteria. By default, Amazon Macie creates findings for S3 objects that contain at least one occurrence of text that matches the detection criteria, and Macie assigns the `MEDIUM` severity to those findings.

Type: Array of type SeverityLevel
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
Required: False

InternalServerException

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

SeverityLevel

Specifies a severity level for findings that a custom data identifier produces. A severity level determines which severity is assigned to the findings, based on the number of occurrences of text that match the custom data identifier's detection criteria.

occurrencesThreshold

The minimum number of occurrences of text that must match the custom data identifier's detection criteria in order to produce a finding with the specified severity (`severity`).

Type: integer
Required: True
Format: int64

severity

The severity to assign to a finding: if the number of occurrences is greater than or equal to the specified threshold (`occurrencesThreshold`); and, if applicable, the number of occurrences is less than the threshold for the next consecutive severity level for the custom data identifier, moving from `LOW` to `HIGH`.

Type: DataIdentifierSeverity
Required: True

TagMap

A string-to-string map of key-value pairs that specifies the tags (keys and values) for an Amazon Macie resource.

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:

DeleteCustomDataIdentifier

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

GetCustomDataIdentifier

- AWS Command Line Interface
- AWS SDK for .NET

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

Custom Data Identifier Creation

A *custom data identifier* is a set of criteria that you define to detect sensitive data in a data source. The criteria consist of a regular expression (*regex*) that defines a text pattern to match and, optionally, character sequences and a proximity rule that refine the analysis of data. The character sequences can be: *keywords*, which are words or phrases that must be in proximity of text that matches the regex, or *ignore words*, which are words or phrases to exclude from the results. 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.

In addition to detection criteria, you can optionally specify severity levels for findings that a custom data identifier produces. Each severity level is based on the number of occurrences of text that match the custom data identifier's detection criteria. If you don't specify any severity levels for a custom data identifier, Macie automatically assigns the *Medium* severity to all findings that the custom data identifier produces. For more information, see Building custom data identifiers in the *Amazon Macie User Guide*.

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 to 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 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	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
409	ConflictException	The request failed because it conflicts with the current state of the specified resource.

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

Schemas

Request bodies

POST schema

```
{
  "clientToken": "string",
  "description": "string",
  "ignoreWords": [
    "string"
  ],
  "keywords": [
    "string"
  ],
  "maximumMatchDistance": integer,
  "name": "string",
  "regex": "string",
  "severityLevels": [
    {
      "occurrencesThreshold": integer,
      "severity": enum
    }
  ],
  "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"
}
```

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

clientToken

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

Type: string
Required: False

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 this description, depending on the actions that they're allowed to perform in Amazon Macie.

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 contains 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

keywords

An array that lists specific character sequences (*keywords*), one of which must precede and 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

maximumMatchDistance

The maximum number of characters that can exist between the end of at least one complete character sequence specified by the `keywords` array and the end of the text that matches the regex pattern. If a complete keyword precedes all the text that matches the pattern and the keyword is within the specified distance, Amazon Macie includes the result. The distance can be 1-300 characters. The default value is 50.

Type: integer
Required: False
Format: int32

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 this name, depending on the actions that they're allowed to perform in Amazon Macie.

Type: string
Required: True

regex

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

Type: string
Required: True

severityLevels

The severity to assign to findings that the custom data identifier produces, based on the number of occurrences of text that match the custom data identifier's detection criteria. You can specify as many as three `SeverityLevel` objects in this array, one for each severity: `LOW`, `MEDIUM`, or `HIGH`. If you specify more than one, the occurrences thresholds must be in ascending order by severity, moving from `LOW` to `HIGH`. For example, `1` for `LOW`, `50` for `MEDIUM`, and `100` for `HIGH`. If an S3 object contains fewer occurrences than the lowest specified threshold, Amazon Macie doesn't create a finding.

If you don't specify any values for this array, Macie creates findings for S3 objects that contain at least one occurrence of text that matches the detection criteria, and Macie assigns the `MEDIUM` severity to those findings.

Type: Array of type SeverityLevel
Required: False

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
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

DataIdentifierSeverity

The severity of a finding, ranging from `LOW`, for least severe, to `HIGH`, for most severe. Valid values are:

```
LOW
MEDIUM
HIGH
```

InternalServerException

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

SeverityLevel

Specifies a severity level for findings that a custom data identifier produces. A severity level determines which severity is assigned to the findings, based on the number of occurrences of text that match the custom data identifier's detection criteria.

occurrencesThreshold

The minimum number of occurrences of text that must match the custom data identifier's detection criteria in order to produce a finding with the specified severity (`severity`).

Type: integer

Required: True

Format: int64

severity

The severity to assign to a finding: if the number of occurrences is greater than or equal to the specified threshold (`occurrencesThreshold`); and, if applicable, the number of occurrences is less than the threshold for the next consecutive severity level for the custom data identifier, moving from `LOW` to `HIGH`.

Type: DataIdentifierSeverity

Required: True

TagMap

A string-to-string map of key-value pairs that specifies the tags (keys and values) for an Amazon Macie resource.

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python

- AWS SDK for Ruby V3

Custom Data Identifier Descriptions

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

You can use this resource to retrieve a subset of 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 detection criteria and other settings for an individual custom data identifier, use the Custom Data Identifier 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	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would

Status code	Response model	Description
		exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
409	ConflictException	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	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": [
    {
      "arn": "string",
      "createdAt": "string",
      "deleted": boolean,
      "description": "string",
      "id": "string",
      "name": "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"
}
```

InternalServerException 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.

arn

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

Type: string
Required: False

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

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

name

The custom name 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 matches the criteria specified in the request.

Type: Array of type BatchGetCustomDataIdentifierSummary
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

InternalServerException

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Custom Data Identifier List

The Custom Data Identifier List resource represents the repository of custom data identifiers for your Amazon Macie account. A *custom data identifier* is a set of criteria that you define to detect sensitive data in a data source.

You can use this resource to retrieve a subset of information about the custom data identifiers for your account. To retrieve detailed information about the detection criteria and other settings for an individual custom data identifier, use the Custom Data Identifier resource.

URI

`/custom-data-identifiers/list`

HTTP methods

POST

Operation ID: `ListCustomDataIdentifiers`

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

Responses

Status code	Response model	Description
`200`	`ListCustomDataIdentifiersResponse`	The request succeeded.

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

Schemas

Request bodies

POST schema

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

Response bodies

ListCustomDataIdentifiersResponse schema

```
{
  "items": [
    {
      "arn": "string",
      "createdAt": "string",
      "description": "string",
      "id": "string",
      "name": "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"
}
```

InternalServerException 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.

arn

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

Type: string
Required: False

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

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

name

The custom name of the custom data identifier.

Type: string
Required: False

InternalServerException

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.

maxResults

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

Type: integer

Required: False
Format: int32

nextToken

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

Type: string
Required: False

ListCustomDataIdentifiersResponse

Provides the results of a request for information about custom data identifiers.

items

An array of objects, one for each custom data identifier.

Type: Array of type CustomDataIdentifierSummary
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

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

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 in 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.

When you develop a custom 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 data. The character sequences can be: *keywords*, which are words or phrases that must be in proximity of text that matches the regex, or *ignore words*, which are words or phrases to exclude from the results. For more information, see Building custom data identifiers in the *Amazon Macie User Guide*.

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 later 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 resource to create it.

URI

```
/custom-data-identifiers/test
```

HTTP methods

POST

Operation ID: `TestCustomDataIdentifier`

Tests criteria for a custom data identifier.

Responses

Status code	Response model	Description
200	TestCustomDataIdentifierResponse	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
409	ConflictException	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException	The request failed because you sent too many requests

Status code	Response model	Description
		during a certain amount of time.
500	InternalServerException	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

POST schema

```
{
  "ignoreWords": [
    "string"
  ],
  "keywords": [
    "string"
  ],
  "maximumMatchDistance": integer,
  "regex": "string",
  "sampleText": "string"
}
```

POST schema

```
{
  "ignoreWords": [
    "string"
  ],
  "keywords": [
    "string"
  ],
  "maximumMatchDistance": integer,
  "regex": "string",
  "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"
}
```

InternalServerException 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

InternalServerException

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.

ignoreWords

An array that lists specific character sequences (*ignore words*) to exclude from the results. If the text matched by the regular expression contains 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

keywords

An array that lists specific character sequences (*keywords*), one of which must precede and 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

maximumMatchDistance

The maximum number of characters that can exist between the end of at least one complete character sequence specified by the `keywords` array and the end of the text that matches the regex pattern. If a complete keyword precedes all the text that matches the pattern and the keyword is within the specified distance, Amazon Macie includes the result. The distance can be 1-300 characters. The default value is 50.

Type: integer
Required: False
Format: int32

regex

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

Type: string
Required: True

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 occurrences of sample text that matched the criteria specified by 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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Data 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 and encryption settings. It also includes details about the size and number of objects that Macie can analyze to detect sensitive data in a bucket, and whether and when that analysis occurred. The data is available for all the S3 buckets that Macie monitors and analyzes for your account. If you're the Macie administrator for an organization, this includes S3 buckets that your member accounts own.

Note that the data is available only for S3 general purpose buckets. Macie doesn't monitor or analyze S3 directory buckets. In addition, complete data is available for an S3 bucket only if Macie can retrieve and process metadata from Amazon S3 for the bucket and the bucket's objects. Errors or permissions settings might prevent Macie from retrieving and processing information about a

bucket or its objects. If this happens, 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 one or more S3 general purpose buckets that Macie monitors and analyzes for your account. To customize and refine your query, you can use the supported parameters to specify how to filter, sort, and paginate the query results. For more information about filter options, see Filtering your S3 bucket inventory in the *Amazon Macie User Guide*.

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 for an account.

Responses

Status code	Response model	Description
200	DescribeBucketsResponse	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.

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

Schemas

Request bodies

POST schema

```
{
  "criteria": {
  },
  "maxResults": integer,
  "nextToken": "string",
  "sortCriteria": {
    "attributeName": "string",
    "orderBy": enum
```

```
  }
}
```

Response bodies

DescribeBucketsResponse schema

```
{
  "buckets": [
    {
      "accountId": "string",
      "allowsUnencryptedObjectUploads": enum,
      "automatedDiscoveryMonitoringStatus": enum,
      "bucketArn": "string",
      "bucketCreatedAt": "string",
      "bucketName": "string",
      "classifiableObjectCount": integer,
      "classifiableSizeInBytes": integer,
      "errorCode": enum,
      "errorMessage": "string",
      "jobDetails": {
        "isDefinedInJob": enum,
        "isMonitoredByJob": enum,
        "lastJobId": "string",
        "lastJobRunTime": "string"
      },
      "lastAutomatedDiscoveryTime": "string",
      "lastUpdated": "string",
      "objectCount": integer,
      "objectCountByEncryptionType": {
        "customerManaged": integer,
        "kmsManaged": integer,
        "s3Managed": integer,
        "unencrypted": integer,
        "unknown": integer
      },
      "publicAccess": {
        "effectivePermission": enum,
        "permissionConfiguration": {
          "accountLevelPermissions": {
            "blockPublicAccess": {
              "blockPublicAcls": boolean,
              "blockPublicPolicy": boolean,
```

```
            "ignorePublicAcls": boolean,
            "restrictPublicBuckets": boolean
          }
        },
        "bucketLevelPermissions": {
          "accessControlList": {
            "allowsPublicReadAccess": boolean,
            "allowsPublicWriteAccess": boolean
          },
          "blockPublicAccess": {
            "blockPublicAcls": boolean,
            "blockPublicPolicy": boolean,
            "ignorePublicAcls": boolean,
            "restrictPublicBuckets": boolean
          },
          "bucketPolicy": {
            "allowsPublicReadAccess": boolean,
            "allowsPublicWriteAccess": boolean
          }
        }
      },
      "region": "string",
      "replicationDetails": {
        "replicated": boolean,
        "replicatedExternally": boolean,
        "replicationAccounts": [
          "string"
        ]
      },
      "sensitivityScore": integer,
      "serverSideEncryption": {
        "kmsMasterKeyId": "string",
        "type": enum
      },
      "sharedAccess": enum,
      "sizeInBytes": integer,
      "sizeInBytesCompressed": integer,
      "tags": [
        {
          "key": "string",
          "value": "string"
        }
      ],
```

```
      "unclassifiableObjectCount": {
        "fileType": integer,
        "storageClass": integer,
        "total": integer
      },
      "unclassifiableObjectSizeInBytes": {
        "fileType": integer,
        "storageClass": integer,
        "total": integer
      },
      "versioning": boolean
    }
  ],
  "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"
}
```

InternalServerException 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
Required: False

AutomatedDiscoveryMonitoringStatus

Specifies whether automated sensitive data discovery is currently configured to analyze objects in an S3 bucket. Possible values are:

```
MONITORED
NOT_MONITORED
```

BlockPublicAccess

Provides information about the block public access settings for an S3 bucket. These settings can apply to a bucket at the account 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*.

blockPublicAcls

Specifies whether Amazon S3 blocks public access control lists (ACLs) for the bucket and objects in the bucket.

Type: boolean
Required: False

blockPublicPolicy

Specifies whether Amazon S3 blocks public bucket policies for 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

restrictPublicBuckets

Specifies whether Amazon S3 restricts public bucket policies for 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.

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

gte

The value for the property is greater than or equal to the specified value.

Type: integer
Required: False
Format: int64

lt

The value for the property is less than the specified value.

Type: integer
Required: False
Format: int64

lte

The value for the property is less 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

prefix

The name of the bucket begins with the specified value.

Type: string
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
Required: False

blockPublicAccess

The block public access settings for the bucket.

Type: BlockPublicAccess
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

Required: False

BucketMetadata

Provides statistical data and other information about an S3 bucket that Amazon Macie monitors and analyzes for your account. By default, object count and storage size values include data for object parts that are the result of incomplete multipart uploads. For more information, see How Macie monitors Amazon S3 data security in the *Amazon Macie User Guide*.

If an error occurs when Macie attempts to retrieve and process metadata from Amazon S3 for the bucket or the bucket's objects, the value for the `versioning` property is `false` and the value for most other properties is null. Key exceptions are `accountId`, `bucketArn`, `bucketCreatedAt`, `bucketName`, `lastUpdated`, and `region`. To identify the cause of the error, refer to the `errorCode` and `errorMessage` values.

accountId

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

Type: string
Required: False

allowsUnencryptedObjectUploads

Specifies whether the bucket policy for the bucket requires server-side encryption of objects when objects are added to the bucket. Possible values are:

- `FALSE` - The bucket policy requires server-side encryption of new objects. `PutObject` requests must include a valid server-side encryption header.
- `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 a valid server-side encryption header.
- `UNKNOWN` - Amazon Macie can't determine whether the bucket policy requires server-side encryption of new objects.

Valid server-side encryption headers are: `x-amz-server-side-encryption` with a value of `AES256` or `aws:kms`, and `x-amz-server-side-encryption-customer-algorithm` with a value of `AES256`.

Type: string
Required: False
Values: `TRUE | FALSE | UNKNOWN`

automatedDiscoveryMonitoringStatus

Specifies whether automated sensitive data discovery is currently configured to analyze objects in the bucket. Possible values are: `MONITORED`, the bucket is included in analyses; and, `NOT_MONITORED`, the bucket is excluded from analyses. If automated sensitive data discovery is disabled for your account, this value is `NOT_MONITORED`.

Type: AutomatedDiscoveryMonitoringStatus
Required: False

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. This value can also indicate when changes such as edits to the bucket's policy were most recently made to the bucket.

Type: string
Required: False
Format: date-time

bucketName

The name of the bucket.

Type: string
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

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

errorCode

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
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

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
Required: False

lastAutomatedDiscoveryTime

The date and time, in UTC and extended ISO 8601 format, when Amazon Macie most recently analyzed objects in the bucket while performing automated sensitive data discovery. This value is null if automated sensitive data discovery is disabled for your account.

Type: string
Required: False
Format: date-time

lastUpdated

The date and time, in UTC and extended ISO 8601 format, when Amazon Macie most recently retrieved bucket or object metadata from Amazon S3 for the bucket.

Type: string
Required: False
Format: date-time

objectCount

The total number of objects in the bucket.

Type: integer
Required: False
Format: int64

objectCountByEncryptionType

The total number of objects 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
Required: False

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
Required: False

region

The AWS Region that hosts the bucket.

Type: string
Required: False

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
Required: False

sensitivityScore

The sensitivity score for the bucket, ranging from -1 (classification error) to 100 (sensitive).

If automated sensitive data discovery has never been enabled for your account or it's been disabled for your organization or your standalone account for more than 30 days, possible values are: 1, the bucket is empty; or, 50, the bucket stores objects but it's been excluded from recent analyses.

Type: integer

Required: False

Format: int32

serverSideEncryption

The default server-side encryption settings for the bucket.

Type: BucketServerSideEncryption

Required: False

sharedAccess

Specifies whether the bucket is shared with another AWS account, an Amazon CloudFront origin access identity (OAI), or a CloudFront origin access control (OAC). Possible values are:

- `EXTERNAL` - The bucket is shared with one or more of the following or any combination of the following: a CloudFront OAI, a CloudFront OAC, or an AWS account that isn't part of your Amazon Macie organization.
- `INTERNAL` - The bucket is shared with one or more AWS accounts that are part of your Amazon Macie organization. It isn't shared with a CloudFront OAI or OAC.
- `NOT_SHARED` - The bucket isn't shared with another AWS account, a CloudFront OAI, or a CloudFront OAC.
- `UNKNOWN` - Amazon Macie wasn't able to evaluate the shared access settings for the bucket.

An *Amazon Macie organization* is a set of Macie accounts that are centrally managed as a group of related accounts through AWS Organizations or by Macie invitation.

Type: string

Required: False

Values: `EXTERNAL | INTERNAL | NOT_SHARED | UNKNOWN`

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

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

tags

An array that specifies the tags (keys and values) that are associated with the bucket.

Type: Array of type KeyValuePair
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
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
Required: False

versioning

Specifies whether versioning is enabled for the bucket.

Type: boolean
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
```

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
Required: False

bucketLevelPermissions

The bucket-level permissions settings for the bucket.

Type: BucketLevelPermissions
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
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 is configured to use an Amazon S3 managed key to encrypt new objects.

Type: string
Required: False

type

The server-side encryption algorithm that's used by default to encrypt objects that are added to the bucket. Possible values are:

- `AES256` - New objects use SSE-S3 encryption. They're encrypted with an Amazon S3 managed key.
- `aws:kms` - New objects use SSE-KMS encryption. They're encrypted with an AWS KMS key (`kmsMasterKeyId`), either an AWS managed key or a customer managed key.
- `aws:kms:dsse` - New objects use DSSE-KMS encryption. They're encrypted with an AWS KMS key (`kmsMasterKeyId`), either an AWS managed key or a customer managed key.
- `NONE` - The bucket's default encryption settings don't specify server-side encryption behavior for new objects.

Type: string

Required: False
Values: `NONE | AES256 | aws:kms | aws:kms:dsse`

BucketSortCriteria

Specifies criteria for sorting the results of a query for information about S3 buckets.

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`, `sensitivityScore`, or `sizeInBytes`.

Type: string
Required: False

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`

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
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

nextToken

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

Type: string
Required: False

sortCriteria

The criteria to use to sort the query results.

Type: BucketSortCriteria
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.

buckets

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

Type: Array of type BucketMetadata
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

InternalServerException

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 objects in an S3 bucket, and, if so, the details of the job that ran most recently.

isDefinedInJob

Specifies whether any one-time or recurring jobs are configured to analyze objects 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 objects 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

lastJobId

The unique identifier for the job that ran most recently and is configured to analyze objects 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

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.

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

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

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.

customerManaged

The total number of objects that are encrypted with customer-provided keys. The objects use server-side encryption with customer-provided keys (SSE-C).

Type: integer
Required: False
Format: int64

kmsManaged

The total number of objects that are encrypted with AWS KMS keys, either AWS managed keys or customer managed keys. The objects use dual-layer server-side encryption or server-side encryption with AWS KMS keys (DSSE-KMS or SSE-KMS).

Type: integer
Required: False
Format: int64

s3Managed

The total number of objects that are encrypted with Amazon S3 managed keys. The objects use server-side encryption with Amazon S3 managed keys (SSE-S3).

Type: integer
Required: False
Format: int64

unencrypted

The total number of objects that use client-side encryption or aren't encrypted.

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 all the buckets in the query results. If versioning is enabled for a bucket, storage size values are based on the size of the latest version of each applicable object in the bucket.

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

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

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

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.

replicated

Specifies whether the bucket is configured to replicate one or more objects to any destination.

Type: boolean
Required: False

replicatedExternally

Specifies whether the bucket is configured to replicate one or more objects to a bucket for an AWS account that isn't part of your Amazon Macie organization. An *Amazon Macie organization* is a set of Macie accounts that are centrally managed as a group of related accounts through AWS Organizations or by Macie invitation.

Type: boolean
Required: False

replicationAccounts

An array of AWS account IDs, one for each AWS account that owns a bucket that the bucket is configured to replicate one or more objects to.

Type: Array of 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:

DescribeBuckets

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

Data 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. If you're the Macie administrator for an organization, this includes S3 buckets that your member accounts own.

This resource provides aggregated data for key security metrics such as the number of S3 buckets that are publicly accessible or shared with other AWS accounts. If automated sensitive data discovery is enabled, it also provides aggregated data for metrics such as the number of buckets that Macie has found sensitive data in. Note that statistical data is available only for S3 general purpose buckets. Macie doesn't monitor or analyze S3 directory buckets.

You can use the Amazon S3 Data Source Statistics resource to retrieve (query) aggregated data for data security and sensitivity metrics that apply to all the S3 general purpose buckets that Macie monitors and analyzes for your account. To retrieve additional data for these buckets, use the Amazon S3 Data Sources resource.

URI

`/datasources/s3/statistics`

HTTP methods

POST

Operation ID: `GetBucketStatistics`

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

Responses

Status code	Response model	Description
200	GetBucketStatisticsResponse	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.

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

Schemas

Request bodies

POST schema

```
{
  "accountId": "string"
}
```

Response bodies

GetBucketStatisticsResponse schema

```
{
  "bucketCount": integer,
  "bucketCountByEffectivePermission": {
    "publiclyAccessible": integer,
    "publiclyReadable": integer,
```

```
    "publiclyWritable": integer,
    "unknown": integer
  },
  "bucketCountByEncryptionType": {
    "kmsManaged": integer,
    "s3Managed": integer,
    "unencrypted": integer,
    "unknown": integer
  },
  "bucketCountByObjectEncryptionRequirement": {
    "allowsUnencryptedObjectUploads": integer,
    "deniesUnencryptedObjectUploads": integer,
    "unknown": integer
  },
  "bucketCountBySharedAccessType": {
    "external": integer,
    "internal": integer,
    "notShared": integer,
    "unknown": integer
  },
  "bucketStatisticsBySensitivity": {
    "classificationError": {
      "classifiableSizeInBytes": integer,
      "publiclyAccessibleCount": integer,
      "totalCount": integer,
      "totalSizeInBytes": integer
    },
    "notClassified": {
      "classifiableSizeInBytes": integer,
      "publiclyAccessibleCount": integer,
      "totalCount": integer,
      "totalSizeInBytes": integer
    },
    "notSensitive": {
      "classifiableSizeInBytes": integer,
      "publiclyAccessibleCount": integer,
      "totalCount": integer,
      "totalSizeInBytes": integer
    },
    "sensitive": {
      "classifiableSizeInBytes": integer,
      "publiclyAccessibleCount": integer,
      "totalCount": integer,
      "totalSizeInBytes": integer
```

```
    }
  },
  "classifiableObjectCount": integer,
  "classifiableSizeInBytes": integer,
  "lastUpdated": "string",
  "objectCount": integer,
  "sizeInBytes": integer,
  "sizeInBytesCompressed": integer,
  "unclassifiableObjectCount": {
    "fileType": integer,
    "storageClass": integer,
    "total": integer
  },
  "unclassifiableObjectSizeInBytes": {
    "fileType": integer,
    "storageClass": integer,
    "total": 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"
}
```

InternalServerException 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 due to a combination of permissions settings for each bucket.

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

publiclyReadable

The total number of buckets that allow the general public to have read access to the bucket.

Type: integer
Required: False
Format: int64

publiclyWritable

The total number of buckets that allow the general public to have 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 whose settings do or don't specify default server-side encryption behavior for objects that are added to the buckets. 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 whose default encryption settings are configured to encrypt new objects with an AWS KMS key, either an AWS managed key or a customer managed key. By default, these buckets encrypt new objects automatically using DSSE-KMS or SSE-KMS encryption.

Type: integer
Required: False
Format: int64

s3Managed

The total number of buckets whose default encryption settings are configured to encrypt new objects with an Amazon S3 managed key. By default, these buckets encrypt new objects automatically using SSE-S3 encryption.

Type: integer
Required: False
Format: int64

unencrypted

The total number of buckets that don't specify default server-side encryption behavior for new objects. Default encryption settings aren't configured 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, Amazon CloudFront origin access identities (OAIs), or CloudFront origin access controls (OACs). In this data, an *Amazon Macie organization* is defined as a set of Macie accounts that are centrally managed as a group of related accounts through AWS Organizations or by Macie invitation.

external

The total number of buckets that are shared with one or more of the following or any combination of the following: an Amazon CloudFront OAI, a CloudFront OAC, or an AWS account that isn't in the same Amazon Macie organization.

Type: integer
Required: False
Format: int64

internal

The total number of buckets that are shared with one or more AWS accounts in the same Amazon Macie organization. These buckets aren't shared with Amazon CloudFront OAIs or OACs.

Type: integer
Required: False
Format: int64

notShared

The total number of buckets that aren't shared with other AWS accounts, Amazon CloudFront OAIs, or CloudFront OACs.

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, Amazon CloudFront OAIs, or CloudFront OACs.

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 added to the buckets.

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 a valid server-side encryption header: the `x-amz-server-side-encryption` header with a value of `AES256` or `aws:kms`, or the `x-amz-server-side-encryption-customer-algorithm` header with a value of `AES256`.

Type: integer
Required: False
Format: int64

deniesUnencryptedObjectUploads

The total number of buckets whose bucket policies require server-side encryption of new objects. `PutObject` requests for these buckets must include a valid server-side encryption header: the `x-amz-server-side-encryption` header with a value of `AES256` or `aws:kms`, or the `x-amz-server-side-encryption-customer-algorithm` header with a value of `AES256`.

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

BucketStatisticsBySensitivity

Provides aggregated statistical data for sensitive data discovery metrics that apply to S3 buckets, grouped by bucket sensitivity score (`sensitivityScore`). If automated sensitive data discovery is currently disabled for your account, the value for each metric is `0`.

classificationError

The aggregated statistical data for all buckets that have a sensitivity score of `-1`.

Type: SensitivityAggregations
Required: False

notClassified

The aggregated statistical data for all buckets that have a sensitivity score of `50`.

Type: SensitivityAggregations

Required: False

notSensitive

The aggregated statistical data for all buckets that have a sensitivity score of `1-49`.

Type: SensitivityAggregations
Required: False

sensitive

The aggregated statistical data for all buckets that have a sensitivity score of `51-100`.

Type: SensitivityAggregations
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

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. By default, object count and storage size values include data for object parts that are the result of incomplete multipart uploads. For more information, see How Macie monitors Amazon S3 data security in the *Amazon Macie User Guide*.

bucketCount

The total number of buckets.

Type: integer
Required: False
Format: int64

bucketCountByEffectivePermission

The total number of buckets that are publicly accessible due to a combination of permissions settings for each bucket.

Type: BucketCountByEffectivePermission
Required: False

bucketCountByEncryptionType

The total number of buckets whose settings do or don't specify default server-side encryption behavior for objects that are added to the buckets.

Type: BucketCountByEncryptionType
Required: False

bucketCountByObjectEncryptionRequirement

The total number of buckets whose bucket policies do or don't require server-side encryption of objects when objects are added to the buckets.

Type: BucketCountPolicyAllowsUnencryptedObjectUploads
Required: False

bucketCountBySharedAccessType

The total number of buckets that are or aren't shared with other AWS accounts, Amazon CloudFront origin access identities (OAIs), or CloudFront origin access controls (OACs).

Type: BucketCountBySharedAccessType
Required: False

bucketStatisticsBySensitivity

The aggregated sensitive data discovery statistics for the buckets. If automated sensitive data discovery is currently disabled for your account, the value for each statistic is `0`.

Type: BucketStatisticsBySensitivity
Required: False

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, this value is based on the size of the latest version of each applicable object in the 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

lastUpdated

The date and time, in UTC and extended ISO 8601 format, when Amazon Macie most recently retrieved bucket or object metadata from Amazon S3 for the buckets.

Type: string
Required: False
Format: date-time

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, this value is based on the size of the latest version of each object in the buckets. This value doesn't reflect the storage size of all versions of the objects in the buckets.

Type: integer
Required: False
Format: int64

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, this value is based on the size of the latest version of each applicable object in the 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

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
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
Required: False

InternalServerException

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 all the buckets in the query results. If versioning is enabled for a bucket, storage size values are based on the size of the latest version of each applicable object in the bucket.

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

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

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

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

SensitivityAggregations

Provides aggregated statistical data for sensitive data discovery metrics that apply to S3 buckets. Each field contains aggregated data for all the buckets that have a sensitivity score (`sensitivityScore`) of a specified value or within a specified range (`BucketStatisticsBySensitivity`). If automated sensitive data discovery is currently disabled for your account, the value for each field is `0`.

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, this value is based on the size of the latest version of each applicable object in the 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

publiclyAccessibleCount

The total number of buckets that are publicly accessible due to a combination of permissions settings for each bucket.

Type: integer
Required: False
Format: int64

totalCount

The total number of buckets.

Type: integer
Required: False
Format: int64

totalSizeInBytes

The total storage size, in bytes, of the buckets.

If versioning is enabled for any of the buckets, this value is based on the size of the latest version of each object in the buckets. This value doesn't reflect the storage size of all versions of the objects in the buckets.

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

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Data 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, and whether and when that analysis occurred. The data is available for all the AWS resources that Macie monitors and analyzes for your account. If you're the Macie administrator for an organization, this includes resources that your member accounts own.

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, the available statistical data and other information is limited. It includes only 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 the Search Data Sources resource to build, test, and refine runtime criteria for new classification jobs. These criteria can determine which Amazon Simple Storage Service (Amazon S3) general purpose buckets a job analyzes when it runs. For existing classification jobs, you can use this resource to create a snapshot of the S3 general purpose buckets that currently match the criteria. This is because the `SearchResourcesBucketCriteria` structure for this resource is the same as the `S3BucketCriteriaForJob` structure for classification jobs. The exception is the `automatedDiscoveryMonitoringStatus` field. Jobs don't support use of that field in runtime criteria. To learn more about specifying runtime criteria for jobs, see Scope options for jobs in the *Amazon Macie User Guide*.

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 the supported parameters to specify 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`	The request succeeded.

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

Schemas

Request bodies

POST schema

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

```
          }
        }
      ]
    }
  },
  "maxResults": integer,
  "nextToken": "string",
  "sortCriteria": {
    "attributeName": enum,
    "orderBy": enum
  }
}
```

Response bodies

SearchResourcesResponse schema

```
{
  "matchingResources": [
    {
      "matchingBucket": {
        "accountId": "string",
        "automatedDiscoveryMonitoringStatus": enum,
        "bucketName": "string",
        "classifiableObjectCount": integer,
        "classifiableSizeInBytes": integer,
        "errorCode": enum,
        "errorMessage": "string",
        "jobDetails": {
          "isDefinedInJob": enum,
          "isMonitoredByJob": enum,
          "lastJobId": "string",
          "lastJobRunTime": "string"
        },
        "lastAutomatedDiscoveryTime": "string",
        "objectCount": integer,
        "objectCountByEncryptionType": {
          "customerManaged": integer,
          "kmsManaged": integer,
          "s3Managed": integer,
          "unencrypted": integer,
          "unknown": integer
        },
```

```
        "sensitivityScore": integer,
        "sizeInBytes": integer,
        "sizeInBytesCompressed": integer,
        "unclassifiableObjectCount": {
          "fileType": integer,
          "storageClass": integer,
          "total": integer
        },
        "unclassifiableObjectSizeInBytes": {
          "fileType": integer,
          "storageClass": integer,
          "total": integer
        }
      }
    }
  ],
  "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"
}
```

InternalServerException 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

AutomatedDiscoveryMonitoringStatus

Specifies whether automated sensitive data discovery is currently configured to analyze objects in an S3 bucket. Possible values are:

MONITORED
NOT_MONITORED

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

InternalServerException

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 objects in an S3 bucket, and, if so, the details of the job that ran most recently.

isDefinedInJob

Specifies whether any one-time or recurring jobs are configured to analyze objects 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 objects 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`

lastJobId

The unique identifier for the job that ran most recently and is configured to analyze objects 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

MatchingBucket

Provides statistical data and other information about an S3 bucket that Amazon Macie monitors and analyzes for your account. By default, object count and storage size values include data for object parts that are the result of incomplete multipart uploads. For more information, see How Macie monitors Amazon S3 data security in the *Amazon Macie User Guide*.

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. Key exceptions are `accountId` and `bucketName`. To identify the cause of the error, refer to the `errorCode` and `errorMessage` values.

accountId

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

Type: string
Required: False

automatedDiscoveryMonitoringStatus

Specifies whether automated sensitive data discovery is currently configured to analyze objects in the bucket. Possible values are: `MONITORED`, the bucket is included in analyses; and, `NOT_MONITORED`, the bucket is excluded from analyses. If automated sensitive data discovery is disabled for your account, this value is `NOT_MONITORED`.

Type: AutomatedDiscoveryMonitoringStatus
Required: False

bucketName

The name of the bucket.

Type: string
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

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

errorCode

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
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

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
Required: False

lastAutomatedDiscoveryTime

The date and time, in UTC and extended ISO 8601 format, when Amazon Macie most recently analyzed objects in the bucket while performing automated sensitive data discovery. This value is null if automated sensitive data discovery is disabled for your account.

Type: string

Required: False

Format: date-time

objectCount

The total number of objects in the bucket.

Type: integer

Required: False

Format: int64

objectCountByEncryptionType

The total number of objects 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

Required: False

sensitivityScore

The sensitivity score for the bucket, ranging from `-1` (classification error) to `100` (sensitive).

If automated sensitive data discovery has never been enabled for your account or it's been disabled for your organization or your standalone account for more than 30 days, possible values are: `1`, the bucket is empty; or, `50`, the bucket stores objects but it's been excluded from recent analyses.

Type: integer

Required: False

Format: int32

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

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

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
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
Required: False

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
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.

customerManaged

The total number of objects that are encrypted with customer-provided keys. The objects use server-side encryption with customer-provided keys (SSE-C).

Type: integer
Required: False
Format: int64

kmsManaged

The total number of objects that are encrypted with AWS KMS keys, either AWS managed keys or customer managed keys. The objects use dual-layer server-side encryption or server-side encryption with AWS KMS keys (DSSE-KMS or SSE-KMS).

Type: integer
Required: False
Format: int64

s3Managed

The total number of objects that are encrypted with Amazon S3 managed keys. The objects use server-side encryption with Amazon S3 managed keys (SSE-S3).

Type: integer
Required: False
Format: int64

unencrypted

The total number of objects that use client-side encryption or aren't encrypted.

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 all the buckets in the query results. If versioning is enabled for a bucket, storage size values are based on the size of the latest version of each applicable object in the bucket.

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

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

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

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

Required: False

includes

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

Type: SearchResourcesCriteriaBlock

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.

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

Required: False

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

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
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.

bucketCriteria

The filter conditions that determine which S3 buckets to include or exclude from the query results.

Type: SearchResourcesBucketCriteria
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

nextToken

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

Type: string

Required: False

sortCriteria

The criteria to use to sort the results.

Type: SearchResourcesSortCriteria
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.

matchingResources

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

Type: Array of type MatchingResource
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

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
Required: False

key

The property to use in the condition.

Type: SearchResourcesSimpleCriterionKey
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.
- `AUTOMATED_DISCOVERY_MONITORING_STATUS` - A string that represents an enumerated value that Macie defines for the BucketMetadata.automatedDiscoveryMonitoringStatus property of an S3 bucket.
- `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

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
```

AUTOMATED_DISCOVERY_MONITORING_STATUS

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.

attributeName

The property to sort the results by.

Type: SearchResourcesSortAttributeName
Required: False

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`

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
Required: False

tagValues

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

Type: Array of type SearchResourcesTagCriterionPair
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.

key

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

Type: string
Required: False

value

The tag value 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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Finding List

The Finding List resource provides a subset of information about the findings for your Amazon Macie account. A *finding* is a detailed report of a potential issue with the security or privacy of an Amazon Simple Storage Service (Amazon S3) general purpose bucket or sensitive data in an S3 object.

This resource doesn't provide access to all the data for a finding. Instead, it provides only a subset of metadata, primarily the unique identifier for a finding. To retrieve all the data for one or more findings, use the Findings resource.

You can use the Finding List resource to retrieve a subset of information about one or more findings for your account. To customize and refine your query, you can use the supported parameters to specify how to filter, sort, and paginate the results. For more information about filter options, see Filtering findings in the *Amazon Macie User Guide*.

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	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
409	ConflictException	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

POST schema

```
{
  "findingCriteria": {
    "criterion": {
    }
  },
  "maxResults": integer,
  "nextToken": "string",
  "sortCriteria": {
    "attributeName": "string",
    "orderBy": enum
  }
}
```

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"
}
```

InternalServerException 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*.

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

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

gt

The value for the property is greater 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

lt

The value for the property is less than the specified value.

Type: integer
Required: False

Format: int64

lte

The value for the property is less 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

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
Required: False

InternalServerException

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.

findingCriteria

The criteria to use to filter the results.

Type: FindingCriteria
Required: False

maxResults

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

Type: integer
Required: False
Format: int32

nextToken

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

Type: string
Required: False

sortCriteria

The criteria to use to sort the results.

Type: SortCriteria
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 matches 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.

attributeName

The name of the property to sort the results by. Valid values are: `count`, `createdAt`, `policyDetails.action.apiCallDetails.firstSeen`, `policyDetails.action.apiCallDetails.lastSeen`, `resourcesAffected`, `severity.score`, `type`, and `updatedAt`.

Type: string
Required: False

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`

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Finding Samples

The Finding Samples resource provides a set of findings that use example data and placeholder values to help you understand and analyze the types of findings that Amazon Macie can generate. A *finding* is a detailed report of a potential issue with the security or privacy of an Amazon Simple Storage Service (Amazon S3) general purpose bucket or sensitive data in an S3 object. For information about the types of findings that Macie can generate, see Types of 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 review and

work with the samples by using the Amazon Macie API or the Amazon Macie console. Depending on the findings filters and publication settings for your Macie account, you can also work with the samples by using Amazon EventBridge and AWS Security Hub. To help you identify a sample finding, Macie sets the value for the `sample` field of each finding to `true`. For more information about creating and managing sample findings, see Working with sample findings in the *Amazon Macie User Guide*.

You can use the Finding Samples resource to create one or more sample findings. To create only certain types of sample findings, use the supported request parameter to specify each type of sample finding that you want to create.

URI

`/findings/sample`

HTTP methods

POST

Operation ID: `CreateSampleFindings`

Creates sample findings.

Responses

Status code	Response model	Description
`200`	`Empty Schema`	The request succeeded and there isn't any content to include in the body of the response (No Content).
`400`	`ValidationException`	The request failed because the input doesn't satisfy the constraints specified by the service.
`402`	`ServiceQuotaExceededException`	The request failed because fulfilling the request would

Status code	Response model	Description
		exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
409	ConflictException	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	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"
}
```

InternalServerException 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 sample findings to create.

findingTypes

An array of finding types, one for each type of sample finding to create. To create a sample of every type of finding that Amazon Macie supports, don't include this array in your request.

Type: Array of type FindingType
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 findings in the *Amazon Macie User Guide*. Possible 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
Policy:IAMUser/S3BucketSharedWithCloudFront
```

InternalServerException

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Finding Statistics

The Finding 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 the Finding Statistics resource to retrieve (query) aggregated statistical data about findings for your account. To customize and refine your query, you can use the supported

parameters to specify how to filter, group, and sort the query results. For more information about filter options, see Filtering findings in the *Amazon Macie User Guide*.

URI

`/findings/statistics`

HTTP methods

POST

Operation ID: `GetFindingStatistics`

Retrieves (queries) aggregated statistical data about findings.

Responses

Status code	Response model	Description
200	GetFindingStatisticsResponse	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.

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

Schemas

Request bodies

POST schema

```
{
  "findingCriteria": {
    "criterion": {
    }
  },
  "groupBy": enum,
  "size": integer,
  "sortCriteria": {
    "attributeName": enum,
    "orderBy": 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"
}
```

InternalServerException 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*.

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

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

gt

The value for the property is greater 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

lt

The value for the property is less than the specified value.

Type: integer
Required: False
Format: int64

lte

The value for the property is less 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

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

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.

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, `groupKey`, sort the results by the name of each group of results.

Type: FindingStatisticsSortAttributeName

Required: False

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`

GetFindingStatisticsRequest

Specifies criteria for filtering, grouping, sorting, and paginating the results of a query that retrieves aggregated statistical data about findings.

findingCriteria

The criteria to use to filter the query results.

Type: FindingCriteria
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`

size

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 query results.

Type: FindingStatisticsSortCriteria
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 matches the filter criteria specified in the request.

Type: Array of type GroupCount
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

InternalServerException

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 v2
- AWS SDK for Java V2

- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Findings

The Findings resource represents the repository of findings for your Amazon Macie account. A *finding* is a detailed report of a potential issue with the security or privacy of an Amazon Simple Storage Service (Amazon S3) general purpose bucket or sensitive data in an S3 object. Each finding provides details such as a severity rating, information about the affected resource, and when and how Macie found the issue. The severity and details of each finding vary depending on the type and nature of the finding. For information about the types of findings that Macie can generate, see Types of findings in the *Amazon Macie User Guide*.

You can use the Findings resource to retrieve the details of one or more findings for your account. To refine your results, you can use the supported parameters to specify how to sort the results. When you use this resource, you have to specify the unique identifier for each finding to retrieve. To find this identifier, you can use the Finding List resource.

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`	The request succeeded.

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

Schemas

Request bodies

POST schema

```
{
  "findingIds": [
    "string"
  ],
  "sortCriteria": {
    "attributeName": "string",
    "orderBy": enum
  }
}
```

Response bodies

GetFindingsResponse schema

```
{
  "findings": [
    {
      "accountId": "string",
      "archived": boolean,
      "category": enum,
      "classificationDetails": {
        "detailedResultsLocation": "string",
        "jobArn": "string",
        "jobId": "string",
        "originType": enum,
        "result": {
          "additionalOccurrences": boolean,
          "customDataIdentifiers": {
            "detections": [
              {
                "arn": "string",
                "count": integer,
                "name": "string",
                "occurrences": {
                  "cells": [
                    {
                      "cellReference": "string",
                      "column": integer,
                      "columnName": "string",
                      "row": integer
                    }
```

```
                ],
                "lineRanges": [
                  {
                    "end": integer,
                    "start": integer,
                    "startColumn": integer
                  }
                ],
                "offsetRanges": [
                  {
                    "end": integer,
                    "start": integer,
                    "startColumn": integer
                  }
                ],
                "pages": [
                  {
                    "lineRange": {
                      "end": integer,
                      "start": integer,
                      "startColumn": integer
                    },
                    "offsetRange": {
                      "end": integer,
                      "start": integer,
                      "startColumn": integer
                    },
                    "pageNumber": integer
                  }
                ],
                "records": [
                  {
                    "jsonPath": "string",
                    "recordIndex": integer
                  }
                ]
              }
            }
          ],
          "totalCount": integer
        },
        "mimeType": "string",
        "sensitiveData": [
          {
```

```
      "category": enum,
      "detections": [
        {
          "count": integer,
          "occurrences": {
            "cells": [
              {
                "cellReference": "string",
                "column": integer,
                "columnName": "string",
                "row": integer
              }
            ],
            "lineRanges": [
              {
                "end": integer,
                "start": integer,
                "startColumn": integer
              }
            ],
            "offsetRanges": [
              {
                "end": integer,
                "start": integer,
                "startColumn": integer
              }
            ],
            "pages": [
              {
                "lineRange": {
                  "end": integer,
                  "start": integer,
                  "startColumn": integer
                },
                "offsetRange": {
                  "end": integer,
                  "start": integer,
                  "startColumn": integer
                },
                "pageNumber": integer
              }
            ],
            "records": [
              {
```

```
                    "jsonPath": "string",
                    "recordIndex": integer
                  }
                ]
              },
              "type": "string"
            }
          ],
          "totalCount": integer
        }
      ],
      "sizeClassified": integer,
      "status": {
        "code": "string",
        "reason": "string"
      }
    }
  },
  "count": integer,
  "createdAt": "string",
  "description": "string",
  "id": "string",
  "partition": "string",
  "policyDetails": {
    "action": {
      "actionType": enum,
      "apiCallDetails": {
        "api": "string",
        "apiServiceName": "string",
        "firstSeen": "string",
        "lastSeen": "string"
      }
    },
    "actor": {
      "domainDetails": {
        "domainName": "string"
      },
      "ipAddressDetails": {
        "ipAddressV4": "string",
        "ipCity": {
          "name": "string"
        },
        "ipCountry": {
          "code": "string",
```

```
            "name": "string"
          },
          "ipGeoLocation": {
            "lat": number,
            "lon": number
          },
          "ipOwner": {
            "asn": "string",
            "asnOrg": "string",
            "isp": "string",
            "org": "string"
          }
        },
        "userIdentity": {
          "assumedRole": {
            "accessKeyId": "string",
            "accountId": "string",
            "arn": "string",
            "principalId": "string",
            "sessionContext": {
              "attributes": {
                "creationDate": "string",
                "mfaAuthenticated": boolean
              },
              "sessionIssuer": {
                "accountId": "string",
                "arn": "string",
                "principalId": "string",
                "type": "string",
                "userName": "string"
              }
            }
          },
          "awsAccount": {
            "accountId": "string",
            "principalId": "string"
          },
          "awsService": {
            "invokedBy": "string"
          },
          "federatedUser": {
            "accessKeyId": "string",
            "accountId": "string",
            "arn": "string",
```

```
            "principalId": "string",
            "sessionContext": {
              "attributes": {
                "creationDate": "string",
                "mfaAuthenticated": boolean
              },
              "sessionIssuer": {
                "accountId": "string",
                "arn": "string",
                "principalId": "string",
                "type": "string",
                "userName": "string"
              }
            }
          },
          "iamUser": {
            "accountId": "string",
            "arn": "string",
            "principalId": "string",
            "userName": "string"
          },
          "root": {
            "accountId": "string",
            "arn": "string",
            "principalId": "string"
          },
          "type": enum
        }
      }
    },
    "region": "string",
    "resourcesAffected": {
      "s3Bucket": {
        "allowsUnencryptedObjectUploads": enum,
        "arn": "string",
        "createdAt": "string",
        "defaultServerSideEncryption": {
          "encryptionType": enum,
          "kmsMasterKeyId": "string"
        },
        "name": "string",
        "owner": {
          "displayName": "string",
          "id": "string"
```

```
        },
        "publicAccess": {
          "effectivePermission": enum,
          "permissionConfiguration": {
            "accountLevelPermissions": {
              "blockPublicAccess": {
                "blockPublicAcls": boolean,
                "blockPublicPolicy": boolean,
                "ignorePublicAcls": boolean,
                "restrictPublicBuckets": boolean
              }
            },
            "bucketLevelPermissions": {
              "accessControlList": {
                "allowsPublicReadAccess": boolean,
                "allowsPublicWriteAccess": boolean
              },
              "blockPublicAccess": {
                "blockPublicAcls": boolean,
                "blockPublicPolicy": boolean,
                "ignorePublicAcls": boolean,
                "restrictPublicBuckets": boolean
              },
              "bucketPolicy": {
                "allowsPublicReadAccess": boolean,
                "allowsPublicWriteAccess": boolean
              }
            }
          }
        },
        "tags": [
          {
            "key": "string",
            "value": "string"
          }
        ]
      },
      "s3Object": {
        "bucketArn": "string",
        "eTag": "string",
        "extension": "string",
        "key": "string",
        "lastModified": "string",
        "path": "string",
```

```
          "publicAccess": boolean,
          "serverSideEncryption": {
            "encryptionType": enum,
            "kmsMasterKeyId": "string"
          },
          "size": integer,
          "storageClass": enum,
          "tags": [
            {
              "key": "string",
              "value": "string"
            }
          ],
          "versionId": "string"
        }
      },
      "sample": boolean,
      "schemaVersion": "string",
      "severity": {
        "description": enum,
        "score": integer
      },
      "title": "string",
      "type": enum,
      "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"
}
```

InternalServerException 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
Required: False

ApiCallDetails

Provides information about an API operation that an entity invoked for an affected resource.

api

The name of the operation that was invoked most recently and produced the finding.

Type: string
Required: False

apiServiceName

The URL of the AWS service that provides the operation, for example: `s3.amazonaws.com`.

Type: string
Required: False

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

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

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

accountId

The unique identifier for the AWS account that owns 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

principalId

The unique identifier for the entity that was used to get 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
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 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*.

blockPublicAcls

Specifies whether Amazon S3 blocks public access control lists (ACLs) for the bucket and objects in the bucket.

Type: boolean
Required: False

blockPublicPolicy

Specifies whether Amazon S3 blocks public bucket policies for 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

restrictPublicBuckets

Specifies whether Amazon S3 restricts public bucket policies for 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
Required: False

blockPublicAccess

The block public access settings for the bucket.

Type: BlockPublicAccess
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
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
Required: False

bucketLevelPermissions

The bucket-level permissions settings for the bucket.

Type: BucketLevelPermissions
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
Required: False

Cell

Specifies the location of an occurrence of sensitive data in a Microsoft Excel workbook, CSV file, or TSV file.

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

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

columnName

The name of the column that contains the sensitive data, if available.

Type: string
Required: False

row

The row number of the row that contains the sensitive data.

Type: integer
Required: False
Format: int64

ClassificationDetails

Provides information about a sensitive data finding and the details of the finding.

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. This value is null if the origin of the finding (`originType`) is `AUTOMATED_SENSITIVE_DATA_DISCOVERY`.

Type: string
Required: False

jobId

The unique identifier for the classification job that produced the finding. This value is null if the origin of the finding (`originType`) is `AUTOMATED_SENSITIVE_DATA_DISCOVERY`.

Type: string
Required: False

originType

Specifies how Amazon Macie found the sensitive data that produced the finding. Possible values are: `SENSITIVE_DATA_DISCOVERY_JOB`, for a classification job; and, `AUTOMATED_SENSITIVE_DATA_DISCOVERY`, for automated sensitive data discovery.

Type: OriginType
Required: False

result

The status and other details of the finding.

Type: ClassificationResult

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.

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

customDataIdentifiers

The custom data identifiers that detected the sensitive data and the number of occurrences of the data that they detected.

Type: CustomDataIdentifiers
Required: False

mimeType

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

sensitiveData

The category, types, and number of occurrences of the sensitive data that produced the finding.

Type: Array of type SensitiveDataItem

Required: False

sizeClassified

The total size, in bytes, of the data that the finding applies to.

Type: integer

Required: False

Format: int64

status

The status of the finding.

Type: ClassificationResultStatus

Required: False

ClassificationResultStatus

Provides information about the status of a sensitive data finding.

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 that uses an unsupported format.

Type: string

Required: False

reason

A brief description of the status of the finding. This value is null if the status (code) of the finding is COMPLETE.

Amazon Macie uses this value to notify you of any errors, warnings, or considerations that might impact your analysis of the finding and the affected S3 object. Possible values are:

- ARCHIVE_CONTAINS_UNPROCESSED_FILES - The object is an archive file and Macie extracted and analyzed only some or none of the files in the archive. To determine which files Macie analyzed, if any, refer to the corresponding sensitive data discovery result for the finding (classificationDetails.detailedResultsLocation).
- ARCHIVE_EXCEEDS_SIZE_LIMIT - The object is an archive file whose total storage size exceeds the size quota for this type of archive.
- ARCHIVE_NESTING_LEVEL_OVER_LIMIT - The object is an archive file whose nested depth exceeds the quota for the maximum number of nested levels that Macie analyzes for this type of archive.
- ARCHIVE_TOTAL_BYTES_EXTRACTED_OVER_LIMIT - The object is an archive file that exceeds the quota for the maximum amount of data that Macie extracts and analyzes for this type of archive.
- ARCHIVE_TOTAL_DOCUMENTS_PROCESSED_OVER_LIMIT - The object is an archive file that contains more than the maximum number of files that Macie extracts and analyzes for this type of archive.
- FILE_EXCEEDS_SIZE_LIMIT - The storage size of the object exceeds the size quota for this type of file.
- INVALID_ENCRYPTION - The object is encrypted using server-side encryption but Macie isn't allowed to use the key. Macie can't decrypt and analyze the object.
- INVALID_KMS_KEY - The object is encrypted with an AWS KMS key that was disabled or is being deleted. Macie can't decrypt and analyze the object.
- INVALID_OBJECT_STATE - The object doesn't use a supported Amazon S3 storage class.
- JSON_NESTING_LEVEL_OVER_LIMIT - The object contains JSON data and the nested depth of the data exceeds the quota for the number of nested levels that Macie analyzes for this type of file.
- MALFORMED_FILE - The object is a malformed or corrupted file. An error occurred when Macie attempted to detect the file's type or extract data from the file.

- `MALFORMED_OR_FILE_SIZE_EXCEEDS_LIMIT` - The object is a Microsoft Office file that is malformed or exceeds the size quota for this type of file. If the file is malformed, an error occurred when Macie attempted to extract data from the file.
- `NO_SUCH_BUCKET_AVAILABLE` - The object was in a bucket that was deleted shortly before or when Macie attempted to analyze the object.
- `OBJECT_VERSION_MISMATCH` - The object was changed while Macie was analyzing it.
- `OOXML_UNCOMPRESSED_RATIO_EXCEEDS_LIMIT` - The object is an Office Open XML file whose compression ratio exceeds the compression quota for this type of file.
- `OOXML_UNCOMPRESSED_SIZE_EXCEEDS_LIMIT` - The object is an Office Open XML file that exceeds the size quota for this type of file.
- `PERMISSION_DENIED` - Macie isn't allowed to access the object. The object's permissions settings prevent Macie from analyzing the object.
- `SOURCE_OBJECT_NO_LONGER_AVAILABLE` - The object was deleted shortly before or when Macie attempted to analyze it.
- `TIME_CUT_OFF_REACHED` - Macie started analyzing the object but additional analysis would exceed the time quota for analyzing an object.
- `UNABLE_TO_PARSE_FILE` - The object is a file that contains structured data and an error occurred when Macie attempted to parse the data.
- `UNSUPPORTED_FILE_TYPE_EXCEPTION` - The object is a file that uses an unsupported file or storage format.

For information about quotas, supported storage classes, and supported file and storage formats, see Quotas and Supported storage classes and formats in the *Amazon Macie User Guide*.

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.

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
Required: False

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

CustomDetection

Provides information about a custom data identifier that produced a sensitive data finding, and the sensitive data that it detected for the finding.

arn

The unique identifier for the custom data identifier.

Type: string
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

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
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.

count

The total number of occurrences of the type of sensitive data that was detected.

Type: integer
Required: False
Format: int64

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
Required: False

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 server-side encryption algorithm that was used to encrypt an S3 object or is used by default to encrypt objects that are added to an S3 bucket. Possible values are:

`NONE`
`AES256`
`aws:kms`
`UNKNOWN`
`aws:kms:dsse`

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

accountId

The unique identifier for the AWS account that owns 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

principalId

The unique identifier for the entity that was used to get 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
Required: False

Finding

Provides the details of a finding.

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

archived

Specifies whether the finding is archived (suppressed).

Type: boolean
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
Required: False

classificationDetails

The details of a sensitive data finding. This value is null for a policy finding.

Type: ClassificationDetails
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 unique.

Type: integer
Required: False
Format: int64

createdAt

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

Type: string
Required: False
Format: date-time

description

The description of the finding.

Type: string
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

partition

The AWS partition that Amazon Macie created the finding in.

Type: string
Required: False

policyDetails

The details of a policy finding. This value is null for a sensitive data finding.

Type: PolicyDetails
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
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

schemaVersion

The version of the schema that was used to define the data structures in the finding.

Type: string
Required: False

severity

The severity level and score for the finding.

Type: Severity
Required: False

title

The brief description of the finding.

Type: string
Required: False

type

The type of the finding.

Type: FindingType
Required: False

updatedAt

The date and time, in UTC and extended ISO 8601 format, when Amazon Macie last updated the finding. For sensitive data findings, this value is the same as the value for the `createdAt` property. All sensitive data findings are considered new.

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
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
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
Required: False

ipAddressDetails

The IP address and related details about the device that the entity used to perform the action on the affected resource. The details can include information such as the owner and geographic location of the IP address.

Type: IpAddressDetails
Required: False

userIdentity

The type and other characteristics of the entity that performed the action on the affected resource. This value is null if the action was performed by an anonymous (unauthenticated) entity.

Type: UserIdentity
Required: False

FindingCategory

The category of the finding. Possible values are:

CLASSIFICATION
POLICY

FindingType

The type of finding. For details about each type, see Types of findings in the *Amazon Macie User Guide*. Possible 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
Policy:IAMUser/S3BucketSharedWithCloudFront

GetFindingsRequest

Specifies one or more findings to retrieve.

findingIds

An array of strings that lists the unique identifiers for the findings to retrieve. You can specify as many as 50 unique identifiers in this array.

Type: Array of type string
Required: True

sortCriteria

The criteria for sorting the results of the request.

Type: SortCriteria

Required: False

GetFindingsResponse

Provides the results of a request for one or more findings.

findings

An array of objects, one for each finding that matches the criteria specified in the request.

Type: Array of type Finding
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

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

principalId

The unique identifier for the IAM user who performed the action.

Type: string

Required: False

userName

The username of the IAM user who performed the action.

Type: string
Required: False

InternalServerException

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.

ipAddressV4

The Internet Protocol version 4 (IPv4) address of the device.

Type: string
Required: False

ipCity

The city that the IP address originated from.

Type: IpCity
Required: False

ipCountry

The country that the IP address originated from.

Type: IpCountry
Required: False

ipGeoLocation

The geographic coordinates of the location that the IP address originated from.

Type: IpGeoLocation
Required: False

ipOwner

The registered owner of the IP address.

Type: IpOwner
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.

lat

The latitude coordinate of the location, rounded to four decimal places.

Type: number
Required: False

lon

The longitude coordinate of the location, rounded to four decimal places.

Type: number
Required: False

IpOwner

Provides information about the registered owner of an IP address.

asn

The autonomous system number (ASN) for the autonomous system that included 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

org

The name of the organization that owned 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.

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

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

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.

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
Required: False

lineRanges

An array of objects, one for each occurrence of sensitive data in an email message or 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
Required: False

offsetRanges

Reserved for future use.

Type: Array of type Range
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
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
Required: False

OriginType

Specifies how Amazon Macie found the sensitive data that produced a finding. Possible values are:

```
SENSITIVE_DATA_DISCOVERY_JOB
AUTOMATED_SENSITIVE_DATA_DISCOVERY
```

Page

Specifies the location of an occurrence of sensitive data in an Adobe Portable Document Format file.

lineRange

Reserved for future use.

Type: Range

Required: False

offsetRange

Reserved for future use.

Type: Range
Required: False

pageNumber

The page number of the page that contains the sensitive data.

Type: integer
Required: False
Format: int64

PolicyDetails

Provides the details of a policy finding.

action

The action that produced the finding.

Type: FindingAction
Required: False

actor

The entity that performed the action that produced the finding.

Type: FindingActor
Required: False

Range

Specifies the location of an occurrence of sensitive data in an email message or a non-binary text file such as an HTML, TXT, or XML file.

end

The number of lines from the beginning of the file to the end 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

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

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 240 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.

s3Bucket

The details of the S3 bucket that the finding applies to.

Type: S3Bucket
Required: False

s3Object

The details of the S3 object that the finding applies to.

Type: S3Object
Required: False

S3Bucket

Provides information about the S3 bucket that a finding applies to.

allowsUnencryptedObjectUploads

Specifies whether the bucket policy for the bucket requires server-side encryption of objects when objects are added to the bucket. Possible values are:

- `FALSE` - The bucket policy requires server-side encryption of new objects. `PutObject` requests must include a valid server-side encryption header.
- `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 a valid server-side encryption header.
- `UNKNOWN` - Amazon Macie can't determine whether the bucket policy requires server-side encryption of new objects.

Valid server-side encryption headers are: `x-amz-server-side-encryption` with a value of `AES256` or `aws:kms`, and `x-amz-server-side-encryption-customer-algorithm` with a value of `AES256`.

Type: string
Required: False
Values: `TRUE | FALSE | UNKNOWN`

arn

The Amazon Resource Name (ARN) of the bucket.

Type: string
Required: False

createdAt

The date and time, in UTC and extended ISO 8601 format, when the bucket was created. This value can also indicate when changes such as edits to the bucket's policy were most recently made to the bucket, relative to when the finding was created or last updated.

Type: string
Required: False
Format: date-time

defaultServerSideEncryption

The default server-side encryption settings for the bucket.

Type: ServerSideEncryption
Required: False

name

The name of the bucket.

Type: string
Required: False

owner

The display name and canonical user ID for the AWS account that owns the bucket.

Type: S3BucketOwner
Required: False

publicAccess

The permissions settings that determine whether the bucket is publicly accessible.

Type: BucketPublicAccess
Required: False

tags

The tags that are associated with the bucket.

Type: Array of type KeyValuePair
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.

bucketArn

The Amazon Resource Name (ARN) of the bucket that contains the object.

Type: string
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

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

key

The full name (*key*) of the object, including the object's prefix if applicable.

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

path

The full path to the affected object, including the name of the affected bucket and the object's name (key).

Type: string

Required: False

publicAccess

Specifies whether the object is publicly accessible due to the combination of permissions settings that apply to the object.

Type: boolean
Required: False

serverSideEncryption

The type of server-side encryption that was used to encrypt the object.

Type: ServerSideEncryption
Required: False

size

The total storage size, in bytes, of the object.

Type: integer
Required: False
Format: int64

storageClass

The storage class of the object.

Type: StorageClass
Required: False

tags

The tags that are associated with the object.

Type: Array of type KeyValuePair
Required: False

versionId

The identifier for the affected version of the object.

Type: string
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 access 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
Required: False

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
Required: False

totalCount

The total number of occurrences of the sensitive data that was detected.

Type: integer
Required: False
Format: int64

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 default server-side encryption settings for an S3 bucket or the encryption settings for an S3 object.

encryptionType

The server-side encryption algorithm that's used when storing data in the bucket or object. If default encryption settings aren't configured for the bucket or the object isn't encrypted using server-side encryption, this value is `NONE`.

Type: EncryptionType
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.

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
Required: False

sessionIssuer

The source and type of credentials that were issued to the entity.

Type: SessionIssuer
Required: False

SessionContextAttributes

Provides information about the context in which temporary security credentials were issued to an entity.

creationDate

The date and time, in UTC and ISO 8601 format, when the credentials were issued.

Type: string
Required: False
Format: date-time

mfaAuthenticated

Specifies whether the credentials were authenticated with a multi-factor authentication (MFA) device.

Type: boolean
Required: False

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

arn

The Amazon Resource Name (ARN) of the source account, AWS Identity and Access Management (IAM) user, or role 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

type

The source of the temporary security credentials, such as `Root`, `IAMUser`, or `Role`.

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

Severity

Provides the numerical and qualitative representations of a finding's severity.

description

The qualitative representation of the finding's severity, ranging from `Low` (least severe) to `High` (most severe).

Type: SeverityDescription
Required: False

score

The numerical representation of the finding's severity, ranging from `1` (least severe) to `3` (most severe).

Type: integer
Required: False
Format: int64

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.

attributeName

The name of the property to sort the results by. Valid values are: `count`, `createdAt`, `policyDetails.action.apiCallDetails.firstSeen`, `policyDetails.action.apiCallDetails.lastSeen`, `resourcesAffected`, `severity.score`, `type`, and `updatedAt`.

Type: string
Required: False

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`

StorageClass

The storage class of the S3 object. Possible values are:

```
STANDARD
REDUCED_REDUNDANCY
STANDARD_IA
INTELLIGENT_TIERING
DEEP_ARCHIVE
ONEZONE_IA
GLACIER
GLACIER_IR
OUTPOSTS
```

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.

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
Required: False

awsAccount

If the action was performed using the credentials for another AWS account, the details of that account.

Type: AwsAccount
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

Required: False

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
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
Required: False

root

If the action was performed using the credentials for your AWS account, the details of your account.

Type: UserIdentityRoot
Required: False

type

The type of entity that performed the action.

Type: UserIdentityType
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

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

principalId

The unique identifier for the entity 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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Findings - Publication Configuration

The Publication Configuration resource for findings provides settings for publishing findings to AWS Security Hub. With these settings, you can configure Amazon 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 Evaluating findings with AWS 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. It also 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) 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 Publication Configuration resource for findings 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. To specify the publication frequency for these updates, use the Account Administration 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	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.

Status code	Response model	Description
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
409	ConflictException	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	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).

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

Schemas

Request bodies

PUT schema

```
{
  "clientToken": "string",
  "securityHubConfiguration": {
    "publishClassificationFindings": boolean,
    "publishPolicyFindings": boolean
  }
}
```

Response bodies

GetFindingsPublicationConfigurationResponse schema

```
{
  "securityHubConfiguration": {
    "publishClassificationFindings": boolean,
    "publishPolicyFindings": 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"
}
```

InternalServerException 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

Required: False

InternalServerException

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.

clientToken

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

Type: string
Required: False

securityHubConfiguration

The configuration settings that determine which findings to publish to AWS Security Hub.

Type: SecurityHubConfiguration
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 Evaluating findings with AWS Security Hub in the *Amazon Macie User Guide*.

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

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

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutFindingsPublicationConfiguration

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

- AWS SDK for Python
- AWS SDK for Ruby V3

Findings - Reveal Sensitive Data Occurrences

The Reveal Sensitive Data Occurrences resource provides options for retrieving sample occurrences of sensitive data that Amazon Macie reported in a finding. The samples can help you verify the nature of the sensitive data that Macie found. You can also use them to tailor your investigation of the affected Amazon Simple Storage Service (Amazon S3) object or bucket. You can retrieve sensitive data samples in all the AWS Regions where Macie is currently available except the Asia Pacific (Osaka) and Israel (Tel Aviv) Regions.

When you retrieve sensitive data samples, you specify the unique identifier for a particular sensitive data finding. Macie then uses location data in the corresponding sensitive data discovery result to locate and extract sample occurrences of sensitive data from the affected S3 object. Macie encrypts the extracted data with an AWS Key Management Service (AWS KMS) key that you specify, temporarily stores the encrypted data in a cache, and returns the data in your results. Soon after extraction and encryption, Macie permanently deletes the data from the cache unless additional retention is temporarily required to resolve an operational issue.

To retrieve sensitive data samples for a finding, the finding must meet all the following criteria:

- Include one or more `occurrences` objects that indicate the location of specific occurrences of sensitive data in the affected S3 object.
- Specify the location of a valid, corresponding sensitive data discovery result in the `classificationDetails.detailedResultsLocation` field.
- Specify one of the following values in the `mimeType` field: `application/avro`, `application/gzip`, `application/json`, `application/parquet`, `application/vnd.openxmlformats-officedocument.spreadsheetml.sheet`, `application/zip`, `text/csv`, `text/plain`, or `text/tab-separated-values`.

For additional requirements, see Retrieving sensitive data samples with findings in the *Amazon Macie User Guide*.

By using the Reveal Sensitive Data Occurrences resource, you can retrieve sample occurrences of sensitive data that Macie reported in a particular finding. When you use this resource, you have to

specify the unique identifier for the finding that your request applies to. To find this identifier, you can use the Finding List resource.

Before you can use this resource, you have to configure and enable Macie to retrieve sensitive data samples for findings. To do this, use the Reveal Sensitive Data Occurrences Configuration resource.

URI

`/findings/findingId/reveal`

HTTP methods

GET

Operation ID: `GetSensitiveDataOccurrences`

Retrieves occurrences of sensitive data reported by a finding.

Path parameters

Name	Type	Required	Description
findingId	String	True	The unique identifier for the finding.

Responses

Status code	Response model	Description
200	GetSensitiveDataOccurrencesResponse	The request succeeded.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have

Status code	Response model	Description
		sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
422	UnprocessableEntityException	The request failed because it contains instructions that Amazon Macie can't process (Unprocessable Entity).
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Response bodies

GetSensitiveDataOccurrencesResponse schema

```
{
  "error": "string",
  "sensitiveDataOccurrences": {
  },
  "status": enum
}
```

ServiceQuotaExceededException schema

```
{
```

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

AccessDeniedException schema

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

ResourceNotFoundException schema

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

UnprocessableEntityException schema

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

ThrottlingException schema

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

InternalServerException 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

DetectedDataDetails

Specifies 1-10 occurrences of a specific type of sensitive data reported by a finding.

value

An occurrence of the specified type of sensitive data. Each occurrence contains 1-128 characters.

Type: string
Required: True
Format: password
MinLength: 1
MaxLength: 128

GetSensitiveDataOccurrencesResponse

Provides the results of a request to retrieve occurrences of sensitive data reported by a finding.

error

If an error occurred when Amazon Macie attempted to retrieve occurrences of sensitive data reported by the finding, a description of the error that occurred. This value is null if the status (`status`) of the request is `PROCESSING` or `SUCCESS`.

Type: string
Required: False

sensitiveDataOccurrences

A map that specifies 1-100 types of sensitive data reported by the finding and, for each type, 1-10 occurrences of sensitive data.

Type: SensitiveDataOccurrences
Required: False

status

The status of the request to retrieve occurrences of sensitive data reported by the finding. Possible values are:

- `ERROR` - An error occurred when Amazon Macie attempted to locate, retrieve, or encrypt the sensitive data. The `error` value indicates the nature of the error that occurred.
- `PROCESSING` - Macie is processing the request.
- `SUCCESS` - Macie successfully located, retrieved, and encrypted the sensitive data.

Type: RevealRequestStatus
Required: False

InternalServerException

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

RevealRequestStatus

The status of a request to retrieve occurrences of sensitive data reported by a finding. Possible values are:

SUCCESS
PROCESSING
ERROR

SensitiveDataOccurrences

Specifies a type of sensitive data reported by a finding and provides occurrences of the specified type of sensitive data.

key-value pairs

An array of DetectedDataDetails objects. Each object specifies 1-10 occurrences of a specified type of sensitive data.

Type: array

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

UnprocessableEntityException

Provides information about an error that occurred due to an unprocessable entity.

message

The type of error that occurred and prevented Amazon Macie from retrieving occurrences of sensitive data reported by the finding. Possible values are:

- `ACCOUNT_NOT_IN_ORGANIZATION` - The affected account isn't currently part of your organization. Or the account is part of your organization but Macie isn't currently enabled for the account. You're not allowed to access the affected S3 object by using Macie.
- `INVALID_CLASSIFICATION_RESULT` - There isn't a corresponding sensitive data discovery result for the finding. Or the corresponding sensitive data discovery result isn't available in the current AWS Region, is malformed or corrupted, or uses an unsupported storage format. Macie can't verify the location of the sensitive data to retrieve.
- `INVALID_RESULT_SIGNATURE` - The corresponding sensitive data discovery result is stored in an S3 object that wasn't signed by Macie. Macie can't verify the integrity and authenticity of the sensitive data discovery result. Therefore, Macie can't verify the location of the sensitive data to retrieve.
- `MEMBER_ROLE_TOO_PERMISSIVE` - The trust or permissions policy for the IAM role in the affected member account doesn't meet Macie requirements for restricting access to the role. Or the role's trust policy doesn't specify the correct external ID for your organization. Macie can't assume the role to retrieve the sensitive data.
- `MISSING_GET_MEMBER_PERMISSION` - You're not allowed to retrieve information about the association between your account and the affected account. Macie can't determine whether you’re allowed to access the affected S3 object as the delegated Macie administrator for the affected account.
- `OBJECT_EXCEEDS_SIZE_QUOTA` - The storage size of the affected S3 object exceeds the size quota for retrieving occurrences of sensitive data from this type of file.

- `OBJECT_UNAVAILABLE` - The affected S3 object isn't available. The object was renamed, moved, deleted, or changed after Macie created the finding. Or the object is encrypted with an AWS KMS key that isn't available. For example, the key is disabled, is scheduled for deletion, or was deleted.
- `RESULT_NOT_SIGNED` - The corresponding sensitive data discovery result is stored in an S3 object that hasn't been signed. Macie can't verify the integrity and authenticity of the sensitive data discovery result. Therefore, Macie can't verify the location of the sensitive data to retrieve.
- `ROLE_TOO_PERMISSIVE` - Your account is configured to retrieve occurrences of sensitive data by using an IAM role whose trust or permissions policy doesn't meet Macie requirements for restricting access to the role. Macie can't assume the role to retrieve the sensitive data.
- `UNSUPPORTED_FINDING_TYPE` - The specified finding isn't a sensitive data finding.
- `UNSUPPORTED_OBJECT_TYPE` - The affected S3 object uses a file or storage format that Macie doesn't support for retrieving occurrences of sensitive data.

Type: string
Required: True

See also

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

GetSensitiveDataOccurrences

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

Findings - Reveal Sensitive Data Occurrences Availability

The Reveal Sensitive Data Occurrences Availability resource provides an environment for determining whether you can retrieve sample occurrences of sensitive data that Amazon Macie reported in a finding. You can use this resource in all the AWS Regions where Macie is currently available except the Asia Pacific (Osaka) and Israel (Tel Aviv) Regions.

To retrieve sensitive data samples for a finding, the finding must meet all the following criteria:

- Include one or more `occurrences` objects that indicate the location of specific occurrences of sensitive data in the affected Amazon Simple Storage Service (Amazon S3) object.
- Specify the location of a valid, corresponding sensitive data discovery result in the `classificationDetails.detailedResultsLocation` field.
- Specify one of the following values in the `mimeType` field: `application/avro`, `application/gzip`, `application/json`, `application/parquet`, `application/vnd.openxmlformats-officedocument.spreadsheetml.sheet`, `application/zip`, `text/csv`, `text/plain`, or `text/tab-separated-values`.

For additional requirements, see Retrieving sensitive data samples with findings in the *Amazon Macie User Guide*.

By using the Reveal Sensitive Data Occurrences Availability resource, you can determine whether you can retrieve sample occurrences of sensitive data for a particular finding. To use this resource, you have to specify the unique identifier for the finding that your request applies to. To find this identifier, you can use the Finding List resource. If samples are available for a finding, use the Reveal Sensitive Data Occurrences resource to retrieve the samples.

Before you can use this resource, you have to configure and enable Macie to retrieve sensitive data samples for findings. To do this, use the Reveal Sensitive Data Occurrences Configuration resource.

URI

`/findings/findingId/reveal/availability`

HTTP methods

GET

Operation ID: `GetSensitiveDataOccurrencesAvailability`

Checks whether occurrences of sensitive data can be retrieved for a finding.

Path parameters

Name	Type	Required	Description
findingId	String	True	The unique identifier for the finding.

Responses

Status code	Response model	Description
200	GetSensitiveDataOccurrencesAvailabilityResponse	The request succeeded.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Response bodies

GetSensitiveDataOccurrencesAvailabilityResponse schema

```
{
  "code": enum,
  "reasons": [
    enum
  ]
}
```

AccessDeniedException schema

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

ResourceNotFoundException schema

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

ThrottlingException schema

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

InternalServerException 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

AvailabilityCode

Specifies whether occurrences of sensitive data can be retrieved for a finding. Possible values are:

`AVAILABLE`
`UNAVAILABLE`

GetSensitiveDataOccurrencesAvailabilityResponse

Provides information about whether occurrences of sensitive data can be retrieved for a finding and, if not, why the data can't be retrieved.

code

Specifies whether occurrences of sensitive data can be retrieved for the finding. Possible values are: `AVAILABLE`, the sensitive data can be retrieved; and, `UNAVAILABLE`, the sensitive data can't be retrieved. If this value is `UNAVAILABLE`, the `reasons` array indicates why the data can't be retrieved.

Type: AvailabilityCode
Required: True

reasons

Specifies why occurrences of sensitive data can't be retrieved for the finding. Possible values are:

- `ACCOUNT_NOT_IN_ORGANIZATION` - The affected account isn't currently part of your organization. Or the account is part of your organization but Macie isn't currently enabled for the account. You're not allowed to access the affected S3 object by using Macie.
- `INVALID_CLASSIFICATION_RESULT` - There isn't a corresponding sensitive data discovery result for the finding. Or the corresponding sensitive data discovery result isn't available in the

current AWS Region, is malformed or corrupted, or uses an unsupported storage format. Macie can't verify the location of the sensitive data to retrieve.

- `INVALID_RESULT_SIGNATURE` - The corresponding sensitive data discovery result is stored in an S3 object that wasn't signed by Macie. Macie can't verify the integrity and authenticity of the sensitive data discovery result. Therefore, Macie can't verify the location of the sensitive data to retrieve.
- `MEMBER_ROLE_TOO_PERMISSIVE` - The trust or permissions policy for the IAM role in the affected member account doesn't meet Macie requirements for restricting access to the role. Or the role's trust policy doesn't specify the correct external ID for your organization. Macie can't assume the role to retrieve the sensitive data.
- `MISSING_GET_MEMBER_PERMISSION` - You're not allowed to retrieve information about the association between your account and the affected account. Macie can't determine whether you're allowed to access the affected S3 object as the delegated Macie administrator for the affected account.
- `OBJECT_EXCEEDS_SIZE_QUOTA` - The storage size of the affected S3 object exceeds the size quota for retrieving occurrences of sensitive data from this type of file.
- `OBJECT_UNAVAILABLE` - The affected S3 object isn't available. The object was renamed, moved, deleted, or changed after Macie created the finding. Or the object is encrypted with an AWS KMS key that isn't available. For example, the key is disabled, is scheduled for deletion, or was deleted.
- `RESULT_NOT_SIGNED` - The corresponding sensitive data discovery result is stored in an S3 object that hasn't been signed. Macie can't verify the integrity and authenticity of the sensitive data discovery result. Therefore, Macie can't verify the location of the sensitive data to retrieve.
- `ROLE_TOO_PERMISSIVE` - Your account is configured to retrieve occurrences of sensitive data by using an IAM role whose trust or permissions policy doesn't meet Macie requirements for restricting access to the role. Macie can't assume the role to retrieve the sensitive data.
- `UNSUPPORTED_FINDING_TYPE` - The specified finding isn't a sensitive data finding.
- `UNSUPPORTED_OBJECT_TYPE` - The affected S3 object uses a file or storage format that Macie doesn't support for retrieving occurrences of sensitive data.

This value is null if sensitive data can be retrieved for the finding.

Type: Array of type UnavailabilityReasonCode
Required: True
MinItems: 0

InternalServerException

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

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

UnavailabilityReasonCode

Specifies why occurrences of sensitive data can't be retrieved for a finding. Possible values are:

```
OBJECT_EXCEEDS_SIZE_QUOTA
UNSUPPORTED_OBJECT_TYPE
```

```
UNSUPPORTED_FINDING_TYPE
INVALID_CLASSIFICATION_RESULT
OBJECT_UNAVAILABLE
ACCOUNT_NOT_IN_ORGANIZATION
MISSING_GET_MEMBER_PERMISSION
ROLE_TOO_PERMISSIVE
MEMBER_ROLE_TOO_PERMISSIVE
INVALID_RESULT_SIGNATURE
RESULT_NOT_SIGNED
```

See also

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

GetSensitiveDataOccurrencesAvailability

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

Findings - Reveal Sensitive Data Occurrences Configuration

The Reveal Sensitive Data Occurrences Configuration resource provides access to settings for retrieving sample occurrences of sensitive data that Amazon Macie reports in findings. The samples can help you verify the nature of the sensitive data that Macie found. They can also help you tailor your investigation of an affected Amazon Simple Storage Service (Amazon S3) object or bucket. You can retrieve sensitive data samples for findings in all the AWS Regions where Macie is currently available except the Asia Pacific (Osaka) and Israel (Tel Aviv) Regions.

When you retrieve sensitive data samples, you specify the unique identifier for a sensitive data finding. Macie then uses location data in the corresponding sensitive data discovery result to locate and extract sample occurrences of sensitive data from the affected S3 object. Macie encrypts the extracted data with an AWS Key Management Service (AWS KMS) key that you specify, temporarily stores the encrypted data in a cache, and returns the data in your results. Soon after extraction and encryption, Macie permanently deletes the data from the cache unless additional retention is temporarily required to resolve an operational issue.

By using the Reveal Sensitive Data Occurrences Configuration resource, you can specify configuration settings for retrieving sensitive data samples from affected S3 objects. When you configure the settings for your Macie account, you specify how to access affected objects and which AWS KMS key to use to encrypt the samples.

To access affected S3 objects, you have two options. You can configure Macie to use AWS Identity and Access Management (IAM) user credentials or assume an IAM role:

- **Use IAM user credentials** - With this option (`CALLER_CREDENTIALS`), each user of your account uses their individual IAM identity to locate, retrieve, encrypt, and reveal sensitive data samples for a finding.
- **Assume an IAM role** - With this option (`ASSUME_ROLE`), you create an IAM role that delegates access to Macie. You also ensure that the trust and permissions policies for the role meet all requirements for Macie to assume the role. Macie then assumes the role when a user of your account chooses to locate, retrieve, encrypt, and reveal sensitive data samples for a finding.

To encrypt sensitive data samples, configure Macie to use an AWS KMS key that you specify. The KMS key must be a customer managed, symmetric encryption key. It must also be a single-Region key that's enabled in the same AWS Region as your Macie account.

For more information about configuration options and requirements, see Configuring Macie to retrieve sensitive data samples in the *Amazon Macie User Guide*.

In addition to specifying configuration settings, you can use the Reveal Sensitive Data Occurrences Configuration resource to enable or disable the configuration for your Macie account. If you enable the configuration, use the Reveal Sensitive Data Occurrences resource to retrieve sensitive data samples for individual findings.

Before you enable the configuration, verify that you configured Macie to store your sensitive data discovery results in an S3 bucket. Otherwise, you won't be able to retrieve sensitive data

samples for findings. To check your configuration, use the Export Configuration resource for data classification results.

URI

`/reveal-configuration`

HTTP methods

GET

Operation ID: `GetRevealConfiguration`

Retrieves the status and configuration settings for retrieving occurrences of sensitive data reported by findings.

Responses

Status code	Response model	Description
200	GetRevealConfigurationResponse	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	The request failed due to an unknown internal server error, exception, or failure.

PUT

Operation ID: `UpdateRevealConfiguration`

Updates the status and configuration settings for retrieving occurrences of sensitive data reported by findings.

Responses

Status code	Response model	Description
200	UpdateRevealConfigurationResponse	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

PUT schema

```
{
```

```
  "configuration": {
    "kmsKeyId": "string",
    "status": enum
  },
  "retrievalConfiguration": {
    "retrievalMode": enum,
    "roleName": "string"
  }
}
```

Response bodies

GetRevealConfigurationResponse schema

```
{
  "configuration": {
    "kmsKeyId": "string",
    "status": enum
  },
  "retrievalConfiguration": {
    "externalId": "string",
    "retrievalMode": enum,
    "roleName": "string"
  }
}
```

UpdateRevealConfigurationResponse schema

```
{
  "configuration": {
    "kmsKeyId": "string",
    "status": enum
  },
  "retrievalConfiguration": {
    "externalId": "string",
    "retrievalMode": enum,
    "roleName": "string"
  }
}
```

ValidationException schema

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

AccessDeniedException schema

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

ThrottlingException schema

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

InternalServerException 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

GetRevealConfigurationResponse

Provides information about the configuration settings for retrieving occurrences of sensitive data reported by findings, and the status of the configuration for an Amazon Macie account.

configuration

The AWS KMS key that's used to encrypt the sensitive data, and the status of the configuration for the Amazon Macie account.

Type: RevealConfiguration
Required: True

retrievalConfiguration

The access method and settings that are used to retrieve the sensitive data.

Type: RetrievalConfiguration
Required: False

InternalServerException

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

RetrievalConfiguration

Provides information about the access method and settings that are used to retrieve occurrences of sensitive data reported by findings.

externalId

The external ID to specify in the trust policy for the IAM role to assume when retrieving sensitive data from affected S3 objects (`roleName`). This value is null if the value for `retrievalMode` is `CALLER_CREDENTIALS`.

This ID is a unique alphanumeric string that Amazon Macie generates automatically after you configure it to assume an IAM role. For a Macie administrator to retrieve sensitive data from an affected S3 object for a member account, the trust policy for the role in the member account must include an `sts:ExternalId` condition that requires this ID.

Type: string
Required: False

retrievalMode

The access method that's used to retrieve sensitive data from affected S3 objects. Valid values are: `ASSUME_ROLE`, assume an IAM role that is in the affected AWS account and delegates access to Amazon Macie (`roleName`); and, `CALLER_CREDENTIALS`, use the credentials of the IAM user who requests the sensitive data.

Type: RetrievalMode
Required: True

roleName

The name of the IAM role that is in the affected AWS account and Amazon Macie is allowed to assume when retrieving sensitive data from affected S3 objects for the account. This value is null if the value for `retrievalMode` is `CALLER_CREDENTIALS`.

Type: string
Required: False
Pattern: `^[\w+=,.@-]*$`
MinLength: 1
MaxLength: 64

RetrievalMode

The access method to use when retrieving occurrences of sensitive data reported by findings. Valid values are:

`CALLER_CREDENTIALS`
`ASSUME_ROLE`

RevealConfiguration

Specifies the status of the Amazon Macie configuration for retrieving occurrences of sensitive data reported by findings, and the AWS Key Management Service (AWS KMS) key to use to encrypt sensitive data that's retrieved. When you enable the configuration for the first time, your request must specify an AWS KMS key. Otherwise, an error occurs.

kmsKeyId

The Amazon Resource Name (ARN), ID, or alias of the AWS KMS key to use to encrypt sensitive data that's retrieved. The key must be an existing, customer managed, symmetric encryption key that's enabled in the same AWS Region as the Amazon Macie account.

If this value specifies an alias, it must include the following prefix: `alias/`. If this value specifies a key that's owned by another AWS account, it must specify the ARN of the key or the ARN of the key's alias.

Type: string
Required: False
MinLength: 1
MaxLength: 2048

status

The status of the configuration for the Amazon Macie account. In a response, possible values are: `ENABLED`, the configuration is currently enabled for the account; and, `DISABLED`, the configuration is currently disabled for the account. In a request, valid values are: `ENABLED`, enable the configuration for the account; and, `DISABLED`, disable the configuration for the account.

> **Important**
>
> If you disable the configuration, you also permanently delete current settings that specify how to access affected S3 objects. If your current access method is ASSUME_ROLE, Macie also deletes the external ID and role name currently specified for the configuration. These settings can't be recovered after they're deleted.

Type: RevealStatus
Required: True

RevealStatus

The status of the configuration for retrieving occurrences of sensitive data reported by findings. Valid values are:

```
ENABLED
DISABLED
```

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

UpdateRetrievalConfiguration

Specifies the access method and settings to use when retrieving occurrences of sensitive data reported by findings. If your request specifies an AWS Identity and Access Management (IAM) role to assume, Amazon Macie verifies that the role exists and the attached policies are configured correctly. If there's an issue, Macie returns an error. For information about addressing the issue, see Configuration options for retrieving sensitive data samples in the *Amazon Macie User Guide*.

retrievalMode

The access method to use when retrieving sensitive data from affected S3 objects. Valid values are: `ASSUME_ROLE`, assume an IAM role that is in the affected AWS account and delegates access to Amazon Macie; and, `CALLER_CREDENTIALS`, use the credentials of the IAM user who requests the sensitive data. If you specify `ASSUME_ROLE`, also specify the name of an existing IAM role for Macie to assume (`roleName`).

> **Important**
>
> If you change this value from `ASSUME_ROLE` to `CALLER_CREDENTIALS` for an existing configuration, Macie permanently deletes the external ID and role name currently specified for the configuration. These settings can't be recovered after they're deleted.

Type: RetrievalMode
Required: True

roleName

The name of the IAM role that is in the affected AWS account and Amazon Macie is allowed to assume when retrieving sensitive data from affected S3 objects for the account. The trust and permissions policies for the role must meet all requirements for Macie to assume the role.

Type: string
Required: False
Pattern: `^[\w+=,.@-]*$`
MinLength: 1
MaxLength: 64

UpdateRevealConfigurationRequest

Specifies configuration settings for retrieving occurrences of sensitive data reported by findings, and the status of the configuration for an Amazon Macie account. If you don't specify `retrievalConfiguration` settings for an existing configuration, Macie sets the access method to `CALLER_CREDENTIALS`. If your current access method is `ASSUME_ROLE`, Macie also deletes the external ID and role name currently specified for the configuration. To keep these settings for an existing configuration, specify your current `retrievalConfiguration` settings in your request.

configuration

The AWS KMS key to use to encrypt the sensitive data, and the status of the configuration for the Amazon Macie account.

Type: RevealConfiguration
Required: True

retrievalConfiguration

The access method and settings to use when retrieving the sensitive data.

Type: UpdateRetrievalConfiguration
Required: False

UpdateRevealConfigurationResponse

Provides information about updated configuration settings for retrieving occurrences of sensitive data reported by findings, and the status of the configuration for an Amazon Macie account.

configuration

The AWS KMS key to use to encrypt the sensitive data, and the status of the configuration for the Amazon Macie account.

Type: RevealConfiguration
Required: True

retrievalConfiguration

The access method and settings to use when retrieving the sensitive data.

Type: RetrievalConfiguration
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:

GetRevealConfiguration

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

UpdateRevealConfiguration

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

- AWS SDK for Ruby V3

Findings Filter

The Findings Filter resource represents an individual filter that you created and saved to review, 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 match the filter's criteria. For example, you can configure a filter to suppress (automatically archive) findings that match 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 resource.

URI

`/findingsfilters/id`

HTTP methods

DELETE

Operation ID: `DeleteFindingsFilter`

Deletes a findings filter.

Path parameters

Name	Type	Required	Description
id	String	True	The unique identifier for the Amazon Macie resource that the request applies to.

Responses

Status code	Response model	Description
200	Empty Schema	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	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
409	ConflictException	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.

Status code	Response model	Description
500	InternalServerException	The request failed due to an unknown internal server error, exception, or failure.

GET

Operation ID: `GetFindingsFilter`

Retrieves the criteria and other settings for a findings filter.

Path parameters

Name	Type	Required	Description
id	String	True	The unique identifier for the Amazon Macie resource that the request applies to.

Responses

Status code	Response model	Description
200	GetFindingsFilterResponse	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.

Status code	Response model	Description
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
409	ConflictException	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	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
id	String	True	The unique identifier for the Amazon Macie resource that the request applies to.

Responses

Status code	Response model	Description
200	UpdateFindingsFilterResponse	The request succeeded. The specified findings filter was updated.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
409	ConflictException	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.

Status code	Response model	Description
500	InternalServerException	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

PATCH schema

```
{
  "action": enum,
  "clientToken": "string",
  "description": "string",
  "findingCriteria": {
    "criterion": {
    }
  },
  "name": "string",
  "position": integer
}
```

Response bodies

Empty Schema schema

```
{
}
```

GetFindingsFilterResponse schema

```
{
  "action": enum,
  "arn": "string",
  "description": "string",
  "findingCriteria": {
    "criterion": {
```

```
    }
  },
  "id": "string",
  "name": "string",
  "position": integer,
  "tags": {
  }
}
```

UpdateFindingsFilterResponse schema

```
{
  "arn": "string",
  "id": "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"
}
```

InternalServerException 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*.

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

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

gt

The value for the property is greater 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

lt

The value for the property is less than the specified value.

Type: integer
Required: False
Format: int64

lte

The value for the property is less 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

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
Required: False

FindingsFilterAction

The action to perform on findings that match the filter criteria. To suppress (automatically archive) findings that match 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.

action

The action that's performed on findings that match 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
Required: False

arn

The Amazon Resource Name (ARN) of the filter.

Type: string
Required: False

description

The custom description of the filter.

Type: string
Required: False

findingCriteria

The criteria that's used to filter findings.

Type: FindingCriteria
Required: False

id

The unique identifier for the filter.

Type: string
Required: False

name

The custom name 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

tags

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

Type: TagMap
Required: False

InternalServerException

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 an Amazon Macie resource.

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.

action

The action to perform on findings that match 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
Required: False

clientToken

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

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 of your account might be able to see this description, depending on the actions that they're allowed to perform in Amazon Macie.

Type: string
Required: False

findingCriteria

The criteria to use to filter findings.

Type: FindingCriteria
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 this name, depending on the actions that they're allowed to perform in Amazon Macie.

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

UpdateFindingsFilterResponse

Provides information about a findings filter that was updated in response to a request.

arn

The Amazon Resource Name (ARN) of the filter that was updated.

Type: string
Required: False

id

The unique identifier for 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:

DeleteFindingsFilter

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

GetFindingsFilter

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2

- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateFindingsFilter

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

Findings Filters

The Findings Filters resource represents the repository of filters that you create and save to review, 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 match the filter's criteria. For example, you can configure a filter to suppress (automatically archive) findings that match 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 Amazon Macie account. To update, delete, or retrieve detailed information about an individual filter, use the Findings Filter 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
`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`	`ListFindingsFilterSResponse`	The request succeeded.
`400`	`ValidationException`	The request failed because the input doesn't satisfy the constraints specified by the service.
`402`	`ServiceQuotaExceededException`	The request failed because fulfilling the request would

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

Schemas

Request bodies

POST schema

```
{
  "action": enum,
  "clientToken": "string",
  "description": "string",
  "findingCriteria": {
    "criterion": {
    }
  },
  "name": "string",
  "position": integer,
  "tags": {
  }
}
```

Response bodies

ListFindingsFiltersResponse schema

```
{
  "findingsFilterListItems": [
    {
      "action": enum,
      "arn": "string",
      "id": "string",
      "name": "string",
      "tags": {
      }
    }
  ],
  "nextToken": "string"
}
```

CreateFindingsFilterResponse schema

```
{
```

```
  "arn": "string",
  "id": "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"
}
```

InternalServerException 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.

action

The action to perform on findings that match 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
Required: True

clientToken

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

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 of your account might be able to see this description, depending on the actions that they're allowed to perform in Amazon Macie.

Type: string
Required: False

findingCriteria

The criteria to use to filter findings.

Type: FindingCriteria
Required: True

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 this name, depending on the actions that they're allowed to perform in Amazon Macie.

Type: string
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
Required: False

CreateFindingsFilterResponse

Provides information about a findings filter that was created in response to a request.

arn

The Amazon Resource Name (ARN) of the filter that was created.

Type: string
Required: False

id

The unique identifier for 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*.

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

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

gt

The value for the property is greater 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

lt

The value for the property is less than the specified value.

Type: integer
Required: False
Format: int64

lte

The value for the property is less 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

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
Required: False

FindingsFilterAction

The action to perform on findings that match the filter criteria. To suppress (automatically archive) findings that match the criteria, set this value to `ARCHIVE`. Valid values are:

```
ARCHIVE
NOOP
```

FindingsFilterListItem

Provides information about a findings filter.

action

The action that's performed on findings that match the filter criteria. Possible values are: `ARCHIVE`, suppress (automatically archive) the findings; and, `NOOP`, don't perform any action on the findings.

Type: FindingsFilterAction
Required: False

arn

The Amazon Resource Name (ARN) of the filter.

Type: string
Required: False

id

The unique identifier for the filter.

Type: string
Required: False

name

The custom name of the filter.

Type: string
Required: False

tags

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

Type: TagMap
Required: False

InternalServerException

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.

findingsFilterListItems

An array of objects, one for each filter that's associated with the account.

Type: Array of type FindingsFilterListItem
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

TagMap

A string-to-string map of key-value pairs that specifies the tags (keys and values) for an Amazon Macie resource.

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateFindingsFilter

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

Invitation Acceptance

In Amazon Macie, an *invitation*, also referred to as a *membership invitation*, is a request to become a member of an organization in Macie. An *organization* is a set of Macie accounts that are centrally managed as a group of related accounts. For more information, see Managing multiple accounts in the *Amazon Macie User Guide*.

You can use the Invitation Acceptance resource to access membership invitations that you've received and haven't responded to, and to accept one of those invitations. To accept an invitation, you have to specify the unique identifier for the invitation and the account ID for the AWS account that sent the invitation. To find these IDs, you can use the Invitation List 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	The request succeeded and there isn't any content to include in the body of the response (No Content).
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.

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

Schemas

Request bodies

POST schema

```
{
  "administratorAccountId": "string",
  "invitationId": "string",
  "masterAccount": "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"
}
```

InternalServerException 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.

administratorAccountId

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

Type: string
Required: False

invitationId

The unique identifier for the invitation to accept.

Type: string
Required: True

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

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).

InternalServerException

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Invitation Count

In Amazon Macie, an *invitation*, also referred to as a *membership invitation*, is a request to become a member of an organization in Macie. An *organization* is a set of Macie accounts that are centrally managed as a group of related accounts. For more information, see Managing multiple accounts in the *Amazon Macie User Guide*.

You can use the Invitation Count resource to retrieve the total number of Macie membership invitations that you've received and haven't deleted. If you accepted an invitation to join your current organization, this number doesn't include that 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	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
409	ConflictException	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.

Status code	Response model	Description
500	InternalServerException	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"
}
```

InternalServerException 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

InternalServerException

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Invitation Decline

In Amazon Macie, an *invitation*, also referred to as a *membership invitation*, is a request to become a member of an organization in Macie. An *organization* is a set of Macie accounts that are centrally managed as a group of related accounts. For more information, see Managing multiple accounts in the *Amazon Macie User Guide*.

You can use the Invitation Decline resource to access membership invitations that you've received and haven't responded to, and to decline one or more of those invitations. To decline an invitation, you have to specify the account ID for the AWS account that sent the invitation. To find this ID, you can use the Invitation List resource. After you decline an invitation, you can optionally delete it by using the Invitation Deletion 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	The request succeeded. Processing might not be complete.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
409	ConflictException	The request failed because it conflicts with the current state of the specified resource.

Status code	Response model	Description
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	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",
      "errorCode": enum,
      "errorMessage": "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"
}
```

InternalServerException 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
Required: False

ErrorCode

The source of an issue or delay. Possible values are:

```
ClientError
InternalError
```

InternalServerException

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

errorCode

The source of the issue or delay in processing the request.

Type: ErrorCode
Required: False

errorMessage

The reason why the request hasn't been processed.

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:

DeclineInvitations

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

Invitation Deletion

In Amazon Macie, an *invitation*, also referred to as a *membership invitation*, is a request to become a member of an organization in Macie. An *organization* is a set of Macie accounts that are centrally managed as a group of related accounts. For more information, see Managing multiple accounts in the *Amazon Macie User Guide*.

You can use the Invitation Deletion resource to access membership invitations that you've received and declined, and to delete one or more of those invitations. If you accepted an invitation to join your current organization, you cannot delete that invitation.

To delete an invitation, you have to specify the account ID for the AWS account that sent the invitation. To find this ID, you can use the Invitation List 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	The request succeeded. Processing might not be complete.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would

Status code	Response model	Description
		exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
409	ConflictException	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	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",
      "errorCode": enum,
      "errorMessage": "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"
}
```

InternalServerException 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
Required: False

ErrorCode

The source of an issue or delay. Possible values are:

```
ClientError
InternalError
```

InternalServerException

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

errorCode

The source of the issue or delay in processing the request.

Type: ErrorCode
Required: False

errorMessage

The reason why the request hasn't been processed.

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:

DeleteInvitations

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

Invitation List

In Amazon Macie, an *invitation*, also referred to as a *membership invitation*, is a request to become a member of an organization in Macie. An *organization* is a set of Macie accounts that are centrally managed as a group of related accounts. For more information, see Managing multiple accounts in the *Amazon Macie User Guide*.

You can use the Invitation List resource to retrieve information about all the Macie membership invitations that you've received and haven't deleted. For each invitation, this information includes:

- The unique identifier for the invitation.
- The account ID for the AWS account that sent the invitation.
- The current status of the relationship between your account and the account that sent the invitation.

You can also use this resource to send a membership invitation to other AWS accounts. To send an invitation to another account, you first have to associate the account with your account. You can do this by using the Members resource.

URI

`/invitations`

HTTP methods

GET

Operation ID: `ListInvitations`

Retrieves information about 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`	The request succeeded.
`400`	`ValidationException`	The request failed because the input doesn't satisfy the constraints specified by the service.
`402`	`ServiceQuotaExceededException`	The request failed because fulfilling the request would

Status code	Response model	Description
		exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
409	ConflictException	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	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	The request succeeded. Processing might not be complete.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
409	ConflictException	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.

Status code	Response model	Description
500	InternalServerException	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

POST schema

```
{
  "accountIds": [
    "string"
  ],
  "disableEmailNotification": boolean,
  "message": "string"
}
```

Response bodies

ListInvitationsResponse schema

```
{
  "invitations": [
    {
      "accountId": "string",
      "invitationId": "string",
      "invitedAt": "string",
      "relationshipStatus": enum
    }
  ],
  "nextToken": "string"
}
```

CreateInvitationsResponse schema

```
{
```

```
  "unprocessedAccounts": [
    {
      "accountId": "string",
      "errorCode": enum,
      "errorMessage": "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"
}
```

InternalServerException 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. When you send an invitation, Macie notifies the recipient by creating an AWS Health event for the recipient's account and, if Macie is already enabled for the account, displaying an **Accounts** badge and notification on the recipient's console. You can optionally notify the recipient by also sending the invitation as an email message.

accountIds

An array that lists AWS account IDs, one for each account to send the invitation to.

Type: Array of type string
Required: True

disableEmailNotification

Specifies whether to send the invitation as an email message. If this value is `false`, Amazon Macie sends the invitation (as an email message) to the email address that you specified for the recipient's account when you associated the account with your account. The default value is `false`.

Type: boolean
Required: False

message

Custom text to include in the email message that contains the invitation. The text can contain as many as 80 alphanumeric characters.

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
Required: False

ErrorCode

The source of an issue or delay. Possible values are:

```
ClientError
InternalError
```

InternalServerException

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.

accountId

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

Type: string
Required: False

invitationId

The unique identifier for the invitation.

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 status of the relationship between the account that sent the invitation and the account that received the invitation.

Type: RelationshipStatus
Required: False

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
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. 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

errorCode

The source of the issue or delay in processing the request.

Type: ErrorCode
Required: False

errorMessage

The reason why the request hasn't been processed.

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:

ListInvitations

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

CreateInvitations

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2

- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

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 are designed to detect a specific type of sensitive data. The types include credit card numbers, AWS secret access keys, and passport numbers for particular countries and regions. Managed data identifiers can detect a large and growing list of sensitive data types for many countries and regions, including multiple types of personally identifiable information (PII), financial information, and credentials data. 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, create and run classification jobs. If you're the Macie administrator for an organization or you have a standalone Macie account, you can also enable automated sensitive data discovery. Both options provide settings for specifying which managed data identifiers you want Macie to use when it analyzes objects in Amazon Simple Storage Service (Amazon S3) buckets. When you configure the settings, you specify the unique identifier (ID) for one or more managed data identifiers. You can use this resource to determine which IDs to specify.

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

```
{
  "items": [
    {
      "category": enum,
      "id": "string"
    }
  ],
  "nextToken": "string"
}
```

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.

items

An array of objects, one for each managed data identifier.

Type: Array of type ManagedDataIdentifierSummary
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

ManagedDataIdentifierSummary

Provides information about a managed data identifier. For additional information, see Using managed data identifiers in the *Amazon Macie User Guide*.

category

The category of sensitive data that the managed data identifier detects: `CREDENTIALS`, for credentials data such as private keys or AWS secret access 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

Required: False

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

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Master Account

This resource has been deprecated and is retained only for backward compatibility. It provides information about the Amazon Macie administrator account for your account. To retrieve information about the Macie administrator account for your account, use the Administrator resource instead of this resource. To learn about the relationship between your account and its Macie administrator account, see Managing multiple accounts in the *Amazon Macie User Guide*.

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 operation.

Responses

Status code	Response model	Description
200	GetMasterAccountResponse	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would

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

Schemas

Response bodies

GetMasterAccountResponse schema

```
{
  "master": {
    "accountId": "string",
    "invitationId": "string",
    "invitedAt": "string",
```

```
    "relationshipStatus": 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"
}
```

InternalServerException 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
Required: False

InternalServerException

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.

accountId

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

Type: string
Required: False

invitationId

The unique identifier for the invitation.

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 status of the relationship between the account that sent the invitation and the account that received the invitation.

Type: RelationshipStatus
Required: False

RelationshipStatus

The current status of the relationship between an account and an associated Amazon Macie administrator 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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Master Disassociation

This resource has been deprecated and is retained only for backward compatibility. If you joined an organization by accepting an Amazon Macie membership invitation, use the Administrator Disassociation resource instead of this resource to disassociate your Macie account from its Macie administrator account. To learn more about disassociating your account from its administrator account, see Managing your membership in an organization in the *Amazon Macie User Guide*.

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 operation.

Responses

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

Status code	Response model	Description
500	InternalServerException	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"
}
```

InternalServerException 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).

InternalServerException

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Member

The Member resource provides information about an individual account that's currently 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 and the email address that you sent it to. For information about the relationship between administrator and member accounts, see Managing multiple accounts in the *Amazon Macie User Guide*.

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 resource.

URI

`/members/id`

HTTP methods

DELETE

Operation ID: `DeleteMember`

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

Path parameters

Name	Type	Required	Description
id	String	True	The unique identifier for the Amazon Macie resource that the request applies to.

Responses

Status code	Response model	Description
200	Empty Schema	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	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.

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

GET

Operation ID: `GetMember`

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

Path parameters

Name	Type	Required	Description
id	String	True	The unique identifier for the Amazon Macie resource that the request applies to.

Responses

Status code	Response model	Description
200	GetMemberResponse	The request succeeded.

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

Schemas

Response bodies

Empty Schema schema

```
{
}
```

GetMemberResponse schema

```
{
  "accountId": "string",
  "administratorAccountId": "string",
  "arn": "string",
  "email": "string",
  "invitedAt": "string",
  "masterAccountId": "string",
  "relationshipStatus": enum,
  "tags": {
  },
  "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"
}
```

InternalServerException 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

administratorAccountId

The AWS account ID for the administrator account.

Type: string
Required: False

arn

The Amazon Resource Name (ARN) of the account.

Type: string

Required: False

email

The email address for the account. This value is null if the account is associated with the administrator account through AWS Organizations.

Type: string

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 membership invitation hasn't been sent to the account.

Type: string

Required: False

Format: date-time

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

relationshipStatus

The current status of the relationship between the account and the administrator account.

Type: RelationshipStatus

Required: False

tags

A map of key-value pairs that specifies which tags (keys and values) are associated with the account in Amazon Macie.

Type: TagMap
Required: False

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

InternalServerException

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. 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 an Amazon Macie resource.

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:

DeleteMember

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

- AWS SDK for Ruby V3

GetMember

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

Member Disassociation

The Member Disassociation resource provides access to associations between an Amazon Macie administrator account and its member accounts. If you're a Macie administrator, you can use this resource to disassociate a member account from your account. For information about managing relationships between administrator and member accounts, see Managing multiple accounts in the *Amazon Macie User Guide*.

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 resource.

If you have a member account and you want to disassociate your account from its Macie administrator account, use the Administrator Disassociation 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
id	String	True	The unique identifier for the Amazon Macie resource that the request applies to.

Responses

Status code	Response model	Description
200	Empty Schema	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
409	ConflictException	The request failed because it conflicts with the current

Status code	Response model	Description
		state of the specified resource.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	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"
}
```

InternalServerException 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).

InternalServerException

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Member Status

The Member Status resource provides access to the status of Amazon Macie for a member account in an organization. If you're the delegated Macie administrator for an organization in AWS Organizations, you can use this resource to manage the status of Macie for a member account in your organization. For more information, see Managing multiple accounts with AWS Organizations in the *Amazon Macie User Guide*.

If you suspend Macie for an account, Macie stops performing all activities and cancels all classification jobs for that account. However, the service retains the session identifier, settings, and resources for the account. For example, the account's findings remain intact and aren't affected for up to 90 days. If you later re-enable Macie for the account, Macie resumes all activities for the account. For more information, see Managing member accounts for an organization in the *Amazon Macie User Guide*.

URI

`/macie/members/id`

HTTP methods

PATCH

Operation ID: `UpdateMemberSession`

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

Path parameters

Name	Type	Required	Description
id	String	True	The unique identifier for the Amazon Macie resource that the request applies to.

Responses

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

Status code	Response model	Description
409	ConflictException	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	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"
}
```

InternalServerException 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).

InternalServerException

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 Amazon Macie for a 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
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 v2

- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Members

The Members resource provides information about all the accounts that are currently associated with your Amazon Macie account, typically a Macie administrator account. 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 and the email address that you sent it to. For information about the relationship between administrator and member accounts, see Managing multiple accounts in the *Amazon Macie User Guide*.

If you want to associate additional accounts with your Macie account, you can use this resource to do so. You can then invite those accounts to enable Macie and allow you to administer and manage Macie on their behalf. For more information, see Managing multiple accounts by invitation in the *Amazon Macie User Guide*.

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 administr ator account. By default, the response includes only current member accounts. To include all accounts, set this value to false.
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	ListMembersResponse	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the

Status code	Response model	Description
		constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
409	ConflictException	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	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	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
409	ConflictException	The request failed because it conflicts with the current state of the specified resource.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	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

```
{
  "members": [
    {
      "accountId": "string",
      "administratorAccountId": "string",
      "arn": "string",
      "email": "string",
      "invitedAt": "string",
      "masterAccountId": "string",
      "relationshipStatus": enum,
      "tags": {
      },
      "updatedAt": "string"
    }
  ],
  "nextToken": "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"
}
```

InternalServerException 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
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
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

InternalServerException

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.

members

An array of objects, one for each account that's associated with the administrator account and matches the criteria specified in the request.

Type: Array of type Member
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

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

administratorAccountId

The AWS account ID for the administrator account.

Type: string
Required: False

arn

The Amazon Resource Name (ARN) of the account.

Type: string
Required: False

email

The email address for the account. This value is null if the account is associated with the administrator account through AWS Organizations.

Type: string
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 membership invitation hasn't been sent to the account.

Type: string

Required: False

Format: date-time

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

relationshipStatus

The current status of the relationship between the account and the administrator account.

Type: RelationshipStatus

Required: False

tags

A map of key-value pairs that specifies which tags (keys and values) are associated with the account in Amazon Macie.

Type: TagMap

Required: False

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. 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 an Amazon Macie resource.

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateMember

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

Resource Sensitivity Profile

The Resource Sensitivity Profile resource provides statistical data for sensitive data discovery metrics that apply to individual Amazon Simple Storage Service (Amazon S3) buckets for your account. If you're the Amazon Macie administrator for an organization, this includes S3 buckets that your member accounts own.

For each S3 bucket, the data includes metrics such as:

- The number of objects that Amazon Macie has analyzed.
- The number of objects that Macie has found sensitive data in.
- The number of occurrences of sensitive data that Macie has found.

The data captures the results of automated sensitive data discovery activities that Macie has performed for an S3 bucket. For more information, see Performing automated sensitive data discovery in the *Amazon Macie User Guide*.

This resource also provides access to the sensitivity score for individual S3 buckets. By default, Macie calculates this score based on the intersection of two primary dimensions: the amount of data that Macie has analyzed in a bucket, and the amount of sensitive data that Macie has found in a bucket. If you're a Macie administrator or you have a standalone Macie account, you can optionally override the calculated score for a bucket. You can assign the maximum score (`100`), which also applies the *Sensitive* label to the bucket. If you override the calculated score, Macie continues to perform automated sensitive data discovery for the bucket. However, later analyses don't affect the bucket's score.

You can use the Resource Sensitivity Profile resource to retrieve (query) sensitive data discovery statistics and the sensitivity score for an S3 bucket. If you're a Macie administrator or you have a standalone Macie account, you can also use this resource to change the sensitivity score for a bucket.

To use this resource, you must first enable automated sensitive data discovery. To enable it for an organization or a standalone account, use the Configuration resource for automated sensitive data discovery. To enable it for a member account in an organization, use the Accounts resource for automated sensitive data discovery.

URI

`/resource-profiles`

HTTP methods

GET

Operation ID: `GetResourceProfile`

Retrieves (queries) sensitive data discovery statistics and the sensitivity score for an S3 bucket.

Query parameters

Name	Type	Required	Description
resourceArn	String	True	The Amazon Resource Name (ARN) of the S3 bucket that the request applies to.

Responses

Status code	Response model	Description
200	GetResourceProfileResponse	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.

Status code	Response model	Description
500	InternalServerException	The request failed due to an unknown internal server error, exception, or failure.

PATCH

Operation ID: UpdateResourceProfile

Updates the sensitivity score for an S3 bucket.

Query parameters

Name	Type	Required	Description
resourceArn	String	True	The Amazon Resource Name (ARN) of the S3 bucket that the request applies to.

Responses

Status code	Response model	Description
200	Empty Schema	The request succeeded. The S3 bucket's sensitivity score was updated and there isn't any content to include in the body of the response (No Content).
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.

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

Schemas

Request bodies

PATCH schema

```
{
  "sensitivityScoreOverride": integer
}
```

Response bodies

GetResourceProfileResponse schema

```
{
  "profileUpdatedAt": "string",
  "sensitivityScore": integer,
  "sensitivityScoreOverridden": boolean,
  "statistics": {
    "totalBytesClassified": integer,
    "totalDetections": integer,
    "totalDetectionsSuppressed": integer,
    "totalItemsClassified": integer,
    "totalItemsSensitive": integer,
    "totalItemsSkipped": integer,
    "totalItemsSkippedInvalidEncryption": integer,
    "totalItemsSkippedInvalidKms": integer,
    "totalItemsSkippedPermissionDenied": integer
  }
}
```

Empty Schema schema

```
{
}
```

ValidationException schema

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

ServiceQuotaExceededException schema

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

AccessDeniedException schema

```
{
```

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

ResourceNotFoundException schema

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

ThrottlingException schema

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

InternalServerException 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

Empty

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

GetResourceProfileResponse

Provides sensitive data discovery statistics and the sensitivity score for an S3 bucket that Amazon Macie monitors and analyzes for an account. This data is available only if automated sensitive data discovery has been enabled for the account.

profileUpdatedAt

The date and time, in UTC and extended ISO 8601 format, when Amazon Macie most recently recalculated sensitive data discovery statistics and details for the bucket. If the bucket's sensitivity score is calculated automatically, this includes the score.

Type: string
Required: True
Format: date-time

sensitivityScore

The current sensitivity score for the bucket, ranging from `-1` (classification error) to `100` (sensitive). By default, this score is calculated automatically based on the amount of data that Amazon Macie has analyzed in the bucket and the amount of sensitive data that Macie has found in the bucket.

Type: integer
Required: True
Format: int32

sensitivityScoreOverridden

Specifies whether the bucket's current sensitivity score was set manually. If this value is `true`, the score was manually changed to `100`. If this value is `false`, the score was calculated automatically by Amazon Macie.

Type: boolean
Required: False

statistics

The sensitive data discovery statistics for the bucket. The statistics capture the results of automated sensitive data discovery activities that Amazon Macie has performed for the bucket.

Type: ResourceStatistics
Required: True

InternalServerException

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

ResourceStatistics

Provides statistical data for sensitive data discovery metrics that apply to an S3 bucket that Amazon Macie monitors and analyzes for an account, if automated sensitive data discovery has been enabled for the account. The data captures the results of automated sensitive data discovery activities that Macie has performed for the bucket.

totalBytesClassified

The total amount of data, in bytes, that Amazon Macie has analyzed in the bucket.

Type: integer
Required: False

Format: int64

totalDetections

The total number of occurrences of sensitive data that Amazon Macie has found in the bucket's objects. This includes occurrences that are currently suppressed by the sensitivity scoring settings for the bucket (`totalDetectionsSuppressed`).

Type: integer
Required: False
Format: int64

totalDetectionsSuppressed

The total number of occurrences of sensitive data that are currently suppressed by the sensitivity scoring settings for the bucket. These represent occurrences of sensitive data that Amazon Macie found in the bucket's objects, but the occurrences were manually suppressed. By default, suppressed occurrences are excluded from the bucket's sensitivity score.

Type: integer
Required: False
Format: int64

totalItemsClassified

The total number of objects that Amazon Macie has analyzed in the bucket.

Type: integer
Required: False
Format: int64

totalItemsSensitive

The total number of the bucket's objects that Amazon Macie has found sensitive data in.

Type: integer
Required: False
Format: int64

totalItemsSkipped

The total number of objects that Amazon Macie wasn't able to analyze in the bucket due to an object-level issue or error. For example, an object is a malformed file. This value includes objects that Macie wasn't able to analyze for reasons reported by other statistics in the `ResourceStatistics` object.

Type: integer
Required: False
Format: int64

totalItemsSkippedInvalidEncryption

The total number of objects that Amazon Macie wasn't able to analyze in the bucket because the objects are encrypted with a key that Macie can't access. The objects use server-side encryption with customer-provided keys (SSE-C).

Type: integer
Required: False
Format: int64

totalItemsSkippedInvalidKms

The total number of objects that Amazon Macie wasn't able to analyze in the bucket because the objects are encrypted with AWS KMS keys that were disabled, are scheduled for deletion, or were deleted.

Type: integer
Required: False
Format: int64

totalItemsSkippedPermissionDenied

The total number of objects that Amazon Macie wasn't able to analyze in the bucket due to the permissions settings for the objects or the permissions settings for the keys that were used to encrypt the objects.

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

UpdateResourceProfileRequest

Specifies a new sensitivity score for an S3 bucket that Amazon Macie monitors and analyzes for an account. To update the score, automated sensitive data discovery must be enabled for the account.

sensitivityScoreOverride

The new sensitivity score for the bucket. Valid values are: `100`, assign the maximum score and apply the *Sensitive* label to the bucket; and, null (empty), assign a score that Amazon Macie calculates automatically after you submit the request.

Type: integer
Required: False
Format: int32

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:

GetResourceProfile

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

UpdateResourceProfile

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

- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Resource Sensitivity Profile - Artifacts

The Resource Sensitivity Profile Artifacts resource provides information about Amazon Simple Storage Service (Amazon S3) objects that Amazon Macie selected for analysis from individual S3 buckets for your account. If you're the Macie administrator for an organization, this includes objects in S3 buckets that your member accounts own.

For each S3 object, the information includes:

- The Amazon Resource Name (ARN) of the object.
- Whether Macie successfully completed its analysis of the object.
- Whether Macie found sensitive data in the object.

The information captures the results of automated sensitive data discovery activities that Macie has performed for an S3 bucket. For more information, see Performing automated sensitive data discovery in the *Amazon Macie User Guide*.

You can use the Resource Sensitivity Profile Artifacts resource to retrieve information about objects that Macie selected for analysis from an S3 bucket, and the status and results of the analysis. To use this resource, you must first enable automated sensitive data discovery. To enable it for an organization or a standalone account, use the Configuration resource for automated sensitive data discovery. To enable it for a member account in an organization, use the Accounts resource for automated sensitive data discovery.

URI

`/resource-profiles/artifacts`

HTTP methods

GET

Operation ID: `ListResourceProfileArtifacts`

Retrieves information about objects that Amazon Macie selected from an S3 bucket for automated sensitive data discovery.

Query parameters

Name	Type	Required	Description
`resourceArn`	String	True	The Amazon Resource Name (ARN) of the S3 bucket that the request applies to.
`nextToken`	String	False	The `nextToken` string that specifies which page of results to return in a paginated response.

Responses

Status code	Response model	Description
`200`	`ListResourceProfileArtifactsResponse`	The request succeeded.
`400`	`ValidationException`	The request failed because the input doesn't satisfy the constraints specified by the service.
`403`	`AccessDeniedException`	The request was denied because you don't have sufficient access to the specified resource.
`404`	`ResourceNotFoundException`	The request failed because the specified resource wasn't found.

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

Schemas

Response bodies

ListResourceProfileArtifactsResponse schema

```
{
  "artifacts": [
    {
      "arn": "string",
      "classificationResultStatus": "string",
      "sensitive": boolean
    }
  ],
  "nextToken": "string"
}
```

ValidationException schema

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

AccessDeniedException schema

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

```
}
```

ResourceNotFoundException schema

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

ThrottlingException schema

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

InternalServerException 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

InternalServerException

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

ListResourceProfileArtifactsResponse

Provides information about objects that Amazon Macie selected from an S3 bucket while performing automated sensitive data discovery for an account. This information is available only if automated sensitive data discovery has been enabled for the account.

artifacts

An array of objects, one for each of 1-100 S3 objects that Amazon Macie selected for analysis.

If Macie has analyzed more than 100 objects in the bucket, Macie populates the array based on the value for the `ResourceProfileArtifact.sensitive` field for an object: `true` (sensitive), followed by `false` (not sensitive). Macie then populates any remaining items in the array with information about objects where the value for the `ResourceProfileArtifact.classificationResultStatus` field is `SKIPPED`.

Type: Array of type ResourceProfileArtifact
Required: True

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

ResourceProfileArtifact

Provides information about an S3 object that Amazon Macie selected for analysis while performing automated sensitive data discovery for an account, and the status and results of the analysis. This information is available only if automated sensitive data discovery has been enabled for the account.

arn

The Amazon Resource Name (ARN) of the object.

Type: string
Required: True

classificationResultStatus

The status of the analysis. Possible values are:

- `COMPLETE` - Amazon Macie successfully completed its analysis of the object.
- `PARTIAL` - Macie analyzed only a subset of data in the object. For example, the object is an archive file that contains files in an unsupported format.
- `SKIPPED` - Macie wasn't able to analyze the object. For example, the object is a malformed file.

Type: string
Required: True

sensitive

Specifies whether Amazon Macie found sensitive data in the object.

Type: boolean

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:

ListResourceProfileArtifacts

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

- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Resource Sensitivity Profile - Detections

The Resource Sensitivity Profile Detections resource provides information about the types and amount of sensitive data that Amazon Macie has found in individual Amazon Simple Storage Service (Amazon S3) buckets for your account. If you're the Macie administrator for an organization, this includes S3 buckets that your member accounts own.

For each S3 bucket, the information includes an inventory of the types of sensitive data that Macie has found and the number of occurrences of each type. It also includes details about the custom data identifier or managed data identifier that detected each type. The information captures the results of automated sensitive data discovery activities that Macie has performed for an S3 bucket. For more information, see Performing automated sensitive data discovery in the *Amazon Macie User Guide*.

This resource also provides access to the sensitivity scoring settings for individual S3 buckets. By default, Macie calculates a bucket's sensitivity score based partly on the amount of sensitive data that Macie has found in a bucket. If you're a Macie administrator or you have a standalone Macie account, you can optionally adjust these calculations by excluding (*suppressing*) or including specific types of sensitive data in a bucket's score.

You can use the Resource Sensitivity Profile Detections resource to retrieve information about the types and amount of sensitive data that Macie has found in an S3 bucket. If you're a Macie administrator or you have a standalone Macie account, you can also use this resource to adjust the sensitivity scoring settings for a bucket.

To use this resource, you must first enable automated sensitive data discovery. To enable it for an organization or a standalone account, use the Configuration resource for automated sensitive data discovery. To enable it for a member account in an organization, use the Accounts resource for automated sensitive data discovery.

URI

```
/resource-profiles/detections
```

HTTP methods

GET

Operation ID: `ListResourceProfileDetections`

Retrieves information about the types and amount of sensitive data that Amazon Macie found in an S3 bucket.

Query parameters

Name	Type	Required	Description
`resourceArn`	String	True	The Amazon Resource Name (ARN) of the S3 bucket that the request applies to.
`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`	`ListResourceProfileDetectionsResponse`	The request succeeded.
`400`	`ValidationException`	The request failed because the input doesn't satisfy the

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

PATCH

Operation ID: `UpdateResourceProfileDetections`

Updates the sensitivity scoring settings for an S3 bucket.

Query parameters

Name	Type	Required	Description
`resourceArn`	String	True	The Amazon Resource Name (ARN) of the

Name	Type	Required	Description
			S3 bucket that the request applies to.

Responses

Status code	Response model	Description
200	Empty Schema	The request succeeded. The settings were updated and there isn't any content to include in the body of the response (No Content).
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.

Status code	Response model	Description
500	InternalServerException	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

PATCH schema

```
{
  "suppressDataIdentifiers": [
    {
      "id": "string",
      "type": enum
    }
  ]
}
```

Response bodies

ListResourceProfileDetectionsResponse schema

```
{
  "detections": [
    {
      "arn": "string",
      "count": integer,
      "id": "string",
      "name": "string",
      "suppressed": boolean,
      "type": enum
    }
  ],
  "nextToken": "string"
}
```

Empty Schema schema

```
{
}
```

ValidationException schema

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

ServiceQuotaExceededException schema

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

AccessDeniedException schema

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

ResourceNotFoundException schema

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

ThrottlingException schema

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

InternalServerException 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

DataIdentifierType

The type of data identifier that detected a specific type of sensitive data in an S3 bucket. Possible values are:

CUSTOM
MANAGED

Detection

Provides information about a type of sensitive data that Amazon Macie found in an S3 bucket while performing automated sensitive data discovery for an account. The information also specifies the custom or managed data identifier that detected the data. This information is available only if automated sensitive data discovery has been enabled for the account.

arn

If the sensitive data was detected by a custom data identifier, the Amazon Resource Name (ARN) of the custom data identifier that detected the data. Otherwise, this value is null.

Type: string
Required: False

count

The total number of occurrences of the sensitive data.

Type: integer
Required: False
Format: int64

id

The unique identifier for the custom data identifier or managed data identifier that detected the sensitive data. For additional details about a specified managed data identifier, see Using managed data identifiers in the *Amazon Macie User Guide*.

Type: string
Required: False

name

The name of the custom data identifier or managed data identifier that detected the sensitive data. For a managed data identifier, this value is the same as the unique identifier (`id`).

Type: string
Required: False

suppressed

Specifies whether occurrences of this type of sensitive data are excluded (`true`) or included (`false`) in the bucket's sensitivity score.

Type: boolean
Required: False

type

The type of data identifier that detected the sensitive data. Possible values are: `CUSTOM`, for a custom data identifier; and, `MANAGED`, for a managed data identifier.

Type: DataIdentifierType

Required: False

Empty

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

InternalServerException

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

ListResourceProfileDetectionsResponse

Provides information about the types and amount of sensitive data that Amazon Macie found in an S3 bucket while performing automated sensitive data discovery for an account. This information is available only if automated sensitive data discovery has been enabled for the account.

detections

An array of objects, one for each type of sensitive data that Amazon Macie found in the bucket. Each object reports the number of occurrences of the specified type and provides information about the custom data identifier or managed data identifier that detected the data.

Type: Array of type Detection
Required: True

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

SuppressDataIdentifier

Specifies a custom data identifier or managed data identifier that detected a type of sensitive data to start excluding or including in an S3 bucket's sensitivity score.

id

The unique identifier for the custom data identifier or managed data identifier that detected the type of sensitive data to exclude or include in the score.

Type: string
Required: False

type

The type of data identifier that detected the sensitive data. Possible values are: `CUSTOM`, for a custom data identifier; and, `MANAGED`, for a managed data identifier.

Type: DataIdentifierType
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

UpdateResourceProfileDetectionsRequest

Updates the sensitivity scoring settings for an S3 bucket that Amazon Macie monitors and analyzes for an account. The settings specify whether to exclude or include occurrences of specific types of sensitive data in the bucket's sensitivity score. To update the settings, automated sensitive data discovery must be enabled for the account.

suppressDataIdentifiers

An array of objects, one for each custom data identifier or managed data identifier that detected the type of sensitive data to start excluding or including in the bucket's score. To start including all sensitive data types in the score, don't specify any values for this array.

Type: Array of type SuppressDataIdentifier
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:

ListResourceProfileDetections

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

UpdateResourceProfileDetections

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

- AWS SDK for Ruby V3

Sensitivity Inspection Template

The Sensitivity Inspection Template resource provides access to the sensitivity inspection template for your Amazon Macie account. The template stores the collection of settings that specify which allow lists, custom data identifiers, and managed data identifiers you want Macie to use when performing automated sensitive data discovery. For more information, see Performing automated sensitive data discovery in the *Amazon Macie User Guide*.

The first time you or your Macie administrator enables automated sensitive data discovery for your account, Macie automatically creates the sensitivity inspection template for your account. Macie uses the template's settings to determine whether to use (*include*) or not use (*exclude*) individual allow lists, custom data identifiers, and managed data identifiers when it analyzes data. If your account is part of an organization that centrally manages multiple Macie accounts, Macie uses the template settings for your Macie administrator's account when it analyzes data for accounts in your organization. Contact your Macie administrator for information about the settings for your organization.

By default, Macie analyzes data by using only the set of managed data identifiers that we recommend for automated sensitive data discovery. For a list of these identifiers, see Default settings for automated sensitive data discovery in the *Amazon Macie User Guide*. If you're a Macie administrator or you have a standalone Macie account, you can customize the analyses by updating the template settings for your account. You can include allow lists and custom data identifiers that you've defined, and include or exclude specific managed data identifiers that Macie provides. You can use allow lists in all the AWS Regions where Macie is currently available except the Asia Pacific (Osaka) Region.

You can use the Sensitivity Inspection Template resource to retrieve or update the template settings for your account. When you use this resource, you have to specify the unique identifier for the template. To obtain this identifier, use the Sensitivity Inspection Templates resource.

URI

`/templates/sensitivity-inspections/id`

HTTP methods

GET

Operation ID: `GetSensitivityInspectionTemplate`

Retrieves the settings for the sensitivity inspection template for an account.

Path parameters

Name	Type	Required	Description
id	String	True	The unique identifier for the Amazon Macie resource that the request applies to.

Responses

Status code	Response model	Description
200	GetSensitivityInspectionTemplateResponse	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.

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

PUT

Operation ID: `UpdateSensitivityInspectionTemplate`

Updates the settings for the sensitivity inspection template for an account.

Path parameters

Name	Type	Required	Description
id	String	True	The unique identifier for the Amazon Macie resource that the request applies to.

Responses

Status code	Response model	Description
200	Empty Schema	The request succeeded. The template's settings were updated and there isn't any content to include in the body of the response (No Content).
400	ValidationException	The request failed because the input doesn't satisfy the

Status code	Response model	Description
		constraints specified by the service.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
404	ResourceNotFoundException	The request failed because the specified resource wasn't found.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Request bodies

PUT schema

```
{
  "description": "string",
  "excludes": {
    "managedDataIdentifierIds": [
      "string"
    ]
  },
  "includes": {
    "allowListIds": [
      "string"
    ],
```

```
    "customDataIdentifierIds": [
      "string"
    ],
    "managedDataIdentifierIds": [
      "string"
    ]
  }
}
```

Response bodies

GetSensitivityInspectionTemplateResponse schema

```
{
  "description": "string",
  "excludes": {
    "managedDataIdentifierIds": [
      "string"
    ]
  },
  "includes": {
    "allowListIds": [
      "string"
    ],
    "customDataIdentifierIds": [
      "string"
    ],
    "managedDataIdentifierIds": [
      "string"
    ]
  },
  "name": "string",
  "sensitivityInspectionTemplateId": "string"
}
```

Empty Schema schema

```
{
}
```

ValidationException schema

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

AccessDeniedException schema

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

ResourceNotFoundException schema

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

ThrottlingException schema

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

InternalServerException 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

Empty

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

GetSensitivityInspectionTemplateResponse

Provides information about the settings for the sensitivity inspection template for an Amazon Macie account.

description

The custom description of the template.

Type: string
Required: False

excludes

The managed data identifiers that are explicitly excluded (not used) when performing automated sensitive data discovery.

Type: SensitivityInspectionTemplateExcludes
Required: False

includes

The allow lists, custom data identifiers, and managed data identifiers that are explicitly included (used) when performing automated sensitive data discovery.

Type: SensitivityInspectionTemplateIncludes
Required: False

name

The name of the template: `automated-sensitive-data-discovery`.

Type: string
Required: True

sensitivityInspectionTemplateId

The unique identifier for the template.

Type: string
Required: True

InternalServerException

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

SensitivityInspectionTemplateExcludes

Specifies managed data identifiers to exclude (not use) when performing automated sensitive data discovery. For information about the managed data identifiers that Amazon Macie currently provides, see Using managed data identifiers in the *Amazon Macie User Guide*.

managedDataIdentifierIds

An array of unique identifiers, one for each managed data identifier to exclude. To retrieve a list of valid values, use the `ListManagedDataIdentifiers` operation.

Type: Array of type string
Required: False

SensitivityInspectionTemplateIncludes

Specifies the allow lists, custom data identifiers, and managed data identifiers to include (use) when performing automated sensitive data discovery. The configuration must specify at least one custom data identifier or managed data identifier. For information about the managed data identifiers that Amazon Macie currently provides, see Using managed data identifiers in the *Amazon Macie User Guide*.

allowListIds

An array of unique identifiers, one for each allow list to include.

Type: Array of type string
Required: False

customDataIdentifierIds

An array of unique identifiers, one for each custom data identifier to include.

Type: Array of type string
Required: False

managedDataIdentifierIds

An array of unique identifiers, one for each managed data identifier to include.

Amazon Macie uses these managed data identifiers in addition to managed data identifiers that are subsequently released and recommended for automated sensitive data discovery. To retrieve a list of valid values for the managed data identifiers that are currently available, use the `ListManagedDataIdentifiers` operation.

Type: Array of 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

UpdateSensitivityInspectionTemplateRequest

Specifies settings for the sensitivity inspection template for an Amazon Macie account. To update the settings, automated sensitive data discovery must be enabled for the account.

description

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

Type: string
Required: False

excludes

The managed data identifiers to explicitly exclude (not use) when performing automated sensitive data discovery.

To exclude an allow list or custom data identifier that's currently included by the template, update the values for the `SensitivityInspectionTemplateIncludes.allowListIds` and `SensitivityInspectionTemplateIncludes.customDataIdentifierIds` properties, respectively.

Type: SensitivityInspectionTemplateExcludes

Required: False

includes

The allow lists, custom data identifiers, and managed data identifiers to explicitly include (use) when performing automated sensitive data discovery.

Type: SensitivityInspectionTemplateIncludes
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:

GetSensitivityInspectionTemplate

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

- AWS SDK for Ruby V3

UpdateSensitivityInspectionTemplate

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

Sensitivity Inspection Templates

The Sensitivity Inspection Templates resource provides a subset of information about the sensitivity inspection template for your Amazon Macie account. This template stores the collection of settings that specify which allow lists, custom data identifiers, and managed data identifiers you want Macie to use when performing automated sensitive data discovery. The first time you or your Macie administrator enables automated sensitive data discovery for your account, Macie automatically creates the template for your account.

You can use this resource to retrieve the unique identifier and name of the template that Macie created for your account. You can then use the unique identifier to retrieve or update the template's settings by using the Sensitivity Inspection Template resource.

If your account is part of an organization that centrally manages multiple Macie accounts, Macie uses the sensitivity inspection template for your Macie administrator's account when it analyzes data for accounts in your organization. Contact your Macie administrator for information about the template settings for your organization.

URI

`/templates/sensitivity-inspections`

HTTP methods

GET

Operation ID: `ListSensitivityInspectionTemplates`

Retrieves a subset of information about the sensitivity inspection template for 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`	`ListSensitivityInspectionTemplatesResponse`	The request succeeded.
`400`	`ValidationException`	The request failed because the input doesn't satisfy the constraints specified by the service.
`402`	`ServiceQuotaExceededException`	The request failed because fulfilling the request would

Status code	Response model	Description
		exceed one or more service quotas for your account.
403	AccessDeniedException	The request was denied because you don't have sufficient access to the specified resource.
429	ThrottlingException	The request failed because you sent too many requests during a certain amount of time.
500	InternalServerException	The request failed due to an unknown internal server error, exception, or failure.

Schemas

Response bodies

ListSensitivityInspectionTemplatesResponse schema

```
{
  "nextToken": "string",
  "sensitivityInspectionTemplates": [
    {
      "id": "string",
      "name": "string"
    }
  ]
}
```

ValidationException schema

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

```
}
```

ServiceQuotaExceededException schema

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

AccessDeniedException schema

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

ThrottlingException schema

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

InternalServerException 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

InternalServerException

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

ListSensitivityInspectionTemplatesResponse

Provides the results of a request for information about the sensitivity inspection template for an Amazon Macie 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

sensitivityInspectionTemplates

An array that specifies the unique identifier and name of the sensitivity inspection template for the account.

Type: Array of type SensitivityInspectionTemplatesEntry
Required: False

SensitivityInspectionTemplatesEntry

Provides information about the sensitivity inspection template for an Amazon Macie account.

id

The unique identifier for the sensitivity inspection template.

Type: string
Required: False

name

The name of the sensitivity inspection template: `automated-sensitive-data-discovery`.

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:

ListSensitivityInspectionTemplates

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

Tags

A *tag* is a label that you can define and associate with AWS resources, including certain types of Amazon Macie resources. Tags can help you identify, categorize, and manage resources in different ways, such as by purpose, owner, environment, or other criteria. For example, you can use tags to: apply policies, allocate costs, distinguish between versions of resources, or identify resources that support certain compliance requirements or workflows.

You can associate tags with the following types of Macie resources:

- Allow lists
- 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 more information, see Tagging resources in the *Amazon Macie User Guide*.

You can use the Tags resource to add, retrieve, update, or remove tags from an allow list, classification job, custom data identifier, findings filter, or member account.

URI

`/tags/resourceArn`

HTTP methods

DELETE

Operation ID: `UntagResource`

Removes one or more tags (keys and values) from an Amazon Macie resource.

Path parameters

Name	Type	Required	Description
resourceArn	String	True	The Amazon Resource Name (ARN) of the resource.

Query parameters

Name	Type	Required	Description
tagKeys	String	True	One or more tags (keys) to remove

Name	Type	Required	Description
			from the resource. In an HTTP request to remove multiple tags, append the `tagKeys` parameter and argument for each tag to remove, separated by an ampersand (&).

Responses

Status code	Response model	Description
204	UntagResourceResponse	The request succeeded and there isn't any content to include in the body of the response (No Content).

GET

Operation ID: `ListTagsForResource`

Retrieves the tags (keys and values) that are associated with an Amazon Macie resource.

Path parameters

Name	Type	Required	Description
resourceArn	String	True	The Amazon Resource Name (ARN) of the resource.

Responses

Status code	Response model	Description
200	ListTagsForResourceResponse	The request succeeded.

POST

Operation ID: TagResource

Adds or updates one or more tags (keys and values) that are associated with an Amazon Macie resource.

Path parameters

Name	Type	Required	Description
resourceArn	String	True	The Amazon Resource Name (ARN) of the resource.

Responses

Status code	Response model	Description
204	TagResourceResponse	The request succeeded and there isn't any content to include in the body of the response (No Content).

Schemas

Request bodies

POST schema

```
{
```

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

Response bodies

ListTagsForResourceResponse schema

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

UntagResourceResponse schema

```
{
}
```

TagResourceResponse schema

```
{
}
```

Properties

ListTagsForResourceResponse

Provides information about the tags (keys and values) that are associated with an Amazon Macie resource.

tags

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

Type: TagMap
Required: False

TagMap

A string-to-string map of key-value pairs that specifies the tags (keys and values) for an Amazon Macie resource.

key-value pairs

Type: string

TagResourceRequest

Specifies the tags (keys and values) to associate with an Amazon Macie resource.

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
Required: True

TagResourceResponse

The request succeeded. The specified tags were added or updated for 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:

UntagResource

- AWS Command Line Interface

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

ListTagsForResource

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

TagResource

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

Usage Statistics

The Usage Statistics resource provides information about current quotas and usage statistics for your Amazon Macie account. This includes metrics that report the estimated cost of using Macie to perform specific types of tasks, and 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. For information about how Macie calculates usage statistics and data for your account, see Forecasting and monitoring costs in the *Amazon Macie User Guide*.

If you're participating in a 30-day free trial, the applicable cost estimates are based on your use of Macie thus far during the trial. They can help you understand what your usage costs might be after the trial ends. This resource also provides information about when each trial started for your account.

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. If you're the Macie administrator for an organization, this resource provides a breakdown of quota, usage, and free-trial data for individual member accounts in your organization.

To customize your query, you can use supported parameters to filter and sort the data. You can also specify a time range for the data. The time range can be the preceding 30 days or the current calendar month to date.

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`	`GetUsageStatistics Response`	The request succeeded.

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

Schemas

Request bodies

POST schema

```
{
  "filterBy": [
    {
      "comparator": enum,
      "key": enum,
      "values": [
        "string"
      ]
    }
  ],
  "maxResults": integer,
  "nextToken": "string",
  "sortBy": {
    "key": enum,
    "orderBy": enum
  },
  "timeRange": enum
}
```

Response bodies

GetUsageStatisticsResponse schema

```
{
  "nextToken": "string",
  "records": [
    {
      "accountId": "string",
      "automatedDiscoveryFreeTrialStartDate": "string",
      "freeTrialStartDate": "string",
      "usage": [
        {
          "currency": enum,
          "estimatedCost": "string",
          "serviceLimit": {
            "isServiceLimited": boolean,
            "unit": enum,
            "value": integer
          },
          "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"
}
```

InternalServerException 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.

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
Required: False

maxResults

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

Type: integer
Required: False
Format: int32

nextToken

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

Type: string
Required: False

sortBy

The criteria to use to sort the query results.

Type: UsageStatisticsSortBy

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
Required: False

GetUsageStatisticsResponse

Provides the results of a query that retrieved quotas and aggregated usage data for one or more Amazon Macie accounts.

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

records

An array of objects that contains the results of the query. Each object contains the data for an account that matches the filter criteria specified in the request.

Type: Array of type UsageRecord
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
Required: False

InternalServerException

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.

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

unit

The unit of measurement for the value specified by the `value` field.

Type: string
Required: False

Values: TERABYTES

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.

currency

The type of currency that the value for the metric (`estimatedCost`) is reported in.

Type: Currency
Required: False

estimatedCost

The estimated value for the metric.

Type: string
Required: False

serviceLimit

The current value for the quota that corresponds to the metric specified by the `type` field.

Type: ServiceLimit
Required: False

type

The name of the metric. Possible values are: `AUTOMATED_OBJECT_MONITORING`, to monitor S3 objects for automated sensitive data discovery; `AUTOMATED_SENSITIVE_DATA_DISCOVERY`, to analyze S3 objects for automated sensitive data discovery; `DATA_INVENTORY_EVALUATION`, to monitor S3 buckets; and, `SENSITIVE_DATA_DISCOVERY`, to run classification jobs.

Type: UsageType
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

automatedDiscoveryFreeTrialStartDate

The date and time, in UTC and extended ISO 8601 format, when the free trial of automated sensitive data discovery started for the account. This value is null if automated sensitive data discovery hasn't been enabled for the account.

Type: string
Required: False
Format: date-time

freeTrialStartDate

The date and time, in UTC and extended ISO 8601 format, when the Amazon Macie 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
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
Required: False

key

The field to use in the condition.

Type: UsageStatisticsFilterKey
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 Amazon Macie 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

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.

key

The field to sort the results by.

Type: UsageStatisticsSortKey
Required: False

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

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
AUTOMATED_SENSITIVE_DATA_DISCOVERY
AUTOMATED_OBJECT_MONITORING
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Usage Totals

The Usage Totals resource provides aggregated usage data for your Amazon Macie account. The data can provide insight into the estimated cost of using Macie to monitor and analyze your Amazon Simple Storage Service (Amazon S3) data. If you're currently participating in a 30-day free trial, the applicable cost estimates can help you understand what your usage costs might be after the trial ends. For information about how Macie calculates this data for your account, see Forecasting and monitoring costs in the *Amazon Macie User Guide*.

You can use the Usage Totals 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 the Macie administrator for an organization, the data reports cumulative usage for all the 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 resource.

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	The request succeeded.
400	ValidationException	The request failed because the input doesn't satisfy the constraints specified by the service.
402	ServiceQuotaExceededException	The request failed because fulfilling the request would

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

Schemas

Response bodies

GetUsageTotalsResponse schema

```
{
  "timeRange": enum,
  "usageTotals": [
    {
      "currency": enum,
```

```
      "estimatedCost": "string",
      "type": 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"
}
```

InternalServerException 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.

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
Required: False

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
Required: False

InternalServerException

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
Required: False

estimatedCost

The estimated value for the metric.

Type: string
Required: False

type

The name of the metric. Possible values are: AUTOMATED_OBJECT_MONITORING, to monitor S3 objects for automated sensitive data discovery; AUTOMATED_SENSITIVE_DATA_DISCOVERY, to analyze S3 objects for automated sensitive data discovery; DATA_INVENTORY_EVALUATION, to monitor S3 buckets; and, SENSITIVE_DATA_DISCOVERY, to run classification jobs.

Type: UsageType
Required: False

UsageType

The name of an Amazon Macie usage metric for an account. Possible values are:

DATA_INVENTORY_EVALUATION
SENSITIVE_DATA_DISCOVERY

AUTOMATED_SENSITIVE_DATA_DISCOVERY
AUTOMATED_OBJECT_MONITORING

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Document history for the Amazon Macie API Reference

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:** July 22, 2024

Change	Description	Date
Updated API descriptions	Updated descriptions of data source statistics, resource sensitivity profiles, and other information that Macie provides about the results of automated sensitive data discovery. Members of an organization now have read access to this information for their Amazon S3 data, if their Macie administrator enables automated sensitive data discovery.	July 22, 2024
Added APIs	Added support for enabling or disabling automated sensitive data discovery for individual accounts in an organization, and enabling automated sensitive data discovery automatically for particular types of accounts in an organization. Also added metadata indicating whether individual Amazon Simple	June 14, 2024

	Storage Service (Amazon S3) buckets are included in the scope of the analyses.	
Updated API descriptions	Updated descriptions of statistics and metadata that Macie provides about encryption settings for Amazon Simple Storage Service (Amazon S3) buckets and objects. Statistics and metadata now include data for buckets and objects that use dual-layer server-side encryption with AWS KMS keys (DSSE-KMS). In addition, Macie can now analyze objects that use DSSE-KMS encryption. For information about DSSE-KMS, see Using dual-layer server-side encryption with AWS KMS keys in the *Amazon Simple Storage Service User Guide*.	January 16, 2024
Added APIs	Added support for configuring Macie to assume an AWS Identity and Access Management (IAM) role when retrieving sample occurrences of sensitive data reported by findings.	November 16, 2023

Changed APIs	The default `ManagedDataIdentifierSelector` setting for new classification jobs is now `RECOMMENDED`. By default, new classification jobs now use the recommended set of managed data identifiers. For a list of the managed data identifiers included in the set, see Managed data identifiers recommended for jobs in the *Amazon Macie User Guide*.	September 18, 2023
Added APIs	Added support for configuring new classification jobs to automatically use the set of managed data identifiers that we recommend for jobs.	June 27, 2023

Updated API descriptions	Updated descriptions of statistics and metadata that Macie provides about default encryption settings for Amazon Simple Storage Service (Amazon S3) buckets. Amazon S3 now automatically applies server-side encryption with Amazon S3 managed keys (SSE-S3) as the base level of encryption for objects that are added to new and existing buckets. For information about this change in Amazon S3, see Setting default server-side encryption behavior for S3 buckets in the *Amazon Simple Storage Service User Guide*.	February 27, 2023
Added APIs	Added support for a new type of policy finding, `Policy:IAMUser/S3BucketSharedWithCloudFront`. Also updated descriptions of statistics and metadata that Macie provides about shared access to S3 buckets. The data now indicates whether a bucket is shared with an Amazon CloudFront origin access identity (OAI) or CloudFront origin access control (OAC).	February 23, 2023

Added APIs	Added support for analyzing S3 objects that use the S3 Glacier Instant Retrieval (`Glacier_IR`) storage class. For sensitive data discovery and in data source statistics and metadata, S3 objects that use this Amazon S3 storage class are now considered *classifiable objects*.	December 21, 2022
Added APIs	Added support for configuri ng Macie to perform automated sensitive data discovery for Amazon S3 data, and accessing the results in data source statistics, resource sensitivity profiles, findings, and other information that Macie provides about Amazon S3 data.	November 28, 2022
Added APIs	Added support for using allow lists to define specific text and text patterns to ignore when inspecting data sources for sensitive data.	August 30, 2022
Added APIs	Added support for configuri ng and using Macie to retrieve sample occurrences of sensitive data reported by findings.	July 26, 2022

Added APIs	Added support for specifying the severity of findings that a custom data identifier produces.	November 3, 2021
Added APIs	Added S3 bucket metadata that indicates whether a bucket's permissions settings or an error prevented Macie from retrieving and processing information about the bucket or the bucket's objects. Also updated references to AWS KMS keys and customer managed keys to reflect current terminology.	September 30, 2021
Added APIs	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	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	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	Replaced the term *master account* with the term *administrator account*. This includes adding APIs that use the new term and deprecating APIs that use the previous term. The new APIs provide the same functionality as the deprecated APIs. An *administrator account* is used to centrally manage multiple accounts.	February 12, 2021
Added APIs	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	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	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	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	Added criteria for sorting and filtering query results for account quotas and usage statistics.	July 24, 2020
Removed APIs	Removed support for the **ArchiveFindings** and **UnarchiveFindings** operations. To suppress findings, use the `action` parameter of the CreateFindingsFilter and UpdateFindingsFilter operations.	June 11, 2020
General availability	This release introduces version 2020-01-01 of the Amazon Macie API.	May 13, 2020