

# Package ‘paws.security.identity’

January 10, 2024

**Title** 'Amazon Web Services' Security, Identity, & Compliance Services

**Version** 0.5.0

**Description** Interface to 'Amazon Web Services' security, identity, and compliance services, including the 'Identity & Access Management' (IAM) service for managing access to services and resources, and more <<https://aws.amazon.com/>>.

**License** Apache License (>= 2.0)

**URL** <https://github.com/paws-r/paws>

**BugReports** <https://github.com/paws-r/paws/issues>

**Imports** paws.common (>= 0.6.0)

**Suggests** testthat

**Encoding** UTF-8

**RoxygenNote** 7.2.3

**Collate** 'accessanalyzer\_service.R' 'accessanalyzer\_interfaces.R'  
'accessanalyzer\_operations.R' 'account\_service.R'  
'account\_interfaces.R' 'account\_operations.R' 'acm\_service.R'  
'acm\_interfaces.R' 'acm\_operations.R' 'acmpca\_service.R'  
'acmpca\_interfaces.R' 'acmpca\_operations.R'  
'clouddirectory\_service.R' 'clouddirectory\_interfaces.R'  
'clouddirectory\_operations.R' 'cloudhsm\_service.R'  
'cloudhsm\_interfaces.R' 'cloudhsm\_operations.R'  
'cloudhsmv2\_service.R' 'cloudhsmv2\_interfaces.R'  
'cloudhsmv2\_operations.R' 'cognitoidentity\_service.R'  
'cognitoidentity\_interfaces.R' 'cognitoidentity\_operations.R'  
'cognitoidentityprovider\_service.R'  
'cognitoidentityprovider\_interfaces.R'  
'cognitoidentityprovider\_operations.R' 'cognitosync\_service.R'  
'cognitosync\_interfaces.R' 'cognitosync\_operations.R'  
'detective\_service.R' 'detective\_interfaces.R'  
'detective\_operations.R' 'directoryservice\_service.R'  
'directoryservice\_interfaces.R' 'directoryservice\_operations.R'  
'fms\_service.R' 'fms\_interfaces.R' 'fms\_operations.R'

'guardduty\_service.R' 'guardduty\_interfaces.R'  
 'guardduty\_operations.R' 'iam\_service.R' 'iam\_interfaces.R'  
 'iam\_operations.R' 'iamrolesanywhere\_service.R'  
 'iamrolesanywhere\_interfaces.R' 'iamrolesanywhere\_operations.R'  
 'identitystore\_service.R' 'identitystore\_interfaces.R'  
 'identitystore\_operations.R' 'inspector2\_service.R'  
 'inspector2\_interfaces.R' 'inspector2\_operations.R'  
 'inspector\_service.R' 'inspector\_interfaces.R'  
 'inspector\_operations.R' 'kms\_service.R' 'kms\_interfaces.R'  
 'kms\_operations.R' 'macie2\_service.R' 'macie2\_interfaces.R'  
 'macie2\_operations.R' 'pcaconnectorad\_service.R'  
 'pcaconnectorad\_interfaces.R' 'pcaconnectorad\_operations.R'  
 'ram\_service.R' 'ram\_interfaces.R' 'ram\_operations.R'  
 'reexports\_paws.common.R' 'secretsmanager\_service.R'  
 'secretsmanager\_interfaces.R' 'secretsmanager\_operations.R'  
 'securityhub\_service.R' 'securityhub\_interfaces.R'  
 'securityhub\_operations.R' 'securitylake\_service.R'  
 'securitylake\_interfaces.R' 'securitylake\_operations.R'  
 'shield\_service.R' 'shield\_interfaces.R' 'shield\_operations.R'  
 'sso\_service.R' 'sso\_interfaces.R' 'sso\_operations.R'  
 'ssoadmin\_service.R' 'ssoadmin\_interfaces.R'  
 'ssoadmin\_operations.R' 'ssooidc\_service.R'  
 'ssooidc\_interfaces.R' 'ssooidc\_operations.R' 'sts\_service.R'  
 'sts\_interfaces.R' 'sts\_operations.R'  
 'verifiedpermissions\_service.R'  
 'verifiedpermissions\_interfaces.R'  
 'verifiedpermissions\_operations.R' 'waf\_service.R'  
 'waf\_interfaces.R' 'waf\_operations.R' 'wafregional\_service.R'  
 'wafregional\_interfaces.R' 'wafregional\_operations.R'  
 'wafv2\_service.R' 'wafv2\_interfaces.R' 'wafv2\_operations.R'

**NeedsCompilation** no

**Author** David Kretch [aut],  
 Adam Banker [aut],  
 Dyfan Jones [cre],  
 Amazon.com, Inc. [cph]

**Maintainer** Dyfan Jones <dyfan.r.jones@gmail.com>

**Repository** CRAN

**Date/Publication** 2024-01-10 11:30:02 UTC

## R topics documented:

|                          |    |
|--------------------------|----|
| accessanalyzer . . . . . | 3  |
| account . . . . .        | 7  |
| acm . . . . .            | 9  |
| acmpca . . . . .         | 11 |
| clouddirectory . . . . . | 14 |

|                                   |     |
|-----------------------------------|-----|
| cloudhsm . . . . .                | 18  |
| cloudhsmv2 . . . . .              | 21  |
| cognitoidentity . . . . .         | 23  |
| cognitoidentityprovider . . . . . | 26  |
| cognitosync . . . . .             | 32  |
| detective . . . . .               | 35  |
| directoryservice . . . . .        | 38  |
| fms . . . . .                     | 42  |
| guardduty . . . . .               | 45  |
| iam . . . . .                     | 49  |
| iamrolesanywhere . . . . .        | 55  |
| identitystore . . . . .           | 58  |
| inspector . . . . .               | 61  |
| inspector2 . . . . .              | 64  |
| kms . . . . .                     | 67  |
| macie2 . . . . .                  | 72  |
| pcaconnectorad . . . . .          | 75  |
| ram . . . . .                     | 78  |
| secretsmanager . . . . .          | 81  |
| securityhub . . . . .             | 84  |
| securitylake . . . . .            | 89  |
| shield . . . . .                  | 92  |
| sso . . . . .                     | 95  |
| ssoadmin . . . . .                | 99  |
| ssooidc . . . . .                 | 103 |
| sts . . . . .                     | 106 |
| verifiedpermissions . . . . .     | 109 |
| waf . . . . .                     | 112 |
| wafregional . . . . .             | 116 |
| wafv2 . . . . .                   | 120 |

**Index** **125**

---

|                |                        |
|----------------|------------------------|
| accessanalyzer | <i>Access Analyzer</i> |
|----------------|------------------------|

---

**Description**

Identity and Access Management Access Analyzer helps you to set, verify, and refine your IAM policies by providing a suite of capabilities. Its features include findings for external and unused access, basic and custom policy checks for validating policies, and policy generation to generate fine-grained policies. To start using IAM Access Analyzer to identify external or unused access, you first need to create an analyzer.

**External access analyzers** help identify potential risks of accessing resources by enabling you to identify any resource policies that grant access to an external principal. It does this by using logic-based reasoning to analyze resource-based policies in your Amazon Web Services environment. An external principal can be another Amazon Web Services account, a root user, an IAM user or role,

a federated user, an Amazon Web Services service, or an anonymous user. You can also use IAM Access Analyzer to preview public and cross-account access to your resources before deploying permissions changes.

**Unused access analyzers** help identify potential identity access risks by enabling you to identify unused IAM roles, unused access keys, unused console passwords, and IAM principals with unused service and action-level permissions.

Beyond findings, IAM Access Analyzer provides basic and custom policy checks to validate IAM policies before deploying permissions changes. You can use policy generation to refine permissions by attaching a policy generated using access activity logged in CloudTrail logs.

This guide describes the IAM Access Analyzer operations that you can call programmatically. For general information about IAM Access Analyzer, see [Identity and Access Management Access Analyzer](#) in the **IAM User Guide**.

## Usage

```
accessanalyzer(
    config = list(),
    credentials = list(),
    endpoint = NULL,
    region = NULL
)
```

## Arguments

|             |  |
|-------------|--|
| config      | Optional configuration of credentials, endpoint, and/or region. <ul style="list-style-type: none"> <li>• <b>credentials:</b> <ul style="list-style-type: none"> <li>– <b>creds:</b> <ul style="list-style-type: none"> <li>* <b>access_key_id:</b> AWS access key ID</li> <li>* <b>secret_access_key:</b> AWS secret access key</li> <li>* <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>– <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>– <b>anonymous:</b> Set anonymous credentials.</li> </ul> </li> <li>• <b>endpoint:</b> The complete URL to use for the constructed client.</li> <li>• <b>region:</b> The AWS Region used in instantiating the client.</li> <li>• <b>close_connection:</b> Immediately close all HTTP connections.</li> <li>• <b>timeout:</b> The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.</li> <li>• <b>s3_force_path_style:</b> Set this to <code>true</code> to force the request to use path-style addressing, i.e. <code>http://s3.amazonaws.com/BUCKET/KEY</code>.</li> <li>• <b>sts_regional_endpoint:</b> Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul> |
| credentials | Optional credentials shorthand for the config parameter <ul style="list-style-type: none"> <li>• <b>creds:</b></li> </ul>  |

- **access\_key\_id**: AWS access key ID
  - **secret\_access\_key**: AWS secret access key
  - **session\_token**: AWS temporary session token
  - **profile**: The name of a profile to use. If not given, then the default profile is used.
  - **anonymous**: Set anonymous credentials.
- endpoint           Optional shorthand for complete URL to use for the constructed client.
- region             Optional shorthand for AWS Region used in instantiating the client.

### Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

### Service syntax

```
svc <- accessanalyzer(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
    creds = list(
      access_key_id = "string",
      secret_access_key = "string",
      session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
  ),
  endpoint = "string",
  region = "string"
)
```

## Operations

|   |   |
|---|---|
| <code>apply_archive_rule</code>           | Retroactively applies the archive rule to existing findings that meet the archive rule criteria       |
| <code>cancel_policy_generation</code>     | Cancels the requested policy generation   |
| <code>check_access_not_granted</code>     | Checks whether the specified access isn't allowed by a policy   |
| <code>check_no_new_access</code>          | Checks whether new access is allowed for an updated policy when compared to the existing policy       |
| <code>create_access_preview</code>        | Creates an access preview that allows you to preview IAM Access Analyzer findings for your account    |
| <code>create_analyzer</code>              | Creates an analyzer for your account  |
| <code>create_archive_rule</code>          | Creates an archive rule for the specified analyzer  |
| <code>delete_analyzer</code>              | Deletes the specified analyzer  |
| <code>delete_archive_rule</code>          | Deletes the specified archive rule  |
| <code>get_access_preview</code>           | Retrieves information about an access preview for the specified analyzer                              |
| <code>get_analyzed_resource</code>        | Retrieves information about a resource that was analyzed  |
| <code>get_analyzer</code>                 | Retrieves information about the specified analyzer  |
| <code>get_archive_rule</code>             | Retrieves information about an archive rule   |
| <code>get_finding</code>                  | Retrieves information about the specified finding   |
| <code>get_finding_v2</code>               | Retrieves information about the specified finding   |
| <code>get_generated_policy</code>         | Retrieves the policy that was generated using StartPolicyGeneration                                   |
| <code>list_access_preview_findings</code> | Retrieves a list of access preview findings generated by the specified access preview                 |
| <code>list_access_previews</code>         | Retrieves a list of access previews for the specified analyzer  |
| <code>list_analyzed_resources</code>      | Retrieves a list of resources of the specified type that have been analyzed by the specified analyzer |
| <code>list_analyzers</code>               | Retrieves a list of analyzers   |
| <code>list_archive_rules</code>           | Retrieves a list of archive rules created for the specified analyzer                                  |
| <code>list_findings</code>                | Retrieves a list of findings generated by the specified analyzer                                      |
| <code>list_findings_v2</code>             | Retrieves a list of findings generated by the specified analyzer                                      |
| <code>list_policy_generations</code>      | Lists all of the policy generations requested in the last seven days                                  |
| <code>list_tags_for_resource</code>       | Retrieves a list of tags applied to the specified resource  |
| <code>start_policy_generation</code>      | Starts the policy generation request  |
| <code>start_resource_scan</code>          | Immediately starts a scan of the policies applied to the specified resource                           |
| <code>tag_resource</code>                 | Adds a tag to the specified resource  |
| <code>untag_resource</code>               | Removes a tag from the specified resource   |
| <code>update_archive_rule</code>          | Updates the criteria and values for the specified archive rule  |
| <code>update_findings</code>              | Updates the status for the specified findings   |
| <code>validate_policy</code>              | Requests the validation of a policy and returns a list of findings                                    |

## Examples

```
## Not run:
svc <- accessanalyzer()
svc$apply_archive_rule(
  Foo = 123
)

## End(Not run)
```

---

|         |                    |
|---------|--------------------|
| account | <i>AWS Account</i> |
|---------|--------------------|

---

## Description

Operations for Amazon Web Services Account Management

## Usage

```
account(config = list(), credentials = list(), endpoint = NULL, region = NULL)
```

## Arguments

|             |   |
|-------------|---|
| config      | Optional configuration of credentials, endpoint, and/or region. <ul style="list-style-type: none"> <li>• <b>credentials:</b> <ul style="list-style-type: none"> <li>– <b>creds:</b> <ul style="list-style-type: none"> <li>* <b>access_key_id:</b> AWS access key ID</li> <li>* <b>secret_access_key:</b> AWS secret access key</li> <li>* <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>– <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>– <b>anonymous:</b> Set anonymous credentials.</li> </ul> </li> <li>• <b>endpoint:</b> The complete URL to use for the constructed client.</li> <li>• <b>region:</b> The AWS Region used in instantiating the client.</li> <li>• <b>close_connection:</b> Immediately close all HTTP connections.</li> <li>• <b>timeout:</b> The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.</li> <li>• <b>s3_force_path_style:</b> Set this to true to force the request to use path-style addressing, i.e. <code>http://s3.amazonaws.com/BUCKET/KEY</code>.</li> <li>• <b>sts_regional_endpoint:</b> Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul> |
| credentials | Optional credentials shorthand for the config parameter <ul style="list-style-type: none"> <li>• <b>creds:</b> <ul style="list-style-type: none"> <li>– <b>access_key_id:</b> AWS access key ID</li> <li>– <b>secret_access_key:</b> AWS secret access key</li> <li>– <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>• <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>• <b>anonymous:</b> Set anonymous credentials.</li> </ul>   |
| endpoint    | Optional shorthand for complete URL to use for the constructed client.  |
| region      | Optional shorthand for AWS Region used in instantiating the client.   |

**Value**

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

**Service syntax**

```
svc <- account(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
    creds = list(
      access_key_id = "string",
      secret_access_key = "string",
      session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
  ),
  endpoint = "string",
  region = "string"
)
```

**Operations**

|  |  |
|--|--|
| <a href="#">delete_alternate_contact</a> | Deletes the specified alternate contact from an Amazon Web Services account          |
| <a href="#">disable_region</a>           | Disables (opts-out) a particular Region for an account                               |
| <a href="#">enable_region</a>            | Enables (opts-in) a particular Region for an account                                 |
| <a href="#">get_alternate_contact</a>    | Retrieves the specified alternate contact attached to an Amazon Web Services account |
| <a href="#">get_contact_information</a>  | Retrieves the primary contact information of an Amazon Web Services account          |
| <a href="#">get_region_opt_status</a>    | Retrieves the opt-in status of a particular Region                                   |
| <a href="#">list_regions</a>             | Lists all the Regions for a given account and their respective opt-in statuses       |
| <a href="#">put_alternate_contact</a>    | Modifies the specified alternate contact attached to an Amazon Web Services account  |



[put\\_contact\\_information](#) Updates the primary contact information of an Amazon Web Services account

## Examples

```
## Not run:
svc <- account()
svc$delete_alternate_contact(
  Foo = 123
)

## End(Not run)
```

---

 acm

*AWS Certificate Manager*


---

## Description

Certificate Manager

You can use Certificate Manager (ACM) to manage SSL/TLS certificates for your Amazon Web Services-based websites and applications. For more information about using ACM, see the [Certificate Manager User Guide](#).

## Usage

```
acm(config = list(), credentials = list(), endpoint = NULL, region = NULL)
```

## Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

- **credentials:**
  - **creds:**
    - \* **access\_key\_id:** AWS access key ID
    - \* **secret\_access\_key:** AWS secret access key
    - \* **session\_token:** AWS temporary session token
  - **profile:** The name of a profile to use. If not given, then the default profile is used.
  - **anonymous:** Set anonymous credentials.
- **endpoint:** The complete URL to use for the constructed client.
- **region:** The AWS Region used in instantiating the client.
- **close\_connection:** Immediately close all HTTP connections.
- **timeout:** The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.

|             |  |
|-------------|--|
|             | <ul style="list-style-type: none"> <li>• <b>s3_force_path_style</b>: Set this to <code>true</code> to force the request to use path-style addressing, i.e. <code>http://s3.amazonaws.com/BUCKET/KEY</code>.</li> <li>• <b>sts_regional_endpoint</b>: Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul> |
| credentials | Optional credentials shorthand for the config parameter <ul style="list-style-type: none"> <li>• <b>creds</b>: <ul style="list-style-type: none"> <li>– <b>access_key_id</b>: AWS access key ID</li> <li>– <b>secret_access_key</b>: AWS secret access key</li> <li>– <b>session_token</b>: AWS temporary session token</li> </ul> </li> <li>• <b>profile</b>: The name of a profile to use. If not given, then the default profile is used.</li> <li>• <b>anonymous</b>: Set anonymous credentials.</li> </ul>      |
| endpoint    | Optional shorthand for complete URL to use for the constructed client.   |
| region      | Optional shorthand for AWS Region used in instantiating the client.  |

## Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

## Service syntax

```
svc <- acm(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
    creds = list(
      access_key_id = "string",
      secret_access_key = "string",
      session_token = "string"
    )
  )
)
```

```

    ),
    profile = "string",
    anonymous = "logical"
  ),
  endpoint = "string",
  region = "string"
)

```

## Operations

|  |  |
|--|--|
| <a href="#">add_tags_to_certificate</a>      | Adds one or more tags to an ACM certificate  |
| <a href="#">delete_certificate</a>           | Deletes a certificate and its associated private key   |
| <a href="#">describe_certificate</a>         | Returns detailed metadata about the specified ACM certificate  |
| <a href="#">export_certificate</a>           | Exports a private certificate issued by a private certificate authority (CA) for use anywhere          |
| <a href="#">get_account_configuration</a>    | Returns the account configuration options associated with an Amazon Web Services account               |
| <a href="#">get_certificate</a>              | Retrieves an Amazon-issued certificate and its certificate chain                                       |
| <a href="#">import_certificate</a>           | Imports a certificate into Certificate Manager (ACM) to use with services that are integrated with ACM |
| <a href="#">list_certificates</a>            | Retrieves a list of certificate ARNs and domain names  |
| <a href="#">list_tags_for_certificate</a>    | Lists the tags that have been applied to the ACM certificate   |
| <a href="#">put_account_configuration</a>    | Adds or modifies account-level configurations in ACM   |
| <a href="#">remove_tags_from_certificate</a> | Remove one or more tags from an ACM certificate  |
| <a href="#">renew_certificate</a>            | Renews an eligible ACM certificate   |
| <a href="#">request_certificate</a>          | Requests an ACM certificate for use with other Amazon Web Services services                            |
| <a href="#">resend_validation_email</a>      | Resends the email that requests domain ownership validation  |
| <a href="#">update_certificate_options</a>   | Updates a certificate  |

## Examples

```

## Not run:
svc <- acm()
svc$add_tags_to_certificate(
  Foo = 123
)

## End(Not run)

```

## Description

This is the *Amazon Web Services Private Certificate Authority API Reference*. It provides descriptions, syntax, and usage examples for each of the actions and data types involved in creating and managing a private certificate authority (CA) for your organization.

The documentation for each action shows the API request parameters and the JSON response. Alternatively, you can use one of the Amazon Web Services SDKs to access an API that is tailored to the programming language or platform that you prefer. For more information, see [Amazon Web Services SDKs](#).

Each Amazon Web Services Private CA API operation has a quota that determines the number of times the operation can be called per second. Amazon Web Services Private CA throttles API requests at different rates depending on the operation. Throttling means that Amazon Web Services Private CA rejects an otherwise valid request because the request exceeds the operation's quota for the number of requests per second. When a request is throttled, Amazon Web Services Private CA returns a `ThrottlingException` error. Amazon Web Services Private CA does not guarantee a minimum request rate for APIs.

To see an up-to-date list of your Amazon Web Services Private CA quotas, or to request a quota increase, log into your Amazon Web Services account and visit the Service Quotas console.

## Usage

```
acmpca(config = list(), credentials = list(), endpoint = NULL, region = NULL)
```

## Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

- **credentials:**

- **creds:**

- \* **access\_key\_id:** AWS access key ID
- \* **secret\_access\_key:** AWS secret access key
- \* **session\_token:** AWS temporary session token

- **profile:** The name of a profile to use. If not given, then the default profile is used.

- **anonymous:** Set anonymous credentials.

- **endpoint:** The complete URL to use for the constructed client.

- **region:** The AWS Region used in instantiating the client.

- **close\_connection:** Immediately close all HTTP connections.

- **timeout:** The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.

- **s3\_force\_path\_style:** Set this to `true` to force the request to use path-style addressing, i.e. `http://s3.amazonaws.com/BUCKET/KEY`.

- **sts\_regional\_endpoint:** Set sts regional endpoint resolver to regional or legacy <https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html>

`credentials` Optional credentials shorthand for the config parameter

- **creds:**

- **access\_key\_id:** AWS access key ID
- **secret\_access\_key:** AWS secret access key
- **session\_token:** AWS temporary session token

- **profile:** The name of a profile to use. If not given, then the default profile is used.
  - **anonymous:** Set anonymous credentials.
- endpoint      Optional shorthand for complete URL to use for the constructed client.
- region        Optional shorthand for AWS Region used in instantiating the client.

### Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

### Service syntax

```
svc <- acmpca(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
    creds = list(
      access_key_id = "string",
      secret_access_key = "string",
      session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
  ),
  endpoint = "string",
  region = "string"
)
```

### Operations

[create\\_certificate\\_authority](#)

Creates a root or subordinate private certificate authority (CA)

|  |   |
|--|---|
| <code>create_certificate_authority_audit_report</code>   | Creates an audit report that lists every time that your CA private key is used  |
| <code>create_permission</code>                           | Grants one or more permissions on a private CA to the Certificate Manager (ACM)   |
| <code>delete_certificate_authority</code>                | Deletes a private certificate authority (CA)  |
| <code>delete_permission</code>                           | Revokes permissions on a private CA granted to the Certificate Manager (ACM)  |
| <code>delete_policy</code>                               | Deletes the resource-based policy attached to a private CA  |
| <code>describe_certificate_authority</code>              | Lists information about your private certificate authority (CA) or one that has been shared with you                          |
| <code>describe_certificate_authority_audit_report</code> | Lists information about a specific audit report created by calling the <code>CreateCertificateAuthorityAuditReport</code> API |
| <code>get_certificate</code>                             | Retrieves a certificate from your private CA or one that has been shared with you   |
| <code>get_certificate_authority_certificate</code>       | Retrieves the certificate and certificate chain for your private certificate authority  |
| <code>get_certificate_authority_csr</code>               | Retrieves the certificate signing request (CSR) for your private certificate authority  |
| <code>get_policy</code>                                  | Retrieves the resource-based policy attached to a private CA  |
| <code>import_certificate_authority_certificate</code>    | Imports a signed private CA certificate into Amazon Web Services Private CA   |
| <code>issue_certificate</code>                           | Uses your private certificate authority (CA), or one that has been shared with you, to issue a certificate                    |
| <code>list_certificate_authorities</code>                | Lists the private certificate authorities that you created by using the <code>CreateCertificateAuthority</code> API           |
| <code>list_permissions</code>                            | List all permissions on a private CA, if any, granted to the Certificate Manager (ACM)  |
| <code>list_tags</code>                                   | Lists the tags, if any, that are associated with your private CA or one that has been shared with you                         |
| <code>put_policy</code>                                  | Attaches a resource-based policy to a private CA  |
| <code>restore_certificate_authority</code>               | Restores a certificate authority (CA) that is in the DELETED state  |
| <code>revoke_certificate</code>                          | Revokes a certificate that was issued inside Amazon Web Services Private CA   |
| <code>tag_certificate_authority</code>                   | Adds one or more tags to your private CA  |
| <code>untag_certificate_authority</code>                 | Remove one or more tags from your private CA  |
| <code>update_certificate_authority</code>                | Updates the status or configuration of a private certificate authority (CA)   |

## Examples

```
## Not run:
svc <- acmpca()
svc$create_certificate_authority(
  Foo = 123
)

## End(Not run)
```

---

clouddirectory

*Amazon CloudDirectory*

---

## Description

Amazon Cloud Directory

Amazon Cloud Directory is a component of the AWS Directory Service that simplifies the development and management of cloud-scale web, mobile, and IoT applications. This guide describes the Cloud Directory operations that you can call programmatically and includes detailed information on data types and errors. For information about Cloud Directory features, see [AWS Directory Service](#) and the [Amazon Cloud Directory Developer Guide](#).

**Usage**

```
clouddirectory(
  config = list(),
  credentials = list(),
  endpoint = NULL,
  region = NULL
)
```

**Arguments**

|             |  |
|-------------|--|
| config      | <p>Optional configuration of credentials, endpoint, and/or region.</p> <ul style="list-style-type: none"> <li>• <b>credentials:</b> <ul style="list-style-type: none"> <li>– <b>creds:</b> <ul style="list-style-type: none"> <li>* <b>access_key_id:</b> AWS access key ID</li> <li>* <b>secret_access_key:</b> AWS secret access key</li> <li>* <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>– <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>– <b>anonymous:</b> Set anonymous credentials.</li> </ul> </li> <li>• <b>endpoint:</b> The complete URL to use for the constructed client.</li> <li>• <b>region:</b> The AWS Region used in instantiating the client.</li> <li>• <b>close_connection:</b> Immediately close all HTTP connections.</li> <li>• <b>timeout:</b> The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.</li> <li>• <b>s3_force_path_style:</b> Set this to true to force the request to use path-style addressing, i.e. <code>http://s3.amazonaws.com/BUCKET/KEY</code>.</li> <li>• <b>sts_regional_endpoint:</b> Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul> |
| credentials | <p>Optional credentials shorthand for the config parameter</p> <ul style="list-style-type: none"> <li>• <b>creds:</b> <ul style="list-style-type: none"> <li>– <b>access_key_id:</b> AWS access key ID</li> <li>– <b>secret_access_key:</b> AWS secret access key</li> <li>– <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>• <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>• <b>anonymous:</b> Set anonymous credentials.</li> </ul>   |
| endpoint    | Optional shorthand for complete URL to use for the constructed client.   |
| region      | Optional shorthand for AWS Region used in instantiating the client.  |

**Value**

A client for the service. You can call the service’s operations using syntax like `svc$operation(...)`, where `svc` is the name you’ve assigned to the client. The available operations are listed in the Operations section.

**Service syntax**

```

svc <- clouddirectory(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
    creds = list(
      access_key_id = "string",
      secret_access_key = "string",
      session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
  ),
  endpoint = "string",
  region = "string"
)

```

**Operations**

|   |   |
|---|---|
| <a href="#">add_facet_to_object</a>     | Adds a new Facet to an object   |
| <a href="#">apply_schema</a>            | Copies the input published schema, at the specified version, into the Directory with the sa |
| <a href="#">attach_object</a>           | Attaches an existing object to another object   |
| <a href="#">attach_policy</a>           | Attaches a policy object to a regular object  |
| <a href="#">attach_to_index</a>         | Attaches the specified object to the specified index  |
| <a href="#">attach_typed_link</a>       | Attaches a typed link to a specified source and target object                               |
| <a href="#">batch_read</a>              | Performs all the read operations in a batch   |
| <a href="#">batch_write</a>             | Performs all the write operations in a batch  |
| <a href="#">create_directory</a>        | Creates a Directory by copying the published schema into the directory                      |
| <a href="#">create_facet</a>            | Creates a new Facet in a schema   |
| <a href="#">create_index</a>            | Creates an index object   |
| <a href="#">create_object</a>           | Creates an object in a Directory  |
| <a href="#">create_schema</a>           | Creates a new schema in a development state   |
| <a href="#">create_typed_link_facet</a> | Creates a TypedLinkFacet  |



|  |   |
|--|---|
| <a href="#">delete_directory</a>                 | Deletes a directory   |
| <a href="#">delete_facet</a>                     | Deletes a given Facet   |
| <a href="#">delete_object</a>                    | Deletes an object and its associated attributes   |
| <a href="#">delete_schema</a>                    | Deletes a given schema  |
| <a href="#">delete_typed_link_facet</a>          | Deletes a TypedLinkFacet  |
| <a href="#">detach_from_index</a>                | Detaches the specified object from the specified index  |
| <a href="#">detach_object</a>                    | Detaches a given object from the parent object  |
| <a href="#">detach_policy</a>                    | Detaches a policy from an object  |
| <a href="#">detach_typed_link</a>                | Detaches a typed link from a specified source and target object                               |
| <a href="#">disable_directory</a>                | Disables the specified directory  |
| <a href="#">enable_directory</a>                 | Enables the specified directory   |
| <a href="#">get_applied_schema_version</a>       | Returns current applied schema version ARN, including the minor version in use                |
| <a href="#">get_directory</a>                    | Retrieves metadata about a directory  |
| <a href="#">get_facet</a>                        | Gets details of the Facet, such as facet name, attributes, Rules, or ObjectType               |
| <a href="#">get_link_attributes</a>              | Retrieves attributes that are associated with a typed link                                    |
| <a href="#">get_object_attributes</a>            | Retrieves attributes within a facet that are associated with an object                        |
| <a href="#">get_object_information</a>           | Retrieves metadata about an object  |
| <a href="#">get_schema_as_json</a>               | Retrieves a JSON representation of the schema   |
| <a href="#">get_typed_link_facet_information</a> | Returns the identity attribute order for a specific TypedLinkFacet                            |
| <a href="#">list_applied_schema_arns</a>         | Lists schema major versions applied to a directory  |
| <a href="#">list_attached_indices</a>            | Lists indices attached to the specified object  |
| <a href="#">list_development_schema_arns</a>     | Retrieves each Amazon Resource Name (ARN) of schemas in the development state                 |
| <a href="#">list_directories</a>                 | Lists directories created within an account   |
| <a href="#">list_facet_attributes</a>            | Retrieves attributes attached to the facet  |
| <a href="#">list_facet_names</a>                 | Retrieves the names of facets that exist in a schema  |
| <a href="#">list_incoming_typed_links</a>        | Returns a paginated list of all the incoming TypedLinkSpecifier information for an object     |
| <a href="#">list_index</a>                       | Lists objects attached to the specified index   |
| <a href="#">list_managed_schema_arns</a>         | Lists the major version families of each managed schema                                       |
| <a href="#">list_object_attributes</a>           | Lists all attributes that are associated with an object                                       |
| <a href="#">list_object_children</a>             | Returns a paginated list of child objects that are associated with a given object             |
| <a href="#">list_object_parent_paths</a>         | Retrieves all available parent paths for any object type such as node, leaf node, policy node |
| <a href="#">list_object_parents</a>              | Lists parent objects that are associated with a given object in pagination fashion            |
| <a href="#">list_object_policies</a>             | Returns policies attached to an object in pagination fashion                                  |
| <a href="#">list_outgoing_typed_links</a>        | Returns a paginated list of all the outgoing TypedLinkSpecifier information for an object     |
| <a href="#">list_policy_attachments</a>          | Returns all of the ObjectIdentifiers to which a given policy is attached                      |
| <a href="#">list_published_schema_arns</a>       | Lists the major version families of each published schema                                     |
| <a href="#">list_tags_for_resource</a>           | Returns tags for a resource   |
| <a href="#">list_typed_link_facet_attributes</a> | Returns a paginated list of all attribute definitions for a particular TypedLinkFacet         |
| <a href="#">list_typed_link_facet_names</a>      | Returns a paginated list of TypedLink facet names for a particular schema                     |
| <a href="#">lookup_policy</a>                    | Lists all policies from the root of the Directory to the object specified                     |
| <a href="#">publish_schema</a>                   | Publishes a development schema with a major version and a recommended minor version           |
| <a href="#">put_schema_from_json</a>             | Allows a schema to be updated using JSON upload   |
| <a href="#">remove_facet_from_object</a>         | Removes the specified facet from the specified object   |
| <a href="#">tag_resource</a>                     | An API operation for adding tags to a resource  |
| <a href="#">untag_resource</a>                   | An API operation for removing tags from a resource  |
| <a href="#">update_facet</a>                     | Does the following:   |
| <a href="#">update_link_attributes</a>           | Updates a given typed link's attributes   |
| <a href="#">update_object_attributes</a>         | Updates a given object's attributes   |

|  |  |
|--|--|
| <a href="#">update_schema</a>            | Updates the schema name with a new name  |
| <a href="#">update_typed_link_facet</a>  | Updates a TypedLinkFacet   |
| <a href="#">upgrade_applied_schema</a>   | Upgrades a single directory in-place using the PublishedSchemaArn with schema updates    |
| <a href="#">upgrade_published_schema</a> | Upgrades a published schema under a new minor version revision using the current content |

## Examples

```
## Not run:
svc <- clouddirectory()
svc$add_facet_to_object(
  Foo = 123
)

## End(Not run)
```

---

cloudhsm

*Amazon CloudHSM*

---

## Description

AWS CloudHSM Service

This is documentation for **AWS CloudHSM Classic**. For more information, see [AWS CloudHSM Classic FAQs](#), the [AWS CloudHSM Classic User Guide](#), and the [AWS CloudHSM Classic API Reference](#).

**For information about the current version of AWS CloudHSM**, see [AWS CloudHSM](#), the [AWS CloudHSM User Guide](#), and the [AWS CloudHSM API Reference](#).

## Usage

```
cloudhsm(config = list(), credentials = list(), endpoint = NULL, region = NULL)
```

## Arguments

- config      Optional configuration of credentials, endpoint, and/or region.
- **credentials:**
    - **creds:**
      - \* **access\_key\_id:** AWS access key ID
      - \* **secret\_access\_key:** AWS secret access key
      - \* **session\_token:** AWS temporary session token
    - **profile:** The name of a profile to use. If not given, then the default profile is used.
    - **anonymous:** Set anonymous credentials.
  - **endpoint:** The complete URL to use for the constructed client.

|             |   |
|-------------|---|
|             | <ul style="list-style-type: none"> <li>• <b>region</b>: The AWS Region used in instantiating the client.</li> <li>• <b>close_connection</b>: Immediately close all HTTP connections.</li> <li>• <b>timeout</b>: The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.</li> <li>• <b>s3_force_path_style</b>: Set this to true to force the request to use path-style addressing, i.e. <code>http://s3.amazonaws.com/BUCKET/KEY</code>.</li> <li>• <b>sts_regional_endpoint</b>: Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul> |
| credentials | <p>Optional credentials shorthand for the config parameter</p> <ul style="list-style-type: none"> <li>• <b>creds</b>: <ul style="list-style-type: none"> <li>– <b>access_key_id</b>: AWS access key ID</li> <li>– <b>secret_access_key</b>: AWS secret access key</li> <li>– <b>session_token</b>: AWS temporary session token</li> </ul> </li> <li>• <b>profile</b>: The name of a profile to use. If not given, then the default profile is used.</li> <li>• <b>anonymous</b>: Set anonymous credentials.</li> </ul>  |
| endpoint    | Optional shorthand for complete URL to use for the constructed client.  |
| region      | Optional shorthand for AWS Region used in instantiating the client.   |

## Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

## Service syntax

```
svc <- cloudhsm(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
```

```

credentials = list(
  creds = list(
    access_key_id = "string",
    secret_access_key = "string",
    session_token = "string"
  ),
  profile = "string",
  anonymous = "logical"
),
endpoint = "string",
region = "string"
)

```

## Operations

|   |  |
|---|--|
| <a href="#">add_tags_to_resource</a>      | This is documentation for AWS CloudHSM Classic |
| <a href="#">create_hapg</a>               | This is documentation for AWS CloudHSM Classic |
| <a href="#">create_hsm</a>                | This is documentation for AWS CloudHSM Classic |
| <a href="#">create_luna_client</a>        | This is documentation for AWS CloudHSM Classic |
| <a href="#">delete_hapg</a>               | This is documentation for AWS CloudHSM Classic |
| <a href="#">delete_hsm</a>                | This is documentation for AWS CloudHSM Classic |
| <a href="#">delete_luna_client</a>        | This is documentation for AWS CloudHSM Classic |
| <a href="#">describe_hapg</a>             | This is documentation for AWS CloudHSM Classic |
| <a href="#">describe_hsm</a>              | This is documentation for AWS CloudHSM Classic |
| <a href="#">describe_luna_client</a>      | This is documentation for AWS CloudHSM Classic |
| <a href="#">get_config</a>                | This is documentation for AWS CloudHSM Classic |
| <a href="#">list_available_zones</a>      | This is documentation for AWS CloudHSM Classic |
| <a href="#">list_hapgs</a>                | This is documentation for AWS CloudHSM Classic |
| <a href="#">list_hsms</a>                 | This is documentation for AWS CloudHSM Classic |
| <a href="#">list_luna_clients</a>         | This is documentation for AWS CloudHSM Classic |
| <a href="#">list_tags_for_resource</a>    | This is documentation for AWS CloudHSM Classic |
| <a href="#">modify_hapg</a>               | This is documentation for AWS CloudHSM Classic |
| <a href="#">modify_hsm</a>                | This is documentation for AWS CloudHSM Classic |
| <a href="#">modify_luna_client</a>        | This is documentation for AWS CloudHSM Classic |
| <a href="#">remove_tags_from_resource</a> | This is documentation for AWS CloudHSM Classic |

## Examples

```

## Not run:
svc <- cloudhsm()
svc$add_tags_to_resource(
  Foo = 123
)

## End(Not run)

```

cloudhsmv2

AWS CloudHSM V2

**Description**

For more information about AWS CloudHSM, see [AWS CloudHSM](#) and the [AWS CloudHSM User Guide](#).

**Usage**

```
cloudhsmv2(
    config = list(),
    credentials = list(),
    endpoint = NULL,
    region = NULL
)
```

**Arguments**

`config` Optional configuration of credentials, endpoint, and/or region.

- **credentials:**

- **creds:**

- \* **access\_key\_id:** AWS access key ID
- \* **secret\_access\_key:** AWS secret access key
- \* **session\_token:** AWS temporary session token

- **profile:** The name of a profile to use. If not given, then the default profile is used.

- **anonymous:** Set anonymous credentials.

- **endpoint:** The complete URL to use for the constructed client.

- **region:** The AWS Region used in instantiating the client.

- **close\_connection:** Immediately close all HTTP connections.

- **timeout:** The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.

- **s3\_force\_path\_style:** Set this to `true` to force the request to use path-style addressing, i.e. `http://s3.amazonaws.com/BUCKET/KEY`.

- **sts\_regional\_endpoint:** Set sts regional endpoint resolver to regional or legacy <https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html>

`credentials` Optional credentials shorthand for the config parameter

- **creds:**

- **access\_key\_id:** AWS access key ID
- **secret\_access\_key:** AWS secret access key
- **session\_token:** AWS temporary session token

- **profile:** The name of a profile to use. If not given, then the default profile is used.
  - **anonymous:** Set anonymous credentials.
- endpoint      Optional shorthand for complete URL to use for the constructed client.
- region        Optional shorthand for AWS Region used in instantiating the client.

### Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

### Service syntax

```
svc <- cloudhsmv2(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
    creds = list(
      access_key_id = "string",
      secret_access_key = "string",
      session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
  ),
  endpoint = "string",
  region = "string"
)
```

### Operations

[copy\\_backup\\_to\\_region](#)      Copy an AWS CloudHSM cluster backup to a different region

|  |  |
|--|--|
| <a href="#">create_cluster</a>           | Creates a new AWS CloudHSM cluster   |
| <a href="#">create_hsm</a>               | Creates a new hardware security module (HSM) in the specified AWS CloudHSM cluster             |
| <a href="#">delete_backup</a>            | Deletes a specified AWS CloudHSM backup  |
| <a href="#">delete_cluster</a>           | Deletes the specified AWS CloudHSM cluster   |
| <a href="#">delete_hsm</a>               | Deletes the specified HSM  |
| <a href="#">describe_backups</a>         | Gets information about backups of AWS CloudHSM clusters  |
| <a href="#">describe_clusters</a>        | Gets information about AWS CloudHSM clusters   |
| <a href="#">initialize_cluster</a>       | Claims an AWS CloudHSM cluster by submitting the cluster certificate issued by your issuing ce |
| <a href="#">list_tags</a>                | Gets a list of tags for the specified AWS CloudHSM cluster                                     |
| <a href="#">modify_backup_attributes</a> | Modifies attributes for AWS CloudHSM backup  |
| <a href="#">modify_cluster</a>           | Modifies AWS CloudHSM cluster  |
| <a href="#">restore_backup</a>           | Restores a specified AWS CloudHSM backup that is in the PENDING_DELETION state                 |
| <a href="#">tag_resource</a>             | Adds or overwrites one or more tags for the specified AWS CloudHSM cluster                     |
| <a href="#">untag_resource</a>           | Removes the specified tag or tags from the specified AWS CloudHSM cluster                      |

## Examples

```
## Not run:
svc <- cloudhsmv2()
svc$copy_backup_to_region(
  Foo = 123
)

## End(Not run)
```

---

cognitoidentity

*Amazon Cognito Identity*

---

## Description

### Amazon Cognito Federated Identities

Amazon Cognito Federated Identities is a web service that delivers scoped temporary credentials to mobile devices and other untrusted environments. It uniquely identifies a device and supplies the user with a consistent identity over the lifetime of an application.

Using Amazon Cognito Federated Identities, you can enable authentication with one or more third-party identity providers (Facebook, Google, or Login with Amazon) or an Amazon Cognito user pool, and you can also choose to support unauthenticated access from your app. Cognito delivers a unique identifier for each user and acts as an OpenID token provider trusted by AWS Security Token Service (STS) to access temporary, limited-privilege AWS credentials.

For a description of the authentication flow from the Amazon Cognito Developer Guide see [Authentication Flow](#).

For more information see [Amazon Cognito Federated Identities](#).

**Usage**

```
cognitoidentity(
  config = list(),
  credentials = list(),
  endpoint = NULL,
  region = NULL
)
```

**Arguments**

|             |   |
|-------------|---|
| config      | Optional configuration of credentials, endpoint, and/or region. <ul style="list-style-type: none"> <li>• <b>credentials:</b> <ul style="list-style-type: none"> <li>– <b>creds:</b> <ul style="list-style-type: none"> <li>* <b>access_key_id:</b> AWS access key ID</li> <li>* <b>secret_access_key:</b> AWS secret access key</li> <li>* <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>– <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>– <b>anonymous:</b> Set anonymous credentials.</li> </ul> </li> <li>• <b>endpoint:</b> The complete URL to use for the constructed client.</li> <li>• <b>region:</b> The AWS Region used in instantiating the client.</li> <li>• <b>close_connection:</b> Immediately close all HTTP connections.</li> <li>• <b>timeout:</b> The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.</li> <li>• <b>s3_force_path_style:</b> Set this to true to force the request to use path-style addressing, i.e. <code>http://s3.amazonaws.com/BUCKET/KEY</code>.</li> <li>• <b>sts_regional_endpoint:</b> Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul> |
| credentials | Optional credentials shorthand for the config parameter <ul style="list-style-type: none"> <li>• <b>creds:</b> <ul style="list-style-type: none"> <li>– <b>access_key_id:</b> AWS access key ID</li> <li>– <b>secret_access_key:</b> AWS secret access key</li> <li>– <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>• <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>• <b>anonymous:</b> Set anonymous credentials.</li> </ul>   |
| endpoint    | Optional shorthand for complete URL to use for the constructed client.  |
| region      | Optional shorthand for AWS Region used in instantiating the client.   |

**Value**

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.



**Service syntax**

```

svc <- cognitoidentity(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
    creds = list(
      access_key_id = "string",
      secret_access_key = "string",
      session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
  ),
  endpoint = "string",
  region = "string"
)

```

**Operations**

|  |   |
|--|---|
| <a href="#">create_identity_pool</a>                     | Creates a new identity pool   |
| <a href="#">delete_identities</a>                        | Deletes identities from an identity pool  |
| <a href="#">delete_identity_pool</a>                     | Deletes an identity pool  |
| <a href="#">describe_identity</a>                        | Returns metadata related to the given identity, including when the identity was created                   |
| <a href="#">describe_identity_pool</a>                   | Gets details about a particular identity pool, including the pool name, ID description, and creation time |
| <a href="#">get_credentials_for_identity</a>             | Returns credentials for the provided identity ID  |
| <a href="#">get_id</a>                                   | Generates (or retrieves) a Cognito ID   |
| <a href="#">get_identity_pool_roles</a>                  | Gets the roles for an identity pool   |
| <a href="#">get_open_id_token</a>                        | Gets an OpenID token, using a known Cognito ID  |
| <a href="#">get_open_id_token_for_developer_identity</a> | Registers (or retrieves) a Cognito IdentityId and an OpenID Connect token for a developer identity        |
| <a href="#">get_principal_tag_attribute_map</a>          | Use GetPrincipalTagAttributeMap to list all mappings between PrincipalTags and AttributeKeys              |
| <a href="#">list_identities</a>                          | Lists the identities in an identity pool  |
| <a href="#">list_identity_pools</a>                      | Lists all of the Cognito identity pools registered for your account                                       |
| <a href="#">list_tags_for_resource</a>                   | Lists the tags that are assigned to an Amazon Cognito identity pool                                       |

|   |   |
|---|---|
| <a href="#">lookup_developer_identity</a>       | Retrieves the IdentityID associated with a DeveloperUserIdentifier or the list of |
| <a href="#">merge_developer_identities</a>      | Merges two users having different IdentityIds, existing in the same identity pool |
| <a href="#">set_identity_pool_roles</a>         | Sets the roles for an identity pool   |
| <a href="#">set_principal_tag_attribute_map</a> | You can use this operation to use default (username and clientID) attribute or cu |
| <a href="#">tag_resource</a>                    | Assigns a set of tags to the specified Amazon Cognito identity pool               |
| <a href="#">unlink_developer_identity</a>       | Unlinks a DeveloperUserIdentifier from an existing identity                       |
| <a href="#">unlink_identity</a>                 | Unlinks a federated identity from an existing account                             |
| <a href="#">untag_resource</a>                  | Removes the specified tags from the specified Amazon Cognito identity pool        |
| <a href="#">update_identity_pool</a>            | Updates an identity pool  |

## Examples

```
## Not run:
svc <- cognitoidentity()
svc$create_identity_pool(
  Foo = 123
)

## End(Not run)
```

---

cognitoidentityprovider

*Amazon Cognito Identity Provider*

---

## Description

With the Amazon Cognito user pools API, you can configure user pools and authenticate users. To authenticate users from third-party identity providers (IdPs) in this API, you can [link IdP users to native user profiles](#). Learn more about the authentication and authorization of federated users at [Adding user pool sign-in through a third party](#) and in the [User pool federation endpoints and hosted UI reference](#).

This API reference provides detailed information about API operations and object types in Amazon Cognito.

Along with resource management operations, the Amazon Cognito user pools API includes classes of operations and authorization models for client-side and server-side authentication of users. You can interact with operations in the Amazon Cognito user pools API as any of the following subjects.

1. An administrator who wants to configure user pools, app clients, users, groups, or other user pool functions.
2. A server-side app, like a web application, that wants to use its Amazon Web Services privileges to manage, authenticate, or authorize a user.
3. A client-side app, like a mobile app, that wants to make unauthenticated requests to manage, authenticate, or authorize a user.

For more information, see [Using the Amazon Cognito user pools API and user pool endpoints](#) in the *Amazon Cognito Developer Guide*.

With your Amazon Web Services SDK, you can build the logic to support operational flows in every use case for this API. You can also make direct REST API requests to [Amazon Cognito user pools service endpoints](#). The following links can get you started with the CognitoIdentityProvider client in other supported Amazon Web Services SDKs.

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

To get started with an Amazon Web Services SDK, see [Tools to Build on Amazon Web Services](#). For example actions and scenarios, see [Code examples for Amazon Cognito Identity Provider using Amazon Web Services SDKs](#).

## Usage

```
cognitoidentityprovider(  
    config = list(),  
    credentials = list(),  
    endpoint = NULL,  
    region = NULL  
)
```

## Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

- **credentials:**
  - **creds:**
    - \* **access\_key\_id:** AWS access key ID
    - \* **secret\_access\_key:** AWS secret access key
    - \* **session\_token:** AWS temporary session token
  - **profile:** The name of a profile to use. If not given, then the default profile is used.
  - **anonymous:** Set anonymous credentials.
- **endpoint:** The complete URL to use for the constructed client.
- **region:** The AWS Region used in instantiating the client.
- **close\_connection:** Immediately close all HTTP connections.

|             |  |
|-------------|--|
|             | <ul style="list-style-type: none"> <li>• <b>timeout:</b> The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.</li> <li>• <b>s3_force_path_style:</b> Set this to true to force the request to use path-style addressing, i.e. <code>http://s3.amazonaws.com/BUCKET/KEY</code>.</li> <li>• <b>sts_regional_endpoint:</b> Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul> |
| credentials | Optional credentials shorthand for the config parameter <ul style="list-style-type: none"> <li>• <b>creds:</b> <ul style="list-style-type: none"> <li>– <b>access_key_id:</b> AWS access key ID</li> <li>– <b>secret_access_key:</b> AWS secret access key</li> <li>– <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>• <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>• <b>anonymous:</b> Set anonymous credentials.</li> </ul>  |
| endpoint    | Optional shorthand for complete URL to use for the constructed client.   |
| region      | Optional shorthand for AWS Region used in instantiating the client.  |

### Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

### Service syntax

```
svc <- cognitoidentityprovider(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
    creds = list(
      access_key_id = "string",
```

```

        secret_access_key = "string",
        session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
),
endpoint = "string",
region = "string"
)

```

## Operations

|  |  |
|--|--|
| <a href="#">add_custom_attributes</a>            | Adds additional user attributes to the user pool schema                                  |
| <a href="#">admin_add_user_to_group</a>          | Adds a user to a group   |
| <a href="#">admin_confirm_sign_up</a>            | This IAM-authenticated API operation provides a code that Amazon Cognito sent to you     |
| <a href="#">admin_create_user</a>                | Creates a new user in the specified user pool  |
| <a href="#">admin_delete_user</a>                | Deletes a user as an administrator   |
| <a href="#">admin_delete_user_attributes</a>     | Deletes the user attributes in a user pool as an administrator                           |
| <a href="#">admin_disable_provider_for_user</a>  | Prevents the user from signing in with the specified external (SAML or social) identity  |
| <a href="#">admin_disable_user</a>               | Deactivates a user and revokes all access tokens for the user                            |
| <a href="#">admin_enable_user</a>                | Enables the specified user as an administrator   |
| <a href="#">admin_forget_device</a>              | Forgets the device, as an administrator  |
| <a href="#">admin_get_device</a>                 | Gets the device, as an administrator   |
| <a href="#">admin_get_user</a>                   | Gets the specified user by user name in a user pool as an administrator                  |
| <a href="#">admin_initiate_auth</a>              | Initiates the authentication flow, as an administrator                                   |
| <a href="#">admin_link_provider_for_user</a>     | Links an existing user account in a user pool (DestinationUser) to an identity from an e |
| <a href="#">admin_list_devices</a>               | Lists devices, as an administrator   |
| <a href="#">admin_list_groups_for_user</a>       | Lists the groups that a user belongs to  |
| <a href="#">admin_list_user_auth_events</a>      | A history of user activity and any risks detected as part of Amazon Cognito advanced s   |
| <a href="#">admin_remove_user_from_group</a>     | Removes the specified user from the specified group                                      |
| <a href="#">admin_reset_user_password</a>        | Resets the specified user's password in a user pool as an administrator                  |
| <a href="#">admin_respond_to_auth_challenge</a>  | Some API operations in a user pool generate a challenge, like a prompt for an MFA co     |
| <a href="#">admin_set_user_mfa_preference</a>    | The user's multi-factor authentication (MFA) preference, including which MFA option      |
| <a href="#">admin_set_user_password</a>          | Sets the specified user's password in a user pool as an administrator                    |
| <a href="#">admin_set_user_settings</a>          | This action is no longer supported   |
| <a href="#">admin_update_auth_event_feedback</a> | Provides feedback for an authentication event indicating if it was from a valid user     |
| <a href="#">admin_update_device_status</a>       | Updates the device status as an administrator  |
| <a href="#">admin_update_user_attributes</a>     | This action might generate an SMS text message   |
| <a href="#">admin_user_global_sign_out</a>       | Invalidates the identity, access, and refresh tokens that Amazon Cognito issued to a use |
| <a href="#">associate_software_token</a>         | Begins setup of time-based one-time password (TOTP) multi-factor authentication (MF      |
| <a href="#">change_password</a>                  | Changes the password for a specified user in a user pool                                 |
| <a href="#">confirm_device</a>                   | Confirms tracking of the device  |
| <a href="#">confirm_forgot_password</a>          | Allows a user to enter a confirmation code to reset a forgotten password                 |
| <a href="#">confirm_sign_up</a>                  | This public API operation provides a code that Amazon Cognito sent to your user whe      |
| <a href="#">create_group</a>                     | Creates a new group in the specified user pool   |
| <a href="#">create_identity_provider</a>         | Creates an IdP for a user pool   |
| <a href="#">create_resource_server</a>           | Creates a new OAuth2   |
| <a href="#">create_user_import_job</a>           | Creates a user import job  |

|   |  |
|---|--|
| <code>create_user_pool</code>                     | This action might generate an SMS text message   |
| <code>create_user_pool_client</code>              | Creates the user pool client   |
| <code>create_user_pool_domain</code>              | Creates a new domain for a user pool   |
| <code>delete_group</code>                         | Deletes a group  |
| <code>delete_identity_provider</code>             | Deletes an IdP for a user pool   |
| <code>delete_resource_server</code>               | Deletes a resource server  |
| <code>delete_user</code>                          | Allows a user to delete their own user profile   |
| <code>delete_user_attributes</code>               | Deletes the attributes for a user  |
| <code>delete_user_pool</code>                     | Deletes the specified Amazon Cognito user pool   |
| <code>delete_user_pool_client</code>              | Allows the developer to delete the user pool client  |
| <code>delete_user_pool_domain</code>              | Deletes a domain for a user pool   |
| <code>describe_identity_provider</code>           | Gets information about a specific IdP  |
| <code>describe_resource_server</code>             | Describes a resource server  |
| <code>describe_risk_configuration</code>          | Describes the risk configuration   |
| <code>describe_user_import_job</code>             | Describes the user import job  |
| <code>describe_user_pool</code>                   | Returns the configuration information and metadata of the specified user pool                                  |
| <code>describe_user_pool_client</code>            | Client method for returning the configuration information and metadata of the specified user pool client       |
| <code>describe_user_pool_domain</code>            | Gets information about a domain  |
| <code>forget_device</code>                        | Forgets the specified device   |
| <code>forgot_password</code>                      | Calling this API causes a message to be sent to the end user with a confirmation code to reset their password  |
| <code>get_csv_header</code>                       | Gets the header information for the comma-separated value (CSV) file to be used as input for a user import job |
| <code>get_device</code>                           | Gets the device  |
| <code>get_group</code>                            | Gets a group   |
| <code>get_identity_provider_by_identifier</code>  | Gets the specified IdP   |
| <code>get_log_delivery_configuration</code>       | Gets the detailed activity logging configuration for a user pool   |
| <code>get_signing_certificate</code>              | This method takes a user pool ID, and returns the signing certificate  |
| <code>get_ui_customization</code>                 | Gets the user interface (UI) Customization information for a particular app client's app                       |
| <code>get_user</code>                             | Gets the user attributes and metadata for a user   |
| <code>get_user_attribute_verification_code</code> | Generates a user attribute verification code for the specified attribute name                                  |
| <code>get_user_pool_mfa_config</code>             | Gets the user pool multi-factor authentication (MFA) configuration   |
| <code>global_sign_out</code>                      | Invalidates the identity, access, and refresh tokens that Amazon Cognito issued to a user                      |
| <code>initiate_auth</code>                        | Initiates sign-in for a user in the Amazon Cognito user directory  |
| <code>list_devices</code>                         | Lists the sign-in devices that Amazon Cognito has registered to the current user                               |
| <code>list_groups</code>                          | Lists the groups associated with a user pool   |
| <code>list_identity_providers</code>              | Lists information about all IdPs for a user pool   |
| <code>list_resource_servers</code>                | Lists the resource servers for a user pool   |
| <code>list_tags_for_resource</code>               | Lists the tags that are assigned to an Amazon Cognito user pool  |
| <code>list_user_import_jobs</code>                | Lists user import jobs for a user pool   |
| <code>list_user_pool_clients</code>               | Lists the clients that have been created for the specified user pool   |
| <code>list_user_pools</code>                      | Lists the user pools associated with an Amazon Web Services account  |
| <code>list_users</code>                           | Lists users and their basic details in a user pool   |
| <code>list_users_in_group</code>                  | Lists the users in the specified group   |
| <code>resend_confirmation_code</code>             | Resends the confirmation (for confirmation of registration) to a specific user in the user pool                |
| <code>respond_to_auth_challenge</code>            | Some API operations in a user pool generate a challenge, like a prompt for an MFA code                         |
| <code>revoke_token</code>                         | Revokes all of the access tokens generated by, and at the same time as, the specified refresh token            |
| <code>set_log_delivery_configuration</code>       | Sets up or modifies the detailed activity logging configuration of a user pool                                 |
| <code>set_risk_configuration</code>               | Configures actions on detected risks   |
| <code>set_ui_customization</code>                 | Sets the user interface (UI) customization information for a user pool's built-in app UI                       |

|   |   |
|---|---|
| <code>set_user_mfa_preference</code>    | Set the user's multi-factor authentication (MFA) method preference, including which MFA method is preferred |
| <code>set_user_pool_mfa_config</code>   | Sets the user pool multi-factor authentication (MFA) configuration  |
| <code>set_user_settings</code>          | This action is no longer supported  |
| <code>sign_up</code>                    | Registers the user in the specified user pool and creates a user name, password, and user attributes        |
| <code>start_user_import_job</code>      | Starts the user import  |
| <code>stop_user_import_job</code>       | Stops the user import job   |
| <code>tag_resource</code>               | Assigns a set of tags to an Amazon Cognito user pool  |
| <code>untag_resource</code>             | Removes the specified tags from an Amazon Cognito user pool   |
| <code>update_auth_event_feedback</code> | Provides the feedback for an authentication event, whether it was from a valid user or not                  |
| <code>update_device_status</code>       | Updates the device status   |
| <code>update_group</code>               | Updates the specified group with the specified attributes   |
| <code>update_identity_provider</code>   | Updates IdP information for a user pool   |
| <code>update_resource_server</code>     | Updates the name and scopes of resource server  |
| <code>update_user_attributes</code>     | With this operation, your users can update one or more of their attributes with their own user attributes   |
| <code>update_user_pool</code>           | This action might generate an SMS text message  |
| <code>update_user_pool_client</code>    | Updates the specified user pool app client with the specified attributes                                    |
| <code>update_user_pool_domain</code>    | Updates the Secure Sockets Layer (SSL) certificate for the custom domain for your user pool                 |
| <code>verify_software_token</code>      | Use this API to register a user's entered time-based one-time password (TOTP) code and verify it            |
| <code>verify_user_attribute</code>      | Verifies the specified user attributes in the user pool   |

## Examples

```
## Not run:
svc <- cognitoidentityprovider()
# This request submits a value for all possible parameters for
# AdminCreateUser.
svc$admin_create_user(
  DesiredDeliveryMediums = list(
    "SMS"
  ),
  MessageAction = "SUPPRESS",
  TemporaryPassword = "This-is-my-test-99!",
  UserAttributes = list(
    list(
      Name = "name",
      Value = "John"
    ),
    list(
      Name = "phone_number",
      Value = "+12065551212"
    ),
    list(
      Name = "email",
      Value = "testuser@example.com"
    )
  ),
  UserPoolId = "us-east-1_EXAMPLE",
  Username = "testuser"
)
```

```
## End(Not run)
```

---

cognitosync

*Amazon Cognito Sync*

---

## Description

Amazon Cognito Sync provides an AWS service and client library that enable cross-device syncing of application-related user data. High-level client libraries are available for both iOS and Android. You can use these libraries to persist data locally so that it's available even if the device is offline. Developer credentials don't need to be stored on the mobile device to access the service. You can use Amazon Cognito to obtain a normalized user ID and credentials. User data is persisted in a dataset that can store up to 1 MB of key-value pairs, and you can have up to 20 datasets per user identity.

With Amazon Cognito Sync, the data stored for each identity is accessible only to credentials assigned to that identity. In order to use the Cognito Sync service, you need to make API calls using credentials retrieved with [Amazon Cognito Identity service](#).

If you want to use Cognito Sync in an Android or iOS application, you will probably want to make API calls via the AWS Mobile SDK. To learn more, see the [Developer Guide for Android](#) and the [Developer Guide for iOS](#).

## Usage

```
cognitosync(
  config = list(),
  credentials = list(),
  endpoint = NULL,
  region = NULL
)
```

## Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

- **credentials:**
  - **creds:**
    - \* **access\_key\_id:** AWS access key ID
    - \* **secret\_access\_key:** AWS secret access key
    - \* **session\_token:** AWS temporary session token
  - **profile:** The name of a profile to use. If not given, then the default profile is used.
  - **anonymous:** Set anonymous credentials.
- **endpoint:** The complete URL to use for the constructed client.
- **region:** The AWS Region used in instantiating the client.



|             |  |
|-------------|--|
|             | <ul style="list-style-type: none"> <li>• <b>close_connection</b>: Immediately close all HTTP connections.</li> <li>• <b>timeout</b>: The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.</li> <li>• <b>s3_force_path_style</b>: Set this to true to force the request to use path-style addressing, i.e. <code>http://s3.amazonaws.com/BUCKET/KEY</code>.</li> <li>• <b>sts_regional_endpoint</b>: Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul> |
| credentials | Optional credentials shorthand for the config parameter <ul style="list-style-type: none"> <li>• <b>creds</b>: <ul style="list-style-type: none"> <li>– <b>access_key_id</b>: AWS access key ID</li> <li>– <b>secret_access_key</b>: AWS secret access key</li> <li>– <b>session_token</b>: AWS temporary session token</li> </ul> </li> <li>• <b>profile</b>: The name of a profile to use. If not given, then the default profile is used.</li> <li>• <b>anonymous</b>: Set anonymous credentials.</li> </ul>  |
| endpoint    | Optional shorthand for complete URL to use for the constructed client.   |
| region      | Optional shorthand for AWS Region used in instantiating the client.  |

### Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

### Service syntax

```
svc <- cognitosync(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
```

```

    creds = list(
      access_key_id = "string",
      secret_access_key = "string",
      session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
  ),
  endpoint = "string",
  region = "string"
)

```

## Operations

|   |   |
|---|---|
| <a href="#">bulk_publish</a>                    | Initiates a bulk publish of all existing datasets for an Identity Pool to the configured stream |
| <a href="#">delete_dataset</a>                  | Deletes the specific dataset  |
| <a href="#">describe_dataset</a>                | Gets meta data about a dataset by identity and dataset name                                     |
| <a href="#">describe_identity_pool_usage</a>    | Gets usage details (for example, data storage) about a particular identity pool                 |
| <a href="#">describe_identity_usage</a>         | Gets usage information for an identity, including number of datasets and data usage             |
| <a href="#">get_bulk_publish_details</a>        | Get the status of the last BulkPublish operation for an identity pool                           |
| <a href="#">get_cognito_events</a>              | Gets the events and the corresponding Lambda functions associated with an identity pool         |
| <a href="#">get_identity_pool_configuration</a> | Gets the configuration settings of an identity pool   |
| <a href="#">list_datasets</a>                   | Lists datasets for an identity  |
| <a href="#">list_identity_pool_usage</a>        | Gets a list of identity pools registered with Cognito   |
| <a href="#">list_records</a>                    | Gets paginated records, optionally changed after a particular sync count for a dataset and id   |
| <a href="#">register_device</a>                 | Registers a device to receive push sync notifications   |
| <a href="#">set_cognito_events</a>              | Sets the AWS Lambda function for a given event type for an identity pool                        |
| <a href="#">set_identity_pool_configuration</a> | Sets the necessary configuration for push sync  |
| <a href="#">subscribe_to_dataset</a>            | Subscribes to receive notifications when a dataset is modified by another device                |
| <a href="#">unsubscribe_from_dataset</a>        | Unsubscribes from receiving notifications when a dataset is modified by another device          |
| <a href="#">update_records</a>                  | Posts updates to records and adds and deletes records for a dataset and user                    |

## Examples

```

## Not run:
svc <- cognitosync()
svc$bulk_publish(
  Foo = 123
)

## End(Not run)

```

**Description**

Detective uses machine learning and purpose-built visualizations to help you to analyze and investigate security issues across your Amazon Web Services (Amazon Web Services) workloads. Detective automatically extracts time-based events such as login attempts, API calls, and network traffic from CloudTrail and Amazon Virtual Private Cloud (Amazon VPC) flow logs. It also extracts findings detected by Amazon GuardDuty.

The Detective API primarily supports the creation and management of behavior graphs. A behavior graph contains the extracted data from a set of member accounts, and is created and managed by an administrator account.

To add a member account to the behavior graph, the administrator account sends an invitation to the account. When the account accepts the invitation, it becomes a member account in the behavior graph.

Detective is also integrated with Organizations. The organization management account designates the Detective administrator account for the organization. That account becomes the administrator account for the organization behavior graph. The Detective administrator account is also the delegated administrator account for Detective in Organizations.

The Detective administrator account can enable any organization account as a member account in the organization behavior graph. The organization accounts do not receive invitations. The Detective administrator account can also invite other accounts to the organization behavior graph.

Every behavior graph is specific to a Region. You can only use the API to manage behavior graphs that belong to the Region that is associated with the currently selected endpoint.

The administrator account for a behavior graph can use the Detective API to do the following:

- Enable and disable Detective. Enabling Detective creates a new behavior graph.
- View the list of member accounts in a behavior graph.
- Add member accounts to a behavior graph.
- Remove member accounts from a behavior graph.
- Apply tags to a behavior graph.

The organization management account can use the Detective API to select the delegated administrator for Detective.

The Detective administrator account for an organization can use the Detective API to do the following:

- Perform all of the functions of an administrator account.
- Determine whether to automatically enable new organization accounts as member accounts in the organization behavior graph.

An invited member account can use the Detective API to do the following:

- View the list of behavior graphs that they are invited to.

- Accept an invitation to contribute to a behavior graph.
- Decline an invitation to contribute to a behavior graph.
- Remove their account from a behavior graph.

All API actions are logged as CloudTrail events. See [Logging Detective API Calls with CloudTrail](#).

We replaced the term "master account" with the term "administrator account." An administrator account is used to centrally manage multiple accounts. In the case of Detective, the administrator account manages the accounts in their behavior graph.

## Usage

```
detective(
  config = list(),
  credentials = list(),
  endpoint = NULL,
  region = NULL
)
```

## Arguments

|             |   |
|-------------|---|
| config      | Optional configuration of credentials, endpoint, and/or region. <ul style="list-style-type: none"> <li>• <b>credentials:</b> <ul style="list-style-type: none"> <li>– <b>creds:</b> <ul style="list-style-type: none"> <li>* <b>access_key_id:</b> AWS access key ID</li> <li>* <b>secret_access_key:</b> AWS secret access key</li> <li>* <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>– <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>– <b>anonymous:</b> Set anonymous credentials.</li> </ul> </li> <li>• <b>endpoint:</b> The complete URL to use for the constructed client.</li> <li>• <b>region:</b> The AWS Region used in instantiating the client.</li> <li>• <b>close_connection:</b> Immediately close all HTTP connections.</li> <li>• <b>timeout:</b> The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.</li> <li>• <b>s3_force_path_style:</b> Set this to true to force the request to use path-style addressing, i.e. <code>http://s3.amazonaws.com/BUCKET/KEY</code>.</li> <li>• <b>sts_regional_endpoint:</b> Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul> |
| credentials | Optional credentials shorthand for the config parameter <ul style="list-style-type: none"> <li>• <b>creds:</b> <ul style="list-style-type: none"> <li>– <b>access_key_id:</b> AWS access key ID</li> <li>– <b>secret_access_key:</b> AWS secret access key</li> <li>– <b>session_token:</b> AWS temporary session token</li> </ul> </li> </ul>  |

- **profile:** The name of a profile to use. If not given, then the default profile is used.
  - **anonymous:** Set anonymous credentials.
- endpoint      Optional shorthand for complete URL to use for the constructed client.
- region        Optional shorthand for AWS Region used in instantiating the client.

### Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

### Service syntax

```
svc <- detective(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
    creds = list(
      access_key_id = "string",
      secret_access_key = "string",
      session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
  ),
  endpoint = "string",
  region = "string"
)
```

### Operations

[accept\\_invitation](#)

Accepts an invitation for the member account to contribute data to a behavior graph

|  |   |
|--|---|
| <code>batch_get_graph_member_datasources</code>  | Gets data source package information for the behavior graph   |
| <code>batch_get_membership_datasources</code>    | Gets information on the data source package history for an account  |
| <code>create_graph</code>                        | Creates a new behavior graph for the calling account, and sets that account as the administrator. CreateMembers is used to send invitations to accounts |
| <code>create_members</code>                      | CreateMembers is used to send invitations to accounts   |
| <code>delete_graph</code>                        | Disables the specified behavior graph and queues it to be deleted   |
| <code>delete_members</code>                      | Removes the specified member accounts from the behavior graph   |
| <code>describe_organization_configuration</code> | Returns information about the configuration for the organization behavior graph   |
| <code>disable_organization_admin_account</code>  | Removes the Detective administrator account in the current Region   |
| <code>disassociate_membership</code>             | Removes the member account from the specified behavior graph  |
| <code>enable_organization_admin_account</code>   | Designates the Detective administrator account for the organization in the current Region   |
| <code>get_investigation</code>                   | Returns the investigation results of an investigation for a behavior graph  |
| <code>get_members</code>                         | Returns the membership details for specified member accounts for a behavior graph   |
| <code>list_datasource_packages</code>            | Lists data source packages in the behavior graph  |
| <code>list_graphs</code>                         | Returns the list of behavior graphs that the calling account is an administrator account for  |
| <code>list_indicators</code>                     | Get the indicators from an investigation  |
| <code>list_investigations</code>                 | List all Investigations   |
| <code>list_invitations</code>                    | Retrieves the list of open and accepted behavior graph invitations for the member account   |
| <code>list_members</code>                        | Retrieves the list of member accounts for a behavior graph  |
| <code>list_organization_admin_accounts</code>    | Returns information about the Detective administrator account for an organization   |
| <code>list_tags_for_resource</code>              | Returns the tag values that are assigned to a behavior graph  |
| <code>reject_invitation</code>                   | Rejects an invitation to contribute the account data to a behavior graph  |
| <code>start_investigation</code>                 | initiate an investigation on an entity in a graph   |
| <code>start_monitoring_member</code>             | Sends a request to enable data ingest for a member account that has a status of ACCREDITED  |
| <code>tag_resource</code>                        | Applies tag values to a behavior graph  |
| <code>untag_resource</code>                      | Removes tags from a behavior graph  |
| <code>update_datasource_packages</code>          | Starts a data source packages for the behavior graph  |
| <code>update_investigation_state</code>          | Update the state of an investigation  |
| <code>update_organization_configuration</code>   | Updates the configuration for the Organizations integration in the current Region   |

## Examples

```
## Not run:
svc <- detective()
svc$accept_invitation(
  Foo = 123
)

## End(Not run)
```

## Description

### Directory Service

Directory Service is a web service that makes it easy for you to setup and run directories in the Amazon Web Services cloud, or connect your Amazon Web Services resources with an existing self-managed Microsoft Active Directory. This guide provides detailed information about Directory Service operations, data types, parameters, and errors. For information about Directory Services features, see [Directory Service](#) and the [Directory Service Administration Guide](#).

Amazon Web Services provides SDKs that consist of libraries and sample code for various programming languages and platforms (Java, Ruby, .Net, iOS, Android, etc.). The SDKs provide a convenient way to create programmatic access to Directory Service and other Amazon Web Services services. For more information about the Amazon Web Services SDKs, including how to download and install them, see [Tools for Amazon Web Services](#).

## Usage

```
directoryservice(
  config = list(),
  credentials = list(),
  endpoint = NULL,
  region = NULL
)
```

## Arguments

|             |  |
|-------------|--|
| config      | <p>Optional configuration of credentials, endpoint, and/or region.</p> <ul style="list-style-type: none"> <li>• <b>credentials:</b> <ul style="list-style-type: none"> <li>– <b>creds:</b> <ul style="list-style-type: none"> <li>* <b>access_key_id:</b> AWS access key ID</li> <li>* <b>secret_access_key:</b> AWS secret access key</li> <li>* <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>– <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>– <b>anonymous:</b> Set anonymous credentials.</li> </ul> </li> <li>• <b>endpoint:</b> The complete URL to use for the constructed client.</li> <li>• <b>region:</b> The AWS Region used in instantiating the client.</li> <li>• <b>close_connection:</b> Immediately close all HTTP connections.</li> <li>• <b>timeout:</b> The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.</li> <li>• <b>s3_force_path_style:</b> Set this to true to force the request to use path-style addressing, i.e. <code>http://s3.amazonaws.com/BUCKET/KEY</code>.</li> <li>• <b>sts_regional_endpoint:</b> Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul> |
| credentials | <p>Optional credentials shorthand for the config parameter</p> <ul style="list-style-type: none"> <li>• <b>creds:</b></li> </ul>   |

- **access\_key\_id**: AWS access key ID
  - **secret\_access\_key**: AWS secret access key
  - **session\_token**: AWS temporary session token
  - **profile**: The name of a profile to use. If not given, then the default profile is used.
  - **anonymous**: Set anonymous credentials.
- endpoint           Optional shorthand for complete URL to use for the constructed client.
- region             Optional shorthand for AWS Region used in instantiating the client.

### Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

### Service syntax

```
svc <- directoryservice(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
    creds = list(
      access_key_id = "string",
      secret_access_key = "string",
      session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
  ),
  endpoint = "string",
  region = "string"
)
```



**Operations**

|   |  |
|---|--|
| <a href="#">accept_shared_directory</a>                 | Accepts a directory sharing request that was sent from the directory owner account.  |
| <a href="#">add_ip_routes</a>                           | If the DNS server for your self-managed domain uses a publicly addressable IP address, you can add IP address blocks to your domain.   |
| <a href="#">add_region</a>                              | Adds two domain controllers in the specified Region for the specified directory.   |
| <a href="#">add_tags_to_resource</a>                    | Adds or overwrites one or more tags for the specified directory.   |
| <a href="#">cancel_schema_extension</a>                 | Cancels an in-progress schema extension to a Microsoft AD directory.   |
| <a href="#">connect_directory</a>                       | Creates an AD Connector to connect to a self-managed directory.  |
| <a href="#">create_alias</a>                            | Creates an alias for a directory and assigns the alias to the directory.   |
| <a href="#">create_computer</a>                         | Creates an Active Directory computer object in the specified directory.  |
| <a href="#">create_conditional_forwarder</a>            | Creates a conditional forwarder associated with your Amazon Web Services directory.  |
| <a href="#">create_directory</a>                        | Creates a Simple AD directory.   |
| <a href="#">create_log_subscription</a>                 | Creates a subscription to forward real-time Directory Service domain controller security events to an Amazon SNS topic.  |
| <a href="#">create_microsoft_ad</a>                     | Creates a Microsoft AD directory in the Amazon Web Services Cloud.   |
| <a href="#">create_snapshot</a>                         | Creates a snapshot of a Simple AD or Microsoft AD directory in the Amazon Web Services Cloud.  |
| <a href="#">create_trust</a>                            | Directory Service for Microsoft Active Directory allows you to configure trust relationships between your Managed Microsoft AD directory and other Active Directory domains. |
| <a href="#">delete_conditional_forwarder</a>            | Deletes a conditional forwarder that has been set up for your Amazon Web Services directory.   |
| <a href="#">delete_directory</a>                        | Deletes an Directory Service directory.  |
| <a href="#">delete_log_subscription</a>                 | Deletes the specified log subscription.  |
| <a href="#">delete_snapshot</a>                         | Deletes a directory snapshot.  |
| <a href="#">delete_trust</a>                            | Deletes an existing trust relationship between your Managed Microsoft AD directory and another Active Directory domain.  |
| <a href="#">deregister_certificate</a>                  | Deletes from the system the certificate that was registered for secure LDAP or client authentication.  |
| <a href="#">deregister_event_topic</a>                  | Removes the specified directory as a publisher to the specified Amazon SNS topic.  |
| <a href="#">describe_certificate</a>                    | Displays information about the certificate registered for secure LDAP or client authentication.  |
| <a href="#">describe_client_authentication_settings</a> | Retrieves information about the type of client authentication for the specified directory.   |
| <a href="#">describe_conditional_forwarders</a>         | Obtains information about the conditional forwarders for this account.   |
| <a href="#">describe_directories</a>                    | Obtains information about the directories that belong to this account.   |
| <a href="#">describe_domain_controllers</a>             | Provides information about any domain controllers in your directory.   |
| <a href="#">describe_event_topics</a>                   | Obtains information about which Amazon SNS topics receive status messages from this account.   |
| <a href="#">describe_ldaps_settings</a>                 | Describes the status of LDAP security for the specified directory.   |
| <a href="#">describe_regions</a>                        | Provides information about the Regions that are configured for multi-Region replication.   |
| <a href="#">describe_settings</a>                       | Retrieves information about the configurable settings for the specified directory.   |
| <a href="#">describe_shared_directories</a>             | Returns the shared directories in your account.  |
| <a href="#">describe_snapshots</a>                      | Obtains information about the directory snapshots that belong to this account.   |
| <a href="#">describe_trusts</a>                         | Obtains information about the trust relationships for this account.  |
| <a href="#">describe_update_directory</a>               | Describes the updates of a directory for a particular update type.   |
| <a href="#">disable_client_authentication</a>           | Disables alternative client authentication methods for the specified directory.  |
| <a href="#">disable_ldaps</a>                           | Deactivates LDAP secure calls for the specified directory.   |
| <a href="#">disable_radius</a>                          | Disables multi-factor authentication (MFA) with the Remote Authentication Dial In User Service (RADIUS) protocol.  |
| <a href="#">disable_sso</a>                             | Disables single-sign on for a directory.   |
| <a href="#">enable_client_authentication</a>            | Enables alternative client authentication methods for the specified directory.   |
| <a href="#">enable_ldaps</a>                            | Activates the switch for the specific directory to always use LDAP secure calls.   |
| <a href="#">enable_radius</a>                           | Enables multi-factor authentication (MFA) with the Remote Authentication Dial In User Service (RADIUS) protocol.   |
| <a href="#">enable_sso</a>                              | Enables single sign-on for a directory.  |
| <a href="#">get_directory_limits</a>                    | Obtains directory limit information for the current Region.  |
| <a href="#">get_snapshot_limits</a>                     | Obtains the manual snapshot limits for a directory.  |
| <a href="#">list_certificates</a>                       | For the specified directory, lists all the certificates registered for a secure LDAP or client authentication.   |
| <a href="#">list_ip_routes</a>                          | Lists the address blocks that you have added to a directory.   |

|   |  |
|---|--|
| <a href="#">list_log_subscriptions</a>              | Lists the active log subscriptions for the Amazon Web Services account               |
| <a href="#">list_schema_extensions</a>              | Lists all schema extensions applied to a Microsoft AD Directory                      |
| <a href="#">list_tags_for_resource</a>              | Lists all tags on a directory  |
| <a href="#">register_certificate</a>                | Registers a certificate for a secure LDAP or client certificate authentication       |
| <a href="#">register_event_topic</a>                | Associates a directory with an Amazon SNS topic                                      |
| <a href="#">reject_shared_directory</a>             | Rejects a directory sharing request that was sent from the directory owner account   |
| <a href="#">remove_ip_routes</a>                    | Removes IP address blocks from a directory   |
| <a href="#">remove_region</a>                       | Stops all replication and removes the domain controllers from the specified Region   |
| <a href="#">remove_tags_from_resource</a>           | Removes tags from a directory  |
| <a href="#">reset_user_password</a>                 | Resets the password for any user in your Managed Microsoft AD or Simple AD directory |
| <a href="#">restore_from_snapshot</a>               | Restores a directory using an existing directory snapshot                            |
| <a href="#">share_directory</a>                     | Shares a specified directory (DirectoryId) in your Amazon Web Services account (d    |
| <a href="#">start_schema_extension</a>              | Applies a schema extension to a Microsoft AD directory                               |
| <a href="#">unshare_directory</a>                   | Stops the directory sharing between the directory owner and consumer accounts        |
| <a href="#">update_conditional_forwarder</a>        | Updates a conditional forwarder that has been set up for your Amazon Web Services    |
| <a href="#">update_directory_setup</a>              | Updates the directory for a particular update type                                   |
| <a href="#">update_number_of_domain_controllers</a> | Adds or removes domain controllers to or from the directory                          |
| <a href="#">update_radius</a>                       | Updates the Remote Authentication Dial In User Service (RADIUS) server informa       |
| <a href="#">update_settings</a>                     | Updates the configurable settings for the specified directory                        |
| <a href="#">update_trust</a>                        | Updates the trust that has been set up between your Managed Microsoft AD directo     |
| <a href="#">verify_trust</a>                        | Directory Service for Microsoft Active Directory allows you to configure and verify  |

## Examples

```
## Not run:
svc <- directoryservice()
svc$accept_shared_directory(
  Foo = 123
)

## End(Not run)
```

---

fms

*Firewall Management Service*

---

## Description

This is the *Firewall Manager API Reference*. This guide is for developers who need detailed information about the Firewall Manager API actions, data types, and errors. For detailed information about Firewall Manager features, see the [Firewall Manager Developer Guide](#).

Some API actions require explicit resource permissions. For information, see the developer guide topic [Service roles for Firewall Manager](#).

**Usage**

```
fms(config = list(), credentials = list(), endpoint = NULL, region = NULL)
```

**Arguments**

|             |  |
|-------------|--|
| config      | <p>Optional configuration of credentials, endpoint, and/or region.</p> <ul style="list-style-type: none"> <li>• <b>credentials:</b> <ul style="list-style-type: none"> <li>– <b>creds:</b> <ul style="list-style-type: none"> <li>* <b>access_key_id:</b> AWS access key ID</li> <li>* <b>secret_access_key:</b> AWS secret access key</li> <li>* <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>– <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>– <b>anonymous:</b> Set anonymous credentials.</li> </ul> </li> <li>• <b>endpoint:</b> The complete URL to use for the constructed client.</li> <li>• <b>region:</b> The AWS Region used in instantiating the client.</li> <li>• <b>close_connection:</b> Immediately close all HTTP connections.</li> <li>• <b>timeout:</b> The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.</li> <li>• <b>s3_force_path_style:</b> Set this to true to force the request to use path-style addressing, i.e. <code>http://s3.amazonaws.com/BUCKET/KEY</code>.</li> <li>• <b>sts_regional_endpoint:</b> Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul> |
| credentials | <p>Optional credentials shorthand for the config parameter</p> <ul style="list-style-type: none"> <li>• <b>creds:</b> <ul style="list-style-type: none"> <li>– <b>access_key_id:</b> AWS access key ID</li> <li>– <b>secret_access_key:</b> AWS secret access key</li> <li>– <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>• <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>• <b>anonymous:</b> Set anonymous credentials.</li> </ul>   |
| endpoint    | Optional shorthand for complete URL to use for the constructed client.   |
| region      | Optional shorthand for AWS Region used in instantiating the client.  |

**Value**

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

**Service syntax**

```

svc <- fms(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
    creds = list(
      access_key_id = "string",
      secret_access_key = "string",
      session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
  ),
  endpoint = "string",
  region = "string"
)

```

**Operations**

|   |  |
|---|--|
| <a href="#">associate_admin_account</a>           | Sets a Firewall Manager default administrator account  |
| <a href="#">associate_third_party_firewall</a>    | Sets the Firewall Manager policy administrator as a tenant administrator of a third-party firewall |
| <a href="#">batch_associate_resource</a>          | Associate resources to a Firewall Manager resource set   |
| <a href="#">batch_disassociate_resource</a>       | Disassociates resources from a Firewall Manager resource set                                       |
| <a href="#">delete_apps_list</a>                  | Permanently deletes an Firewall Manager applications list  |
| <a href="#">delete_notification_channel</a>       | Deletes an Firewall Manager association with the IAM role and the Amazon SNS notification channel  |
| <a href="#">delete_policy</a>                     | Permanently deletes an Firewall Manager policy   |
| <a href="#">delete_protocols_list</a>             | Permanently deletes an Firewall Manager protocols list   |
| <a href="#">delete_resource_set</a>               | Deletes the specified ResourceSet  |
| <a href="#">disassociate_admin_account</a>        | Disassociates an Firewall Manager administrator account  |
| <a href="#">disassociate_third_party_firewall</a> | Disassociates a Firewall Manager policy administrator from a third-party firewall                  |
| <a href="#">get_admin_account</a>                 | Returns the Organizations account that is associated with Firewall Manager as the administrator    |
| <a href="#">get_admin_scope</a>                   | Returns information about the specified account's administrative scope                             |
| <a href="#">get_apps_list</a>                     | Returns information about the specified Firewall Manager applications list                         |

|  |   |
|--|---|
| <code>get_compliance_detail</code>                       | Returns detailed compliance information about the specified member account            |
| <code>get_notification_channel</code>                    | Information about the Amazon Simple Notification Service (SNS) topic that is u        |
| <code>get_policy</code>                                  | Returns information about the specified Firewall Manager policy                       |
| <code>get_protection_status</code>                       | If you created a Shield Advanced policy, returns policy-level attack summary in       |
| <code>get_protocols_list</code>                          | Returns information about the specified Firewall Manager protocols list               |
| <code>get_resource_set</code>                            | Gets information about a specific resource set  |
| <code>get_third_party_firewall_association_status</code> | The onboarding status of a Firewall Manager admin account to third-party firew        |
| <code>get_violation_details</code>                       | Retrieves violations for a resource based on the specified Firewall Manager poli      |
| <code>list_admin_accounts_for_organization</code>        | Returns a AdminAccounts object that lists the Firewall Manager administrators         |
| <code>list_admins_managing_account</code>                | Lists the accounts that are managing the specified Organizations member accou         |
| <code>list_apps_lists</code>                             | Returns an array of AppsListDataSummary objects                                       |
| <code>list_compliance_status</code>                      | Returns an array of PolicyComplianceStatus objects                                    |
| <code>list_discovered_resources</code>                   | Returns an array of resources in the organization's accounts that are available to    |
| <code>list_member_accounts</code>                        | Returns a MemberAccounts object that lists the member accounts in the admini          |
| <code>list_policies</code>                               | Returns an array of PolicySummary objects   |
| <code>list_protocols_lists</code>                        | Returns an array of ProtocolsListDataSummary objects                                  |
| <code>list_resource_set_resources</code>                 | Returns an array of resources that are currently associated to a resource set         |
| <code>list_resource_sets</code>                          | Returns an array of ResourceSetSummary objects  |
| <code>list_tags_for_resource</code>                      | Retrieves the list of tags for the specified Amazon Web Services resource             |
| <code>list_third_party_firewall_firewall_policies</code> | Retrieves a list of all of the third-party firewall policies that are associated with |
| <code>put_admin_account</code>                           | Creates or updates an Firewall Manager administrator account                          |
| <code>put_apps_list</code>                               | Creates an Firewall Manager applications list   |
| <code>put_notification_channel</code>                    | Designates the IAM role and Amazon Simple Notification Service (SNS) topic            |
| <code>put_policy</code>                                  | Creates an Firewall Manager policy  |
| <code>put_protocols_list</code>                          | Creates an Firewall Manager protocols list  |
| <code>put_resource_set</code>                            | Creates the resource set  |
| <code>tag_resource</code>                                | Adds one or more tags to an Amazon Web Services resource                              |
| <code>untag_resource</code>                              | Removes one or more tags from an Amazon Web Services resource                         |

## Examples

```
## Not run:
svc <- fms()
svc$associate_admin_account(
  Foo = 123
)

## End(Not run)
```

## Description

Amazon GuardDuty is a continuous security monitoring service that analyzes and processes the following foundational data sources - VPC flow logs, Amazon Web Services CloudTrail management event logs, CloudTrail S3 data event logs, EKS audit logs, DNS logs, Amazon EBS volume data, runtime activity belonging to container workloads, such as Amazon EKS, Amazon ECS (including Amazon Web Services Fargate), and Amazon EC2 instances. It uses threat intelligence feeds, such as lists of malicious IPs and domains, and machine learning to identify unexpected, potentially unauthorized, and malicious activity within your Amazon Web Services environment. This can include issues like escalations of privileges, uses of exposed credentials, or communication with malicious IPs, domains, or presence of malware on your Amazon EC2 instances and container workloads. For example, GuardDuty can detect compromised EC2 instances and container workloads serving malware, or mining bitcoin.

GuardDuty also monitors Amazon Web Services account access behavior for signs of compromise, such as unauthorized infrastructure deployments like EC2 instances deployed in a Region that has never been used, or unusual API calls like a password policy change to reduce password strength.

GuardDuty informs you about the status of your Amazon Web Services environment by producing security findings that you can view in the GuardDuty console or through Amazon EventBridge. For more information, see the *Amazon GuardDuty User Guide*.

## Usage

```
guardduty(
  config = list(),
  credentials = list(),
  endpoint = NULL,
  region = NULL
)
```

## Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

- **credentials:**
  - **creds:**
    - \* **access\_key\_id:** AWS access key ID
    - \* **secret\_access\_key:** AWS secret access key
    - \* **session\_token:** AWS temporary session token
  - **profile:** The name of a profile to use. If not given, then the default profile is used.
  - **anonymous:** Set anonymous credentials.
- **endpoint:** The complete URL to use for the constructed client.
- **region:** The AWS Region used in instantiating the client.
- **close\_connection:** Immediately close all HTTP connections.
- **timeout:** The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.
- **s3\_force\_path\_style:** Set this to `true` to force the request to use path-style addressing, i.e. `http://s3.amazonaws.com/BUCKET/KEY`.

|             |  |
|-------------|--|
|             | <ul style="list-style-type: none"> <li>• <b>sts_regional_endpoint</b>: Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul>   |
| credentials | <p>Optional credentials shorthand for the config parameter</p> <ul style="list-style-type: none"> <li>• <b>creds</b>: <ul style="list-style-type: none"> <li>– <b>access_key_id</b>: AWS access key ID</li> <li>– <b>secret_access_key</b>: AWS secret access key</li> <li>– <b>session_token</b>: AWS temporary session token</li> </ul> </li> <li>• <b>profile</b>: The name of a profile to use. If not given, then the default profile is used.</li> <li>• <b>anonymous</b>: Set anonymous credentials.</li> </ul> |
| endpoint    | Optional shorthand for complete URL to use for the constructed client.   |
| region      | Optional shorthand for AWS Region used in instantiating the client.  |

### Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

### Service syntax

```
svc <- guardduty(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
    creds = list(
      access_key_id = "string",
      secret_access_key = "string",
      session_token = "string"
    ),
    profile = "string",
```

```

        anonymous = "logical"
    ),
    endpoint = "string",
    region = "string"
)

```

## Operations

|   |   |
|---|---|
| <a href="#">accept_administrator_invitation</a>         | Accepts the invitation to be a member account and get monitored by a GuardDuty administrator account            |
| <a href="#">accept_invitation</a>                       | Accepts the invitation to be monitored by a GuardDuty administrator account                                     |
| <a href="#">archive_findings</a>                        | Archives GuardDuty findings that are specified by the list of finding IDs                                       |
| <a href="#">create_detector</a>                         | Creates a single Amazon GuardDuty detector  |
| <a href="#">create_filter</a>                           | Creates a filter using the specified finding criteria   |
| <a href="#">create_ip_set</a>                           | Creates a new IPSet, which is called a trusted IP list in the console user interface                            |
| <a href="#">create_members</a>                          | Creates member accounts of the current Amazon Web Services account by specifying the list of member account IDs |
| <a href="#">create_publishing_destination</a>           | Creates a publishing destination to export findings to  |
| <a href="#">create_sample_findings</a>                  | Generates sample findings of types specified by the list of finding types                                       |
| <a href="#">create_threat_intel_set</a>                 | Creates a new ThreatIntelSet  |
| <a href="#">decline_invitations</a>                     | Declines invitations sent to the current member account by Amazon Web Services                                  |
| <a href="#">delete_detector</a>                         | Deletes an Amazon GuardDuty detector that is specified by the detector ID                                       |
| <a href="#">delete_filter</a>                           | Deletes the filter specified by the filter name   |
| <a href="#">delete_invitations</a>                      | Deletes invitations sent to the current member account by Amazon Web Services                                   |
| <a href="#">delete_ip_set</a>                           | Deletes the IPSet specified by the ipSetId  |
| <a href="#">delete_members</a>                          | Deletes GuardDuty member accounts (to the current GuardDuty administrator account)                              |
| <a href="#">delete_publishing_destination</a>           | Deletes the publishing definition with the specified destinationId  |
| <a href="#">delete_threat_intel_set</a>                 | Deletes the ThreatIntelSet specified by the ThreatIntelSet ID   |
| <a href="#">describe_malware_scans</a>                  | Returns a list of malware scans   |
| <a href="#">describe_organization_configuration</a>     | Returns information about the account selected as the delegated administrator for the organization              |
| <a href="#">describe_publishing_destination</a>         | Returns information about the publishing destination specified by the provided destinationId                    |
| <a href="#">disable_organization_admin_account</a>      | Removes the existing GuardDuty delegated administrator of the organization                                      |
| <a href="#">disassociate_from_administrator_account</a> | Disassociates the current GuardDuty member account from its administrator account                               |
| <a href="#">disassociate_from_master_account</a>        | Disassociates the current GuardDuty member account from its administrator account                               |
| <a href="#">disassociate_members</a>                    | Disassociates GuardDuty member accounts (from the current administrator account)                                |
| <a href="#">enable_organization_admin_account</a>       | Designates an Amazon Web Services account within the organization as your GuardDuty administrator account       |
| <a href="#">get_administrator_account</a>               | Provides the details of the GuardDuty administrator account associated with the current organization            |
| <a href="#">get_coverage_statistics</a>                 | Retrieves aggregated statistics for your account  |
| <a href="#">get_detector</a>                            | Retrieves an Amazon GuardDuty detector specified by the detectorId  |
| <a href="#">get_filter</a>                              | Returns the details of the filter specified by the filter name  |
| <a href="#">get_findings</a>                            | Describes Amazon GuardDuty findings specified by finding IDs  |
| <a href="#">get_findings_statistics</a>                 | Lists Amazon GuardDuty findings statistics for the specified detector ID  |
| <a href="#">get_invitations_count</a>                   | Returns the count of all GuardDuty membership invitations that were sent to the current member account          |
| <a href="#">get_ip_set</a>                              | Retrieves the IPSet specified by the ipSetId  |
| <a href="#">get_malware_scan_settings</a>               | Returns the details of the malware scan settings  |
| <a href="#">get_master_account</a>                      | Provides the details for the GuardDuty administrator account associated with the current organization           |
| <a href="#">get_member_detectors</a>                    | Describes which data sources are enabled for the member account's detector                                      |
| <a href="#">get_members</a>                             | Retrieves GuardDuty member accounts (of the current GuardDuty administrator account)                            |
| <a href="#">get_organization_statistics</a>             | Retrieves how many active member accounts in your Amazon Web Services organization                              |
| <a href="#">get_remaining_free_trial_days</a>           | Provides the number of days left for each data source used in the free trial period                             |



|   |  |
|---|--|
| <a href="#">get_threat_intel_set</a>              | Retrieves the ThreatIntelSet that is specified by the ThreatIntelSet ID                  |
| <a href="#">get_usage_statistics</a>              | Lists Amazon GuardDuty usage statistics over the last 30 days for the specified detector |
| <a href="#">invite_members</a>                    | Invites Amazon Web Services accounts to become members of an organization                |
| <a href="#">list_coverage</a>                     | Lists coverage details for your GuardDuty account  |
| <a href="#">list_detectors</a>                    | Lists detectorIds of all the existing Amazon GuardDuty detector resources                |
| <a href="#">list_filters</a>                      | Returns a paginated list of the current filters  |
| <a href="#">list_findings</a>                     | Lists Amazon GuardDuty findings for the specified detector ID                            |
| <a href="#">list_invitations</a>                  | Lists all GuardDuty membership invitations that were sent to the current Amazon account  |
| <a href="#">list_ip_sets</a>                      | Lists the IPsets of the GuardDuty service specified by the detector ID                   |
| <a href="#">list_members</a>                      | Lists details about all member accounts for the current GuardDuty administrator account  |
| <a href="#">list_organization_admin_accounts</a>  | Lists the accounts designated as GuardDuty delegated administrators                      |
| <a href="#">list_publishing_destinations</a>      | Returns a list of publishing destinations associated with the specified detectorId       |
| <a href="#">list_tags_for_resource</a>            | Lists tags for a resource  |
| <a href="#">list_threat_intel_sets</a>            | Lists the ThreatIntelSets of the GuardDuty service specified by the detector ID          |
| <a href="#">start_malware_scan</a>                | Initiates the malware scan   |
| <a href="#">start_monitoring_members</a>          | Turns on GuardDuty monitoring of the specified member accounts                           |
| <a href="#">stop_monitoring_members</a>           | Stops GuardDuty monitoring for the specified member accounts                             |
| <a href="#">tag_resource</a>                      | Adds tags to a resource  |
| <a href="#">unarchive_findings</a>                | Unarchives GuardDuty findings specified by the findingIds                                |
| <a href="#">untag_resource</a>                    | Removes tags from a resource   |
| <a href="#">update_detector</a>                   | Updates the Amazon GuardDuty detector specified by the detectorId                        |
| <a href="#">update_filter</a>                     | Updates the filter specified by the filter name  |
| <a href="#">update_findings_feedback</a>          | Marks the specified GuardDuty findings as useful or not useful                           |
| <a href="#">update_ip_set</a>                     | Updates the IPSet specified by the IPSet ID  |
| <a href="#">update_malware_scan_settings</a>      | Updates the malware scan settings  |
| <a href="#">update_member_detectors</a>           | Contains information on member accounts to be updated                                    |
| <a href="#">update_organization_configuration</a> | Configures the delegated administrator account with the provided values                  |
| <a href="#">update_publishing_destination</a>     | Updates information about the publishing destination specified by the destinationId      |
| <a href="#">update_threat_intel_set</a>           | Updates the ThreatIntelSet specified by the ThreatIntelSet ID                            |

## Examples

```
## Not run:
svc <- guardduty()
svc$accept_administrator_invitation(
  Foo = 123
)

## End(Not run)
```

## Description

Identity and Access Management

Identity and Access Management (IAM) is a web service for securely controlling access to Amazon Web Services services. With IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which Amazon Web Services resources users and applications can access. For more information about IAM, see [Identity and Access Management \(IAM\)](#) and the [Identity and Access Management User Guide](#).

## Usage

```
iam(config = list(), credentials = list(), endpoint = NULL, region = NULL)
```

## Arguments

|             |   |
|-------------|---|
| config      | Optional configuration of credentials, endpoint, and/or region. <ul style="list-style-type: none"> <li>• <b>credentials:</b> <ul style="list-style-type: none"> <li>– <b>creds:</b> <ul style="list-style-type: none"> <li>* <b>access_key_id:</b> AWS access key ID</li> <li>* <b>secret_access_key:</b> AWS secret access key</li> <li>* <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>– <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>– <b>anonymous:</b> Set anonymous credentials.</li> </ul> </li> <li>• <b>endpoint:</b> The complete URL to use for the constructed client.</li> <li>• <b>region:</b> The AWS Region used in instantiating the client.</li> <li>• <b>close_connection:</b> Immediately close all HTTP connections.</li> <li>• <b>timeout:</b> The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.</li> <li>• <b>s3_force_path_style:</b> Set this to true to force the request to use path-style addressing, i.e. <code>http://s3.amazonaws.com/BUCKET/KEY</code>.</li> <li>• <b>sts_regional_endpoint:</b> Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul> |
| credentials | Optional credentials shorthand for the config parameter <ul style="list-style-type: none"> <li>• <b>creds:</b> <ul style="list-style-type: none"> <li>– <b>access_key_id:</b> AWS access key ID</li> <li>– <b>secret_access_key:</b> AWS secret access key</li> <li>– <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>• <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>• <b>anonymous:</b> Set anonymous credentials.</li> </ul>   |
| endpoint    | Optional shorthand for complete URL to use for the constructed client.  |
| region      | Optional shorthand for AWS Region used in instantiating the client.   |

**Value**

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

**Service syntax**

```
svc <- iam(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
    creds = list(
      access_key_id = "string",
      secret_access_key = "string",
      session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
  ),
  endpoint = "string",
  region = "string"
)
```

**Operations**

[add\\_client\\_id\\_to\\_open\\_id\\_connect\\_provider](#)  
[add\\_role\\_to\\_instance\\_profile](#)  
[add\\_user\\_to\\_group](#)  
[attach\\_group\\_policy](#)  
[attach\\_role\\_policy](#)  
[attach\\_user\\_policy](#)  
[change\\_password](#)  
[create\\_access\\_key](#)

Adds a new client ID (also known as audience) to the list of client IDs a  
 Adds the specified IAM role to the specified instance profile  
 Adds the specified user to the specified group  
 Attaches the specified managed policy to the specified IAM group  
 Attaches the specified managed policy to the specified IAM role  
 Attaches the specified managed policy to the specified user  
 Changes the password of the IAM user who is calling this operation  
 Creates a new Amazon Web Services secret access key and correspondi

|   |  |
|---|--|
| <code>create_account_alias</code>                   | Creates an alias for your Amazon Web Services account  |
| <code>create_group</code>                           | Creates a new group  |
| <code>create_instance_profile</code>                | Creates a new instance profile   |
| <code>create_login_profile</code>                   | Creates a password for the specified IAM user  |
| <code>create_open_id_connect_provider</code>        | Creates an IAM entity to describe an identity provider (IdP) that supports OpenID Connect                            |
| <code>create_policy</code>                          | Creates a new managed policy for your Amazon Web Services account  |
| <code>create_policy_version</code>                  | Creates a new version of the specified managed policy  |
| <code>create_role</code>                            | Creates a new role for your Amazon Web Services account  |
| <code>create_saml_provider</code>                   | Creates an IAM resource that describes an identity provider (IdP) that supports SAML                                 |
| <code>create_service_linked_role</code>             | Creates an IAM role that is linked to a specific Amazon Web Services service   |
| <code>create_service_specific_credential</code>     | Generates a set of credentials consisting of a user name and password that can be used to access a service           |
| <code>create_user</code>                            | Creates a new IAM user for your Amazon Web Services account  |
| <code>create_virtual_mfa_device</code>              | Creates a new virtual MFA device for the Amazon Web Services account   |
| <code>deactivate_mfa_device</code>                  | Deactivates the specified MFA device and removes it from association with the specified IAM user                     |
| <code>delete_access_key</code>                      | Deletes the access key pair associated with the specified IAM user   |
| <code>delete_account_alias</code>                   | Deletes the specified Amazon Web Services account alias  |
| <code>delete_account_password_policy</code>         | Deletes the password policy for the Amazon Web Services account  |
| <code>delete_group</code>                           | Deletes the specified IAM group  |
| <code>delete_group_policy</code>                    | Deletes the specified inline policy that is embedded in the specified IAM group                                      |
| <code>delete_instance_profile</code>                | Deletes the specified instance profile   |
| <code>delete_login_profile</code>                   | Deletes the password for the specified IAM user, For more information, see <a href="#">IAM User Passwords</a>        |
| <code>delete_open_id_connect_provider</code>        | Deletes an OpenID Connect identity provider (IdP) resource object in IAM   |
| <code>delete_policy</code>                          | Deletes the specified managed policy   |
| <code>delete_policy_version</code>                  | Deletes the specified version from the specified managed policy  |
| <code>delete_role</code>                            | Deletes the specified role   |
| <code>delete_role_permissions_boundary</code>       | Deletes the permissions boundary for the specified IAM role  |
| <code>delete_role_policy</code>                     | Deletes the specified inline policy that is embedded in the specified IAM role                                       |
| <code>delete_saml_provider</code>                   | Deletes a SAML provider resource in IAM  |
| <code>delete_server_certificate</code>              | Deletes the specified server certificate   |
| <code>delete_service_linked_role</code>             | Submits a service-linked role deletion request and returns a <code>DeletionTask</code> object                        |
| <code>delete_service_specific_credential</code>     | Deletes the specified service-specific credential  |
| <code>delete_signing_certificate</code>             | Deletes a signing certificate associated with the specified IAM user   |
| <code>delete_ssh_public_key</code>                  | Deletes the specified SSH public key   |
| <code>delete_user</code>                            | Deletes the specified IAM user   |
| <code>delete_user_permissions_boundary</code>       | Deletes the permissions boundary for the specified IAM user  |
| <code>delete_user_policy</code>                     | Deletes the specified inline policy that is embedded in the specified IAM user                                       |
| <code>delete_virtual_mfa_device</code>              | Deletes a virtual MFA device   |
| <code>detach_group_policy</code>                    | Removes the specified managed policy from the specified IAM group  |
| <code>detach_role_policy</code>                     | Removes the specified managed policy from the specified role   |
| <code>detach_user_policy</code>                     | Removes the specified managed policy from the specified user   |
| <code>enable_mfa_device</code>                      | Enables the specified MFA device and associates it with the specified IAM user                                       |
| <code>generate_credential_report</code>             | Generates a credential report for the Amazon Web Services account  |
| <code>generate_organizations_access_report</code>   | Generates a report for service last accessed data for Organizations  |
| <code>generate_service_last_accessed_details</code> | Generates a report that includes details about when an IAM resource (user, group, role, or policy) was last accessed |
| <code>get_access_key_last_used</code>               | Retrieves information about when the specified access key was last used  |
| <code>get_account_authorization_details</code>      | Retrieves information about all IAM users, groups, roles, and policies in the account                                |
| <code>get_account_password_policy</code>            | Retrieves the password policy for the Amazon Web Services account  |
| <code>get_account_summary</code>                    | Retrieves information about IAM entity usage and IAM quotas in the Amazon Web Services account                       |

|   |  |
|---|--|
| <a href="#">get_context_keys_for_custom_policy</a>              | Gets a list of all of the context keys referenced in the input policies  |
| <a href="#">get_context_keys_for_principal_policy</a>           | Gets a list of all of the context keys referenced in all the IAM policies that are attached to the specified principal                     |
| <a href="#">get_credential_report</a>                           | Retrieves a credential report for the Amazon Web Services account  |
| <a href="#">get_group</a>                                       | Returns a list of IAM users that are in the specified IAM group  |
| <a href="#">get_group_policy</a>                                | Retrieves the specified inline policy document that is embedded in the specified IAM group   |
| <a href="#">get_instance_profile</a>                            | Retrieves information about the specified instance profile, including the associated IAM role  |
| <a href="#">get_login_profile</a>                               | Retrieves the user name for the specified IAM user   |
| <a href="#">get_mfa_device</a>                                  | Retrieves information about an MFA device for a specified user   |
| <a href="#">get_open_id_connect_provider</a>                    | Returns information about the specified OpenID Connect (OIDC) provider   |
| <a href="#">get_organizations_access_report</a>                 | Retrieves the service last accessed data report for Organizations that was created using the GenerateServiceLastAccessedDetails API        |
| <a href="#">get_policy</a>                                      | Retrieves information about the specified managed policy, including the associated IAM role  |
| <a href="#">get_policy_version</a>                              | Retrieves information about the specified version of the specified managed policy  |
| <a href="#">get_role</a>  | Retrieves information about the specified role, including the role's path, permissions, and associated policies                            |
| <a href="#">get_role_policy</a>                                 | Retrieves the specified inline policy document that is embedded with the specified IAM role  |
| <a href="#">get_saml_provider</a>                               | Returns the SAML provider metadocument that was uploaded when the specified IAM role was created   |
| <a href="#">get_server_certificate</a>                          | Retrieves information about the specified server certificate stored in IAM   |
| <a href="#">get_service_last_accessed_details</a>               | Retrieves a service last accessed report that was created using the GenerateServiceLastAccessedDetails API                                 |
| <a href="#">get_service_last_accessed_details_with_entities</a> | After you generate a group or policy report using the GenerateServiceLastAccessedDetails API, this API returns the associated IAM entities |
| <a href="#">get_service_linked_role_deletion_status</a>         | Retrieves the status of your service-linked role deletion  |
| <a href="#">get_ssh_public_key</a>                              | Retrieves the specified SSH public key, including metadata about the key   |
| <a href="#">get_user</a>  | Retrieves information about the specified IAM user, including the user's permissions and associated policies                               |
| <a href="#">get_user_policy</a>                                 | Retrieves the specified inline policy document that is embedded in the specified IAM user  |
| <a href="#">list_access_keys</a>                                | Returns information about the access key IDs associated with the specified IAM user  |
| <a href="#">list_account_aliases</a>                            | Lists the account alias associated with the Amazon Web Services account  |
| <a href="#">list_attached_group_policies</a>                    | Lists all managed policies that are attached to the specified IAM group  |
| <a href="#">list_attached_role_policies</a>                     | Lists all managed policies that are attached to the specified IAM role   |
| <a href="#">list_attached_user_policies</a>                     | Lists all managed policies that are attached to the specified IAM user   |
| <a href="#">list_entities_for_policy</a>                        | Lists all IAM users, groups, and roles that the specified managed policy is attached to  |
| <a href="#">list_group_policies</a>                             | Lists the names of the inline policies that are embedded in the specified IAM group  |
| <a href="#">list_groups</a>                                     | Lists the IAM groups that have the specified path prefix   |
| <a href="#">list_groups_for_user</a>                            | Lists the IAM groups that the specified IAM user belongs to  |
| <a href="#">list_instance_profiles</a>                          | Lists the instance profiles that have the specified path prefix  |
| <a href="#">list_instance_profiles_for_role</a>                 | Lists the instance profiles that have the specified associated IAM role  |
| <a href="#">list_instance_profile_tags</a>                      | Lists the tags that are attached to the specified IAM instance profile   |
| <a href="#">list_mfa_devices</a>                                | Lists the MFA devices for an IAM user  |
| <a href="#">list_mfa_device_tags</a>                            | Lists the tags that are attached to the specified IAM virtual multi-factor authentication device   |
| <a href="#">list_open_id_connect_providers</a>                  | Lists information about the IAM OpenID Connect (OIDC) provider resources   |
| <a href="#">list_open_id_connect_provider_tags</a>              | Lists the tags that are attached to the specified OpenID Connect (OIDC) provider   |
| <a href="#">list_policies</a>                                   | Lists all the managed policies that are available in your Amazon Web Services account  |
| <a href="#">list_policies_granting_service_access</a>           | Retrieves a list of policies that the IAM identity (user, group, or role) can use to grant service access                                  |
| <a href="#">list_policy_tags</a>                                | Lists the tags that are attached to the specified IAM customer managed policy  |
| <a href="#">list_policy_versions</a>                            | Lists information about the versions of the specified managed policy, including the associated IAM role                                    |
| <a href="#">list_role_policies</a>                              | Lists the names of the inline policies that are embedded in the specified IAM role   |
| <a href="#">list_roles</a>                                      | Lists the IAM roles that have the specified path prefix  |
| <a href="#">list_role_tags</a>                                  | Lists the tags that are attached to the specified role   |
| <a href="#">list_saml_providers</a>                             | Lists the SAML provider resource objects defined in IAM in the account   |
| <a href="#">list_saml_provider_tags</a>                         | Lists the tags that are attached to the specified Security Assertion Markup Language (SAML) provider                                       |
| <a href="#">list_server_certificates</a>                        | Lists the server certificates stored in IAM that have the specified path prefix  |

|  |   |
|--|---|
| <a href="#">list_server_certificate_tags</a>                   | Lists the tags that are attached to the specified IAM server certificate  |
| <a href="#">list_service_specific_credentials</a>              | Returns information about the service-specific credentials associated with the specified Amazon Web Services account                  |
| <a href="#">list_signing_certificates</a>                      | Returns information about the signing certificates associated with the specified Amazon Web Services account                          |
| <a href="#">list_ssh_public_keys</a>                           | Returns information about the SSH public keys associated with the specified Amazon Web Services account                               |
| <a href="#">list_user_policies</a>                             | Lists the names of the inline policies embedded in the specified IAM user   |
| <a href="#">list_users</a>                                     | Lists the IAM users that have the specified path prefix   |
| <a href="#">list_user_tags</a>                                 | Lists the tags that are attached to the specified IAM user  |
| <a href="#">list_virtual_mfa_devices</a>                       | Lists the virtual MFA devices defined in the Amazon Web Services account  |
| <a href="#">put_group_policy</a>                               | Adds or updates an inline policy document that is embedded in the specified IAM group   |
| <a href="#">put_role_permissions_boundary</a>                  | Adds or updates the policy that is specified as the IAM role's permissions boundary   |
| <a href="#">put_role_policy</a>                                | Adds or updates an inline policy document that is embedded in the specified IAM role  |
| <a href="#">put_user_permissions_boundary</a>                  | Adds or updates the policy that is specified as the IAM user's permissions boundary   |
| <a href="#">put_user_policy</a>                                | Adds or updates an inline policy document that is embedded in the specified IAM user  |
| <a href="#">remove_client_id_from_open_id_connect_provider</a> | Removes the specified client ID (also known as audience) from the list of client IDs for the specified OpenID Connect (OIDC) provider |
| <a href="#">remove_role_from_instance_profile</a>              | Removes the specified IAM role from the specified EC2 instance profile  |
| <a href="#">remove_user_from_group</a>                         | Removes the specified user from the specified group   |
| <a href="#">reset_service_specific_credential</a>              | Resets the password for a service-specific credential   |
| <a href="#">resync_mfa_device</a>                              | Synchronizes the specified MFA device with its IAM resource object  |
| <a href="#">set_default_policy_version</a>                     | Sets the specified version of the specified policy as the policy's default version  |
| <a href="#">set_security_token_service_preferences</a>         | Sets the specified version of the global endpoint token as the token version  |
| <a href="#">simulate_custom_policy</a>                         | Simulate how a set of IAM policies and optionally a resource-based policy works with a specified IAM entity                           |
| <a href="#">simulate_principal_policy</a>                      | Simulate how a set of IAM policies attached to an IAM entity works with a specified resource  |
| <a href="#">tag_instance_profile</a>                           | Adds one or more tags to an IAM instance profile  |
| <a href="#">tag_mfa_device</a>                                 | Adds one or more tags to an IAM virtual multi-factor authentication (MFA) device  |
| <a href="#">tag_open_id_connect_provider</a>                   | Adds one or more tags to an OpenID Connect (OIDC)-compatible identity provider  |
| <a href="#">tag_policy</a>                                     | Adds one or more tags to an IAM customer managed policy   |
| <a href="#">tag_role</a>                                       | Adds one or more tags to an IAM role  |
| <a href="#">tag_saml_provider</a>                              | Adds one or more tags to a Security Assertion Markup Language (SAML) provider resource  |
| <a href="#">tag_server_certificate</a>                         | Adds one or more tags to an IAM server certificate  |
| <a href="#">tag_user</a>                                       | Adds one or more tags to an IAM user  |
| <a href="#">untag_instance_profile</a>                         | Removes the specified tags from the IAM instance profile  |
| <a href="#">untag_mfa_device</a>                               | Removes the specified tags from the IAM virtual multi-factor authentication (MFA) device  |
| <a href="#">untag_open_id_connect_provider</a>                 | Removes the specified tags from the specified OpenID Connect (OIDC) provider  |
| <a href="#">untag_policy</a>                                   | Removes the specified tags from the customer managed policy   |
| <a href="#">untag_role</a>                                     | Removes the specified tags from the role  |
| <a href="#">untag_saml_provider</a>                            | Removes the specified tags from the specified Security Assertion Markup Language (SAML) provider resource                             |
| <a href="#">untag_server_certificate</a>                       | Removes the specified tags from the IAM server certificate  |
| <a href="#">untag_user</a>                                     | Removes the specified tags from the user  |
| <a href="#">update_access_key</a>                              | Changes the status of the specified access key from Active to Inactive, or vice versa   |
| <a href="#">update_account_password_policy</a>                 | Updates the password policy settings for the Amazon Web Services account  |
| <a href="#">update_assume_role_policy</a>                      | Updates the policy that grants an IAM entity permission to assume a role  |
| <a href="#">update_group</a>                                   | Updates the name and/or the path of the specified IAM group   |
| <a href="#">update_login_profile</a>                           | Changes the password for the specified IAM user   |
| <a href="#">update_open_id_connect_provider_thumbprint</a>     | Replaces the existing list of server certificate thumbprints associated with the specified OpenID Connect (OIDC) provider             |
| <a href="#">update_role</a>                                    | Updates the description or maximum session duration setting of a role   |
| <a href="#">update_role_description</a>                        | Use UpdateRole instead  |
| <a href="#">update_saml_provider</a>                           | Updates the metadata document for an existing SAML provider resource  |
| <a href="#">update_server_certificate</a>                      | Updates the name and/or the path of the specified server certificate store entry  |

|  |  |
|--|--|
| <a href="#">update_service_specific_credential</a> | Sets the status of a service-specific credential to Active or Inactive               |
| <a href="#">update_signing_certificate</a>         | Changes the status of the specified user signing certificate from active to inactive |
| <a href="#">update_ssh_public_key</a>              | Sets the status of an IAM user's SSH public key to active or inactive                |
| <a href="#">update_user</a>                        | Updates the name and/or the path of the specified IAM user                           |
| <a href="#">upload_server_certificate</a>          | Uploads a server certificate entity for the Amazon Web Services account              |
| <a href="#">upload_signing_certificate</a>         | Uploads an X   |
| <a href="#">upload_ssh_public_key</a>              | Uploads an SSH public key and associates it with the specified IAM user              |

## Examples

```
## Not run:
svc <- iam()
# The following add-client-id-to-open-id-connect-provider command adds the
# client ID my-application-ID to the OIDC provider named
# server.example.com:
svc$add_client_id_to_open_id_connect_provider(
  ClientID = "my-application-ID",
  OpenIDConnectProviderArn = "arn:aws:iam::123456789012:oidc-provider/server.example.com"
)

## End(Not run)
```

---

iamrolesanywhere

*IAM Roles Anywhere*


---

## Description

Identity and Access Management Roles Anywhere provides a secure way for your workloads such as servers, containers, and applications that run outside of Amazon Web Services to obtain temporary Amazon Web Services credentials. Your workloads can use the same IAM policies and roles you have for native Amazon Web Services applications to access Amazon Web Services resources. Using IAM Roles Anywhere eliminates the need to manage long-term credentials for workloads running outside of Amazon Web Services.

To use IAM Roles Anywhere, your workloads must use X.509 certificates issued by their certificate authority (CA). You register the CA with IAM Roles Anywhere as a trust anchor to establish trust between your public key infrastructure (PKI) and IAM Roles Anywhere. If you don't manage your own PKI system, you can use Private Certificate Authority to create a CA and then use that to establish trust with IAM Roles Anywhere.

This guide describes the IAM Roles Anywhere operations that you can call programmatically. For more information about IAM Roles Anywhere, see the [IAM Roles Anywhere User Guide](#).

**Usage**

```
iamrolesanywhere(
  config = list(),
  credentials = list(),
  endpoint = NULL,
  region = NULL
)
```

**Arguments**

|             |   |
|-------------|---|
| config      | Optional configuration of credentials, endpoint, and/or region. <ul style="list-style-type: none"> <li>• <b>credentials:</b> <ul style="list-style-type: none"> <li>– <b>creds:</b> <ul style="list-style-type: none"> <li>* <b>access_key_id:</b> AWS access key ID</li> <li>* <b>secret_access_key:</b> AWS secret access key</li> <li>* <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>– <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>– <b>anonymous:</b> Set anonymous credentials.</li> </ul> </li> <li>• <b>endpoint:</b> The complete URL to use for the constructed client.</li> <li>• <b>region:</b> The AWS Region used in instantiating the client.</li> <li>• <b>close_connection:</b> Immediately close all HTTP connections.</li> <li>• <b>timeout:</b> The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.</li> <li>• <b>s3_force_path_style:</b> Set this to true to force the request to use path-style addressing, i.e. <code>http://s3.amazonaws.com/BUCKET/KEY</code>.</li> <li>• <b>sts_regional_endpoint:</b> Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul> |
| credentials | Optional credentials shorthand for the config parameter <ul style="list-style-type: none"> <li>• <b>creds:</b> <ul style="list-style-type: none"> <li>– <b>access_key_id:</b> AWS access key ID</li> <li>– <b>secret_access_key:</b> AWS secret access key</li> <li>– <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>• <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>• <b>anonymous:</b> Set anonymous credentials.</li> </ul>   |
| endpoint    | Optional shorthand for complete URL to use for the constructed client.  |
| region      | Optional shorthand for AWS Region used in instantiating the client.   |

**Value**

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.



**Service syntax**

```

svc <- iamrolesanywhere(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
    creds = list(
      access_key_id = "string",
      secret_access_key = "string",
      session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
  ),
  endpoint = "string",
  region = "string"
)

```

**Operations**

|                                      |   |
|--------------------------------------|---|
| <a href="#">create_profile</a>       | Creates a profile, a list of the roles that Roles Anywhere service is trusted to assume             |
| <a href="#">create_trust_anchor</a>  | Creates a trust anchor to establish trust between IAM Roles Anywhere and your certificate authority |
| <a href="#">delete_crl</a>           | Deletes a certificate revocation list (CRL)   |
| <a href="#">delete_profile</a>       | Deletes a profile   |
| <a href="#">delete_trust_anchor</a>  | Deletes a trust anchor  |
| <a href="#">disable_crl</a>          | Disables a certificate revocation list (CRL)  |
| <a href="#">disable_profile</a>      | Disables a profile  |
| <a href="#">disable_trust_anchor</a> | Disables a trust anchor   |
| <a href="#">enable_crl</a>           | Enables a certificate revocation list (CRL)   |
| <a href="#">enable_profile</a>       | Enables temporary credential requests for a profile   |
| <a href="#">enable_trust_anchor</a>  | Enables a trust anchor  |
| <a href="#">get_crl</a>              | Gets a certificate revocation list (CRL)  |
| <a href="#">get_profile</a>          | Gets a profile  |
| <a href="#">get_subject</a>          | Gets a subject, which associates a certificate identity with authentication attempts                |

|   |  |
|---|--|
| <a href="#">get_trust_anchor</a>            | Gets a trust anchor  |
| <a href="#">import_crl</a>                  | Imports the certificate revocation list (CRL)  |
| <a href="#">list_crls</a>                   | Lists all certificate revocation lists (CRL) in the authenticated account and Amazon Web Services Region |
| <a href="#">list_profiles</a>               | Lists all profiles in the authenticated account and Amazon Web Services Region                           |
| <a href="#">list_subjects</a>               | Lists the subjects in the authenticated account and Amazon Web Services Region                           |
| <a href="#">list_tags_for_resource</a>      | Lists the tags attached to the resource  |
| <a href="#">list_trust_anchors</a>          | Lists the trust anchors in the authenticated account and Amazon Web Services Region                      |
| <a href="#">put_notification_settings</a>   | Attaches a list of notification settings to a trust anchor   |
| <a href="#">reset_notification_settings</a> | Resets the custom notification setting to IAM Roles Anywhere default setting                             |
| <a href="#">tag_resource</a>                | Attaches tags to a resource  |
| <a href="#">untag_resource</a>              | Removes tags from the resource   |
| <a href="#">update_crl</a>                  | Updates the certificate revocation list (CRL)  |
| <a href="#">update_profile</a>              | Updates a profile, a list of the roles that IAM Roles Anywhere service is trusted to assume              |
| <a href="#">update_trust_anchor</a>         | Updates a trust anchor   |

## Examples

```
## Not run:
svc <- iamrolesanywhere()
svc$create_profile(
  Foo = 123
)

## End(Not run)
```

---

identitystore

*AWS SSO Identity Store*

---

## Description

The Identity Store service used by IAM Identity Center provides a single place to retrieve all of your identities (users and groups). For more information, see the [IAM Identity Center User Guide](#).

This reference guide describes the identity store operations that you can call programmatically and includes detailed information about data types and errors.

IAM Identity Center uses the `sso` and `identitystore` API namespaces.

## Usage

```
identitystore(
  config = list(),
  credentials = list(),
  endpoint = NULL,
  region = NULL
)
```

**Arguments**

|             |   |
|-------------|---|
| config      | Optional configuration of credentials, endpoint, and/or region. <ul style="list-style-type: none"> <li>• <b>credentials:</b> <ul style="list-style-type: none"> <li>– <b>creds:</b> <ul style="list-style-type: none"> <li>* <b>access_key_id:</b> AWS access key ID</li> <li>* <b>secret_access_key:</b> AWS secret access key</li> <li>* <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>– <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>– <b>anonymous:</b> Set anonymous credentials.</li> </ul> </li> <li>• <b>endpoint:</b> The complete URL to use for the constructed client.</li> <li>• <b>region:</b> The AWS Region used in instantiating the client.</li> <li>• <b>close_connection:</b> Immediately close all HTTP connections.</li> <li>• <b>timeout:</b> The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.</li> <li>• <b>s3_force_path_style:</b> Set this to true to force the request to use path-style addressing, i.e. <code>http://s3.amazonaws.com/BUCKET/KEY</code>.</li> <li>• <b>sts_regional_endpoint:</b> Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul> |
| credentials | Optional credentials shorthand for the config parameter <ul style="list-style-type: none"> <li>• <b>creds:</b> <ul style="list-style-type: none"> <li>– <b>access_key_id:</b> AWS access key ID</li> <li>– <b>secret_access_key:</b> AWS secret access key</li> <li>– <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>• <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>• <b>anonymous:</b> Set anonymous credentials.</li> </ul>   |
| endpoint    | Optional shorthand for complete URL to use for the constructed client.  |
| region      | Optional shorthand for AWS Region used in instantiating the client.   |

**Value**

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

**Service syntax**

```
svc <- identitystore(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
```

```

        secret_access_key = "string",
        session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
),
endpoint = "string",
region = "string",
close_connection = "logical",
timeout = "numeric",
s3_force_path_style = "logical",
sts_regional_endpoint = "string"
),
credentials = list(
  creds = list(
    access_key_id = "string",
    secret_access_key = "string",
    session_token = "string"
  ),
  profile = "string",
  anonymous = "logical"
),
endpoint = "string",
region = "string"
)

```

## Operations

|   |  |
|---|--|
| <a href="#">create_group</a>                      | Creates a group within the specified identity store  |
| <a href="#">create_group_membership</a>           | Creates a relationship between a member and a group  |
| <a href="#">create_user</a>                       | Creates a user within the specified identity store   |
| <a href="#">delete_group</a>                      | Delete a group within an identity store given GroupId  |
| <a href="#">delete_group_membership</a>           | Delete a membership within a group given MembershipId  |
| <a href="#">delete_user</a>                       | Deletes a user within an identity store given UserId   |
| <a href="#">describe_group</a>                    | Retrieves the group metadata and attributes from GroupId in an identity store                      |
| <a href="#">describe_group_membership</a>         | Retrieves membership metadata and attributes from MembershipId in an identity store                |
| <a href="#">describe_user</a>                     | Retrieves the user metadata and attributes from the UserId in an identity store                    |
| <a href="#">get_group_id</a>                      | Retrieves GroupId in an identity store   |
| <a href="#">get_group_membership_id</a>           | Retrieves the MembershipId in an identity store  |
| <a href="#">get_user_id</a>                       | Retrieves the UserId in an identity store  |
| <a href="#">is_member_in_groups</a>               | Checks the user's membership in all requested groups and returns if the member exists              |
| <a href="#">list_group_memberships</a>            | For the specified group in the specified identity store, returns the list of all GroupMemberships  |
| <a href="#">list_group_memberships_for_member</a> | For the specified member in the specified identity store, returns the list of all GroupMemberships |
| <a href="#">list_groups</a>                       | Lists all groups in the identity store   |
| <a href="#">list_users</a>                        | Lists all users in the identity store  |
| <a href="#">update_group</a>                      | For the specified group in the specified identity store, updates the group metadata and attributes |
| <a href="#">update_user</a>                       | For the specified user in the specified identity store, updates the user metadata and attributes   |

### Examples

```
## Not run:
svc <- identitystore()
svc$create_group(
  Foo = 123
)

## End(Not run)
```

---

inspector

*Amazon Inspector*

---

### Description

Amazon Inspector enables you to analyze the behavior of your AWS resources and to identify potential security issues. For more information, see [Amazon Inspector User Guide](#).

### Usage

```
inspector(
  config = list(),
  credentials = list(),
  endpoint = NULL,
  region = NULL
)
```

### Arguments

- config      Optional configuration of credentials, endpoint, and/or region.
- **credentials:**
    - **creds:**
      - \* **access\_key\_id:** AWS access key ID
      - \* **secret\_access\_key:** AWS secret access key
      - \* **session\_token:** AWS temporary session token
    - **profile:** The name of a profile to use. If not given, then the default profile is used.
    - **anonymous:** Set anonymous credentials.
  - **endpoint:** The complete URL to use for the constructed client.
  - **region:** The AWS Region used in instantiating the client.
  - **close\_connection:** Immediately close all HTTP connections.
  - **timeout:** The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.

|             |   |
|-------------|---|
|             | <ul style="list-style-type: none"> <li>• <b>s3_force_path_style</b>: Set this to true to force the request to use path-style addressing, i.e. <code>http://s3.amazonaws.com/BUCKET/KEY</code>.</li> <li>• <b>sts_regional_endpoint</b>: Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul>         |
| credentials | Optional credentials shorthand for the config parameter <ul style="list-style-type: none"> <li>• <b>creds</b>: <ul style="list-style-type: none"> <li>– <b>access_key_id</b>: AWS access key ID</li> <li>– <b>secret_access_key</b>: AWS secret access key</li> <li>– <b>session_token</b>: AWS temporary session token</li> </ul> </li> <li>• <b>profile</b>: The name of a profile to use. If not given, then the default profile is used.</li> <li>• <b>anonymous</b>: Set anonymous credentials.</li> </ul> |
| endpoint    | Optional shorthand for complete URL to use for the constructed client.  |
| region      | Optional shorthand for AWS Region used in instantiating the client.   |

### Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

### Service syntax

```
svc <- inspector(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
    creds = list(
      access_key_id = "string",
      secret_access_key = "string",
      session_token = "string"
    )
  )
)
```

```

    ),
    profile = "string",
    anonymous = "logical"
  ),
  endpoint = "string",
  region = "string"
)

```

## Operations

|  |   |
|--|---|
| <a href="#">add_attributes_to_findings</a>         | Assigns attributes (key and value pairs) to the findings that are specified by the ARNs of the findings                           |
| <a href="#">create_assessment_target</a>           | Creates a new assessment target using the ARN of the resource group that is generated by the assessment template                  |
| <a href="#">create_assessment_template</a>         | Creates an assessment template for the assessment target that is specified by the ARN of the assessment target                    |
| <a href="#">create_exclusions_preview</a>          | Starts the generation of an exclusions preview for the specified assessment template  |
| <a href="#">create_resource_group</a>              | Creates a resource group using the specified set of tags (key and value pairs) that are used to identify the resource group       |
| <a href="#">delete_assessment_run</a>              | Deletes the assessment run that is specified by the ARN of the assessment run   |
| <a href="#">delete_assessment_target</a>           | Deletes the assessment target that is specified by the ARN of the assessment target   |
| <a href="#">delete_assessment_template</a>         | Deletes the assessment template that is specified by the ARN of the assessment template   |
| <a href="#">describe_assessment_runs</a>           | Describes the assessment runs that are specified by the ARNs of the assessment runs   |
| <a href="#">describe_assessment_targets</a>        | Describes the assessment targets that are specified by the ARNs of the assessment targets   |
| <a href="#">describe_assessment_templates</a>      | Describes the assessment templates that are specified by the ARNs of the assessment templates                                     |
| <a href="#">describe_cross_account_access_role</a> | Describes the IAM role that enables Amazon Inspector to access your AWS account   |
| <a href="#">describe_exclusions</a>                | Describes the exclusions that are specified by the exclusions' ARNs   |
| <a href="#">describe_findings</a>                  | Describes the findings that are specified by the ARNs of the findings   |
| <a href="#">describe_resource_groups</a>           | Describes the resource groups that are specified by the ARNs of the resource groups   |
| <a href="#">describe_rules_packages</a>            | Describes the rules packages that are specified by the ARNs of the rules packages   |
| <a href="#">get_assessment_report</a>              | Produces an assessment report that includes detailed and comprehensive results of a scan  |
| <a href="#">get_exclusions_preview</a>             | Retrieves the exclusions preview (a list of ExclusionPreview objects) specified by the ARN of the assessment template             |
| <a href="#">get_telemetry_metadata</a>             | Information about the data that is collected for the specified assessment run   |
| <a href="#">list_assessment_run_agents</a>         | Lists the agents of the assessment runs that are specified by the ARNs of the assessment runs                                     |
| <a href="#">list_assessment_runs</a>               | Lists the assessment runs that correspond to the assessment templates that are specified by the ARNs of the assessment templates  |
| <a href="#">list_assessment_targets</a>            | Lists the ARNs of the assessment targets within this AWS account  |
| <a href="#">list_assessment_templates</a>          | Lists the assessment templates that correspond to the assessment targets that are specified by the ARNs of the assessment targets |
| <a href="#">list_event_subscriptions</a>           | Lists all the event subscriptions for the assessment template that is specified by the ARN of the assessment template             |
| <a href="#">list_exclusions</a>                    | List exclusions that are generated by the assessment run  |
| <a href="#">list_findings</a>                      | Lists findings that are generated by the assessment runs that are specified by the ARNs of the assessment runs                    |
| <a href="#">list_rules_packages</a>                | Lists all available Amazon Inspector rules packages   |
| <a href="#">list_tags_for_resource</a>             | Lists all tags associated with an assessment template   |
| <a href="#">preview_agents</a>                     | Previews the agents installed on the EC2 instances that are part of the specified assessment run                                  |
| <a href="#">register_cross_account_access_role</a> | Registers the IAM role that grants Amazon Inspector access to AWS Services needed to perform the assessment                       |
| <a href="#">remove_attributes_from_findings</a>    | Removes entire attributes (key and value pairs) from the findings that are specified by the ARNs of the findings                  |
| <a href="#">set_tags_for_resource</a>              | Sets tags (key and value pairs) to the assessment template that is specified by the ARN of the assessment template                |
| <a href="#">start_assessment_run</a>               | Starts the assessment run specified by the ARN of the assessment template   |
| <a href="#">stop_assessment_run</a>                | Stops the assessment run that is specified by the ARN of the assessment run   |
| <a href="#">subscribe_to_event</a>                 | Enables the process of sending Amazon Simple Notification Service (SNS) notifications for the assessment run                      |
| <a href="#">unsubscribe_from_event</a>             | Disables the process of sending Amazon Simple Notification Service (SNS) notifications for the assessment run                     |
| <a href="#">update_assessment_target</a>           | Updates the assessment target that is specified by the ARN of the assessment target   |

## Examples

```
## Not run:
svc <- inspector()
# Assigns attributes (key and value pairs) to the findings that are
# specified by the ARNs of the findings.
svc$add_attributes_to_findings(
  attributes = list(
    list(
      key = "Example",
      value = "example"
    )
  ),
  findingArns = list(
    "arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq/template/0-..."
  )
)

## End(Not run)
```

---

inspector2

*Inspector2*

---

## Description

Amazon Inspector is a vulnerability discovery service that automates continuous scanning for security vulnerabilities within your Amazon EC2, Amazon ECR, and Amazon Web Services Lambda environments.

## Usage

```
inspector2(
  config = list(),
  credentials = list(),
  endpoint = NULL,
  region = NULL
)
```

## Arguments

config           Optional configuration of credentials, endpoint, and/or region.

- **credentials:**
  - **creds:**
    - \* **access\_key\_id:** AWS access key ID
    - \* **secret\_access\_key:** AWS secret access key



- \* **session\_token**: AWS temporary session token
  - **profile**: The name of a profile to use. If not given, then the default profile is used.
  - **anonymous**: Set anonymous credentials.
  - **endpoint**: The complete URL to use for the constructed client.
  - **region**: The AWS Region used in instantiating the client.
  - **close\_connection**: Immediately close all HTTP connections.
  - **timeout**: The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.
  - **s3\_force\_path\_style**: Set this to true to force the request to use path-style addressing, i.e. `http://s3.amazonaws.com/BUCKET/KEY`.
  - **sts\_regional\_endpoint**: Set sts regional endpoint resolver to regional or legacy <https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html>
- credentials      Optional credentials shorthand for the config parameter
- **creds**:
    - **access\_key\_id**: AWS access key ID
    - **secret\_access\_key**: AWS secret access key
    - **session\_token**: AWS temporary session token
  - **profile**: The name of a profile to use. If not given, then the default profile is used.
  - **anonymous**: Set anonymous credentials.
- endpoint          Optional shorthand for complete URL to use for the constructed client.
- region            Optional shorthand for AWS Region used in instantiating the client.

**Value**

A client for the service. You can call the service’s operations using syntax like `svc$operation(...)`, where `svc` is the name you’ve assigned to the client. The available operations are listed in the Operations section.

**Service syntax**

```
svc <- inspector2(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
```

```

        close_connection = "logical",
        timeout = "numeric",
        s3_force_path_style = "logical",
        sts_regional_endpoint = "string"
    ),
    credentials = list(
        creds = list(
            access_key_id = "string",
            secret_access_key = "string",
            session_token = "string"
        ),
        profile = "string",
        anonymous = "logical"
    ),
    endpoint = "string",
    region = "string"
)

```

## Operations

|  |  |
|--|--|
| <a href="#">associate_member</a>                               | Associates an Amazon Web Services account with an Amazon Inspector       |
| <a href="#">batch_get_account_status</a>                       | Retrieves the Amazon Inspector status of multiple Amazon Web Services    |
| <a href="#">batch_get_code_snippet</a>                         | Retrieves code snippets from findings that Amazon Inspector detected     |
| <a href="#">batch_get_finding_details</a>                      | Gets vulnerability details for findings                                  |
| <a href="#">batch_get_free_trial_info</a>                      | Gets free trial status for multiple Amazon Web Services accounts         |
| <a href="#">batch_get_member_ec2_deep_inspection_status</a>    | Retrieves Amazon Inspector deep inspection activation status of multiple |
| <a href="#">batch_update_member_ec2_deep_inspection_status</a> | Activates or deactivates Amazon Inspector deep inspection for the pro    |
| <a href="#">cancel_findings_report</a>                         | Cancels the given findings report  |
| <a href="#">cancel_sbom_export</a>                             | Cancels a software bill of materials (SBOM) report                       |
| <a href="#">create_filter</a>                                  | Creates a filter resource using specified filter criteria                |
| <a href="#">create_findings_report</a>                         | Creates a finding report   |
| <a href="#">create_sbom_export</a>                             | Creates a software bill of materials (SBOM) report                       |
| <a href="#">delete_filter</a>                                  | Deletes a filter resource  |
| <a href="#">describe_organization_configuration</a>            | Describe Amazon Inspector configuration settings for an Amazon Web       |
| <a href="#">disable</a>  | Disables Amazon Inspector scans for one or more Amazon Web Servi         |
| <a href="#">disable_delegated_admin_account</a>                | Disables the Amazon Inspector delegated administrator for your organ     |
| <a href="#">disassociate_member</a>                            | Disassociates a member account from an Amazon Inspector delegated        |
| <a href="#">enable</a>   | Enables Amazon Inspector scans for one or more Amazon Web Servi          |
| <a href="#">enable_delegated_admin_account</a>                 | Enables the Amazon Inspector delegated administrator for your Organ      |
| <a href="#">get_configuration</a>                              | Retrieves setting configurations for Inspector scans                     |
| <a href="#">get_delegated_admin_account</a>                    | Retrieves information about the Amazon Inspector delegated administ      |
| <a href="#">get_ec2_deep_inspection_configuration</a>          | Retrieves the activation status of Amazon Inspector deep inspection an   |
| <a href="#">get_encryption_key</a>                             | Gets an encryption key   |
| <a href="#">get_findings_report_status</a>                     | Gets the status of a findings report                                     |
| <a href="#">get_member</a>                                     | Gets member information for your organization                            |
| <a href="#">get_sbom_export</a>                                | Gets details of a software bill of materials (SBOM) report               |
| <a href="#">list_account_permissions</a>                       | Lists the permissions an account has to configure Amazon Inspector       |
| <a href="#">list_coverage</a>                                  | Lists coverage details for you environment                               |

|   |  |
|---|--|
| <a href="#">list_coverage_statistics</a>                      | Lists Amazon Inspector coverage statistics for your environment                    |
| <a href="#">list_delegated_admin_accounts</a>                 | Lists information about the Amazon Inspector delegated administrators              |
| <a href="#">list_filters</a>                                  | Lists the filters associated with your account                                     |
| <a href="#">list_finding_aggregations</a>                     | Lists aggregated finding data for your environment based on specific criteria      |
| <a href="#">list_findings</a>                                 | Lists findings for your environment  |
| <a href="#">list_members</a>                                  | List members associated with the Amazon Inspector delegated administrator          |
| <a href="#">list_tags_for_resource</a>                        | Lists all tags attached to a given resource  |
| <a href="#">list_usage_totals</a>                             | Lists the Amazon Inspector usage totals over the last 30 days                      |
| <a href="#">reset_encryption_key</a>                          | Resets an encryption key   |
| <a href="#">search_vulnerabilities</a>                        | Lists Amazon Inspector coverage details for a specific vulnerability               |
| <a href="#">tag_resource</a>                                  | Adds tags to a resource  |
| <a href="#">untag_resource</a>                                | Removes tags from a resource   |
| <a href="#">update_configuration</a>                          | Updates setting configurations for your Amazon Inspector account                   |
| <a href="#">update_ec_2_deep_inspection_configuration</a>     | Activates, deactivates Amazon Inspector deep inspection, or updates configurations |
| <a href="#">update_encryption_key</a>                         | Updates an encryption key  |
| <a href="#">update_filter</a>                                 | Specifies the action that is to be applied to the findings that match the filter   |
| <a href="#">update_organization_configuration</a>             | Updates the configurations for your Amazon Inspector organization                  |
| <a href="#">update_org_ec_2_deep_inspection_configuration</a> | Updates the Amazon Inspector deep inspection custom paths for your organization    |

## Examples

```
## Not run:
svc <- inspector2()
svc$associate_member(
  Foo = 123
)

## End(Not run)
```

## Description

### Key Management Service

Key Management Service (KMS) is an encryption and key management web service. This guide describes the KMS operations that you can call programmatically. For general information about KMS, see the [Key Management Service Developer Guide](#).

KMS has replaced the term *customer master key (CMK)* with *KMS key* and *KMS key*. The concept has not changed. To prevent breaking changes, KMS is keeping some variations of this term.

Amazon Web Services provides SDKs that consist of libraries and sample code for various programming languages and platforms (Java, Ruby, .Net, macOS, Android, etc.). The SDKs provide a convenient way to create programmatic access to KMS and other Amazon Web Services services.

For example, the SDKs take care of tasks such as signing requests (see below), managing errors, and retrying requests automatically. For more information about the Amazon Web Services SDKs, including how to download and install them, see [Tools for Amazon Web Services](#).

We recommend that you use the Amazon Web Services SDKs to make programmatic API calls to KMS.

If you need to use FIPS 140-2 validated cryptographic modules when communicating with Amazon Web Services, use the FIPS endpoint in your preferred Amazon Web Services Region. For more information about the available FIPS endpoints, see [Service endpoints](#) in the Key Management Service topic of the *Amazon Web Services General Reference*.

All KMS API calls must be signed and be transmitted using Transport Layer Security (TLS). KMS recommends you always use the latest supported TLS version. Clients must also support cipher suites with Perfect Forward Secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Most modern systems such as Java 7 and later support these modes.

### Signing Requests

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

All KMS requests must be signed with [Signature Version 4](#).

### Logging API Requests

KMS supports CloudTrail, a service that logs Amazon Web Services API calls and related events for your Amazon Web Services account and delivers them to an Amazon S3 bucket that you specify. By using the information collected by CloudTrail, you can determine what requests were made to KMS, who made the request, when it was made, and so on. To learn more about CloudTrail, including how to turn it on and find your log files, see the [CloudTrail User Guide](#).

### Additional Resources

For more information about credentials and request signing, see the following:

- [Amazon Web Services Security Credentials](#) - This topic provides general information about the types of credentials used to access Amazon Web Services.
- [Temporary Security Credentials](#) - This section of the *IAM User Guide* describes how to create and use temporary security credentials.
- [Signature Version 4 Signing Process](#) - This set of topics walks you through the process of signing a request using an access key ID and a secret access key.

### Commonly Used API Operations

Of the API operations discussed in this guide, the following will prove the most useful for most applications. You will likely perform operations other than these, such as creating keys and assigning policies, by using the console.

- [encrypt](#)
- [decrypt](#)
- [generate\\_data\\_key](#)
- [generate\\_data\\_key\\_without\\_plaintext](#)

**Usage**

```
kms(config = list(), credentials = list(), endpoint = NULL, region = NULL)
```

**Arguments**

|             |  |
|-------------|--|
| config      | <p>Optional configuration of credentials, endpoint, and/or region.</p> <ul style="list-style-type: none"> <li>• <b>credentials:</b> <ul style="list-style-type: none"> <li>– <b>creds:</b> <ul style="list-style-type: none"> <li>* <b>access_key_id:</b> AWS access key ID</li> <li>* <b>secret_access_key:</b> AWS secret access key</li> <li>* <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>– <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>– <b>anonymous:</b> Set anonymous credentials.</li> </ul> </li> <li>• <b>endpoint:</b> The complete URL to use for the constructed client.</li> <li>• <b>region:</b> The AWS Region used in instantiating the client.</li> <li>• <b>close_connection:</b> Immediately close all HTTP connections.</li> <li>• <b>timeout:</b> The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.</li> <li>• <b>s3_force_path_style:</b> Set this to true to force the request to use path-style addressing, i.e. <code>http://s3.amazonaws.com/BUCKET/KEY</code>.</li> <li>• <b>sts_regional_endpoint:</b> Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul> |
| credentials | <p>Optional credentials shorthand for the config parameter</p> <ul style="list-style-type: none"> <li>• <b>creds:</b> <ul style="list-style-type: none"> <li>– <b>access_key_id:</b> AWS access key ID</li> <li>– <b>secret_access_key:</b> AWS secret access key</li> <li>– <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>• <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>• <b>anonymous:</b> Set anonymous credentials.</li> </ul>   |
| endpoint    | Optional shorthand for complete URL to use for the constructed client.   |
| region      | Optional shorthand for AWS Region used in instantiating the client.  |

**Value**

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

**Service syntax**

```

svc <- kms(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
    creds = list(
      access_key_id = "string",
      secret_access_key = "string",
      session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
  ),
  endpoint = "string",
  region = "string"
)

```

**Operations**

|  |   |
|--|---|
| <a href="#">cancel_key_deletion</a>          | Cancels the deletion of a KMS key   |
| <a href="#">connect_custom_key_store</a>     | Connects or reconnects a custom key store to its backing key store                        |
| <a href="#">create_alias</a>                 | Creates a friendly name for a KMS key   |
| <a href="#">create_custom_key_store</a>      | Creates a custom key store backed by a key store that you own and manage                  |
| <a href="#">create_grant</a>                 | Adds a grant to a KMS key   |
| <a href="#">create_key</a>                   | Creates a unique customer managed KMS key in your Amazon Web Services account             |
| <a href="#">decrypt</a>                      | Decrypts ciphertext that was encrypted by a KMS key using any of the following operations |
| <a href="#">delete_alias</a>                 | Deletes the specified alias   |
| <a href="#">delete_custom_key_store</a>      | Deletes a custom key store  |
| <a href="#">delete_imported_key_material</a> | Deletes key material that was previously imported   |
| <a href="#">describe_custom_key_stores</a>   | Gets information about custom key stores in the account and Region                        |
| <a href="#">describe_key</a>                 | Provides detailed information about a KMS key   |
| <a href="#">disable_key</a>                  | Sets the state of a KMS key to disabled   |
| <a href="#">disable_key_rotation</a>         | Disables automatic rotation of the key material of the specified symmetric encryption key |

|   |   |
|---|---|
| <code>disconnect_custom_key_store</code>              | Disconnects the custom key store from its backing key store   |
| <code>enable_key</code>                               | Sets the key state of a KMS key to enabled  |
| <code>enable_key_rotation</code>                      | Enables automatic rotation of the key material of the specified symmetric encryption key  |
| <code>encrypt</code>                                  | Encrypts plaintext of up to 4,096 bytes using a KMS key   |
| <code>generate_data_key</code>                        | Returns a unique symmetric data key for use outside of KMS  |
| <code>generate_data_key_pair</code>                   | Returns a unique asymmetric data key pair for use outside of KMS  |
| <code>generate_data_key_pair_without_plaintext</code> | Returns a unique asymmetric data key pair for use outside of KMS  |
| <code>generate_data_key_without_plaintext</code>      | Returns a unique symmetric data key for use outside of KMS  |
| <code>generate_mac</code>                             | Generates a hash-based message authentication code (HMAC) for a message using a KMS key   |
| <code>generate_random</code>                          | Returns a random byte string that is cryptographically secure   |
| <code>get_key_policy</code>                           | Gets a key policy attached to the specified KMS key   |
| <code>get_key_rotation_status</code>                  | Gets a Boolean value that indicates whether automatic rotation of the key material is enabled   |
| <code>get_parameters_for_import</code>                | Returns the public key and an import token you need to import or reimport key material  |
| <code>get_public_key</code>                           | Returns the public key of an asymmetric KMS key   |
| <code>import_key_material</code>                      | Imports or reimports key material into an existing KMS key that was created with the <code>get_parameters_for_import</code> operation |
| <code>list_aliases</code>                             | Gets a list of aliases in the caller's Amazon Web Services account and region   |
| <code>list_grants</code>                              | Gets a list of all grants for the specified KMS key   |
| <code>list_key_policies</code>                        | Gets the names of the key policies that are attached to a KMS key   |
| <code>list_keys</code>                                | Gets a list of all KMS keys in the caller's Amazon Web Services account and Region  |
| <code>list_resource_tags</code>                       | Returns all tags on the specified KMS key   |
| <code>list_retirable_grants</code>                    | Returns information about all grants in the Amazon Web Services account and Region that are eligible for retirement                   |
| <code>put_key_policy</code>                           | Attaches a key policy to the specified KMS key  |
| <code>re_encrypt</code>                               | Decrypts ciphertext and then reencrypts it entirely within KMS  |
| <code>replicate_key</code>                            | Replicates a multi-Region key into the specified Region   |
| <code>retire_grant</code>                             | Deletes a grant   |
| <code>revoke_grant</code>                             | Deletes the specified grant   |
| <code>schedule_key_deletion</code>                    | Schedules the deletion of a KMS key   |
| <code>sign</code>                                     | Creates a digital signature for a message or message digest by using the private key of a KMS key                                     |
| <code>tag_resource</code>                             | Adds or edits tags on a customer managed key  |
| <code>untag_resource</code>                           | Deletes tags from a customer managed key  |
| <code>update_alias</code>                             | Associates an existing KMS alias with a different KMS key   |
| <code>update_custom_key_store</code>                  | Changes the properties of a custom key store  |
| <code>update_key_description</code>                   | Updates the description of a KMS key  |
| <code>update_primary_region</code>                    | Changes the primary key of a multi-Region key   |
| <code>verify</code>                                   | Verifies a digital signature that was generated by the Sign operation   |
| <code>verify_mac</code>                               | Verifies the hash-based message authentication code (HMAC) for a specified message  |

## Examples

```
## Not run:
svc <- kms()
# The following example cancels deletion of the specified KMS key.
svc$cancel_key_deletion(
  KeyId = "1234abcd-12ab-34cd-56ef-1234567890ab"
)

## End(Not run)
```

---

 macie2

 Amazon Macie 2
 

---

## Description

Amazon Macie

## Usage

```
macie2(config = list(), credentials = list(), endpoint = NULL, region = NULL)
```

## Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

- **credentials:**

- **creds:**

- \* **access\_key\_id:** AWS access key ID
- \* **secret\_access\_key:** AWS secret access key
- \* **session\_token:** AWS temporary session token

- **profile:** The name of a profile to use. If not given, then the default profile is used.

- **anonymous:** Set anonymous credentials.

- **endpoint:** The complete URL to use for the constructed client.

- **region:** The AWS Region used in instantiating the client.

- **close\_connection:** Immediately close all HTTP connections.

- **timeout:** The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.

- **s3\_force\_path\_style:** Set this to `true` to force the request to use path-style addressing, i.e. `http://s3.amazonaws.com/BUCKET/KEY`.

- **sts\_regional\_endpoint:** Set sts regional endpoint resolver to regional or legacy <https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html>

`credentials` Optional credentials shorthand for the `config` parameter

- **creds:**

- **access\_key\_id:** AWS access key ID
- **secret\_access\_key:** AWS secret access key
- **session\_token:** AWS temporary session token

- **profile:** The name of a profile to use. If not given, then the default profile is used.

- **anonymous:** Set anonymous credentials.

`endpoint` Optional shorthand for complete URL to use for the constructed client.

`region` Optional shorthand for AWS Region used in instantiating the client.



**Value**

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

**Service syntax**

```
svc <- macie2(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
    creds = list(
      access_key_id = "string",
      secret_access_key = "string",
      session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
  ),
  endpoint = "string",
  region = "string"
)
```

**Operations**

[accept\\_invitation](#)

[batch\\_get\\_custom\\_data\\_identifiers](#)

[create\\_allow\\_list](#)

[create\\_classification\\_job](#)

[create\\_custom\\_data\\_identifier](#)

[create\\_findings\\_filter](#)

[create\\_invitations](#)

[create\\_member](#)

Accepts an Amazon Macie membership invitation that was received from a spe

Retrieves information about one or more custom data identifiers

Creates and defines the settings for an allow list

Creates and defines the settings for a classification job

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

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

Sends an Amazon Macie membership invitation to one or more accounts

Associates an account with an Amazon Macie administrator account

|   |  |
|---|--|
| <a href="#">create_sample_findings</a>                      | Creates sample findings  |
| <a href="#">decline_invitations</a>                         | Declines Amazon Macie membership invitations that were received from specific members                        |
| <a href="#">delete_allow_list</a>                           | Deletes an allow list  |
| <a href="#">delete_custom_data_identifier</a>               | Soft deletes a custom data identifier  |
| <a href="#">delete_findings_filter</a>                      | Deletes a findings filter  |
| <a href="#">delete_invitations</a>                          | Deletes Amazon Macie membership invitations that were received from specific members                         |
| <a href="#">delete_member</a>                               | Deletes the association between an Amazon Macie administrator account and a member account                   |
| <a href="#">describe_buckets</a>                            | Retrieves (queries) statistical data and other information about one or more S3 buckets                      |
| <a href="#">describe_classification_job</a>                 | Retrieves the status and settings for a classification job   |
| <a href="#">describe_organization_configuration</a>         | Retrieves the Amazon Macie configuration settings for an organization in Organization                        |
| <a href="#">disable_macie</a>                               | Disables Amazon Macie and deletes all settings and resources for a Macie account                             |
| <a href="#">disable_organization_admin_account</a>          | Disables an account as the delegated Amazon Macie administrator account for an organization                  |
| <a href="#">disassociate_from_administrator_account</a>     | Disassociates a member account from its Amazon Macie administrator account                                   |
| <a href="#">disassociate_from_master_account</a>            | (Deprecated) Disassociates a member account from its Amazon Macie administrator account                      |
| <a href="#">disassociate_member</a>                         | Disassociates an Amazon Macie administrator account from a member account                                    |
| <a href="#">enable_macie</a>                                | Enables Amazon Macie and specifies the configuration settings for a Macie account                            |
| <a href="#">enable_organization_admin_account</a>           | Designates an account as the delegated Amazon Macie administrator account for an organization                |
| <a href="#">get_administrator_account</a>                   | Retrieves information about the Amazon Macie administrator account for an account                            |
| <a href="#">get_allow_list</a>                              | Retrieves the settings and status of an allow list   |
| <a href="#">get_automated_discovery_configuration</a>       | Retrieves the configuration settings and status of automated sensitive data discovery                        |
| <a href="#">get_bucket_statistics</a>                       | Retrieves (queries) aggregated statistical data about all the S3 buckets that Amazon Macie scans             |
| <a href="#">get_classification_export_configuration</a>     | Retrieves the configuration settings for storing data classification results                                 |
| <a href="#">get_classification_scope</a>                    | Retrieves the classification scope settings for an account   |
| <a href="#">get_custom_data_identifier</a>                  | Retrieves the criteria and other settings for a custom data identifier                                       |
| <a href="#">get_findings</a>                                | Retrieves the details of one or more findings  |
| <a href="#">get_findings_filter</a>                         | Retrieves the criteria and other settings for a findings filter  |
| <a href="#">get_findings_publication_configuration</a>      | Retrieves the configuration settings for publishing findings to Security Hub                                 |
| <a href="#">get_finding_statistics</a>                      | Retrieves (queries) aggregated statistical data about findings   |
| <a href="#">get_invitations_count</a>                       | Retrieves the count of Amazon Macie membership invitations that were received from specific members          |
| <a href="#">get_macie_session</a>                           | Retrieves the status and configuration settings for an Amazon Macie account                                  |
| <a href="#">get_master_account</a>                          | (Deprecated) Retrieves information about the Amazon Macie administrator account for an organization          |
| <a href="#">get_member</a>                                  | Retrieves information about an account that's associated with an Amazon Macie administrator account          |
| <a href="#">get_resource_profile</a>                        | Retrieves (queries) sensitive data discovery statistics and the sensitivity score for an account             |
| <a href="#">get_reveal_configuration</a>                    | Retrieves the status and configuration settings for retrieving occurrences of sensitive data                 |
| <a href="#">get_sensitive_data_occurrences</a>              | Retrieves occurrences of sensitive data reported by a finding  |
| <a href="#">get_sensitive_data_occurrences_availability</a> | Checks whether occurrences of sensitive data can be retrieved for a finding                                  |
| <a href="#">get_sensitivity_inspection_template</a>         | Retrieves the settings for the sensitivity inspection template for an account                                |
| <a href="#">get_usage_statistics</a>                        | Retrieves (queries) quotas and aggregated usage data for one or more accounts                                |
| <a href="#">get_usage_totals</a>                            | Retrieves (queries) aggregated usage data for an account   |
| <a href="#">list_allow_lists</a>                            | Retrieves a subset of information about all the allow lists for an account                                   |
| <a href="#">list_classification_jobs</a>                    | Retrieves a subset of information about one or more classification jobs                                      |
| <a href="#">list_classification_scopes</a>                  | Retrieves a subset of information about the classification scope for an account                              |
| <a href="#">list_custom_data_identifiers</a>                | Retrieves a subset of information about all the custom data identifiers for an account                       |
| <a href="#">list_findings</a>                               | Retrieves a subset of information about one or more findings   |
| <a href="#">list_findings_filters</a>                       | Retrieves a subset of information about all the findings filters for an account                              |
| <a href="#">list_invitations</a>                            | Retrieves information about the Amazon Macie membership invitations that were received from specific members |
| <a href="#">list_managed_data_identifiers</a>               | Retrieves information about all the managed data identifiers that Amazon Macie scans                         |
| <a href="#">list_members</a>                                | Retrieves information about the accounts that are associated with an Amazon Macie administrator account      |

|  |   |
|--|---|
| <a href="#">list_organization_admin_accounts</a>         | Retrieves information about the delegated Amazon Macie administrator account        |
| <a href="#">list_resource_profile_artifacts</a>          | Retrieves information about objects that were selected from an S3 bucket for au     |
| <a href="#">list_resource_profile_detections</a>         | Retrieves information about the types and amount of sensitive data that Amazon      |
| <a href="#">list_sensitivity_inspection_templates</a>    | Retrieves a subset of information about the sensitivity inspection template for a   |
| <a href="#">list_tags_for_resource</a>                   | Retrieves the tags (keys and values) that are associated with an Amazon Macie       |
| <a href="#">put_classification_export_configuration</a>  | Creates or updates the configuration settings for storing data classification resul |
| <a href="#">put_findings_publication_configuration</a>   | Updates the configuration settings for publishing findings to Security Hub          |
| <a href="#">search_resources</a>                         | Retrieves (queries) statistical data and other information about Amazon Web Se      |
| <a href="#">tag_resource</a>                             | Adds or updates one or more tags (keys and values) that are associated with an      |
| <a href="#">test_custom_data_identifier</a>              | Tests a custom data identifier  |
| <a href="#">untag_resource</a>                           | Removes one or more tags (keys and values) from an Amazon Macie resource            |
| <a href="#">update_allow_list</a>                        | Updates the settings for an allow list  |
| <a href="#">update_automated_discovery_configuration</a> | Enables or disables automated sensitive data discovery for an account               |
| <a href="#">update_classification_job</a>                | Changes the status of a classification job  |
| <a href="#">update_classification_scope</a>              | Updates the classification scope settings for an account                            |
| <a href="#">update_findings_filter</a>                   | Updates the criteria and other settings for a findings filter                       |
| <a href="#">update_macie_session</a>                     | Suspends or re-enables Amazon Macie, or updates the configuration settings fo       |
| <a href="#">update_member_session</a>                    | Enables an Amazon Macie administrator to suspend or re-enable Macie for a m         |
| <a href="#">update_organization_configuration</a>        | Updates the Amazon Macie configuration settings for an organization in Organ        |
| <a href="#">update_resource_profile</a>                  | Updates the sensitivity score for an S3 bucket                                      |
| <a href="#">update_resource_profile_detections</a>       | Updates the sensitivity scoring settings for an S3 bucket                           |
| <a href="#">update_reveal_configuration</a>              | Updates the status and configuration settings for retrieving occurrences of sensi   |
| <a href="#">update_sensitivity_inspection_template</a>   | Updates the settings for the sensitivity inspection template for an account         |

## Examples

```
## Not run:
svc <- macie2()
svc$accept_invitation(
  Foo = 123
)

## End(Not run)
```

---

pcaconnectorad

*PcaConnectorAd*

---

## Description

Amazon Web Services Private CA Connector for Active Directory creates a connector between Amazon Web Services Private CA and Active Directory (AD) that enables you to provision security certificates for AD signed by a private CA that you own. For more information, see [Amazon Web Services Private CA Connector for Active Directory](#).

**Usage**

```
pcaconnectorad(
  config = list(),
  credentials = list(),
  endpoint = NULL,
  region = NULL
)
```

**Arguments**

|             |   |
|-------------|---|
| config      | Optional configuration of credentials, endpoint, and/or region. <ul style="list-style-type: none"> <li>• <b>credentials:</b> <ul style="list-style-type: none"> <li>– <b>creds:</b> <ul style="list-style-type: none"> <li>* <b>access_key_id:</b> AWS access key ID</li> <li>* <b>secret_access_key:</b> AWS secret access key</li> <li>* <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>– <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>– <b>anonymous:</b> Set anonymous credentials.</li> </ul> </li> <li>• <b>endpoint:</b> The complete URL to use for the constructed client.</li> <li>• <b>region:</b> The AWS Region used in instantiating the client.</li> <li>• <b>close_connection:</b> Immediately close all HTTP connections.</li> <li>• <b>timeout:</b> The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.</li> <li>• <b>s3_force_path_style:</b> Set this to true to force the request to use path-style addressing, i.e. <code>http://s3.amazonaws.com/BUCKET/KEY</code>.</li> <li>• <b>sts_regional_endpoint:</b> Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul> |
| credentials | Optional credentials shorthand for the config parameter <ul style="list-style-type: none"> <li>• <b>creds:</b> <ul style="list-style-type: none"> <li>– <b>access_key_id:</b> AWS access key ID</li> <li>– <b>secret_access_key:</b> AWS secret access key</li> <li>– <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>• <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>• <b>anonymous:</b> Set anonymous credentials.</li> </ul>   |
| endpoint    | Optional shorthand for complete URL to use for the constructed client.  |
| region      | Optional shorthand for AWS Region used in instantiating the client.   |

**Value**

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

**Service syntax**

```

svc <- pcaconnectorad(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
    creds = list(
      access_key_id = "string",
      secret_access_key = "string",
      session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
  ),
  endpoint = "string",
  region = "string"
)

```

**Operations**

|  |  |
|--|--|
| <a href="#">create_connector</a>                           | Creates a connector between Amazon Web Services Private CA and an Active Directory   |
| <a href="#">create_directory_registration</a>              | Creates a directory registration that authorizes communication between Amazon Web Services Private CA and Active Directory |
| <a href="#">create_service_principal_name</a>              | Creates a service principal name (SPN) for the service account in Active Directory   |
| <a href="#">create_template</a>                            | Creates an Active Directory compatible certificate template  |
| <a href="#">create_template_group_access_control_entry</a> | Create a group access control entry  |
| <a href="#">delete_connector</a>                           | Deletes a connector for Active Directory   |
| <a href="#">delete_directory_registration</a>              | Deletes a directory registration   |
| <a href="#">delete_service_principal_name</a>              | Deletes the service principal name (SPN) used by a connector to authenticate with Active Directory                         |
| <a href="#">delete_template</a>                            | Deletes a template   |
| <a href="#">delete_template_group_access_control_entry</a> | Deletes a group access control entry   |
| <a href="#">get_connector</a>                              | Lists information about your connector   |
| <a href="#">get_directory_registration</a>                 | A structure that contains information about your directory registration  |
| <a href="#">get_service_principal_name</a>                 | Lists the service principal name that the connector uses to authenticate with Active Directory                             |
| <a href="#">get_template</a>                               | Retrieves a certificate template that the connector uses to issue certificates from Amazon Web Services Private CA         |

|  |   |
|--|---|
| <a href="#">get_template_group_access_control_entry</a>    | Retrieves the group access control entries for a template   |
| <a href="#">list_connectors</a>                            | Lists the connectors that you created by using the <a href="https://docs">https://docs</a>              |
| <a href="#">list_directory_registrations</a>               | Lists the directory registrations that you created by using the <a href="https://docs">https://docs</a> |
| <a href="#">list_service_principal_names</a>               | Lists the service principal names that the connector uses to authenticate with                          |
| <a href="#">list_tags_for_resource</a>                     | Lists the tags, if any, that are associated with your resource  |
| <a href="#">list_template_group_access_control_entries</a> | Lists group access control entries you created  |
| <a href="#">list_templates</a>                             | Lists the templates, if any, that are associated with a connector                                       |
| <a href="#">tag_resource</a>                               | Adds one or more tags to your resource  |
| <a href="#">untag_resource</a>                             | Removes one or more tags from your resource   |
| <a href="#">update_template</a>                            | Update template configuration to define the information included in certificate                         |
| <a href="#">update_template_group_access_control_entry</a> | Update a group access control entry you created using <code>CreateTemplateGroup</code>                  |

## Examples

```
## Not run:
svc <- pcaconnectorad()
svc$create_connector(
  Foo = 123
)

## End(Not run)
```

---

ram

*AWS Resource Access Manager*


---

## Description

This is the *Resource Access Manager API Reference*. This documentation provides descriptions and syntax for each of the actions and data types in RAM. RAM is a service that helps you securely share your Amazon Web Services resources to other Amazon Web Services accounts. If you use Organizations to manage your accounts, then you can share your resources with your entire organization or to organizational units (OUs). For supported resource types, you can also share resources with individual Identity and Access Management (IAM) roles and users.

To learn more about RAM, see the following resources:

- [Resource Access Manager product page](#)
- [Resource Access Manager User Guide](#)

## Usage

```
ram(config = list(), credentials = list(), endpoint = NULL, region = NULL)
```

## Arguments

|             |  |
|-------------|--|
| config      | Optional configuration of credentials, endpoint, and/or region. <ul style="list-style-type: none"> <li>• <b>credentials:</b> <ul style="list-style-type: none"> <li>– <b>creds:</b> <ul style="list-style-type: none"> <li>* <b>access_key_id:</b> AWS access key ID</li> <li>* <b>secret_access_key:</b> AWS secret access key</li> <li>* <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>– <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>– <b>anonymous:</b> Set anonymous credentials.</li> </ul> </li> <li>• <b>endpoint:</b> The complete URL to use for the constructed client.</li> <li>• <b>region:</b> The AWS Region used in instantiating the client.</li> <li>• <b>close_connection:</b> Immediately close all HTTP connections.</li> <li>• <b>timeout:</b> The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.</li> <li>• <b>s3_force_path_style:</b> Set this to <code>true</code> to force the request to use path-style addressing, i.e. <code>http://s3.amazonaws.com/BUCKET/KEY</code>.</li> <li>• <b>sts_regional_endpoint:</b> Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul> |
| credentials | Optional credentials shorthand for the config parameter <ul style="list-style-type: none"> <li>• <b>creds:</b> <ul style="list-style-type: none"> <li>– <b>access_key_id:</b> AWS access key ID</li> <li>– <b>secret_access_key:</b> AWS secret access key</li> <li>– <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>• <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>• <b>anonymous:</b> Set anonymous credentials.</li> </ul>  |
| endpoint    | Optional shorthand for complete URL to use for the constructed client.   |
| region      | Optional shorthand for AWS Region used in instantiating the client.  |

## Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

## Service syntax

```
svc <- ram(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
```

```

        secret_access_key = "string",
        session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
),
endpoint = "string",
region = "string",
close_connection = "logical",
timeout = "numeric",
s3_force_path_style = "logical",
sts_regional_endpoint = "string"
),
credentials = list(
    creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
),
endpoint = "string",
region = "string"
)

```

## Operations

|  |   |
|--|---|
| <a href="#">accept_resource_share_invitation</a>       | Accepts an invitation to a resource share from another Amazon Web Services account.                                     |
| <a href="#">associate_resource_share</a>               | Adds the specified list of principals and list of resources to a resource share.  |
| <a href="#">associate_resource_share_permission</a>    | Adds or replaces the RAM permission for a resource type included in a resource share.                                   |
| <a href="#">create_permission</a>                      | Creates a customer managed permission for a specified resource type that you own.                                       |
| <a href="#">create_permission_version</a>              | Creates a new version of the specified customer managed permission.   |
| <a href="#">create_resource_share</a>                  | Creates a resource share.   |
| <a href="#">delete_permission</a>                      | Deletes the specified customer managed permission in the Amazon Web Services account.                                   |
| <a href="#">delete_permission_version</a>              | Deletes one version of a customer managed permission.   |
| <a href="#">delete_resource_share</a>                  | Deletes the specified resource share.   |
| <a href="#">disassociate_resource_share</a>            | Removes the specified principals or resources from participating in the specified resource share.                       |
| <a href="#">disassociate_resource_share_permission</a> | Removes a managed permission from a resource share.   |
| <a href="#">enable_sharing_with_aws_organization</a>   | Enables resource sharing within your organization in Organizations.   |
| <a href="#">get_permission</a>                         | Retrieves the contents of a managed permission in JSON format.  |
| <a href="#">get_resource_policies</a>                  | Retrieves the resource policies for the specified resources that you own and have shared.                               |
| <a href="#">get_resource_share_associations</a>        | Retrieves the lists of resources and principals that are associated for resource shares.                                |
| <a href="#">get_resource_share_invitations</a>         | Retrieves details about invitations that you have received for resource shares.   |
| <a href="#">get_resource_shares</a>                    | Retrieves details about the resource shares that you own or that are shared with you.                                   |
| <a href="#">list_pending_invitation_resources</a>      | Lists the resources in a resource share that is shared with you but for which you have not yet accepted the invitation. |
| <a href="#">list_permission_associations</a>           | Lists information about the managed permission and its associations to any resource type.                               |
| <a href="#">list_permissions</a>                       | Retrieves a list of available RAM permissions that you can use for the support of your resources.                       |



|  |   |
|--|---|
| <a href="#">list_permission_versions</a>                   | Lists the available versions of the specified RAM permission  |
| <a href="#">list_principals</a>                            | Lists the principals that you are sharing resources with or that are sharing resources with you       |
| <a href="#">list_replace_permission_associations_work</a>  | Retrieves the current status of the asynchronous tasks performed by RAM                               |
| <a href="#">list_resources</a>                             | Lists the resources that you added to a resource share or the resources that are shared with you      |
| <a href="#">list_resource_share_permissions</a>            | Lists the RAM permissions that are associated with a resource share                                   |
| <a href="#">list_resource_types</a>                        | Lists the resource types that can be shared by RAM  |
| <a href="#">promote_permission_created_from_policy</a>     | When you attach a resource-based policy to a resource, RAM automatically creates a managed permission |
| <a href="#">promote_resource_share_created_from_policy</a> | When you attach a resource-based policy to a resource, RAM automatically creates a resource share     |
| <a href="#">reject_resource_share_invitation</a>           | Rejects an invitation to a resource share from another Amazon Web Services account                    |
| <a href="#">replace_permission_associations</a>            | Updates all resource shares that use a managed permission to a different managed permission           |
| <a href="#">set_default_permission_version</a>             | Designates the specified version number as the default version for the specified managed permission   |
| <a href="#">tag_resource</a>                               | Adds the specified tag keys and values to a resource share or managed permission                      |
| <a href="#">untag_resource</a>                             | Removes the specified tag key and value pairs from the specified resource share or managed permission |
| <a href="#">update_resource_share</a>                      | Modifies some of the properties of the specified resource share                                       |

## Examples

```
## Not run:
svc <- ram()
svc$accept_resource_share_invitation(
  Foo = 123
)

## End(Not run)
```

---

secretsmanager

*AWS Secrets Manager*


---

## Description

Amazon Web Services Secrets Manager

Amazon Web Services Secrets Manager provides a service to enable you to store, manage, and retrieve, secrets.

This guide provides descriptions of the Secrets Manager API. For more information about using this service, see the [Amazon Web Services Secrets Manager User Guide](#).

### API Version

This version of the Secrets Manager API Reference documents the Secrets Manager API version 2017-10-17.

For a list of endpoints, see [Amazon Web Services Secrets Manager endpoints](#).

### Support and Feedback for Amazon Web Services Secrets Manager

We welcome your feedback. Send your comments to [awssecretsmanager-feedback@amazon.com](mailto:awssecretsmanager-feedback@amazon.com), or post your feedback and questions in the Amazon Web Services Secrets Manager Discussion

Forum. For more information about the Amazon Web Services Discussion Forums, see Forums Help.

### Logging API Requests

Amazon Web Services Secrets Manager supports Amazon Web Services CloudTrail, a service that records Amazon Web Services API calls for your Amazon Web Services account and delivers log files to an Amazon S3 bucket. By using information that's collected by Amazon Web Services CloudTrail, you can determine the requests successfully made to Secrets Manager, who made the request, when it was made, and so on. For more about Amazon Web Services Secrets Manager and support for Amazon Web Services CloudTrail, see [Logging Amazon Web Services Secrets Manager Events with Amazon Web Services CloudTrail](#) in the *Amazon Web Services Secrets Manager User Guide*. To learn more about CloudTrail, including enabling it and find your log files, see the [Amazon Web Services CloudTrail User Guide](#).

### Usage

```
secretsmanager(
  config = list(),
  credentials = list(),
  endpoint = NULL,
  region = NULL
)
```

### Arguments

|             |   |
|-------------|---|
| config      | <p>Optional configuration of credentials, endpoint, and/or region.</p> <ul style="list-style-type: none"> <li>• <b>credentials:</b> <ul style="list-style-type: none"> <li>– <b>creds:</b> <ul style="list-style-type: none"> <li>* <b>access_key_id:</b> AWS access key ID</li> <li>* <b>secret_access_key:</b> AWS secret access key</li> <li>* <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>– <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>– <b>anonymous:</b> Set anonymous credentials.</li> </ul> </li> <li>• <b>endpoint:</b> The complete URL to use for the constructed client.</li> <li>• <b>region:</b> The AWS Region used in instantiating the client.</li> <li>• <b>close_connection:</b> Immediately close all HTTP connections.</li> <li>• <b>timeout:</b> The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.</li> <li>• <b>s3_force_path_style:</b> Set this to <code>true</code> to force the request to use path-style addressing, i.e. <code>http://s3.amazonaws.com/BUCKET/KEY</code>.</li> <li>• <b>sts_regional_endpoint:</b> Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul> |
| credentials | <p>Optional credentials shorthand for the config parameter</p> <ul style="list-style-type: none"> <li>• <b>creds:</b></li> </ul>  |

- **access\_key\_id**: AWS access key ID
  - **secret\_access\_key**: AWS secret access key
  - **session\_token**: AWS temporary session token
  - **profile**: The name of a profile to use. If not given, then the default profile is used.
  - **anonymous**: Set anonymous credentials.
- endpoint           Optional shorthand for complete URL to use for the constructed client.
- region             Optional shorthand for AWS Region used in instantiating the client.

### Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

### Service syntax

```
svc <- secretsmanager(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
    creds = list(
      access_key_id = "string",
      secret_access_key = "string",
      session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
  ),
  endpoint = "string",
  region = "string"
)
```

## Operations

|  |  |
|--|--|
| <code>batch_get_secret_value</code>          | Retrieves the contents of the encrypted fields SecretString or SecretBinary for up to 20 secrets           |
| <code>cancel_rotate_secret</code>            | Turns off automatic rotation, and if a rotation is currently in progress, cancels the rotation             |
| <code>create_secret</code>                   | Creates a new secret   |
| <code>delete_resource_policy</code>          | Deletes the resource-based permission policy attached to the secret  |
| <code>delete_secret</code>                   | Deletes a secret and all of its versions   |
| <code>describe_secret</code>                 | Retrieves the details of a secret  |
| <code>get_random_password</code>             | Generates a random password  |
| <code>get_resource_policy</code>             | Retrieves the JSON text of the resource-based policy document attached to the secret                       |
| <code>get_secret_value</code>                | Retrieves the contents of the encrypted fields SecretString or SecretBinary from the specified secret      |
| <code>list_secrets</code>                    | Lists the secrets that are stored by Secrets Manager in the Amazon Web Services account                    |
| <code>list_secret_version_ids</code>         | Lists the versions of a secret   |
| <code>put_resource_policy</code>             | Attaches a resource-based permission policy to a secret  |
| <code>put_secret_value</code>                | Creates a new version with a new encrypted secret value and attaches it to the secret                      |
| <code>remove_regions_from_replication</code> | For a secret that is replicated to other Regions, deletes the secret replicas from the specified Regions   |
| <code>replicate_secret_to_regions</code>     | Replicates the secret to a new Regions   |
| <code>restore_secret</code>                  | Cancels the scheduled deletion of a secret by removing the DeletedDate time stamp                          |
| <code>rotate_secret</code>                   | Configures and starts the asynchronous process of rotating the secret                                      |
| <code>stop_replication_to_replica</code>     | Removes the link between the replica secret and the primary secret and promotes the replica to the primary |
| <code>tag_resource</code>                    | Attaches tags to a secret  |
| <code>untag_resource</code>                  | Removes specific tags from a secret  |
| <code>update_secret</code>                   | Modifies the details of a secret, including metadata and the secret value                                  |
| <code>update_secret_version_stage</code>     | Modifies the staging labels attached to a version of a secret  |
| <code>validate_resource_policy</code>        | Validates that a resource policy does not grant a wide range of principals access to your secrets          |

## Examples

```
## Not run:
svc <- secretsmanager()
# The following example shows how to cancel rotation for a secret. The
# operation sets the RotationEnabled field to false and cancels all
# scheduled rotations. To resume scheduled rotations, you must re-enable
# rotation by calling the rotate-secret operation.
svc$cancel_rotate_secret(
  SecretId = "MyTestDatabaseSecret"
)

## End(Not run)
```

## Description

Security Hub provides you with a comprehensive view of the security state of your Amazon Web Services environment and resources. It also provides you with the readiness status of your environment based on controls from supported security standards. Security Hub collects security data from Amazon Web Services accounts, services, and integrated third-party products and helps you analyze security trends in your environment to identify the highest priority security issues. For more information about Security Hub, see the *Security Hub User Guide*.

When you use operations in the Security Hub API, the requests are executed only in the Amazon Web Services Region that is currently active or in the specific Amazon Web Services Region that you specify in your request. Any configuration or settings change that results from the operation is applied only to that Region. To make the same change in other Regions, run the same command for each Region in which you want to apply the change.

For example, if your Region is set to us-west-2, when you use `create_members` to add a member account to Security Hub, the association of the member account with the administrator account is created only in the us-west-2 Region. Security Hub must be enabled for the member account in the same Region that the invitation was sent from.

The following throttling limits apply to using Security Hub API operations.

- `batch_enable_standards` - RateLimit of 1 request per second. BurstLimit of 1 request per second.
- `get_findings` - RateLimit of 3 requests per second. BurstLimit of 6 requests per second.
- `batch_import_findings` - RateLimit of 10 requests per second. BurstLimit of 30 requests per second.
- `batch_update_findings` - RateLimit of 10 requests per second. BurstLimit of 30 requests per second.
- `update_standards_control` - RateLimit of 1 request per second. BurstLimit of 5 requests per second.
- All other operations - RateLimit of 10 requests per second. BurstLimit of 30 requests per second.

## Usage

```
securityhub(
  config = list(),
  credentials = list(),
  endpoint = NULL,
  region = NULL
)
```

## Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

- **credentials:**
  - **creds:**
    - \* `access_key_id`: AWS access key ID
    - \* `secret_access_key`: AWS secret access key

|             |   |
|-------------|---|
|             | <ul style="list-style-type: none"> <li>* <b>session_token</b>: AWS temporary session token</li> <li>– <b>profile</b>: The name of a profile to use. If not given, then the default profile is used.</li> <li>– <b>anonymous</b>: Set anonymous credentials.</li> <li>• <b>endpoint</b>: The complete URL to use for the constructed client.</li> <li>• <b>region</b>: The AWS Region used in instantiating the client.</li> <li>• <b>close_connection</b>: Immediately close all HTTP connections.</li> <li>• <b>timeout</b>: The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.</li> <li>• <b>s3_force_path_style</b>: Set this to true to force the request to use path-style addressing, i.e. <code>http://s3.amazonaws.com/BUCKET/KEY</code>.</li> <li>• <b>sts_regional_endpoint</b>: Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul> |
| credentials | Optional credentials shorthand for the config parameter <ul style="list-style-type: none"> <li>• <b>creds</b>: <ul style="list-style-type: none"> <li>– <b>access_key_id</b>: AWS access key ID</li> <li>– <b>secret_access_key</b>: AWS secret access key</li> <li>– <b>session_token</b>: AWS temporary session token</li> </ul> </li> <li>• <b>profile</b>: The name of a profile to use. If not given, then the default profile is used.</li> <li>• <b>anonymous</b>: Set anonymous credentials.</li> </ul>   |
| endpoint    | Optional shorthand for complete URL to use for the constructed client.  |
| region      | Optional shorthand for AWS Region used in instantiating the client.   |

## Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

## Service syntax

```
svc <- securityhub(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
```

```

        close_connection = "logical",
        timeout = "numeric",
        s3_force_path_style = "logical",
        sts_regional_endpoint = "string"
    ),
    credentials = list(
        creds = list(
            access_key_id = "string",
            secret_access_key = "string",
            session_token = "string"
        ),
        profile = "string",
        anonymous = "logical"
    ),
    endpoint = "string",
    region = "string"
)

```

## Operations

|   |  |
|---|--|
| <a href="#">accept_administrator_invitation</a>             | Accepts the invitation to be a member account and be monitored by the Security Hub. This method is deprecated. |
| <a href="#">accept_invitation</a>                           | This method is deprecated.   |
| <a href="#">batch_delete_automation_rules</a>               | Deletes one or more automation rules.  |
| <a href="#">batch_disable_standards</a>                     | Disables the standards specified by the provided StandardsSubscriptionArns.                                    |
| <a href="#">batch_enable_standards</a>                      | Enables the standards specified by the provided StandardsArn.  |
| <a href="#">batch_get_automation_rules</a>                  | Retrieves a list of details for automation rules based on rule Amazon Resource Name (ARN).                     |
| <a href="#">batch_get_configuration_policy_associations</a> | Returns associations between an Security Hub configuration and a batch of tags.                                |
| <a href="#">batch_get_security_controls</a>                 | Provides details about a batch of security controls for the current Amazon Web Services account.               |
| <a href="#">batch_get_standards_control_associations</a>    | For a batch of security controls and standards, identifies whether each control is associated with a standard. |
| <a href="#">batch_import_findings</a>                       | Imports security findings generated by a finding provider into Security Hub.                                   |
| <a href="#">batch_update_automation_rules</a>               | Updates one or more automation rules based on rule Amazon Resource Name (ARN).                                 |
| <a href="#">batch_update_findings</a>                       | Used by Security Hub customers to update information about their investigations.                               |
| <a href="#">batch_update_standards_control_associations</a> | For a batch of security controls and standards, this operation updates the enabled status of each control.     |
| <a href="#">create_action_target</a>                        | Creates a custom action target in Security Hub.  |
| <a href="#">create_automation_rule</a>                      | Creates an automation rule based on input parameters.  |
| <a href="#">create_configuration_policy</a>                 | Creates a configuration policy with the defined configuration.   |
| <a href="#">create_finding_aggregator</a>                   | Used to enable finding aggregation.  |
| <a href="#">create_insight</a>                              | Creates a custom insight in Security Hub.  |
| <a href="#">create_members</a>                              | Creates a member association in Security Hub between the specified accounts.                                   |
| <a href="#">decline_invitations</a>                         | Declines invitations to become a member account.   |
| <a href="#">delete_action_target</a>                        | Deletes a custom action target from Security Hub.  |
| <a href="#">delete_configuration_policy</a>                 | Deletes a configuration policy.  |
| <a href="#">delete_finding_aggregator</a>                   | Deletes a finding aggregator.  |
| <a href="#">delete_insight</a>                              | Deletes the insight specified by the InsightArn.   |
| <a href="#">delete_invitations</a>                          | Deletes invitations received by the Amazon Web Services account to become a member account.                    |
| <a href="#">delete_members</a>                              | Deletes the specified member accounts from Security Hub.   |
| <a href="#">describe_action_targets</a>                     | Returns a list of the custom action targets in Security Hub in your account.                                   |
| <a href="#">describe_hub</a>                                | Returns details about the Hub resource in your account, including the HubArn.                                  |

|  |  |
|--|--|
| <code>describe_organization_configuration</code>       | Returns information about the way your organization is configured in Security Hub                          |
| <code>describe_products</code>                         | Returns information about product integrations in Security Hub   |
| <code>describe_standards</code>                        | Returns a list of the available standards in Security Hub  |
| <code>describe_standards_controls</code>               | Returns a list of security standards controls  |
| <code>disable_import_findings_for_product</code>       | Disables the integration of the specified product with Security Hub  |
| <code>disable_organization_admin_account</code>        | Disables a Security Hub administrator account  |
| <code>disable_security_hub</code>                      | Disables Security Hub in your account only in the current Amazon Web Services Region                       |
| <code>disassociate_from_administrator_account</code>   | Disassociates the current Security Hub member account from the associated administrator account            |
| <code>disassociate_from_master_account</code>          | This method is deprecated  |
| <code>disassociate_members</code>                      | Disassociates the specified member accounts from the associated administrator account                      |
| <code>enable_import_findings_for_product</code>        | Enables the integration of a partner product with Security Hub   |
| <code>enable_organization_admin_account</code>         | Designates the Security Hub administrator account for an organization                                      |
| <code>enable_security_hub</code>                       | Enables Security Hub for your account in the current Region or the Region you specify                      |
| <code>get_administrator_account</code>                 | Provides the details for the Security Hub administrator account for the current Region                     |
| <code>get_configuration_policy</code>                  | Provides information about a configuration policy  |
| <code>get_configuration_policy_association</code>      | Returns the association between a configuration and a target account, organizational unit, or the root     |
| <code>get_enabled_standards</code>                     | Returns a list of the standards that are currently enabled   |
| <code>get_finding_aggregator</code>                    | Returns the current finding aggregation configuration  |
| <code>get_finding_history</code>                       | Returns history for a Security Hub finding in the last 90 days   |
| <code>get_findings</code>                              | Returns a list of findings that match the specified criteria   |
| <code>get_insight_results</code>                       | Lists the results of the Security Hub insight specified by the insight ARN                                 |
| <code>get_insights</code>                              | Lists and describes insights for the specified insight ARNs  |
| <code>get_invitations_count</code>                     | Returns the count of all Security Hub membership invitations that were sent to the current Region          |
| <code>get_master_account</code>                        | This method is deprecated  |
| <code>get_members</code>                               | Returns the details for the Security Hub member accounts for the specified account                         |
| <code>get_security_control_definition</code>           | Retrieves the definition of a security control   |
| <code>invite_members</code>                            | Invites other Amazon Web Services accounts to become member accounts for the current Region                |
| <code>list_automation_rules</code>                     | A list of automation rules and their metadata for the calling account                                      |
| <code>list_configuration_policies</code>               | Lists the configuration policies that the Security Hub delegated administrator account has created         |
| <code>list_configuration_policy_associations</code>    | Provides information about the associations for your configuration policies and configuration policies     |
| <code>list_enabled_products_for_import</code>          | Lists all findings-generating solutions (products) that you are subscribed to receive findings for         |
| <code>list_finding_aggregators</code>                  | If finding aggregation is enabled, then ListFindingAggregators returns the ARNs of the finding aggregators |
| <code>list_invitations</code>                          | Lists all Security Hub membership invitations that were sent to the current Region                         |
| <code>list_members</code>                              | Lists details about all member accounts for the current Security Hub administrator account                 |
| <code>list_organization_admin_accounts</code>          | Lists the Security Hub administrator accounts  |
| <code>list_security_control_definitions</code>         | Lists all of the security controls that apply to a specified standard                                      |
| <code>list_standards_control_associations</code>       | Specifies whether a control is currently enabled or disabled in each enabled standard                      |
| <code>list_tags_for_resource</code>                    | Returns a list of tags associated with a resource  |
| <code>start_configuration_policy_association</code>    | Associates a target account, organizational unit, or the root with a specified configuration policy        |
| <code>start_configuration_policy_disassociation</code> | Disassociates a target account, organizational unit, or the root from a specified configuration policy     |
| <code>tag_resource</code>                              | Adds one or more tags to a resource  |
| <code>untag_resource</code>                            | Removes one or more tags from a resource   |
| <code>update_action_target</code>                      | Updates the name and description of a custom action target in Security Hub                                 |
| <code>update_configuration_policy</code>               | Updates a configuration policy   |
| <code>update_finding_aggregator</code>                 | Updates the finding aggregation configuration  |
| <code>update_findings</code>                           | UpdateFindings is deprecated   |
| <code>update_insight</code>                            | Updates the Security Hub insight identified by the specified insight ARN                                   |
| <code>update_organization_configuration</code>         | Updates the configuration of your organization in Security Hub   |



|   |   |
|---|---|
| <a href="#">update_security_control</a>           | Updates the properties of a security control                                  |
| <a href="#">update_security_hub_configuration</a> | Updates configuration options for Security Hub                                |
| <a href="#">update_standards_control</a>          | Used to control whether an individual security standard control is enabled or |

## Examples

```
## Not run:
svc <- securityhub()
# The following example demonstrates how an account can accept an
# invitation from the Security Hub administrator account to be a member
# account. This operation is applicable only to member accounts that are
# not added through AWS Organizations.
svc$accept_administrator_invitation(
  AdministratorId = "123456789012",
  InvitationId = "7ab938c5d52d7904ad09f9e7c20cc4eb"
)

## End(Not run)
```

---

securitylake

*Amazon Security Lake*

---

## Description

Amazon Security Lake is a fully managed security data lake service. You can use Security Lake to automatically centralize security data from cloud, on-premises, and custom sources into a data lake that's stored in your Amazon Web Services account. Amazon Web Services Organizations is an account management service that lets you consolidate multiple Amazon Web Services accounts into an organization that you create and centrally manage. With Organizations, you can create member accounts and invite existing accounts to join your organization. Security Lake helps you analyze security data for a more complete understanding of your security posture across the entire organization. It can also help you improve the protection of your workloads, applications, and data.

The data lake is backed by Amazon Simple Storage Service (Amazon S3) buckets, and you retain ownership over your data.

Amazon Security Lake integrates with CloudTrail, a service that provides a record of actions taken by a user, role, or an Amazon Web Services service. In Security Lake, CloudTrail captures API calls for Security Lake as events. The calls captured include calls from the Security Lake console and code calls to the Security Lake API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Security Lake. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in Event history. Using the information collected by CloudTrail you can determine the request that was made to Security Lake, the IP address from which the request was made, who made the request, when it was made, and additional details. To learn more about Security Lake information in CloudTrail, see the [Amazon Security Lake User Guide](#).

Security Lake automates the collection of security-related log and event data from integrated Amazon Web Services and third-party services. It also helps you manage the lifecycle of data with customizable retention and replication settings. Security Lake converts ingested data into Apache Parquet format and a standard open-source schema called the Open Cybersecurity Schema Framework (OCSF).

Other Amazon Web Services and third-party services can subscribe to the data that's stored in Security Lake for incident response and security data analytics.

## Usage

```
securitylake(
  config = list(),
  credentials = list(),
  endpoint = NULL,
  region = NULL
)
```

## Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

- **credentials:**

- **creds:**

- \* **access\_key\_id:** AWS access key ID
- \* **secret\_access\_key:** AWS secret access key
- \* **session\_token:** AWS temporary session token

- **profile:** The name of a profile to use. If not given, then the default profile is used.
- **anonymous:** Set anonymous credentials.

- **endpoint:** The complete URL to use for the constructed client.

- **region:** The AWS Region used in instantiating the client.

- **close\_connection:** Immediately close all HTTP connections.

- **timeout:** The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.

- **s3\_force\_path\_style:** Set this to `true` to force the request to use path-style addressing, i.e. `http://s3.amazonaws.com/BUCKET/KEY`.

- **sts\_regional\_endpoint:** Set sts regional endpoint resolver to regional or legacy <https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html>

`credentials` Optional credentials shorthand for the `config` parameter

- **creds:**

- **access\_key\_id:** AWS access key ID
- **secret\_access\_key:** AWS secret access key
- **session\_token:** AWS temporary session token

- **profile:** The name of a profile to use. If not given, then the default profile is used.

- **anonymous:** Set anonymous credentials.
- endpoint      Optional shorthand for complete URL to use for the constructed client.
- region        Optional shorthand for AWS Region used in instantiating the client.

### Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

### Service syntax

```
svc <- securitylake(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
    creds = list(
      access_key_id = "string",
      secret_access_key = "string",
      session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
  ),
  endpoint = "string",
  region = "string"
)
```

### Operations

[create\\_aws\\_log\\_source](#)  
[create\\_custom\\_log\\_source](#)  
[create\\_data\\_lake](#)

Adds a natively supported Amazon Web Service as an Amazon Security Lake source.  
 Adds a third-party custom source in Amazon Security Lake, from the Amazon Security Lake console.  
 Initializes an Amazon Security Lake instance with the provided (or default) configuration.

|  |  |
|--|--|
| <a href="#">create_data_lake_exception_subscription</a>      | Creates the specified notification subscription in Amazon Security Lake for the account.   |
| <a href="#">create_data_lake_organization_configuration</a>  | Automatically enables Amazon Security Lake for new member accounts in your Region.   |
| <a href="#">create_subscriber</a>                            | Creates a subscription permission for accounts that are already enabled in Amazon Security Lake.                                 |
| <a href="#">create_subscriber_notification</a>               | Notifies the subscriber when new data is written to the data lake for the source.  |
| <a href="#">delete_aws_log_source</a>                        | Removes a natively supported Amazon Web Service as an Amazon Security Lake log source.   |
| <a href="#">delete_custom_log_source</a>                     | Removes a custom log source from Amazon Security Lake, to stop sending data to the data lake.                                    |
| <a href="#">delete_data_lake</a>                             | When you disable Amazon Security Lake from your account, Security Lake is disabled for all member accounts.                      |
| <a href="#">delete_data_lake_exception_subscription</a>      | Deletes the specified notification subscription in Amazon Security Lake for the account.   |
| <a href="#">delete_data_lake_organization_configuration</a>  | Turns off automatic enablement of Amazon Security Lake for member accounts in your Region.                                       |
| <a href="#">delete_subscriber</a>                            | Deletes the subscription permission and all notification settings for accounts that are already enabled in Amazon Security Lake. |
| <a href="#">delete_subscriber_notification</a>               | Deletes the specified notification subscription in Amazon Security Lake for the account.   |
| <a href="#">deregister_data_lake_delegated_administrator</a> | Deletes the Amazon Security Lake delegated administrator account for the organization.   |
| <a href="#">get_data_lake_exception_subscription</a>         | Retrieves the details of exception notifications for the account in Amazon Security Lake.  |
| <a href="#">get_data_lake_organization_configuration</a>     | Retrieves the configuration that will be automatically set up for accounts added to your Region.                                 |
| <a href="#">get_data_lake_sources</a>                        | Retrieves a snapshot of the current Region, including whether Amazon Security Lake is enabled.                                   |
| <a href="#">get_subscriber</a>                               | Retrieves the subscription information for the specified subscription ID.  |
| <a href="#">list_data_lake_exceptions</a>                    | Lists the Amazon Security Lake exceptions that you can use to find the source of the data.                                       |
| <a href="#">list_data_lakes</a>                              | Retrieves the Amazon Security Lake configuration object for the specified Amazon Security Lake account ID.                       |
| <a href="#">list_log_sources</a>                             | Retrieves the log sources in the current Amazon Web Services Region.   |
| <a href="#">list_subscribers</a>                             | List all subscribers for the specific Amazon Security Lake account ID.   |
| <a href="#">list_tags_for_resource</a>                       | Retrieves the tags (keys and values) that are associated with an Amazon Security Lake account.                                   |
| <a href="#">register_data_lake_delegated_administrator</a>   | Designates the Amazon Security Lake delegated administrator account for the organization.  |
| <a href="#">tag_resource</a>                                 | Adds or updates one or more tags that are associated with an Amazon Security Lake account.                                       |
| <a href="#">untag_resource</a>                               | Removes one or more tags (keys and values) from an Amazon Security Lake account.   |
| <a href="#">update_data_lake</a>                             | Specifies where to store your security data and for how long.  |
| <a href="#">update_data_lake_exception_subscription</a>      | Updates the specified notification subscription in Amazon Security Lake for the account.   |
| <a href="#">update_subscriber</a>                            | Updates an existing subscription for the given Amazon Security Lake account ID.  |
| <a href="#">update_subscriber_notification</a>               | Updates an existing notification method for the subscription (SQS or HTTP).  |

## Examples

```
## Not run:
svc <- securitylake()
svc$create_aws_log_source(
  Foo = 123
)

## End(Not run)
```

**Description**

Shield Advanced

This is the *Shield Advanced API Reference*. This guide is for developers who need detailed information about the Shield Advanced API actions, data types, and errors. For detailed information about WAF and Shield Advanced features and an overview of how to use the WAF and Shield Advanced APIs, see the [WAF and Shield Developer Guide](#).

**Usage**

```
shield(config = list(), credentials = list(), endpoint = NULL, region = NULL)
```

**Arguments**

|             |  |
|-------------|--|
| config      | Optional configuration of credentials, endpoint, and/or region. <ul style="list-style-type: none"> <li>• <b>credentials:</b> <ul style="list-style-type: none"> <li>– <b>creds:</b> <ul style="list-style-type: none"> <li>* <b>access_key_id:</b> AWS access key ID</li> <li>* <b>secret_access_key:</b> AWS secret access key</li> <li>* <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>– <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>– <b>anonymous:</b> Set anonymous credentials.</li> </ul> </li> <li>• <b>endpoint:</b> The complete URL to use for the constructed client.</li> <li>• <b>region:</b> The AWS Region used in instantiating the client.</li> <li>• <b>close_connection:</b> Immediately close all HTTP connections.</li> <li>• <b>timeout:</b> The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.</li> <li>• <b>s3_force_path_style:</b> Set this to <code>true</code> to force the request to use path-style addressing, i.e. <code>http://s3.amazonaws.com/BUCKET/KEY</code>.</li> <li>• <b>sts_regional_endpoint:</b> Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul> |
| credentials | Optional credentials shorthand for the config parameter <ul style="list-style-type: none"> <li>• <b>creds:</b> <ul style="list-style-type: none"> <li>– <b>access_key_id:</b> AWS access key ID</li> <li>– <b>secret_access_key:</b> AWS secret access key</li> <li>– <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>• <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>• <b>anonymous:</b> Set anonymous credentials.</li> </ul>  |
| endpoint    | Optional shorthand for complete URL to use for the constructed client.   |
| region      | Optional shorthand for AWS Region used in instantiating the client.  |

**Value**

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

**Service syntax**

```
svc <- shield(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
    creds = list(
      access_key_id = "string",
      secret_access_key = "string",
      session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
  ),
  endpoint = "string",
  region = "string"
)
```

**Operations**

[associate\\_drt\\_log\\_bucket](#)

[associate\\_drt\\_role](#)

[associate\\_health\\_check](#)

[associate\\_proactive\\_engagement\\_details](#)

[create\\_protection](#)

[create\\_protection\\_group](#)

[create\\_subscription](#)

[delete\\_protection](#)

Authorizes the Shield Response Team (SRT) to access the specified Amazon

Authorizes the Shield Response Team (SRT) using the specified role, to acce

Adds health-based detection to the Shield Advanced protection for a resourc

Initializes proactive engagement and sets the list of contacts for the Shield R

Enables Shield Advanced for a specific Amazon Web Services resource

Creates a grouping of protected resources so they can be handled as a collect

Activates Shield Advanced for an account

Deletes an Shield Advanced Protection

|   |  |
|---|--|
| <code>delete_protection_group</code>                      | Removes the specified protection group   |
| <code>delete_subscription</code>                          | Removes Shield Advanced from an account  |
| <code>describe_attack</code>                              | Describes the details of a DDoS attack   |
| <code>describe_attack_statistics</code>                   | Provides information about the number and type of attacks Shield has detected  |
| <code>describe_drt_access</code>                          | Returns the current role and list of Amazon S3 log buckets used by the Shield Response Team                                    |
| <code>describe_emergency_contact_settings</code>          | A list of email addresses and phone numbers that the Shield Response Team can use to contact you                               |
| <code>describe_protection</code>                          | Lists the details of a Protection object   |
| <code>describe_protection_group</code>                    | Returns the specification for the specified protection group   |
| <code>describe_subscription</code>                        | Provides details about the Shield Advanced subscription for an account   |
| <code>disable_application_layer_automatic_response</code> | Disable the Shield Advanced automatic application layer DDoS mitigation for the specified Amazon Web Services resource         |
| <code>disable_proactive_engagement</code>                 | Removes authorization from the Shield Response Team (SRT) to notify contacts about DDoS attacks                                |
| <code>disassociate_drt_log_bucket</code>                  | Removes the Shield Response Team's (SRT) access to the specified Amazon S3 log bucket  |
| <code>disassociate_drt_role</code>                        | Removes the Shield Response Team's (SRT) access to your Amazon Web Services account  |
| <code>disassociate_health_check</code>                    | Removes health-based detection from the Shield Advanced protection for a resource  |
| <code>enable_application_layer_automatic_response</code>  | Enable the Shield Advanced automatic application layer DDoS mitigation for the specified Amazon Web Services resource          |
| <code>enable_proactive_engagement</code>                  | Authorizes the Shield Response Team (SRT) to use email and phone to notify contacts about DDoS attacks                         |
| <code>get_subscription_state</code>                       | Returns the SubscriptionState, either Active or Inactive   |
| <code>list_attacks</code>                                 | Returns all ongoing DDoS attacks or all DDoS attacks during a specified time period  |
| <code>list_protection_groups</code>                       | Retrieves ProtectionGroup objects for the account  |
| <code>list_protections</code>                             | Retrieves Protection objects for the account   |
| <code>list_resources_in_protection_group</code>           | Retrieves the resources that are included in the protection group  |
| <code>list_tags_for_resource</code>                       | Gets information about Amazon Web Services tags for a specified Amazon Web Services resource                                   |
| <code>tag_resource</code>                                 | Adds or updates tags for a resource in Shield  |
| <code>untag_resource</code>                               | Removes tags from a resource in Shield   |
| <code>update_application_layer_automatic_response</code>  | Updates an existing Shield Advanced automatic application layer DDoS mitigation for the specified Amazon Web Services resource |
| <code>update_emergency_contact_settings</code>            | Updates the details of the list of email addresses and phone numbers that the Shield Response Team can use to contact you      |
| <code>update_protection_group</code>                      | Updates an existing protection group   |
| <code>update_subscription</code>                          | Updates the details of an existing subscription  |

## Examples

```
## Not run:
svc <- shield()
svc$associate_drt_log_bucket(
  Foo = 123
)

## End(Not run)
```

## Description

AWS IAM Identity Center (successor to AWS Single Sign-On) Portal is a web service that makes it easy for you to assign user access to IAM Identity Center resources such as the AWS access portal. Users can get AWS account applications and roles assigned to them and get federated into the application.

Although AWS Single Sign-On was renamed, the `sso` and `identitystore` API namespaces will continue to retain their original name for backward compatibility purposes. For more information, see [IAM Identity Center rename](#).

This reference guide describes the IAM Identity Center Portal operations that you can call programmatically and includes detailed information on data types and errors.

AWS provides SDKs that consist of libraries and sample code for various programming languages and platforms, such as Java, Ruby, .Net, iOS, or Android. The SDKs provide a convenient way to create programmatic access to IAM Identity Center and other AWS services. For more information about the AWS SDKs, including how to download and install them, see [Tools for Amazon Web Services](#).

## Usage

```
sso(config = list(), credentials = list(), endpoint = NULL, region = NULL)
```

## Arguments

|                          |   |
|--------------------------|---|
| <code>config</code>      | <p>Optional configuration of credentials, endpoint, and/or region.</p> <ul style="list-style-type: none"> <li>• <b>credentials:</b> <ul style="list-style-type: none"> <li>– <b>creds:</b> <ul style="list-style-type: none"> <li>* <b>access_key_id:</b> AWS access key ID</li> <li>* <b>secret_access_key:</b> AWS secret access key</li> <li>* <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>– <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>– <b>anonymous:</b> Set anonymous credentials.</li> </ul> </li> <li>• <b>endpoint:</b> The complete URL to use for the constructed client.</li> <li>• <b>region:</b> The AWS Region used in instantiating the client.</li> <li>• <b>close_connection:</b> Immediately close all HTTP connections.</li> <li>• <b>timeout:</b> The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.</li> <li>• <b>s3_force_path_style:</b> Set this to <code>true</code> to force the request to use path-style addressing, i.e. <code>http://s3.amazonaws.com/BUCKET/KEY</code>.</li> <li>• <b>sts_regional_endpoint:</b> Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul> |
| <code>credentials</code> | <p>Optional credentials shorthand for the <code>config</code> parameter</p> <ul style="list-style-type: none"> <li>• <b>creds:</b> <ul style="list-style-type: none"> <li>– <b>access_key_id:</b> AWS access key ID</li> </ul> </li> </ul>  |



- **secret\_access\_key**: AWS secret access key
  - **session\_token**: AWS temporary session token
  - **profile**: The name of a profile to use. If not given, then the default profile is used.
  - **anonymous**: Set anonymous credentials.
- endpoint           Optional shorthand for complete URL to use for the constructed client.
- region             Optional shorthand for AWS Region used in instantiating the client.

## Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

## Service syntax

```
svc <- sso(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
    creds = list(
      access_key_id = "string",
      secret_access_key = "string",
      session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
  ),
  endpoint = "string",
  region = "string"
)
```

**Operations**

|                                      |   |
|--------------------------------------|---|
| <a href="#">get_role_credentials</a> | Returns the STS short-term credentials for a given role name that is assigned to the user                         |
| <a href="#">list_account_roles</a>   | Lists all roles that are assigned to the user for a given AWS account   |
| <a href="#">list_accounts</a>        | Lists all AWS accounts assigned to the user   |
| <a href="#">logout</a>               | Removes the locally stored SSO tokens from the client-side cache and sends an API call to the IAM Identity Center |

## Examples

```
## Not run:
svc <- sso()
svc$get_role_credentials(
  Foo = 123
)

## End(Not run)
```

---

ssoadmin

*AWS Single Sign-On Admin*

---

## Description

IAM Identity Center (successor to Single Sign-On) helps you securely create, or connect, your workforce identities and manage their access centrally across Amazon Web Services accounts and applications. IAM Identity Center is the recommended approach for workforce authentication and authorization in Amazon Web Services, for organizations of any size and type.

IAM Identity Center uses the `sso` and `identitystore` API namespaces.

This reference guide provides information on single sign-on operations which could be used for access management of Amazon Web Services accounts. For information about IAM Identity Center features, see the [IAM Identity Center User Guide](#).

Many operations in the IAM Identity Center APIs rely on identifiers for users and groups, known as principals. For more information about how to work with principals and principal IDs in IAM Identity Center, see the [Identity Store API Reference](#).

Amazon Web Services provides SDKs that consist of libraries and sample code for various programming languages and platforms (Java, Ruby, .Net, iOS, Android, and more). The SDKs provide a convenient way to create programmatic access to IAM Identity Center and other Amazon Web Services services. For more information about the Amazon Web Services SDKs, including how to download and install them, see [Tools for Amazon Web Services](#).

## Usage

```
ssoadmin(config = list(), credentials = list(), endpoint = NULL, region = NULL)
```

## Arguments

|             |   |
|-------------|---|
| config      | Optional configuration of credentials, endpoint, and/or region. <ul style="list-style-type: none"> <li>• <b>credentials:</b> <ul style="list-style-type: none"> <li>– <b>creds:</b> <ul style="list-style-type: none"> <li>* <b>access_key_id:</b> AWS access key ID</li> <li>* <b>secret_access_key:</b> AWS secret access key</li> <li>* <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>– <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>– <b>anonymous:</b> Set anonymous credentials.</li> </ul> </li> <li>• <b>endpoint:</b> The complete URL to use for the constructed client.</li> <li>• <b>region:</b> The AWS Region used in instantiating the client.</li> <li>• <b>close_connection:</b> Immediately close all HTTP connections.</li> <li>• <b>timeout:</b> The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.</li> <li>• <b>s3_force_path_style:</b> Set this to true to force the request to use path-style addressing, i.e. <code>http://s3.amazonaws.com/BUCKET/KEY</code>.</li> <li>• <b>sts_regional_endpoint:</b> Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul> |
| credentials | Optional credentials shorthand for the config parameter <ul style="list-style-type: none"> <li>• <b>creds:</b> <ul style="list-style-type: none"> <li>– <b>access_key_id:</b> AWS access key ID</li> <li>– <b>secret_access_key:</b> AWS secret access key</li> <li>– <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>• <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>• <b>anonymous:</b> Set anonymous credentials.</li> </ul>   |
| endpoint    | Optional shorthand for complete URL to use for the constructed client.  |
| region      | Optional shorthand for AWS Region used in instantiating the client.   |

## Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

## Service syntax

```
svc <- ssoadmin(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
```

```

        secret_access_key = "string",
        session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
),
endpoint = "string",
region = "string",
close_connection = "logical",
timeout = "numeric",
s3_force_path_style = "logical",
sts_regional_endpoint = "string"
),
credentials = list(
    creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
),
endpoint = "string",
region = "string"
)

```

## Operations

[attach\\_customer\\_managed\\_policy\\_reference\\_to\\_permission\\_set](#)  
[attach\\_managed\\_policy\\_to\\_permission\\_set](#)  
[create\\_account\\_assignment](#)  
[create\\_application](#)  
[create\\_application\\_assignment](#)  
[create\\_instance](#)  
[create\\_instance\\_access\\_control\\_attribute\\_configuration](#)  
[create\\_permission\\_set](#)  
[create\\_trusted\\_token\\_issuer](#)  
[delete\\_account\\_assignment](#)  
[delete\\_application](#)  
[delete\\_application\\_access\\_scope](#)  
[delete\\_application\\_assignment](#)  
[delete\\_application\\_authentication\\_method](#)  
[delete\\_application\\_grant](#)  
[delete\\_inline\\_policy\\_from\\_permission\\_set](#)  
[delete\\_instance](#)  
[delete\\_instance\\_access\\_control\\_attribute\\_configuration](#)  
[delete\\_permissions\\_boundary\\_from\\_permission\\_set](#)  
[delete\\_permission\\_set](#)

Attaches the specified customer managed policy to the s  
 Attaches an Amazon Web Services managed policy AR  
 Assigns access to a principal for a specified Amazon W  
 Creates an application in IAM Identity Center for the gi  
 Grant application access to a user or group  
 Creates an instance of IAM Identity Center for a standa  
 Enables the attributes-based access control (ABAC) fea  
 Creates a permission set within a specified IAM Identity  
 Creates a connection to a trusted token issuer in an insta  
 Deletes a principal's access from a specified Amazon W  
 Deletes the association with the application  
 Deletes an IAM Identity Center access scope from an ap  
 Revoke application access to an application by deleting  
 Deletes an authentication method from an application  
 Deletes a grant from an application  
 Deletes the inline policy from a specified permission set  
 Deletes the instance of IAM Identity Center  
 Disables the attributes-based access control (ABAC) fea  
 Deletes the permissions boundary from a specified Perm  
 Deletes the specified permission set

|   |  |
|---|--|
| <code>delete_trusted_token_issuer</code>                                  | Deletes a trusted token issuer configuration from an instance                          |
| <code>describe_account_assignment_creation_status</code>                  | Describes the status of the assignment creation request                                |
| <code>describe_account_assignment_deletion_status</code>                  | Describes the status of the assignment deletion request                                |
| <code>describe_application</code>   | Retrieves the details of an application associated with an instance                    |
| <code>describe_application_assignment</code>                              | Retrieves a direct assignment of a user or group to an application                     |
| <code>describe_application_provider</code>                                | Retrieves details about a provider that can be used to connect to an application       |
| <code>describe_instance</code>  | Returns the details of an instance of IAM Identity Center                              |
| <code>describe_instance_access_control_attribute_configuration</code>     | Returns the list of IAM Identity Center identity store attributes                      |
| <code>describe_permission_set</code>                                      | Gets the details of the permission set   |
| <code>describe_permission_set_provisioning_status</code>                  | Describes the status for the given permission set provisioning request                 |
| <code>describe_trusted_token_issuer</code>                                | Retrieves details about a trusted token issuer configuration                           |
| <code>detach_customer_managed_policy_reference_from_permission_set</code> | Detaches the specified customer managed policy from the permission set                 |
| <code>detach_managed_policy_from_permission_set</code>                    | Detaches the attached Amazon Web Services managed policy from the permission set       |
| <code>get_application_access_scope</code>                                 | Retrieves the authorized targets for an IAM Identity Center application                |
| <code>get_application_assignment_configuration</code>                     | Retrieves the configuration of PutApplicationAssignment                                |
| <code>get_application_authentication_method</code>                        | Retrieves details about an authentication method used by an application                |
| <code>get_application_grant</code>  | Retrieves details about an application grant   |
| <code>get_inline_policy_for_permission_set</code>                         | Obtains the inline policy assigned to the permission set                               |
| <code>get_permissions_boundary_for_permission_set</code>                  | Obtains the permissions boundary for a specified PermissionSet                         |
| <code>list_account_assignment_creation_status</code>                      | Lists the status of the Amazon Web Services account assignment creation request        |
| <code>list_account_assignment_deletion_status</code>                      | Lists the status of the Amazon Web Services account assignment deletion request        |
| <code>list_account_assignments</code>                                     | Lists the assignee of the specified Amazon Web Services managed policy                 |
| <code>list_account_assignments_for_principal</code>                       | Retrieves a list of the IAM Identity Center associated Amazon Web Services accounts    |
| <code>list_accounts_for_provisioned_permission_set</code>                 | Lists all the Amazon Web Services accounts where the permission set is provisioned     |
| <code>list_application_access_scopes</code>                               | Lists the access scopes and authorized targets associated with an application          |
| <code>list_application_assignments</code>                                 | Lists Amazon Web Services account users that are assigned to an application            |
| <code>list_application_assignments_for_principal</code>                   | Lists the applications to which a specified principal is assigned                      |
| <code>list_application_authentication_methods</code>                      | Lists all of the authentication methods supported by the application                   |
| <code>list_application_grants</code>                                      | List the grants associated with an application   |
| <code>list_application_providers</code>                                   | Lists the application providers configured in the IAM Identity Center instance         |
| <code>list_applications</code>  | Lists all applications associated with the instance of IAM Identity Center             |
| <code>list_customer_managed_policy_references_in_permission_set</code>    | Lists all customer managed policies attached to a specified permission set             |
| <code>list_instances</code>   | Lists the details of the organization and account instances                            |
| <code>list_managed_policies_in_permission_set</code>                      | Lists the Amazon Web Services managed policy that is attached to the permission set    |
| <code>list_permission_set_provisioning_status</code>                      | Lists the status of the permission set provisioning request                            |
| <code>list_permission_sets</code>   | Lists the PermissionSets in an IAM Identity Center instance                            |
| <code>list_permission_sets_provisioned_to_account</code>                  | Lists all the permission sets that are provisioned to a specified account              |
| <code>list_tags_for_resource</code>                                       | Lists the tags that are attached to a specified resource                               |
| <code>list_trusted_token_issuers</code>                                   | Lists all the trusted token issuers configured in an instance                          |
| <code>provision_permission_set</code>                                     | The process by which a specified permission set is provisioned                         |
| <code>put_application_access_scope</code>                                 | Adds or updates the list of authorized targets for an IAM Identity Center application  |
| <code>put_application_assignment_configuration</code>                     | Configure how users gain access to an application                                      |
| <code>put_application_authentication_method</code>                        | Adds or updates an authentication method for an application                            |
| <code>put_application_grant</code>  | Adds a grant to an application   |
| <code>put_inline_policy_to_permission_set</code>                          | Attaches an inline policy to a permission set  |
| <code>put_permissions_boundary_to_permission_set</code>                   | Attaches an Amazon Web Services managed or customer managed policy to a permission set |
| <code>tag_resource</code>   | Associates a set of tags with a specified resource                                     |
| <code>untag_resource</code>   | Disassociates a set of tags from a specified resource                                  |

|  |  |
|--|--|
| <a href="#">update_application</a>                                     | Updates application properties                             |
| <a href="#">update_instance</a>  | Update the details for the instance of IAM Identity Center |
| <a href="#">update_instance_access_control_attribute_configuration</a> | Updates the IAM Identity Center identity store attribute   |
| <a href="#">update_permission_set</a>                                  | Updates an existing permission set                         |
| <a href="#">update_trusted_token_issuer</a>                            | Updates the name of the trusted token issuer, or the path  |

## Examples

```
## Not run:
svc <- ssoadmin()
svc$attach_customer_managed_policy_reference_to_permission_set(
  Foo = 123
)

## End(Not run)
```

---

ssooidc

*AWS SSO OIDC*

---

## Description

IAM Identity Center OpenID Connect (OIDC) is a web service that enables a client (such as CLI or a native application) to register with IAM Identity Center. The service also enables the client to fetch the user's access token upon successful authentication and authorization with IAM Identity Center.

IAM Identity Center uses the `sso` and `identitystore` API namespaces.

### Considerations for Using This Guide

Before you begin using this guide, we recommend that you first review the following important information about how the IAM Identity Center OIDC service works.

- The IAM Identity Center OIDC service currently implements only the portions of the OAuth 2.0 Device Authorization Grant standard (<https://tools.ietf.org/html/rfc8628>) that are necessary to enable single sign-on authentication with the CLI.
- With older versions of the CLI, the service only emits OIDC access tokens, so to obtain a new token, users must explicitly re-authenticate. To access the OIDC flow that supports token refresh and doesn't require re-authentication, update to the latest CLI version (1.27.10 for CLI V1 and 2.9.0 for CLI V2) with support for OIDC token refresh and configurable IAM Identity Center session durations. For more information, see [Configure Amazon Web Services access portal session duration](#).
- The access tokens provided by this service grant access to all Amazon Web Services account entitlements assigned to an IAM Identity Center user, not just a particular application.

- The documentation in this guide does not describe the mechanism to convert the access token into Amazon Web Services Auth (“sigv4”) credentials for use with IAM-protected Amazon Web Services service endpoints. For more information, see [GetRoleCredentials](#) in the *IAM Identity Center Portal API Reference Guide*.

For general information about IAM Identity Center, see [What is IAM Identity Center?](#) in the *IAM Identity Center User Guide*.

## Usage

```
ssooidc(config = list(), credentials = list(), endpoint = NULL, region = NULL)
```

## Arguments

|             |  |
|-------------|--|
| config      | Optional configuration of credentials, endpoint, and/or region. <ul style="list-style-type: none"> <li>• <b>credentials:</b> <ul style="list-style-type: none"> <li>– <b>creds:</b> <ul style="list-style-type: none"> <li>* <b>access_key_id:</b> AWS access key ID</li> <li>* <b>secret_access_key:</b> AWS secret access key</li> <li>* <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>– <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>– <b>anonymous:</b> Set anonymous credentials.</li> </ul> </li> <li>• <b>endpoint:</b> The complete URL to use for the constructed client.</li> <li>• <b>region:</b> The AWS Region used in instantiating the client.</li> <li>• <b>close_connection:</b> Immediately close all HTTP connections.</li> <li>• <b>timeout:</b> The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.</li> <li>• <b>s3_force_path_style:</b> Set this to <code>true</code> to force the request to use path-style addressing, i.e. <code>http://s3.amazonaws.com/BUCKET/KEY</code>.</li> <li>• <b>sts_regional_endpoint:</b> Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul> |
| credentials | Optional credentials shorthand for the config parameter <ul style="list-style-type: none"> <li>• <b>creds:</b> <ul style="list-style-type: none"> <li>– <b>access_key_id:</b> AWS access key ID</li> <li>– <b>secret_access_key:</b> AWS secret access key</li> <li>– <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>• <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>• <b>anonymous:</b> Set anonymous credentials.</li> </ul>  |
| endpoint    | Optional shorthand for complete URL to use for the constructed client.   |
| region      | Optional shorthand for AWS Region used in instantiating the client.  |



**Value**

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

**Service syntax**

```
svc <- ssooidc(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
    creds = list(
      access_key_id = "string",
      secret_access_key = "string",
      session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
  ),
  endpoint = "string",
  region = "string"
)
```

**Operations**

|  |   |
|--|---|
| <a href="#">create_token</a>               | Creates and returns access and refresh tokens for clients that are authenticated using client secrets       |
| <a href="#">create_token_with_iam</a>      | Creates and returns access and refresh tokens for clients and applications that are authenticated using IAM |
| <a href="#">register_client</a>            | Registers a client with IAM Identity Center   |
| <a href="#">start_device_authorization</a> | Initiates device authorization by requesting a pair of verification codes from the authorization server     |

## Examples

```
## Not run:
svc <- ssooidc()
#
svc$create_token(
  clientId = "_yzkThXVzLWVhc3QtMQEXAMPLECLIENTID",
  clientSecret = "VERYLONGSECRETeyJraWQiOiJrZXktMTU2NDY0ODI5ImFsZyI6IkhTMzg0In0",
  deviceCode = "yJraWQiOiJrZXktMTU2NDY0ODI5ImFsZyI6IkhTMzIn0EXAMPLEDEVICECODE",
  grantType = "urn:ietf:params:oauth:grant-type:device-code"
)

## End(Not run)
```

---

 sts

 AWS Security Token Service
 

---

## Description

Security Token Service

Security Token Service (STS) enables you to request temporary, limited-privilege credentials for users. This guide provides descriptions of the STS API. For more information about using this service, see [Temporary Security Credentials](#).

## Usage

```
sts(config = list(), credentials = list(), endpoint = NULL, region = NULL)
```

## Arguments

config      Optional configuration of credentials, endpoint, and/or region.

- **credentials:**
  - **creds:**
    - \* **access\_key\_id:** AWS access key ID
    - \* **secret\_access\_key:** AWS secret access key
    - \* **session\_token:** AWS temporary session token
  - **profile:** The name of a profile to use. If not given, then the default profile is used.
  - **anonymous:** Set anonymous credentials.
- **endpoint:** The complete URL to use for the constructed client.
- **region:** The AWS Region used in instantiating the client.
- **close\_connection:** Immediately close all HTTP connections.
- **timeout:** The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.
- **s3\_force\_path\_style:** Set this to true to force the request to use path-style addressing, i.e. `http://s3.amazonaws.com/BUCKET/KEY`.

|             |  |
|-------------|--|
|             | <ul style="list-style-type: none"> <li>• <b>sts_regional_endpoint</b>: Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul>   |
| credentials | <p>Optional credentials shorthand for the config parameter</p> <ul style="list-style-type: none"> <li>• <b>creds</b>: <ul style="list-style-type: none"> <li>– <b>access_key_id</b>: AWS access key ID</li> <li>– <b>secret_access_key</b>: AWS secret access key</li> <li>– <b>session_token</b>: AWS temporary session token</li> </ul> </li> <li>• <b>profile</b>: The name of a profile to use. If not given, then the default profile is used.</li> <li>• <b>anonymous</b>: Set anonymous credentials.</li> </ul> |
| endpoint    | Optional shorthand for complete URL to use for the constructed client.   |
| region      | Optional shorthand for AWS Region used in instantiating the client.  |

### Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

### Service syntax

```
svc <- sts(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
    creds = list(
      access_key_id = "string",
      secret_access_key = "string",
      session_token = "string"
    ),
    profile = "string",
```

```

    anonymous = "logical"
  ),
  endpoint = "string",
  region = "string"
)

```

## Operations

|   |   |
|---|---|
| <a href="#">assume_role</a>                   | Returns a set of temporary security credentials that you can use to access Amazon Web Services.                             |
| <a href="#">assume_role_with_saml</a>         | Returns a set of temporary security credentials for users who have been authenticated via a SAML assertion.                 |
| <a href="#">assume_role_with_web_identity</a> | Returns a set of temporary security credentials for users who have been authenticated in a web browser.                     |
| <a href="#">decode_authorization_message</a>  | Decodes additional information about the authorization status of a request from an encoded authorization message.           |
| <a href="#">get_access_key_info</a>           | Returns the account identifier for the specified access key ID.   |
| <a href="#">get_caller_identity</a>           | Returns details about the IAM user or role whose credentials are used to call the operation.                                |
| <a href="#">get_federation_token</a>          | Returns a set of temporary security credentials (consisting of an access key ID, a secret access key, and a session token). |
| <a href="#">get_session_token</a>             | Returns a set of temporary credentials for an Amazon Web Services account or IAM user.                                      |

## Examples

```

## Not run:
svc <- sts()
#
svc$assume_role(
  ExternalId = "123ABC",
  Policy = "{ \"Version\": \"2012-10-17\", \"Statement\": [{ \"Sid\": \"Stmnt1\", \"Effect\": \"A...\",
  RoleArn = \"arn:aws:iam::123456789012:role/demo\",
  RoleSessionName = \"testAssumeRoleSession\",
  Tags = list(
    list(
      Key = \"Project\",
      Value = \"Unicorn\"
    ),
    list(
      Key = \"Team\",
      Value = \"Automation\"
    ),
    list(
      Key = \"Cost-Center\",
      Value = \"12345\"
    )
  ),
  TransitiveTagKeys = list(
    \"Project\",
    \"Cost-Center\"
  )
)
## End(Not run)

```

## Description

Amazon Verified Permissions is a permissions management service from Amazon Web Services. You can use Verified Permissions to manage permissions for your application, and authorize user access based on those permissions. Using Verified Permissions, application developers can grant access based on information about the users, resources, and requested actions. You can also evaluate additional information like group membership, attributes of the resources, and session context, such as time of request and IP addresses. Verified Permissions manages these permissions by letting you create and store authorization policies for your applications, such as consumer-facing web sites and enterprise business systems.

Verified Permissions uses Cedar as the policy language to express your permission requirements. Cedar supports both role-based access control (RBAC) and attribute-based access control (ABAC) authorization models.

For more information about configuring, administering, and using Amazon Verified Permissions in your applications, see the [Amazon Verified Permissions User Guide](#).

For more information about the Cedar policy language, see the [Cedar Policy Language Guide](#).

When you write Cedar policies that reference principals, resources and actions, you can define the unique identifiers used for each of those elements. We strongly recommend that you follow these best practices:

- **Use values like universally unique identifiers (UUIDs) for all principal and resource identifiers.**

For example, if user `jane` leaves the company, and you later let someone else use the name `jane`, then that new user automatically gets access to everything granted by policies that still reference `User: "jane"`. Cedar can't distinguish between the new user and the old. This applies to both principal and resource identifiers. Always use identifiers that are guaranteed unique and never reused to ensure that you don't unintentionally grant access because of the presence of an old identifier in a policy.

Where you use a UUID for an entity, we recommend that you follow it with the `//` comment specifier and the 'friendly' name of your entity. This helps to make your policies easier to understand. For example: `principal == User: "a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111", // alice`

- **Do not include personally identifying, confidential, or sensitive information as part of the unique identifier for your principals or resources.** These identifiers are included in log entries shared in CloudTrail trails.

Several operations return structures that appear similar, but have different purposes. As new functionality is added to the product, the structure used in a parameter of one operation might need to change in a way that wouldn't make sense for the same parameter in a different operation. To help you understand the purpose of each, the following naming convention is used for the structures:

- Parameter type structures that end in `Detail` are used in Get operations.

- Parameter type structures that end in `Item` are used in `List` operations.
- Parameter type structures that use neither suffix are used in the mutating (create and update) operations.

### Usage

```
verifiedpermissions(
  config = list(),
  credentials = list(),
  endpoint = NULL,
  region = NULL
)
```

### Arguments

|             |   |
|-------------|---|
| config      | <p>Optional configuration of credentials, endpoint, and/or region.</p> <ul style="list-style-type: none"> <li>• <b>credentials:</b> <ul style="list-style-type: none"> <li>– <b>creds:</b> <ul style="list-style-type: none"> <li>* <b>access_key_id:</b> AWS access key ID</li> <li>* <b>secret_access_key:</b> AWS secret access key</li> <li>* <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>– <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>– <b>anonymous:</b> Set anonymous credentials.</li> </ul> </li> <li>• <b>endpoint:</b> The complete URL to use for the constructed client.</li> <li>• <b>region:</b> The AWS Region used in instantiating the client.</li> <li>• <b>close_connection:</b> Immediately close all HTTP connections.</li> <li>• <b>timeout:</b> The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.</li> <li>• <b>s3_force_path_style:</b> Set this to <code>true</code> to force the request to use path-style addressing, i.e. <code>http://s3.amazonaws.com/BUCKET/KEY</code>.</li> <li>• <b>sts_regional_endpoint:</b> Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul> |
| credentials | <p>Optional credentials shorthand for the config parameter</p> <ul style="list-style-type: none"> <li>• <b>creds:</b> <ul style="list-style-type: none"> <li>– <b>access_key_id:</b> AWS access key ID</li> <li>– <b>secret_access_key:</b> AWS secret access key</li> <li>– <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>• <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>• <b>anonymous:</b> Set anonymous credentials.</li> </ul>  |
| endpoint    | Optional shorthand for complete URL to use for the constructed client.  |
| region      | Optional shorthand for AWS Region used in instantiating the client.   |

**Value**

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

**Service syntax**

```
svc <- verifiedpermissions(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
    creds = list(
      access_key_id = "string",
      secret_access_key = "string",
      session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
  ),
  endpoint = "string",
  region = "string"
)
```

**Operations**

|  |   |
|--|---|
| <a href="#">batch_is_authorized</a>    | Makes a series of decisions about multiple authorization requests for one principal or resource |
| <a href="#">create_identity_source</a> | Creates a reference to an Amazon Cognito user pool as an external identity provider (IdP)       |
| <a href="#">create_policy</a>          | Creates a Cedar policy and saves it in the specified policy store                               |
| <a href="#">create_policy_store</a>    | Creates a policy store  |
| <a href="#">create_policy_template</a> | Creates a policy template   |
| <a href="#">delete_identity_source</a> | Deletes an identity source that references an identity provider (IdP) such as Amazon Cognito    |
| <a href="#">delete_policy</a>          | Deletes the specified policy from the policy store  |
| <a href="#">delete_policy_store</a>    | Deletes the specified policy store  |

|                                       |   |
|---------------------------------------|---|
| <code>delete_policy_template</code>   | Deletes the specified policy template from the policy store   |
| <code>get_identity_source</code>      | Retrieves the details about the specified identity source   |
| <code>get_policy</code>               | Retrieves information about the specified policy  |
| <code>get_policy_store</code>         | Retrieves details about a policy store  |
| <code>get_policy_template</code>      | Retrieve the details for the specified policy template in the specified policy store                |
| <code>get_schema</code>               | Retrieve the details for the specified schema in the specified policy store                         |
| <code>is_authorized</code>            | Makes an authorization decision about a service request described in the parameters                 |
| <code>is_authorized_with_token</code> | Makes an authorization decision about a service request described in the parameters                 |
| <code>list_identity_sources</code>    | Returns a paginated list of all of the identity sources defined in the specified policy store       |
| <code>list_policies</code>            | Returns a paginated list of all policies stored in the specified policy store                       |
| <code>list_policy_stores</code>       | Returns a paginated list of all policy stores in the calling Amazon Web Services account            |
| <code>list_policy_templates</code>    | Returns a paginated list of all policy templates in the specified policy store                      |
| <code>put_schema</code>               | Creates or updates the policy schema in the specified policy store                                  |
| <code>update_identity_source</code>   | Updates the specified identity source to use a new identity provider (IdP) source, or to change the |
| <code>update_policy</code>            | Modifies a Cedar static policy in the specified policy store  |
| <code>update_policy_store</code>      | Modifies the validation setting for a policy store  |
| <code>update_policy_template</code>   | Updates the specified policy template   |

## Examples

```
## Not run:
svc <- verifiedpermissions()
svc$batch_is_authorized(
  Foo = 123
)

## End(Not run)
```

---

waf

AWS WAF

---

## Description

This is **AWS WAF Classic** documentation. For more information, see **AWS WAF Classic** in the developer guide.

**For the latest version of AWS WAF**, use the AWS WAFV2 API and see the **AWS WAF Developer Guide**. With the latest version, AWS WAF has a single set of endpoints for regional and global use.

This is the *AWS WAF Classic API Reference* for using AWS WAF Classic with Amazon CloudFront. The AWS WAF Classic actions and data types listed in the reference are available for protecting Amazon CloudFront distributions. You can use these actions and data types via the endpoint *waf.amazonaws.com*. This guide is for developers who need detailed information about the AWS WAF Classic API actions, data types, and errors. For detailed information about AWS WAF Classic features and an overview of how to use the AWS WAF Classic API, see the **AWS WAF Classic** in the developer guide.



**Usage**

```
waf(config = list(), credentials = list(), endpoint = NULL, region = NULL)
```

**Arguments**

|             |   |
|-------------|---|
| config      | Optional configuration of credentials, endpoint, and/or region. <ul style="list-style-type: none"> <li>• <b>credentials:</b> <ul style="list-style-type: none"> <li>– <b>creds:</b> <ul style="list-style-type: none"> <li>* <b>access_key_id:</b> AWS access key ID</li> <li>* <b>secret_access_key:</b> AWS secret access key</li> <li>* <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>– <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>– <b>anonymous:</b> Set anonymous credentials.</li> </ul> </li> <li>• <b>endpoint:</b> The complete URL to use for the constructed client.</li> <li>• <b>region:</b> The AWS Region used in instantiating the client.</li> <li>• <b>close_connection:</b> Immediately close all HTTP connections.</li> <li>• <b>timeout:</b> The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.</li> <li>• <b>s3_force_path_style:</b> Set this to true to force the request to use path-style addressing, i.e. <code>http://s3.amazonaws.com/BUCKET/KEY</code>.</li> <li>• <b>sts_regional_endpoint:</b> Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul> |
| credentials | Optional credentials shorthand for the config parameter <ul style="list-style-type: none"> <li>• <b>creds:</b> <ul style="list-style-type: none"> <li>– <b>access_key_id:</b> AWS access key ID</li> <li>– <b>secret_access_key:</b> AWS secret access key</li> <li>– <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>• <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>• <b>anonymous:</b> Set anonymous credentials.</li> </ul>   |
| endpoint    | Optional shorthand for complete URL to use for the constructed client.  |
| region      | Optional shorthand for AWS Region used in instantiating the client.   |

**Value**

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

**Service syntax**

```

svc <- waf(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
    creds = list(
      access_key_id = "string",
      secret_access_key = "string",
      session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
  ),
  endpoint = "string",
  region = "string"
)

```

**Operations**

|  |  |
|--|--|
| <a href="#">create_byte_match_set</a>          | This is AWS WAF Classic documentation  |
| <a href="#">create_geo_match_set</a>           | This is AWS WAF Classic documentation  |
| <a href="#">create_ip_set</a>                  | This is AWS WAF Classic documentation  |
| <a href="#">create_rate_based_rule</a>         | This is AWS WAF Classic documentation  |
| <a href="#">create_regex_match_set</a>         | This is AWS WAF Classic documentation  |
| <a href="#">create_regex_pattern_set</a>       | This is AWS WAF Classic documentation  |
| <a href="#">create_rule</a>                    | This is AWS WAF Classic documentation  |
| <a href="#">create_rule_group</a>              | This is AWS WAF Classic documentation  |
| <a href="#">create_size_constraint_set</a>     | This is AWS WAF Classic documentation  |
| <a href="#">create_sql_injection_match_set</a> | This is AWS WAF Classic documentation  |
| <a href="#">create_web_acl</a>                 | This is AWS WAF Classic documentation  |
| <a href="#">create_web_acl_migration_stack</a> | Creates an AWS CloudFormation WAFV2 template for the specified web ACL in the sp |
| <a href="#">create_xss_match_set</a>           | This is AWS WAF Classic documentation  |
| <a href="#">delete_byte_match_set</a>          | This is AWS WAF Classic documentation  |

|  |                                       |
|--|---------------------------------------|
| <a href="#">delete_geo_match_set</a>               | This is AWS WAF Classic documentation |
| <a href="#">delete_ip_set</a>                      | This is AWS WAF Classic documentation |
| <a href="#">delete_logging_configuration</a>       | This is AWS WAF Classic documentation |
| <a href="#">delete_permission_policy</a>           | This is AWS WAF Classic documentation |
| <a href="#">delete_rate_based_rule</a>             | This is AWS WAF Classic documentation |
| <a href="#">delete_regex_match_set</a>             | This is AWS WAF Classic documentation |
| <a href="#">delete_regex_pattern_set</a>           | This is AWS WAF Classic documentation |
| <a href="#">delete_rule</a>                        | This is AWS WAF Classic documentation |
| <a href="#">delete_rule_group</a>                  | This is AWS WAF Classic documentation |
| <a href="#">delete_size_constraint_set</a>         | This is AWS WAF Classic documentation |
| <a href="#">delete_sql_injection_match_set</a>     | This is AWS WAF Classic documentation |
| <a href="#">delete_web_acl</a>                     | This is AWS WAF Classic documentation |
| <a href="#">delete_xss_match_set</a>               | This is AWS WAF Classic documentation |
| <a href="#">get_byte_match_set</a>                 | This is AWS WAF Classic documentation |
| <a href="#">get_change_token</a>                   | This is AWS WAF Classic documentation |
| <a href="#">get_change_token_status</a>            | This is AWS WAF Classic documentation |
| <a href="#">get_geo_match_set</a>                  | This is AWS WAF Classic documentation |
| <a href="#">get_ip_set</a>                         | This is AWS WAF Classic documentation |
| <a href="#">get_logging_configuration</a>          | This is AWS WAF Classic documentation |
| <a href="#">get_permission_policy</a>              | This is AWS WAF Classic documentation |
| <a href="#">get_rate_based_rule</a>                | This is AWS WAF Classic documentation |
| <a href="#">get_rate_based_rule_managed_keys</a>   | This is AWS WAF Classic documentation |
| <a href="#">get_regex_match_set</a>                | This is AWS WAF Classic documentation |
| <a href="#">get_regex_pattern_set</a>              | This is AWS WAF Classic documentation |
| <a href="#">get_rule</a>                           | This is AWS WAF Classic documentation |
| <a href="#">get_rule_group</a>                     | This is AWS WAF Classic documentation |
| <a href="#">get_sampled_requests</a>               | This is AWS WAF Classic documentation |
| <a href="#">get_size_constraint_set</a>            | This is AWS WAF Classic documentation |
| <a href="#">get_sql_injection_match_set</a>        | This is AWS WAF Classic documentation |
| <a href="#">get_web_acl</a>                        | This is AWS WAF Classic documentation |
| <a href="#">get_xss_match_set</a>                  | This is AWS WAF Classic documentation |
| <a href="#">list_activated_rules_in_rule_group</a> | This is AWS WAF Classic documentation |
| <a href="#">list_byte_match_sets</a>               | This is AWS WAF Classic documentation |
| <a href="#">list_geo_match_sets</a>                | This is AWS WAF Classic documentation |
| <a href="#">list_ip_sets</a>                       | This is AWS WAF Classic documentation |
| <a href="#">list_logging_configurations</a>        | This is AWS WAF Classic documentation |
| <a href="#">list_rate_based_rules</a>              | This is AWS WAF Classic documentation |
| <a href="#">list_regex_match_sets</a>              | This is AWS WAF Classic documentation |
| <a href="#">list_regex_pattern_sets</a>            | This is AWS WAF Classic documentation |
| <a href="#">list_rule_groups</a>                   | This is AWS WAF Classic documentation |
| <a href="#">list_rules</a>                         | This is AWS WAF Classic documentation |
| <a href="#">list_size_constraint_sets</a>          | This is AWS WAF Classic documentation |
| <a href="#">list_sql_injection_match_sets</a>      | This is AWS WAF Classic documentation |
| <a href="#">list_subscribed_rule_groups</a>        | This is AWS WAF Classic documentation |
| <a href="#">list_tags_for_resource</a>             | This is AWS WAF Classic documentation |
| <a href="#">list_web_acl_ls</a>                    | This is AWS WAF Classic documentation |
| <a href="#">list_xss_match_sets</a>                | This is AWS WAF Classic documentation |
| <a href="#">put_logging_configuration</a>          | This is AWS WAF Classic documentation |

|  |                                       |
|--|---------------------------------------|
| <a href="#">put_permission_policy</a>          | This is AWS WAF Classic documentation |
| <a href="#">tag_resource</a>                   | This is AWS WAF Classic documentation |
| <a href="#">untag_resource</a>                 | This is AWS WAF Classic documentation |
| <a href="#">update_byte_match_set</a>          | This is AWS WAF Classic documentation |
| <a href="#">update_geo_match_set</a>           | This is AWS WAF Classic documentation |
| <a href="#">update_ip_set</a>                  | This is AWS WAF Classic documentation |
| <a href="#">update_rate_based_rule</a>         | This is AWS WAF Classic documentation |
| <a href="#">update_regex_match_set</a>         | This is AWS WAF Classic documentation |
| <a href="#">update_regex_pattern_set</a>       | This is AWS WAF Classic documentation |
| <a href="#">update_rule</a>                    | This is AWS WAF Classic documentation |
| <a href="#">update_rule_group</a>              | This is AWS WAF Classic documentation |
| <a href="#">update_size_constraint_set</a>     | This is AWS WAF Classic documentation |
| <a href="#">update_sql_injection_match_set</a> | This is AWS WAF Classic documentation |
| <a href="#">update_web_acl</a>                 | This is AWS WAF Classic documentation |
| <a href="#">update_xss_match_set</a>           | This is AWS WAF Classic documentation |

## Examples

```
## Not run:
svc <- waf()
# The following example creates an IP match set named MyIPSetFriendlyName.
svc$create_ip_set(
  ChangeToken = "abcd12f2-46da-4fdb-b8d5-fbd4c466928f",
  Name = "MyIPSetFriendlyName"
)

## End(Not run)
```

---

wafregional

*AWS WAF Regional*


---

## Description

This is **AWS WAF Classic Regional** documentation. For more information, see [AWS WAF Classic](#) in the developer guide.

**For the latest version of AWS WAF**, use the AWS WAFV2 API and see the [AWS WAF Developer Guide](#). With the latest version, AWS WAF has a single set of endpoints for regional and global use.

This is the *AWS WAF Regional Classic API Reference* for using AWS WAF Classic with the AWS resources, Elastic Load Balancing (ELB) Application Load Balancers and API Gateway APIs. The AWS WAF Classic actions and data types listed in the reference are available for protecting Elastic Load Balancing (ELB) Application Load Balancers and API Gateway APIs. You can use these actions and data types by means of the endpoints listed in [AWS Regions and Endpoints](#). This guide is for developers who need detailed information about the AWS WAF Classic API actions, data types, and errors. For detailed information about AWS WAF Classic features and an overview of how to use the AWS WAF Classic API, see the [AWS WAF Classic](#) in the developer guide.

**Usage**

```
wafregional(
  config = list(),
  credentials = list(),
  endpoint = NULL,
  region = NULL
)
```

**Arguments**

|             |   |
|-------------|---|
| config      | Optional configuration of credentials, endpoint, and/or region. <ul style="list-style-type: none"> <li>• <b>credentials:</b> <ul style="list-style-type: none"> <li>– <b>creds:</b> <ul style="list-style-type: none"> <li>* <b>access_key_id:</b> AWS access key ID</li> <li>* <b>secret_access_key:</b> AWS secret access key</li> <li>* <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>– <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>– <b>anonymous:</b> Set anonymous credentials.</li> </ul> </li> <li>• <b>endpoint:</b> The complete URL to use for the constructed client.</li> <li>• <b>region:</b> The AWS Region used in instantiating the client.</li> <li>• <b>close_connection:</b> Immediately close all HTTP connections.</li> <li>• <b>timeout:</b> The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.</li> <li>• <b>s3_force_path_style:</b> Set this to true to force the request to use path-style addressing, i.e. <code>http://s3.amazonaws.com/BUCKET/KEY</code>.</li> <li>• <b>sts_regional_endpoint:</b> Set sts regional endpoint resolver to regional or legacy <a href="https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html">https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html</a></li> </ul> |
| credentials | Optional credentials shorthand for the config parameter <ul style="list-style-type: none"> <li>• <b>creds:</b> <ul style="list-style-type: none"> <li>– <b>access_key_id:</b> AWS access key ID</li> <li>– <b>secret_access_key:</b> AWS secret access key</li> <li>– <b>session_token:</b> AWS temporary session token</li> </ul> </li> <li>• <b>profile:</b> The name of a profile to use. If not given, then the default profile is used.</li> <li>• <b>anonymous:</b> Set anonymous credentials.</li> </ul>   |
| endpoint    | Optional shorthand for complete URL to use for the constructed client.  |
| region      | Optional shorthand for AWS Region used in instantiating the client.   |

**Value**

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

**Service syntax**

```

svc <- wafregional(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string",
      anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
  ),
  credentials = list(
    creds = list(
      access_key_id = "string",
      secret_access_key = "string",
      session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
  ),
  endpoint = "string",
  region = "string"
)

```

**Operations**

|  |  |
|--|--|
| <a href="#">associate_web_acl</a>              | This is AWS WAF Classic Regional documentation                                   |
| <a href="#">create_byte_match_set</a>          | This is AWS WAF Classic documentation  |
| <a href="#">create_geo_match_set</a>           | This is AWS WAF Classic documentation  |
| <a href="#">create_ip_set</a>                  | This is AWS WAF Classic documentation  |
| <a href="#">create_rate_based_rule</a>         | This is AWS WAF Classic documentation  |
| <a href="#">create_regex_match_set</a>         | This is AWS WAF Classic documentation  |
| <a href="#">create_regex_pattern_set</a>       | This is AWS WAF Classic documentation  |
| <a href="#">create_rule</a>                    | This is AWS WAF Classic documentation  |
| <a href="#">create_rule_group</a>              | This is AWS WAF Classic documentation  |
| <a href="#">create_size_constraint_set</a>     | This is AWS WAF Classic documentation  |
| <a href="#">create_sql_injection_match_set</a> | This is AWS WAF Classic documentation  |
| <a href="#">create_web_acl</a>                 | This is AWS WAF Classic documentation  |
| <a href="#">create_web_acl_migration_stack</a> | Creates an AWS CloudFormation WAFV2 template for the specified web ACL in the sp |
| <a href="#">create_xss_match_set</a>           | This is AWS WAF Classic documentation  |

|  |  |
|--|--|
| <a href="#">delete_byte_match_set</a>              | This is AWS WAF Classic documentation          |
| <a href="#">delete_geo_match_set</a>               | This is AWS WAF Classic documentation          |
| <a href="#">delete_ip_set</a>                      | This is AWS WAF Classic documentation          |
| <a href="#">delete_logging_configuration</a>       | This is AWS WAF Classic documentation          |
| <a href="#">delete_permission_policy</a>           | This is AWS WAF Classic documentation          |
| <a href="#">delete_rate_based_rule</a>             | This is AWS WAF Classic documentation          |
| <a href="#">delete_regex_match_set</a>             | This is AWS WAF Classic documentation          |
| <a href="#">delete_regex_pattern_set</a>           | This is AWS WAF Classic documentation          |
| <a href="#">delete_rule</a>                        | This is AWS WAF Classic documentation          |
| <a href="#">delete_rule_group</a>                  | This is AWS WAF Classic documentation          |
| <a href="#">delete_size_constraint_set</a>         | This is AWS WAF Classic documentation          |
| <a href="#">delete_sql_injection_match_set</a>     | This is AWS WAF Classic documentation          |
| <a href="#">delete_web_acl</a>                     | This is AWS WAF Classic documentation          |
| <a href="#">delete_xss_match_set</a>               | This is AWS WAF Classic documentation          |
| <a href="#">disassociate_web_acl</a>               | This is AWS WAF Classic Regional documentation |
| <a href="#">get_byte_match_set</a>                 | This is AWS WAF Classic documentation          |
| <a href="#">get_change_token</a>                   | This is AWS WAF Classic documentation          |
| <a href="#">get_change_token_status</a>            | This is AWS WAF Classic documentation          |
| <a href="#">get_geo_match_set</a>                  | This is AWS WAF Classic documentation          |
| <a href="#">get_ip_set</a>                         | This is AWS WAF Classic documentation          |
| <a href="#">get_logging_configuration</a>          | This is AWS WAF Classic documentation          |
| <a href="#">get_permission_policy</a>              | This is AWS WAF Classic documentation          |
| <a href="#">get_rate_based_rule</a>                | This is AWS WAF Classic documentation          |
| <a href="#">get_rate_based_rule_managed_keys</a>   | This is AWS WAF Classic documentation          |
| <a href="#">get_regex_match_set</a>                | This is AWS WAF Classic documentation          |
| <a href="#">get_regex_pattern_set</a>              | This is AWS WAF Classic documentation          |
| <a href="#">get_rule</a>                           | This is AWS WAF Classic documentation          |
| <a href="#">get_rule_group</a>                     | This is AWS WAF Classic documentation          |
| <a href="#">get_sampled_requests</a>               | This is AWS WAF Classic documentation          |
| <a href="#">get_size_constraint_set</a>            | This is AWS WAF Classic documentation          |
| <a href="#">get_sql_injection_match_set</a>        | This is AWS WAF Classic documentation          |
| <a href="#">get_web_acl</a>                        | This is AWS WAF Classic documentation          |
| <a href="#">get_web_acl_for_resource</a>           | This is AWS WAF Classic Regional documentation |
| <a href="#">get_xss_match_set</a>                  | This is AWS WAF Classic documentation          |
| <a href="#">list_activated_rules_in_rule_group</a> | This is AWS WAF Classic documentation          |
| <a href="#">list_byte_match_sets</a>               | This is AWS WAF Classic documentation          |
| <a href="#">list_geo_match_sets</a>                | This is AWS WAF Classic documentation          |
| <a href="#">list_ip_sets</a>                       | This is AWS WAF Classic documentation          |
| <a href="#">list_logging_configurations</a>        | This is AWS WAF Classic documentation          |
| <a href="#">list_rate_based_rules</a>              | This is AWS WAF Classic documentation          |
| <a href="#">list_regex_match_sets</a>              | This is AWS WAF Classic documentation          |
| <a href="#">list_regex_pattern_sets</a>            | This is AWS WAF Classic documentation          |
| <a href="#">list_resources_for_web_acl</a>         | This is AWS WAF Classic Regional documentation |
| <a href="#">list_rule_groups</a>                   | This is AWS WAF Classic documentation          |
| <a href="#">list_rules</a>                         | This is AWS WAF Classic documentation          |
| <a href="#">list_size_constraint_sets</a>          | This is AWS WAF Classic documentation          |
| <a href="#">list_sql_injection_match_sets</a>      | This is AWS WAF Classic documentation          |
| <a href="#">list_subscribed_rule_groups</a>        | This is AWS WAF Classic documentation          |

|  |                                       |
|--|---------------------------------------|
| <a href="#">list_tags_for_resource</a>         | This is AWS WAF Classic documentation |
| <a href="#">list_web_acl_ls</a>                | This is AWS WAF Classic documentation |
| <a href="#">list_xss_match_sets</a>            | This is AWS WAF Classic documentation |
| <a href="#">put_logging_configuration</a>      | This is AWS WAF Classic documentation |
| <a href="#">put_permission_policy</a>          | This is AWS WAF Classic documentation |
| <a href="#">tag_resource</a>                   | This is AWS WAF Classic documentation |
| <a href="#">untag_resource</a>                 | This is AWS WAF Classic documentation |
| <a href="#">update_byte_match_set</a>          | This is AWS WAF Classic documentation |
| <a href="#">update_geo_match_set</a>           | This is AWS WAF Classic documentation |
| <a href="#">update_ip_set</a>                  | This is AWS WAF Classic documentation |
| <a href="#">update_rate_based_rule</a>         | This is AWS WAF Classic documentation |
| <a href="#">update_regex_match_set</a>         | This is AWS WAF Classic documentation |
| <a href="#">update_regex_pattern_set</a>       | This is AWS WAF Classic documentation |
| <a href="#">update_rule</a>                    | This is AWS WAF Classic documentation |
| <a href="#">update_rule_group</a>              | This is AWS WAF Classic documentation |
| <a href="#">update_size_constraint_set</a>     | This is AWS WAF Classic documentation |
| <a href="#">update_sql_injection_match_set</a> | This is AWS WAF Classic documentation |
| <a href="#">update_web_acl</a>                 | This is AWS WAF Classic documentation |
| <a href="#">update_xss_match_set</a>           | This is AWS WAF Classic documentation |

## Examples

```
## Not run:
svc <- wafregional()
# The following example creates an IP match set named MyIPSetFriendlyName.
svc$create_ip_set(
  ChangeToken = "abcd12f2-46da-4fdb-b8d5-fbd4c466928f",
  Name = "MyIPSetFriendlyName"
)

## End(Not run)
```

---

wafv2

AWS WAFV2

---

## Description

### WAF

This is the latest version of the **WAF** API, released in November, 2019. The names of the entities that you use to access this API, like endpoints and namespaces, all have the versioning information added, like "V2" or "v2", to distinguish from the prior version. We recommend migrating your resources to this version, because it has a number of significant improvements.

If you used WAF prior to this release, you can't use this WAFV2 API to access any WAF resources that you created before. You can access your old rules, web ACLs, and other WAF resources only



through the WAF Classic APIs. The WAF Classic APIs have retained the prior names, endpoints, and namespaces.

For information, including how to migrate your WAF resources to this version, see the [WAF Developer Guide](#).

WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to an Amazon CloudFront distribution, Amazon API Gateway REST API, Application Load Balancer, AppSync GraphQL API, Amazon Cognito user pool, App Runner service, or Amazon Web Services Verified Access instance. WAF also lets you control access to your content, to protect the Amazon Web Services resource that WAF is monitoring. Based on conditions that you specify, such as the IP addresses that requests originate from or the values of query strings, the protected resource responds to requests with either the requested content, an HTTP 403 status code (Forbidden), or with a custom response.

This API guide is for developers who need detailed information about WAF API actions, data types, and errors. For detailed information about WAF features and guidance for configuring and using WAF, see the [WAF Developer Guide](#).

You can make calls using the endpoints listed in [WAF endpoints and quotas](#).

- For regional applications, you can use any of the endpoints in the list. A regional application can be an Application Load Balancer (ALB), an Amazon API Gateway REST API, an AppSync GraphQL API, an Amazon Cognito user pool, an App Runner service, or an Amazon Web Services Verified Access instance.
- For Amazon CloudFront applications, you must use the API endpoint listed for US East (N. Virginia): us-east-1.

Alternatively, you can use one of the Amazon Web Services SDKs to access an API that's tailored to the programming language or platform that you're using. For more information, see [Amazon Web Services SDKs](#).

We currently provide two versions of the WAF API: this API and the prior versions, the classic WAF APIs. This new API provides the same functionality as the older versions, with the following major improvements:

- You use one API for both global and regional applications. Where you need to distinguish the scope, you specify a Scope parameter and set it to CLOUDFRONT or REGIONAL.
- You can define a web ACL or rule group with a single call, and update it with a single call. You define all rule specifications in JSON format, and pass them to your rule group or web ACL calls.
- The limits WAF places on the use of rules more closely reflects the cost of running each type of rule. Rule groups include capacity settings, so you know the maximum cost of a rule group when you use it.

## Usage

```
wafv2(config = list(), credentials = list(), endpoint = NULL, region = NULL)
```

## Arguments

`config`            Optional configuration of credentials, endpoint, and/or region.

- **credentials:**
  - **creds:**
    - \* **access\_key\_id:** AWS access key ID
    - \* **secret\_access\_key:** AWS secret access key
    - \* **session\_token:** AWS temporary session token
  - **profile:** The name of a profile to use. If not given, then the default profile is used.
  - **anonymous:** Set anonymous credentials.
- **endpoint:** The complete URL to use for the constructed client.
- **region:** The AWS Region used in instantiating the client.
- **close\_connection:** Immediately close all HTTP connections.
- **timeout:** The time in seconds till a timeout exception is thrown when attempting to make a connection. The default is 60 seconds.
- **s3\_force\_path\_style:** Set this to `true` to force the request to use path-style addressing, i.e. `http://s3.amazonaws.com/BUCKET/KEY`.
- **sts\_regional\_endpoint:** Set sts regional endpoint resolver to regional or legacy <https://docs.aws.amazon.com/sdkref/latest/guide/feature-sts-regionalized-endpoint.html>

`credentials` Optional credentials shorthand for the config parameter

- **creds:**
  - **access\_key\_id:** AWS access key ID
  - **secret\_access\_key:** AWS secret access key
  - **session\_token:** AWS temporary session token
- **profile:** The name of a profile to use. If not given, then the default profile is used.
- **anonymous:** Set anonymous credentials.

`endpoint` Optional shorthand for complete URL to use for the constructed client.

`region` Optional shorthand for AWS Region used in instantiating the client.

## Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

## Service syntax

```
svc <- wafv2(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
    ),
  ),
```

```

        profile = "string",
        anonymous = "logical"
    ),
    endpoint = "string",
    region = "string",
    close_connection = "logical",
    timeout = "numeric",
    s3_force_path_style = "logical",
    sts_regional_endpoint = "string"
),
credentials = list(
    creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
    ),
    profile = "string",
    anonymous = "logical"
),
endpoint = "string",
region = "string"
)

```

## Operations

|   |  |
|---|--|
| <a href="#">associate_web_acl</a>                   | Associates a web ACL with a regional application resource, to protect the resource.  |
| <a href="#">check_capacity</a>                      | Returns the web ACL capacity unit (WCU) requirements for a specified scope.  |
| <a href="#">create_api_key</a>                      | Creates an API key that contains a set of token domains.   |
| <a href="#">create_ip_set</a>                       | Creates an IPSet, which you use to identify web requests that originate from a specific IP address or range of IP addresses. |
| <a href="#">create_regex_pattern_set</a>            | Creates a RegexPatternSet, which you reference in a RegexPatternSetReference.  |
| <a href="#">create_rule_group</a>                   | Creates a RuleGroup per the specifications provided.   |
| <a href="#">create_web_acl</a>                      | Creates a WebACL per the specifications provided.  |
| <a href="#">delete_firewall_manager_rule_groups</a> | Deletes all rule groups that are managed by Firewall Manager for the specified scope.  |
| <a href="#">delete_ip_set</a>                       | Deletes the specified IPSet.   |
| <a href="#">delete_logging_configuration</a>        | Deletes the LoggingConfiguration from the specified web ACL.   |
| <a href="#">delete_permission_policy</a>            | Permanently deletes an IAM policy from the specified rule group.   |
| <a href="#">delete_regex_pattern_set</a>            | Deletes the specified RegexPatternSet.   |
| <a href="#">delete_rule_group</a>                   | Deletes the specified RuleGroup.   |
| <a href="#">delete_web_acl</a>                      | Deletes the specified WebACL.  |
| <a href="#">describe_all_managed_products</a>       | Provides high-level information for the Amazon Web Services Managed Rule Groups.   |
| <a href="#">describe_managed_products_by_vendor</a> | Provides high-level information for the managed rule groups owned by a specific vendor.                                      |
| <a href="#">describe_managed_rule_group</a>         | Provides high-level information for a managed rule group, including description and capacity.                                |
| <a href="#">disassociate_web_acl</a>                | Disassociates the specified regional application resource from any existing web ACLs.  |
| <a href="#">generate_mobile_sdk_release_url</a>     | Generates a presigned download URL for the specified release of the mobile SDK.  |
| <a href="#">get_decrypted_api_key</a>               | Returns your API key in decrypted form.  |
| <a href="#">get_ip_set</a>                          | Returns the specified IPSet.   |
| <a href="#">get_logging_configuration</a>           | Returns the LoggingConfiguration for the specified web ACL.  |
| <a href="#">get_managed_rule_set</a>                | Returns the specified managed rule set.  |

|  |  |
|--|--|
| <code>get_mobile_sdk_release</code>                      | Retrieves information for the specified mobile SDK release, including release information                |
| <code>get_permission_policy</code>                       | Returns the IAM policy that is attached to the specified rule group                                      |
| <code>get_rate_based_statement_managed_keys</code>       | Retrieves the IP addresses that are currently blocked by a rate-based rule in the specified rule group   |
| <code>get_regex_pattern_set</code>                       | Retrieves the specified RegexPatternSet  |
| <code>get_rule_group</code>                              | Retrieves the specified RuleGroup  |
| <code>get_sampled_requests</code>                        | Gets detailed information about a specified number of requests—a sample—through the specified rule group |
| <code>get_web_acl</code>                                 | Retrieves the specified WebACL   |
| <code>get_web_acl_for_resource</code>                    | Retrieves the WebACL for the specified resource  |
| <code>list_api_keys</code>                               | Retrieves a list of the API keys that you've defined for the specified scope                             |
| <code>list_available_managed_rule_groups</code>          | Retrieves an array of managed rule groups that are available for you to use                              |
| <code>list_available_managed_rule_group_versions</code>  | Returns a list of the available versions for the specified managed rule group                            |
| <code>list_ip_sets</code>                                | Retrieves an array of IPSetSummary objects for the IP sets that you manage                               |
| <code>list_logging_configurations</code>                 | Retrieves an array of your LoggingConfiguration objects  |
| <code>list_managed_rule_sets</code>                      | Retrieves the managed rule sets that you own   |
| <code>list_mobile_sdk_releases</code>                    | Retrieves a list of the available releases for the mobile SDK and the specified region                   |
| <code>list_regex_pattern_sets</code>                     | Retrieves an array of RegexPatternSetSummary objects for the regex pattern sets that you manage          |
| <code>list_resources_for_web_acl</code>                  | Retrieves an array of the Amazon Resource Names (ARNs) for the regional WebACLs that you manage          |
| <code>list_rule_groups</code>                            | Retrieves an array of RuleGroupSummary objects for the rule groups that you manage                       |
| <code>list_tags_for_resource</code>                      | Retrieves the TagInfoForResource for the specified resource  |
| <code>list_web_acl_ls</code>                             | Retrieves an array of WebACLSummary objects for the web ACLs that you manage                             |
| <code>put_logging_configuration</code>                   | Enables the specified LoggingConfiguration, to start logging from a web ACL                              |
| <code>put_managed_rule_set_versions</code>               | Defines the versions of your managed rule set that you are offering to the customer                      |
| <code>put_permission_policy</code>                       | Attaches an IAM policy to the specified resource   |
| <code>tag_resource</code>                                | Associates tags with the specified Amazon Web Services resource  |
| <code>untag_resource</code>                              | Disassociates tags from an Amazon Web Services resource  |
| <code>update_ip_set</code>                               | Updates the specified IPSet  |
| <code>update_managed_rule_set_version_expiry_date</code> | Updates the expiration information for your managed rule set   |
| <code>update_regex_pattern_set</code>                    | Updates the specified RegexPatternSet  |
| <code>update_rule_group</code>                           | Updates the specified RuleGroup  |
| <code>update_web_acl</code>                              | Updates the specified WebACL   |

## Examples

```
## Not run:
svc <- wafv2()
svc$associate_web_acl(
  Foo = 123
)

## End(Not run)
```

# Index

accept\_administrator\_invitation, [48](#), [87](#)  
accept\_invitation, [37](#), [48](#), [73](#), [87](#)  
accept\_resource\_share\_invitation, [80](#)  
accept\_shared\_directory, [41](#)  
accessanalyzer, [3](#)  
account, [7](#)  
acm, [9](#)  
acmpca, [11](#)  
add\_attributes\_to\_findings, [63](#)  
add\_client\_id\_to\_open\_id\_connect\_provider, [51](#)  
add\_custom\_attributes, [29](#)  
add\_facet\_to\_object, [16](#)  
add\_ip\_routes, [41](#)  
add\_region, [41](#)  
add\_role\_to\_instance\_profile, [51](#)  
add\_tags\_to\_certificate, [11](#)  
add\_tags\_to\_resource, [20](#), [41](#)  
add\_user\_to\_group, [51](#)  
admin\_add\_user\_to\_group, [29](#)  
admin\_confirm\_sign\_up, [29](#)  
admin\_create\_user, [29](#)  
admin\_delete\_user, [29](#)  
admin\_delete\_user\_attributes, [29](#)  
admin\_disable\_provider\_for\_user, [29](#)  
admin\_disable\_user, [29](#)  
admin\_enable\_user, [29](#)  
admin\_forget\_device, [29](#)  
admin\_get\_device, [29](#)  
admin\_get\_user, [29](#)  
admin\_initiate\_auth, [29](#)  
admin\_link\_provider\_for\_user, [29](#)  
admin\_list\_devices, [29](#)  
admin\_list\_groups\_for\_user, [29](#)  
admin\_list\_user\_auth\_events, [29](#)  
admin\_remove\_user\_from\_group, [29](#)  
admin\_reset\_user\_password, [29](#)  
admin\_respond\_to\_auth\_challenge, [29](#)  
admin\_set\_user\_mfa\_preference, [29](#)  
admin\_set\_user\_password, [29](#)  
admin\_set\_user\_settings, [29](#)  
admin\_update\_auth\_event\_feedback, [29](#)  
admin\_update\_device\_status, [29](#)  
admin\_update\_user\_attributes, [29](#)  
admin\_user\_global\_sign\_out, [29](#)  
apply\_archive\_rule, [6](#)  
apply\_schema, [16](#)  
archive\_findings, [48](#)  
associate\_admin\_account, [44](#)  
associate\_drt\_log\_bucket, [94](#)  
associate\_drt\_role, [94](#)  
associate\_health\_check, [94](#)  
associate\_member, [66](#)  
associate\_proactive\_engagement\_details, [94](#)  
associate\_resource\_share, [80](#)  
associate\_resource\_share\_permission, [80](#)  
associate\_software\_token, [29](#)  
associate\_third\_party\_firewall, [44](#)  
associate\_web\_acl, [118](#), [123](#)  
assume\_role, [108](#)  
assume\_role\_with\_saml, [108](#)  
assume\_role\_with\_web\_identity, [108](#)  
attach\_customer\_managed\_policy\_reference\_to\_permission\_set, [101](#)  
attach\_group\_policy, [51](#)  
attach\_managed\_policy\_to\_permission\_set, [101](#)  
attach\_object, [16](#)  
attach\_policy, [16](#)  
attach\_role\_policy, [51](#)  
attach\_to\_index, [16](#)  
attach\_typed\_link, [16](#)  
attach\_user\_policy, [51](#)  
batch\_associate\_resource, [44](#)  
batch\_delete\_automation\_rules, [87](#)  
batch\_disable\_standards, [87](#)

- batch\_disassociate\_resource, [44](#)
- batch\_enable\_standards, [85](#), [87](#)
- batch\_get\_account\_status, [66](#)
- batch\_get\_automation\_rules, [87](#)
- batch\_get\_code\_snippet, [66](#)
- batch\_get\_configuration\_policy\_associations, [87](#)
- batch\_get\_custom\_data\_identifiers, [73](#)
- batch\_get\_finding\_details, [66](#)
- batch\_get\_free\_trial\_info, [66](#)
- batch\_get\_graph\_member\_datasources, [38](#)
- batch\_get\_member\_ec\_2\_deep\_inspection\_status, [66](#)
- batch\_get\_membership\_datasources, [38](#)
- batch\_get\_secret\_value, [84](#)
- batch\_get\_security\_controls, [87](#)
- batch\_get\_standards\_control\_associations, [87](#)
- batch\_import\_findings, [85](#), [87](#)
- batch\_is\_authorized, [111](#)
- batch\_read, [16](#)
- batch\_update\_automation\_rules, [87](#)
- batch\_update\_findings, [85](#), [87](#)
- batch\_update\_member\_ec\_2\_deep\_inspection\_status, [66](#)
- batch\_update\_standards\_control\_associations, [87](#)
- batch\_write, [16](#)
- bulk\_publish, [34](#)
  
- cancel\_findings\_report, [66](#)
- cancel\_key\_deletion, [70](#)
- cancel\_policy\_generation, [6](#)
- cancel\_rotate\_secret, [84](#)
- cancel\_sbom\_export, [66](#)
- cancel\_schema\_extension, [41](#)
- change\_password, [29](#), [51](#)
- check\_access\_not\_granted, [6](#)
- check\_capacity, [123](#)
- check\_no\_new\_access, [6](#)
- clouddirectory, [14](#)
- cloudhsm, [18](#)
- cloudhsmv2, [21](#)
- cognitoidentity, [23](#)
- cognitoidentityprovider, [26](#)
- cognitosync, [32](#)
- confirm\_device, [29](#)
- confirm\_forgot\_password, [29](#)
- confirm\_sign\_up, [29](#)
  
- connect\_custom\_key\_store, [70](#)
- connect\_directory, [41](#)
- copy\_backup\_to\_region, [22](#)
- create\_access\_key, [51](#)
- create\_access\_preview, [6](#)
- create\_account\_alias, [52](#)
- create\_account\_assignment, [101](#)
- create\_action\_target, [87](#)
- create\_alias, [41](#), [70](#)
- create\_allow\_list, [73](#)
- create\_analyzer, [6](#)
- create\_api\_key, [123](#)
- create\_application, [101](#)
- create\_application\_assignment, [101](#)
- create\_archive\_rule, [6](#)
- create\_assessment\_target, [63](#)
- create\_assessment\_template, [63](#)
- create\_automation\_rule, [87](#)
- create\_aws\_log\_source, [91](#)
- create\_byte\_match\_set, [114](#), [118](#)
- create\_certificate\_authority, [13](#)
- create\_certificate\_authority\_audit\_report, [14](#)
- create\_classification\_job, [73](#)
- create\_cluster, [23](#)
- create\_computer, [41](#)
- create\_conditional\_forwarder, [41](#)
- create\_configuration\_policy, [87](#)
- create\_connector, [77](#)
- create\_custom\_data\_identifier, [73](#)
- create\_custom\_key\_store, [70](#)
- create\_custom\_log\_source, [91](#)
- create\_data\_lake, [91](#)
- create\_data\_lake\_exception\_subscription, [92](#)
- create\_data\_lake\_organization\_configuration, [92](#)
- create\_detector, [48](#)
- create\_directory, [16](#), [41](#)
- create\_directory\_registration, [77](#)
- create\_exclusions\_preview, [63](#)
- create\_facet, [16](#)
- create\_filter, [48](#), [66](#)
- create\_finding\_aggregator, [87](#)
- create\_findings\_filter, [73](#)
- create\_findings\_report, [66](#)
- create\_geo\_match\_set, [114](#), [118](#)
- create\_grant, [70](#)

- create\_graph, [38](#)
- create\_group, [29](#), [52](#), [60](#)
- create\_group\_membership, [60](#)
- create\_hapg, [20](#)
- create\_hsm, [20](#), [23](#)
- create\_identity\_pool, [25](#)
- create\_identity\_provider, [29](#)
- create\_identity\_source, [111](#)
- create\_index, [16](#)
- create\_insight, [87](#)
- create\_instance, [101](#)
- create\_instance\_access\_control\_attribute\_configuration, [101](#)
- create\_instance\_profile, [52](#)
- create\_invitations, [73](#)
- create\_ip\_set, [48](#), [114](#), [118](#), [123](#)
- create\_key, [70](#)
- create\_log\_subscription, [41](#)
- create\_login\_profile, [52](#)
- create\_luna\_client, [20](#)
- create\_member, [73](#)
- create\_members, [38](#), [48](#), [85](#), [87](#)
- create\_microsoft\_ad, [41](#)
- create\_object, [16](#)
- create\_open\_id\_connect\_provider, [52](#)
- create\_permission, [14](#), [80](#)
- create\_permission\_set, [101](#)
- create\_permission\_version, [80](#)
- create\_policy, [52](#), [111](#)
- create\_policy\_store, [111](#)
- create\_policy\_template, [111](#)
- create\_policy\_version, [52](#)
- create\_profile, [57](#)
- create\_protection, [94](#)
- create\_protection\_group, [94](#)
- create\_publishing\_destination, [48](#)
- create\_rate\_based\_rule, [114](#), [118](#)
- create\_regex\_match\_set, [114](#), [118](#)
- create\_regex\_pattern\_set, [114](#), [118](#), [123](#)
- create\_resource\_group, [63](#)
- create\_resource\_server, [29](#)
- create\_resource\_share, [80](#)
- create\_role, [52](#)
- create\_rule, [114](#), [118](#)
- create\_rule\_group, [114](#), [118](#), [123](#)
- create\_saml\_provider, [52](#)
- create\_sample\_findings, [48](#), [74](#)
- create\_sbom\_export, [66](#)
- create\_schema, [16](#)
- create\_secret, [84](#)
- create\_service\_linked\_role, [52](#)
- create\_service\_principal\_name, [77](#)
- create\_service\_specific\_credential, [52](#)
- create\_size\_constraint\_set, [114](#), [118](#)
- create\_snapshot, [41](#)
- create\_sql\_injection\_match\_set, [114](#), [118](#)
- create\_subscriber, [92](#)
- create\_subscriber\_notification, [92](#)
- create\_subscription, [94](#)
- create\_template, [77](#)
- create\_template\_group\_access\_control\_entry, [77](#)
- create\_threat\_intel\_set, [48](#)
- create\_token, [105](#)
- create\_token\_with\_iam, [105](#)
- create\_trust, [41](#)
- create\_trust\_anchor, [57](#)
- create\_trusted\_token\_issuer, [101](#)
- create\_typed\_link\_facet, [16](#)
- create\_user, [52](#), [60](#)
- create\_user\_import\_job, [29](#)
- create\_user\_pool, [30](#)
- create\_user\_pool\_client, [30](#)
- create\_user\_pool\_domain, [30](#)
- create\_virtual\_mfa\_device, [52](#)
- create\_web\_acl, [114](#), [118](#), [123](#)
- create\_web\_acl\_migration\_stack, [114](#), [118](#)
- create\_xss\_match\_set, [114](#), [118](#)
- deactivate\_mfa\_device, [52](#)
- decline\_invitations, [48](#), [74](#), [87](#)
- decode\_authorization\_message, [108](#)
- decrypt, [68](#), [70](#)
- delete\_access\_key, [52](#)
- delete\_account\_alias, [52](#)
- delete\_account\_assignment, [101](#)
- delete\_account\_password\_policy, [52](#)
- delete\_action\_target, [87](#)
- delete\_alias, [70](#)
- delete\_allow\_list, [74](#)
- delete\_alternate\_contact, [8](#)
- delete\_analyzer, [6](#)
- delete\_application, [101](#)
- delete\_application\_access\_scope, [101](#)
- delete\_application\_assignment, [101](#)

- delete\_application\_authentication\_method, [101](#)
- delete\_application\_grant, [101](#)
- delete\_apps\_list, [44](#)
- delete\_archive\_rule, [6](#)
- delete\_assessment\_run, [63](#)
- delete\_assessment\_target, [63](#)
- delete\_assessment\_template, [63](#)
- delete\_aws\_log\_source, [92](#)
- delete\_backup, [23](#)
- delete\_byte\_match\_set, [114](#), [119](#)
- delete\_certificate, [11](#)
- delete\_certificate\_authority, [14](#)
- delete\_cluster, [23](#)
- delete\_conditional\_forwarder, [41](#)
- delete\_configuration\_policy, [87](#)
- delete\_connector, [77](#)
- delete\_crl, [57](#)
- delete\_custom\_data\_identifier, [74](#)
- delete\_custom\_key\_store, [70](#)
- delete\_custom\_log\_source, [92](#)
- delete\_data\_lake, [92](#)
- delete\_data\_lake\_exception\_subscription, [92](#)
- delete\_data\_lake\_organization\_configuration, [92](#)
- delete\_dataset, [34](#)
- delete\_detector, [48](#)
- delete\_directory, [17](#), [41](#)
- delete\_directory\_registration, [77](#)
- delete\_facet, [17](#)
- delete\_filter, [48](#), [66](#)
- delete\_finding\_aggregator, [87](#)
- delete\_findings\_filter, [74](#)
- delete\_firewall\_manager\_rule\_groups, [123](#)
- delete\_geo\_match\_set, [115](#), [119](#)
- delete\_graph, [38](#)
- delete\_group, [30](#), [52](#), [60](#)
- delete\_group\_membership, [60](#)
- delete\_group\_policy, [52](#)
- delete\_hapg, [20](#)
- delete\_hsm, [20](#), [23](#)
- delete\_identities, [25](#)
- delete\_identity\_pool, [25](#)
- delete\_identity\_provider, [30](#)
- delete\_identity\_source, [111](#)
- delete\_imported\_key\_material, [70](#)
- delete\_inline\_policy\_from\_permission\_set, [101](#)
- delete\_insight, [87](#)
- delete\_instance, [101](#)
- delete\_instance\_access\_control\_attribute\_configuration, [101](#)
- delete\_instance\_profile, [52](#)
- delete\_invitations, [48](#), [74](#), [87](#)
- delete\_ip\_set, [48](#), [115](#), [119](#), [123](#)
- delete\_log\_subscription, [41](#)
- delete\_logging\_configuration, [115](#), [119](#), [123](#)
- delete\_login\_profile, [52](#)
- delete\_luna\_client, [20](#)
- delete\_member, [74](#)
- delete\_members, [38](#), [48](#), [87](#)
- delete\_notification\_channel, [44](#)
- delete\_object, [17](#)
- delete\_open\_id\_connect\_provider, [52](#)
- delete\_permission, [14](#), [80](#)
- delete\_permission\_policy, [115](#), [119](#), [123](#)
- delete\_permission\_set, [101](#)
- delete\_permission\_version, [80](#)
- delete\_permissions\_boundary\_from\_permission\_set, [101](#)
- delete\_policy, [14](#), [44](#), [52](#), [111](#)
- delete\_policy\_store, [111](#)
- delete\_policy\_template, [112](#)
- delete\_policy\_version, [52](#)
- delete\_profile, [57](#)
- delete\_protection, [94](#)
- delete\_protection\_group, [95](#)
- delete\_protocols\_list, [44](#)
- delete\_publishing\_destination, [48](#)
- delete\_rate\_based\_rule, [115](#), [119](#)
- delete\_regex\_match\_set, [115](#), [119](#)
- delete\_regex\_pattern\_set, [115](#), [119](#), [123](#)
- delete\_resource\_policy, [84](#)
- delete\_resource\_server, [30](#)
- delete\_resource\_set, [44](#)
- delete\_resource\_share, [80](#)
- delete\_role, [52](#)
- delete\_role\_permissions\_boundary, [52](#)
- delete\_role\_policy, [52](#)
- delete\_rule, [115](#), [119](#)
- delete\_rule\_group, [115](#), [119](#), [123](#)
- delete\_saml\_provider, [52](#)
- delete\_schema, [17](#)



- delete\_secret, [84](#)
- delete\_server\_certificate, [52](#)
- delete\_service\_linked\_role, [52](#)
- delete\_service\_principal\_name, [77](#)
- delete\_service\_specific\_credential, [52](#)
- delete\_signing\_certificate, [52](#)
- delete\_size\_constraint\_set, [115](#), [119](#)
- delete\_snapshot, [41](#)
- delete\_sql\_injection\_match\_set, [115](#), [119](#)
- delete\_ssh\_public\_key, [52](#)
- delete\_subscriber, [92](#)
- delete\_subscriber\_notification, [92](#)
- delete\_subscription, [95](#)
- delete\_template, [77](#)
- delete\_template\_group\_access\_control\_entry, [77](#)
- delete\_threat\_intel\_set, [48](#)
- delete\_trust, [41](#)
- delete\_trust\_anchor, [57](#)
- delete\_trusted\_token\_issuer, [102](#)
- delete\_typed\_link\_facet, [17](#)
- delete\_user, [30](#), [52](#), [60](#)
- delete\_user\_attributes, [30](#)
- delete\_user\_permissions\_boundary, [52](#)
- delete\_user\_policy, [52](#)
- delete\_user\_pool, [30](#)
- delete\_user\_pool\_client, [30](#)
- delete\_user\_pool\_domain, [30](#)
- delete\_virtual\_mfa\_device, [52](#)
- delete\_web\_acl, [115](#), [119](#), [123](#)
- delete\_xss\_match\_set, [115](#), [119](#)
- deregister\_certificate, [41](#)
- deregister\_data\_lake\_delegated\_administrator, [92](#)
- deregister\_event\_topic, [41](#)
- describe\_account\_assignment\_creation\_status, [102](#)
- describe\_account\_assignment\_deletion\_status, [102](#)
- describe\_action\_targets, [87](#)
- describe\_all\_managed\_products, [123](#)
- describe\_application, [102](#)
- describe\_application\_assignment, [102](#)
- describe\_application\_provider, [102](#)
- describe\_assessment\_runs, [63](#)
- describe\_assessment\_targets, [63](#)
- describe\_assessment\_templates, [63](#)
- describe\_attack, [95](#)
- describe\_attack\_statistics, [95](#)
- describe\_backups, [23](#)
- describe\_buckets, [74](#)
- describe\_certificate, [11](#), [41](#)
- describe\_certificate\_authority, [14](#)
- describe\_certificate\_authority\_audit\_report, [14](#)
- describe\_classification\_job, [74](#)
- describe\_client\_authentication\_settings, [41](#)
- describe\_clusters, [23](#)
- describe\_conditional\_forwarders, [41](#)
- describe\_cross\_account\_access\_role, [63](#)
- describe\_custom\_key\_stores, [70](#)
- describe\_dataset, [34](#)
- describe\_directories, [41](#)
- describe\_domain\_controllers, [41](#)
- describe\_drt\_access, [95](#)
- describe\_emergency\_contact\_settings, [95](#)
- describe\_event\_topics, [41](#)
- describe\_exclusions, [63](#)
- describe\_findings, [63](#)
- describe\_group, [60](#)
- describe\_group\_membership, [60](#)
- describe\_hapg, [20](#)
- describe\_hsm, [20](#)
- describe\_hub, [87](#)
- describe\_identity, [25](#)
- describe\_identity\_pool, [25](#)
- describe\_identity\_pool\_usage, [34](#)
- describe\_identity\_provider, [30](#)
- describe\_identity\_usage, [34](#)
- describe\_instance, [102](#)
- describe\_instance\_access\_control\_attribute\_configuration, [102](#)
- describe\_key, [70](#)
- describe\_ldaps\_settings, [41](#)
- describe\_luna\_client, [20](#)
- describe\_malware\_scans, [48](#)
- describe\_managed\_products\_by\_vendor, [123](#)
- describe\_managed\_rule\_group, [123](#)
- describe\_organization\_configuration, [38](#), [48](#), [66](#), [74](#), [88](#)
- describe\_permission\_set, [102](#)
- describe\_permission\_set\_provisioning\_status,

- [102](#)
- [describe\\_products, 88](#)
- [describe\\_protection, 95](#)
- [describe\\_protection\\_group, 95](#)
- [describe\\_publishing\\_destination, 48](#)
- [describe\\_regions, 41](#)
- [describe\\_resource\\_groups, 63](#)
- [describe\\_resource\\_server, 30](#)
- [describe\\_risk\\_configuration, 30](#)
- [describe\\_rules\\_packages, 63](#)
- [describe\\_secret, 84](#)
- [describe\\_settings, 41](#)
- [describe\\_shared\\_directories, 41](#)
- [describe\\_snapshots, 41](#)
- [describe\\_standards, 88](#)
- [describe\\_standards\\_controls, 88](#)
- [describe\\_subscription, 95](#)
- [describe\\_trusted\\_token\\_issuer, 102](#)
- [describe\\_trusts, 41](#)
- [describe\\_update\\_directory, 41](#)
- [describe\\_user, 60](#)
- [describe\\_user\\_import\\_job, 30](#)
- [describe\\_user\\_pool, 30](#)
- [describe\\_user\\_pool\\_client, 30](#)
- [describe\\_user\\_pool\\_domain, 30](#)
- [detach\\_customer\\_managed\\_policy\\_reference\\_from\\_permission\\_set, 102](#)
- [detach\\_from\\_index, 17](#)
- [detach\\_group\\_policy, 52](#)
- [detach\\_managed\\_policy\\_from\\_permission\\_set, 102](#)
- [detach\\_object, 17](#)
- [detach\\_policy, 17](#)
- [detach\\_role\\_policy, 52](#)
- [detach\\_typed\\_link, 17](#)
- [detach\\_user\\_policy, 52](#)
- [detective, 35](#)
- [directoryservice, 38](#)
- [disable, 66](#)
- [disable\\_application\\_layer\\_automatic\\_response, 95](#)
- [disable\\_client\\_authentication, 41](#)
- [disable\\_crl, 57](#)
- [disable\\_delegated\\_admin\\_account, 66](#)
- [disable\\_directory, 17](#)
- [disable\\_import\\_findings\\_for\\_product, 88](#)
- [disable\\_key, 70](#)
- [disable\\_key\\_rotation, 70](#)
- [disable\\_ldaps, 41](#)
- [disable\\_macie, 74](#)
- [disable\\_organization\\_admin\\_account, 38, 48, 74, 88](#)
- [disable\\_proactive\\_engagement, 95](#)
- [disable\\_profile, 57](#)
- [disable\\_radius, 41](#)
- [disable\\_region, 8](#)
- [disable\\_security\\_hub, 88](#)
- [disable\\_sso, 41](#)
- [disable\\_trust\\_anchor, 57](#)
- [disassociate\\_admin\\_account, 44](#)
- [disassociate\\_drt\\_log\\_bucket, 95](#)
- [disassociate\\_drt\\_role, 95](#)
- [disassociate\\_from\\_administrator\\_account, 48, 74, 88](#)
- [disassociate\\_from\\_master\\_account, 48, 74, 88](#)
- [disassociate\\_health\\_check, 95](#)
- [disassociate\\_member, 66, 74](#)
- [disassociate\\_members, 48, 88](#)
- [disassociate\\_membership, 38](#)
- [disassociate\\_resource\\_share, 80](#)
- [disassociate\\_resource\\_share\\_permission, 80](#)
- [disassociate\\_third\\_party\\_firewall, 44](#)
- [disassociate\\_web\\_acl, 119, 123](#)
- [disconnect\\_custom\\_key\\_store, 71](#)
- [enable, 66](#)
- [enable\\_application\\_layer\\_automatic\\_response, 95](#)
- [enable\\_client\\_authentication, 41](#)
- [enable\\_crl, 57](#)
- [enable\\_delegated\\_admin\\_account, 66](#)
- [enable\\_directory, 17](#)
- [enable\\_import\\_findings\\_for\\_product, 88](#)
- [enable\\_key, 71](#)
- [enable\\_key\\_rotation, 71](#)
- [enable\\_ldaps, 41](#)
- [enable\\_macie, 74](#)
- [enable\\_mfa\\_device, 52](#)
- [enable\\_organization\\_admin\\_account, 38, 48, 74, 88](#)
- [enable\\_proactive\\_engagement, 95](#)
- [enable\\_profile, 57](#)
- [enable\\_radius, 41](#)
- [enable\\_region, 8](#)

- enable\_security\_hub, 88
- enable\_sharing\_with\_aws\_organization, 80
- enable\_sso, 41
- enable\_trust\_anchor, 57
- encrypt, 68, 71
- export\_certificate, 11
  
- fms, 42
- forget\_device, 30
- forgot\_password, 30
  
- generate\_credential\_report, 52
- generate\_data\_key, 68, 71
- generate\_data\_key\_pair, 71
- generate\_data\_key\_pair\_without\_plaintext, 71
- generate\_data\_key\_without\_plaintext, 68, 71
- generate\_mac, 71
- generate\_mobile\_sdk\_release\_url, 123
- generate\_organizations\_access\_report, 52
- generate\_random, 71
- generate\_service\_last\_accessed\_details, 52
- get\_access\_key\_info, 108
- get\_access\_key\_last\_used, 52
- get\_access\_preview, 6
- get\_account\_authorization\_details, 52
- get\_account\_configuration, 11
- get\_account\_password\_policy, 52
- get\_account\_summary, 52
- get\_admin\_account, 44
- get\_admin\_scope, 44
- get\_administrator\_account, 48, 74, 88
- get\_allow\_list, 74
- get\_alternate\_contact, 8
- get\_analyzed\_resource, 6
- get\_analyzer, 6
- get\_application\_access\_scope, 102
- get\_application\_assignment\_configuration, 102
- get\_application\_authentication\_method, 102
- get\_application\_grant, 102
- get\_applied\_schema\_version, 17
- get\_apps\_list, 44
- get\_archive\_rule, 6
- get\_assessment\_report, 63
- get\_automated\_discovery\_configuration, 74
- get\_bucket\_statistics, 74
- get\_bulk\_publish\_details, 34
- get\_byte\_match\_set, 115, 119
- get\_caller\_identity, 108
- get\_certificate, 11, 14
- get\_certificate\_authority\_certificate, 14
- get\_certificate\_authority\_csr, 14
- get\_change\_token, 115, 119
- get\_change\_token\_status, 115, 119
- get\_classification\_export\_configuration, 74
- get\_classification\_scope, 74
- get\_cognito\_events, 34
- get\_compliance\_detail, 45
- get\_config, 20
- get\_configuration, 66
- get\_configuration\_policy, 88
- get\_configuration\_policy\_association, 88
- get\_connector, 77
- get\_contact\_information, 8
- get\_context\_keys\_for\_custom\_policy, 53
- get\_context\_keys\_for\_principal\_policy, 53
- get\_coverage\_statistics, 48
- get\_credential\_report, 53
- get\_credentials\_for\_identity, 25
- get\_crl, 57
- get\_csv\_header, 30
- get\_custom\_data\_identifier, 74
- get\_data\_lake\_exception\_subscription, 92
- get\_data\_lake\_organization\_configuration, 92
- get\_data\_lake\_sources, 92
- get\_decrypted\_api\_key, 123
- get\_delegated\_admin\_account, 66
- get\_detector, 48
- get\_device, 30
- get\_directory, 17
- get\_directory\_limits, 41
- get\_directory\_registration, 77
- get\_ec\_2\_deep\_inspection\_configuration, 66

get\_enabled\_standards, 88  
get\_encryption\_key, 66  
get\_exclusions\_preview, 63  
get\_facet, 17  
get\_federation\_token, 108  
get\_filter, 48  
get\_finding, 6  
get\_finding\_aggregator, 88  
get\_finding\_history, 88  
get\_finding\_statistics, 74  
get\_finding\_v2, 6  
get\_findings, 48, 74, 85, 88  
get\_findings\_filter, 74  
get\_findings\_publication\_configuration, 74  
get\_findings\_report\_status, 66  
get\_findings\_statistics, 48  
get\_generated\_policy, 6  
get\_geo\_match\_set, 115, 119  
get\_group, 30, 53  
get\_group\_id, 60  
get\_group\_membership\_id, 60  
get\_group\_policy, 53  
get\_id, 25  
get\_identity\_pool\_configuration, 34  
get\_identity\_pool\_roles, 25  
get\_identity\_provider\_by\_identifier, 30  
get\_identity\_source, 112  
get\_inline\_policy\_for\_permission\_set, 102  
get\_insight\_results, 88  
get\_insights, 88  
get\_instance\_profile, 53  
get\_investigation, 38  
get\_invitations\_count, 48, 74, 88  
get\_ip\_set, 48, 115, 119, 123  
get\_key\_policy, 71  
get\_key\_rotation\_status, 71  
get\_link\_attributes, 17  
get\_log\_delivery\_configuration, 30  
get\_logging\_configuration, 115, 119, 123  
get\_login\_profile, 53  
get\_macie\_session, 74  
get\_malware\_scan\_settings, 48  
get\_managed\_rule\_set, 123  
get\_master\_account, 48, 74, 88  
get\_member, 66, 74  
get\_member\_detectors, 48  
get\_members, 38, 48, 88  
get\_mfa\_device, 53  
get\_mobile\_sdk\_release, 124  
get\_notification\_channel, 45  
get\_object\_attributes, 17  
get\_object\_information, 17  
get\_open\_id\_connect\_provider, 53  
get\_open\_id\_token, 25  
get\_open\_id\_token\_for\_developer\_identity, 25  
get\_organization\_statistics, 48  
get\_organizations\_access\_report, 53  
get\_parameters\_for\_import, 71  
get\_permission, 80  
get\_permission\_policy, 115, 119, 124  
get\_permissions\_boundary\_for\_permission\_set, 102  
get\_policy, 14, 45, 53, 112  
get\_policy\_store, 112  
get\_policy\_template, 112  
get\_policy\_version, 53  
get\_principal\_tag\_attribute\_map, 25  
get\_profile, 57  
get\_protection\_status, 45  
get\_protocols\_list, 45  
get\_public\_key, 71  
get\_random\_password, 84  
get\_rate\_based\_rule, 115, 119  
get\_rate\_based\_rule\_managed\_keys, 115, 119  
get\_rate\_based\_statement\_managed\_keys, 124  
get\_regex\_match\_set, 115, 119  
get\_regex\_pattern\_set, 115, 119, 124  
get\_region\_opt\_status, 8  
get\_remaining\_free\_trial\_days, 48  
get\_resource\_policies, 80  
get\_resource\_policy, 84  
get\_resource\_profile, 74  
get\_resource\_set, 45  
get\_resource\_share\_associations, 80  
get\_resource\_share\_invitations, 80  
get\_resource\_shares, 80  
get\_reveal\_configuration, 74  
get\_role, 53  
get\_role\_credentials, 99  
get\_role\_policy, 53

- get\_rule, [115](#), [119](#)
- get\_rule\_group, [115](#), [119](#), [124](#)
- get\_saml\_provider, [53](#)
- get\_sampled\_requests, [115](#), [119](#), [124](#)
- get\_sbom\_export, [66](#)
- get\_schema, [112](#)
- get\_schema\_as\_json, [17](#)
- get\_secret\_value, [84](#)
- get\_security\_control\_definition, [88](#)
- get\_sensitive\_data\_occurrences, [74](#)
- get\_sensitive\_data\_occurrences\_availability, [74](#)
- get\_sensitivity\_inspection\_template, [74](#)
- get\_server\_certificate, [53](#)
- get\_service\_last\_accessed\_details, [53](#)
- get\_service\_last\_accessed\_details\_with\_entities, [53](#)
- get\_service\_linked\_role\_deletion\_status, [53](#)
- get\_service\_principal\_name, [77](#)
- get\_session\_token, [108](#)
- get\_signing\_certificate, [30](#)
- get\_size\_constraint\_set, [115](#), [119](#)
- get\_snapshot\_limits, [41](#)
- get\_sql\_injection\_match\_set, [115](#), [119](#)
- get\_ssh\_public\_key, [53](#)
- get\_subject, [57](#)
- get\_subscriber, [92](#)
- get\_subscription\_state, [95](#)
- get\_telemetry\_metadata, [63](#)
- get\_template, [77](#)
- get\_template\_group\_access\_control\_entry, [78](#)
- get\_third\_party\_firewall\_association\_status, [45](#)
- get\_threat\_intel\_set, [49](#)
- get\_trust\_anchor, [58](#)
- get\_typed\_link\_facet\_information, [17](#)
- get\_ui\_customization, [30](#)
- get\_usage\_statistics, [49](#), [74](#)
- get\_usage\_totals, [74](#)
- get\_user, [30](#), [53](#)
- get\_user\_attribute\_verification\_code, [30](#)
- get\_user\_id, [60](#)
- get\_user\_policy, [53](#)
- get\_user\_pool\_mfa\_config, [30](#)
- get\_violation\_details, [45](#)
- get\_web\_acl, [115](#), [119](#), [124](#)
- get\_web\_acl\_for\_resource, [119](#), [124](#)
- get\_xss\_match\_set, [115](#), [119](#)
- global\_sign\_out, [30](#)
- guardduty, [45](#)
- iam, [49](#)
- iamrolesanywhere, [55](#)
- identitystore, [58](#)
- import\_certificate, [11](#)
- import\_certificate\_authority\_certificate, [14](#)
- import\_crl, [58](#)
- import\_key\_material, [71](#)
- initialize\_cluster, [23](#)
- initiate\_auth, [30](#)
- inspector, [61](#)
- inspector2, [64](#)
- invite\_members, [49](#), [88](#)
- is\_authorized, [112](#)
- is\_authorized\_with\_token, [112](#)
- is\_member\_in\_groups, [60](#)
- issue\_certificate, [14](#)
- kms, [67](#)
- list\_access\_keys, [53](#)
- list\_access\_preview\_findings, [6](#)
- list\_access\_previews, [6](#)
- list\_account\_aliases, [53](#)
- list\_account\_assignment\_creation\_status, [102](#)
- list\_account\_assignment\_deletion\_status, [102](#)
- list\_account\_assignments, [102](#)
- list\_account\_assignments\_for\_principal, [102](#)
- list\_account\_permissions, [66](#)
- list\_account\_roles, [99](#)
- list\_accounts, [99](#)
- list\_accounts\_for\_provisioned\_permission\_set, [102](#)
- list\_activated\_rules\_in\_rule\_group, [115](#), [119](#)
- list\_admin\_accounts\_for\_organization, [45](#)
- list\_admins\_managing\_account, [45](#)
- list\_aliases, [71](#)

- list\_allow\_lists, [74](#)
- list\_analyzed\_resources, [6](#)
- list\_analyzers, [6](#)
- list\_api\_keys, [124](#)
- list\_application\_access\_scopes, [102](#)
- list\_application\_assignments, [102](#)
- list\_application\_assignments\_for\_principal, [102](#)
- list\_application\_authentication\_methods, [102](#)
- list\_application\_grants, [102](#)
- list\_application\_providers, [102](#)
- list\_applications, [102](#)
- list\_applied\_schema\_arns, [17](#)
- list\_apps\_lists, [45](#)
- list\_archive\_rules, [6](#)
- list\_assessment\_run\_agents, [63](#)
- list\_assessment\_runs, [63](#)
- list\_assessment\_targets, [63](#)
- list\_assessment\_templates, [63](#)
- list\_attached\_group\_policies, [53](#)
- list\_attached\_indices, [17](#)
- list\_attached\_role\_policies, [53](#)
- list\_attached\_user\_policies, [53](#)
- list\_attacks, [95](#)
- list\_automation\_rules, [88](#)
- list\_available\_managed\_rule\_group\_versions, [124](#)
- list\_available\_managed\_rule\_groups, [124](#)
- list\_available\_zones, [20](#)
- list\_byte\_match\_sets, [115](#), [119](#)
- list\_certificate\_authorities, [14](#)
- list\_certificates, [11](#), [41](#)
- list\_classification\_jobs, [74](#)
- list\_classification\_scopes, [74](#)
- list\_compliance\_status, [45](#)
- list\_configuration\_policies, [88](#)
- list\_configuration\_policy\_associations, [88](#)
- list\_connectors, [78](#)
- list\_coverage, [49](#), [66](#)
- list\_coverage\_statistics, [67](#)
- list\_crls, [58](#)
- list\_custom\_data\_identifiers, [74](#)
- list\_customer\_managed\_policy\_references\_in\_permissions, [102](#)
- list\_data\_lake\_exceptions, [92](#)
- list\_data\_lakes, [92](#)
- list\_datasets, [34](#)
- list\_datasource\_packages, [38](#)
- list\_delegated\_admin\_accounts, [67](#)
- list\_detectors, [49](#)
- list\_development\_schema\_arns, [17](#)
- list\_devices, [30](#)
- list\_directories, [17](#)
- list\_directory\_registrations, [78](#)
- list\_discovered\_resources, [45](#)
- list\_enabled\_products\_for\_import, [88](#)
- list\_entities\_for\_policy, [53](#)
- list\_event\_subscriptions, [63](#)
- list\_exclusions, [63](#)
- list\_facet\_attributes, [17](#)
- list\_facet\_names, [17](#)
- list\_filters, [49](#), [67](#)
- list\_finding\_aggregations, [67](#)
- list\_finding\_aggregators, [88](#)
- list\_findings, [6](#), [49](#), [63](#), [67](#), [74](#)
- list\_findings\_filters, [74](#)
- list\_findings\_v2, [6](#)
- list\_geo\_match\_sets, [115](#), [119](#)
- list\_grants, [71](#)
- list\_graphs, [38](#)
- list\_group\_memberships, [60](#)
- list\_group\_memberships\_for\_member, [60](#)
- list\_group\_policies, [53](#)
- list\_groups, [30](#), [53](#), [60](#)
- list\_groups\_for\_user, [53](#)
- list\_haps, [20](#)
- list\_hsms, [20](#)
- list\_identities, [25](#)
- list\_identity\_pool\_usage, [34](#)
- list\_identity\_pools, [25](#)
- list\_identity\_providers, [30](#)
- list\_identity\_sources, [112](#)
- list\_incoming\_typed\_links, [17](#)
- list\_index, [17](#)
- list\_indicators, [38](#)
- list\_instance\_profile\_tags, [53](#)
- list\_instance\_profiles, [53](#)
- list\_instance\_profiles\_for\_role, [53](#)
- list\_instances, [102](#)
- list\_investigations, [38](#)
- list\_institution\_permissions, [38](#), [49](#), [74](#), [88](#)
- list\_ip\_routes, [41](#)
- list\_ip\_sets, [49](#), [115](#), [119](#), [124](#)

- [list\\_key\\_policies](#), [71](#)
- [list\\_keys](#), [71](#)
- [list\\_log\\_sources](#), [92](#)
- [list\\_log\\_subscriptions](#), [42](#)
- [list\\_logging\\_configurations](#), [115](#), [119](#), [124](#)
- [list\\_luna\\_clients](#), [20](#)
- [list\\_managed\\_data\\_identifiers](#), [74](#)
- [list\\_managed\\_policies\\_in\\_permission\\_set](#), [102](#)
- [list\\_managed\\_rule\\_sets](#), [124](#)
- [list\\_managed\\_schema\\_arns](#), [17](#)
- [list\\_member\\_accounts](#), [45](#)
- [list\\_members](#), [38](#), [49](#), [67](#), [74](#), [88](#)
- [list\\_mfa\\_device\\_tags](#), [53](#)
- [list\\_mfa\\_devices](#), [53](#)
- [list\\_mobile\\_sdk\\_releases](#), [124](#)
- [list\\_object\\_attributes](#), [17](#)
- [list\\_object\\_children](#), [17](#)
- [list\\_object\\_parent\\_paths](#), [17](#)
- [list\\_object\\_parents](#), [17](#)
- [list\\_object\\_policies](#), [17](#)
- [list\\_open\\_id\\_connect\\_provider\\_tags](#), [53](#)
- [list\\_open\\_id\\_connect\\_providers](#), [53](#)
- [list\\_organization\\_admin\\_accounts](#), [38](#), [49](#), [75](#), [88](#)
- [list\\_outgoing\\_typed\\_links](#), [17](#)
- [list\\_pending\\_invitation\\_resources](#), [80](#)
- [list\\_permission\\_associations](#), [80](#)
- [list\\_permission\\_set\\_provisioning\\_status](#), [102](#)
- [list\\_permission\\_sets](#), [102](#)
- [list\\_permission\\_sets\\_provisioned\\_to\\_account](#), [102](#)
- [list\\_permission\\_versions](#), [81](#)
- [list\\_permissions](#), [14](#), [80](#)
- [list\\_policies](#), [45](#), [53](#), [112](#)
- [list\\_policies\\_granting\\_service\\_access](#), [53](#)
- [list\\_policy\\_attachments](#), [17](#)
- [list\\_policy\\_generations](#), [6](#)
- [list\\_policy\\_stores](#), [112](#)
- [list\\_policy\\_tags](#), [53](#)
- [list\\_policy\\_templates](#), [112](#)
- [list\\_policy\\_versions](#), [53](#)
- [list\\_principals](#), [81](#)
- [list\\_profiles](#), [58](#)
- [list\\_protection\\_groups](#), [95](#)
- [list\\_protections](#), [95](#)
- [list\\_protocols\\_lists](#), [45](#)
- [list\\_published\\_schema\\_arns](#), [17](#)
- [list\\_publishing\\_destinations](#), [49](#)
- [list\\_rate\\_based\\_rules](#), [115](#), [119](#)
- [list\\_records](#), [34](#)
- [list\\_regex\\_match\\_sets](#), [115](#), [119](#)
- [list\\_regex\\_pattern\\_sets](#), [115](#), [119](#), [124](#)
- [list\\_regions](#), [8](#)
- [list\\_replace\\_permission\\_associations\\_work](#), [81](#)
- [list\\_resource\\_profile\\_artifacts](#), [75](#)
- [list\\_resource\\_profile\\_detections](#), [75](#)
- [list\\_resource\\_servers](#), [30](#)
- [list\\_resource\\_set\\_resources](#), [45](#)
- [list\\_resource\\_sets](#), [45](#)
- [list\\_resource\\_share\\_permissions](#), [81](#)
- [list\\_resource\\_tags](#), [71](#)
- [list\\_resource\\_types](#), [81](#)
- [list\\_resources](#), [81](#)
- [list\\_resources\\_for\\_web\\_acl](#), [119](#), [124](#)
- [list\\_resources\\_in\\_protection\\_group](#), [95](#)
- [list\\_retirable\\_grants](#), [71](#)
- [list\\_role\\_policies](#), [53](#)
- [list\\_role\\_tags](#), [53](#)
- [list\\_roles](#), [53](#)
- [list\\_rule\\_groups](#), [115](#), [119](#), [124](#)
- [list\\_rules](#), [115](#), [119](#)
- [list\\_rules\\_packages](#), [63](#)
- [list\\_saml\\_provider\\_tags](#), [53](#)
- [list\\_saml\\_providers](#), [53](#)
- [list\\_schema\\_extensions](#), [42](#)
- [list\\_secret\\_version\\_ids](#), [84](#)
- [list\\_secrets](#), [84](#)
- [list\\_security\\_control\\_definitions](#), [88](#)
- [list\\_sensitivity\\_inspection\\_templates](#), [75](#)
- [list\\_server\\_certificate\\_tags](#), [54](#)
- [list\\_server\\_certificates](#), [53](#)
- [list\\_service\\_principal\\_names](#), [78](#)
- [list\\_service\\_specific\\_credentials](#), [54](#)
- [list\\_signing\\_certificates](#), [54](#)
- [list\\_size\\_constraint\\_sets](#), [115](#), [119](#)
- [list\\_sql\\_injection\\_match\\_sets](#), [115](#), [119](#)
- [list\\_ssh\\_public\\_keys](#), [54](#)
- [list\\_standards\\_control\\_associations](#), [88](#)
- [list\\_subjects](#), [58](#)

- list\_subscribed\_rule\_groups, [115](#), [119](#)
- list\_subscribers, [92](#)
- list\_tags, [14](#), [23](#)
- list\_tags\_for\_certificate, [11](#)
- list\_tags\_for\_resource, [6](#), [17](#), [20](#), [25](#), [30](#), [38](#), [42](#), [45](#), [49](#), [58](#), [63](#), [67](#), [75](#), [78](#), [88](#), [92](#), [95](#), [102](#), [115](#), [120](#), [124](#)
- list\_template\_group\_access\_control\_entries, [78](#)
- list\_templates, [78](#)
- list\_third\_party\_firewall\_firewall\_policies, [45](#)
- list\_threat\_intel\_sets, [49](#)
- list\_trust\_anchors, [58](#)
- list\_trusted\_token\_issuers, [102](#)
- list\_typed\_link\_facet\_attributes, [17](#)
- list\_typed\_link\_facet\_names, [17](#)
- list\_usage\_totals, [67](#)
- list\_user\_import\_jobs, [30](#)
- list\_user\_policies, [54](#)
- list\_user\_pool\_clients, [30](#)
- list\_user\_pools, [30](#)
- list\_user\_tags, [54](#)
- list\_users, [30](#), [54](#), [60](#)
- list\_users\_in\_group, [30](#)
- list\_virtual\_mfa\_devices, [54](#)
- list\_web\_ac\_ls, [115](#), [120](#), [124](#)
- list\_xss\_match\_sets, [115](#), [120](#)
- logout, [99](#)
- lookup\_developer\_identity, [26](#)
- lookup\_policy, [17](#)
  
- macie2, [72](#)
- merge\_developer\_identities, [26](#)
- modify\_backup\_attributes, [23](#)
- modify\_cluster, [23](#)
- modify\_hapg, [20](#)
- modify\_hsm, [20](#)
- modify\_luna\_client, [20](#)
  
- pcaconnectorad, [75](#)
- preview\_agents, [63](#)
- promote\_permission\_created\_from\_policy, [81](#)
- promote\_resource\_share\_created\_from\_policy, [81](#)
- provision\_permission\_set, [102](#)
- publish\_schema, [17](#)
- put\_account\_configuration, [11](#)
- put\_admin\_account, [45](#)
- put\_alternate\_contact, [8](#)
- put\_application\_access\_scope, [102](#)
- put\_application\_assignment\_configuration, [102](#)
- put\_application\_authentication\_method, [102](#)
- put\_application\_grant, [102](#)
- put\_apps\_list, [45](#)
- put\_classification\_export\_configuration, [75](#)
- put\_contact\_information, [9](#)
- put\_findings\_publication\_configuration, [75](#)
- put\_group\_policy, [54](#)
- put\_inline\_policy\_to\_permission\_set, [102](#)
- put\_key\_policy, [71](#)
- put\_logging\_configuration, [115](#), [120](#), [124](#)
- put\_managed\_rule\_set\_versions, [124](#)
- put\_notification\_channel, [45](#)
- put\_notification\_settings, [58](#)
- put\_permission\_policy, [116](#), [120](#), [124](#)
- put\_permissions\_boundary\_to\_permission\_set, [102](#)
- put\_policy, [14](#), [45](#)
- put\_protocols\_list, [45](#)
- put\_resource\_policy, [84](#)
- put\_resource\_set, [45](#)
- put\_role\_permissions\_boundary, [54](#)
- put\_role\_policy, [54](#)
- put\_schema, [112](#)
- put\_schema\_from\_json, [17](#)
- put\_secret\_value, [84](#)
- put\_user\_permissions\_boundary, [54](#)
- put\_user\_policy, [54](#)
  
- ram, [78](#)
- re\_encrypt, [71](#)
- register\_certificate, [42](#)
- register\_client, [105](#)
- register\_cross\_account\_access\_role, [63](#)
- register\_data\_lake\_delegated\_administrator, [92](#)
- register\_device, [34](#)
- register\_event\_topic, [42](#)
- reject\_invitation, [38](#)
- reject\_resource\_share\_invitation, [81](#)
- reject\_shared\_directory, [42](#)



- remove\_attributes\_from\_findings, [63](#)
- remove\_client\_id\_from\_open\_id\_connect\_provider, [54](#)
- remove\_facet\_from\_object, [17](#)
- remove\_ip\_routes, [42](#)
- remove\_region, [42](#)
- remove\_regions\_from\_replication, [84](#)
- remove\_role\_from\_instance\_profile, [54](#)
- remove\_tags\_from\_certificate, [11](#)
- remove\_tags\_from\_resource, [20](#), [42](#)
- remove\_user\_from\_group, [54](#)
- renew\_certificate, [11](#)
- replace\_permission\_associations, [81](#)
- replicate\_key, [71](#)
- replicate\_secret\_to\_regions, [84](#)
- request\_certificate, [11](#)
- resend\_confirmation\_code, [30](#)
- resend\_validation\_email, [11](#)
- reset\_encryption\_key, [67](#)
- reset\_notification\_settings, [58](#)
- reset\_service\_specific\_credential, [54](#)
- reset\_user\_password, [42](#)
- respond\_to\_auth\_challenge, [30](#)
- restore\_backup, [23](#)
- restore\_certificate\_authority, [14](#)
- restore\_from\_snapshot, [42](#)
- restore\_secret, [84](#)
- resync\_mfa\_device, [54](#)
- retire\_grant, [71](#)
- revoke\_certificate, [14](#)
- revoke\_grant, [71](#)
- revoke\_token, [30](#)
- rotate\_secret, [84](#)
  
- schedule\_key\_deletion, [71](#)
- search\_resources, [75](#)
- search\_vulnerabilities, [67](#)
- secretsmanager, [81](#)
- securityhub, [84](#)
- securitylake, [89](#)
- set\_cognito\_events, [34](#)
- set\_default\_permission\_version, [81](#)
- set\_default\_policy\_version, [54](#)
- set\_identity\_pool\_configuration, [34](#)
- set\_identity\_pool\_roles, [26](#)
- set\_log\_delivery\_configuration, [30](#)
- set\_principal\_tag\_attribute\_map, [26](#)
- set\_risk\_configuration, [30](#)
  
- set\_security\_token\_service\_preferences,
- set\_tags\_for\_resource, [63](#)
- set\_ui\_customization, [30](#)
- set\_user\_mfa\_preference, [31](#)
- set\_user\_pool\_mfa\_config, [31](#)
- set\_user\_settings, [31](#)
- share\_directory, [42](#)
- shield, [92](#)
- sign, [71](#)
- sign\_up, [31](#)
- simulate\_custom\_policy, [54](#)
- simulate\_principal\_policy, [54](#)
- sso, [95](#)
- ssoadmin, [99](#)
- ssoidc, [103](#)
- start\_assessment\_run, [63](#)
- start\_configuration\_policy\_association, [88](#)
- start\_configuration\_policy\_disassociation, [88](#)
- start\_device\_authorization, [105](#)
- start\_investigation, [38](#)
- start\_malware\_scan, [49](#)
- start\_monitoring\_member, [38](#)
- start\_monitoring\_members, [49](#)
- start\_policy\_generation, [6](#)
- start\_resource\_scan, [6](#)
- start\_schema\_extension, [42](#)
- start\_user\_import\_job, [31](#)
- stop\_assessment\_run, [63](#)
- stop\_monitoring\_members, [49](#)
- stop\_replication\_to\_replica, [84](#)
- stop\_user\_import\_job, [31](#)
- sts, [106](#)
- subscribe\_to\_dataset, [34](#)
- subscribe\_to\_event, [63](#)
  
- tag\_certificate\_authority, [14](#)
- tag\_instance\_profile, [54](#)
- tag\_mfa\_device, [54](#)
- tag\_open\_id\_connect\_provider, [54](#)
- tag\_policy, [54](#)
- tag\_resource, [6](#), [17](#), [23](#), [26](#), [31](#), [38](#), [45](#), [49](#), [58](#), [67](#), [71](#), [75](#), [78](#), [81](#), [84](#), [88](#), [92](#), [95](#), [102](#), [116](#), [120](#), [124](#)
- tag\_role, [54](#)
- tag\_saml\_provider, [54](#)
- tag\_server\_certificate, [54](#)

- tag\_user, [54](#)
- test\_custom\_data\_identifier, [75](#)
  
- unarchive\_findings, [49](#)
- unlink\_developer\_identity, [26](#)
- unlink\_identity, [26](#)
- unshare\_directory, [42](#)
- unsubscribe\_from\_dataset, [34](#)
- unsubscribe\_from\_event, [63](#)
- untag\_certificate\_authority, [14](#)
- untag\_instance\_profile, [54](#)
- untag\_mfa\_device, [54](#)
- untag\_open\_id\_connect\_provider, [54](#)
- untag\_policy, [54](#)
- untag\_resource, [6](#), [17](#), [23](#), [26](#), [31](#), [38](#), [45](#), [49](#), [58](#), [67](#), [71](#), [75](#), [78](#), [81](#), [84](#), [88](#), [92](#), [95](#), [102](#), [116](#), [120](#), [124](#)
- untag\_role, [54](#)
- untag\_saml\_provider, [54](#)
- untag\_server\_certificate, [54](#)
- untag\_user, [54](#)
- update\_access\_key, [54](#)
- update\_account\_password\_policy, [54](#)
- update\_action\_target, [88](#)
- update\_alias, [71](#)
- update\_allow\_list, [75](#)
- update\_application, [103](#)
- update\_application\_layer\_automatic\_response, [95](#)
- update\_archive\_rule, [6](#)
- update\_assessment\_target, [63](#)
- update\_assume\_role\_policy, [54](#)
- update\_auth\_event\_feedback, [31](#)
- update\_automated\_discovery\_configuration, [75](#)
- update\_byte\_match\_set, [116](#), [120](#)
- update\_certificate\_authority, [14](#)
- update\_certificate\_options, [11](#)
- update\_classification\_job, [75](#)
- update\_classification\_scope, [75](#)
- update\_conditional\_forwarder, [42](#)
- update\_configuration, [67](#)
- update\_configuration\_policy, [88](#)
- update\_crl, [58](#)
- update\_custom\_key\_store, [71](#)
- update\_data\_lake, [92](#)
- update\_data\_lake\_exception\_subscription, [92](#)
- update\_datasource\_packages, [38](#)
  
- update\_detector, [49](#)
- update\_device\_status, [31](#)
- update\_directory\_setup, [42](#)
- update\_ec\_2\_deep\_inspection\_configuration, [67](#)
- update\_emergency\_contact\_settings, [95](#)
- update\_encryption\_key, [67](#)
- update\_facet, [17](#)
- update\_filter, [49](#), [67](#)
- update\_finding\_aggregator, [88](#)
- update\_findings, [6](#), [88](#)
- update\_findings\_feedback, [49](#)
- update\_findings\_filter, [75](#)
- update\_geo\_match\_set, [116](#), [120](#)
- update\_group, [31](#), [54](#), [60](#)
- update\_identity\_pool, [26](#)
- update\_identity\_provider, [31](#)
- update\_identity\_source, [112](#)
- update\_insight, [88](#)
- update\_instance, [103](#)
- update\_instance\_access\_control\_attribute\_configuration, [103](#)
- update\_investigation\_state, [38](#)
- update\_ip\_set, [49](#), [116](#), [120](#), [124](#)
- update\_key\_description, [71](#)
- update\_link\_attributes, [17](#)
- update\_login\_profile, [54](#)
- update\_macie\_session, [75](#)
- update\_malware\_scan\_settings, [49](#)
- update\_managed\_rule\_set\_version\_expiry\_date, [124](#)
- update\_member\_detectors, [49](#)
- update\_member\_session, [75](#)
- update\_number\_of\_domain\_controllers, [42](#)
- update\_object\_attributes, [17](#)
- update\_open\_id\_connect\_provider\_thumbprint, [54](#)
- update\_org\_ec\_2\_deep\_inspection\_configuration, [67](#)
- update\_organization\_configuration, [38](#), [49](#), [67](#), [75](#), [88](#)
- update\_permission\_set, [103](#)
- update\_policy, [112](#)
- update\_policy\_store, [112](#)
- update\_policy\_template, [112](#)
- update\_primary\_region, [71](#)
- update\_profile, [58](#)

- update\_protection\_group, 95
- update\_publishing\_destination, 49
- update\_radius, 42
- update\_rate\_based\_rule, 116, 120
- update\_records, 34
- update\_regex\_match\_set, 116, 120
- update\_regex\_pattern\_set, 116, 120, 124
- update\_resource\_profile, 75
- update\_resource\_profile\_detections, 75
- update\_resource\_server, 31
- update\_resource\_share, 81
- update\_reveal\_configuration, 75
- update\_role, 54
- update\_role\_description, 54
- update\_rule, 116, 120
- update\_rule\_group, 116, 120, 124
- update\_saml\_provider, 54
- update\_schema, 18
- update\_secret, 84
- update\_secret\_version\_stage, 84
- update\_security\_control, 89
- update\_security\_hub\_configuration, 89
- update\_sensitivity\_inspection\_template, 75
- update\_server\_certificate, 54
- update\_service\_specific\_credential, 55
- update\_settings, 42
- update\_signing\_certificate, 55
- update\_size\_constraint\_set, 116, 120
- update\_sql\_injection\_match\_set, 116, 120
- update\_ssh\_public\_key, 55
- update\_standards\_control, 85, 89
- update\_subscriber, 92
- update\_subscriber\_notification, 92
- update\_subscription, 95
- update\_template, 78
- update\_template\_group\_access\_control\_entry, 78
- update\_threat\_intel\_set, 49
- update\_trust, 42
- update\_trust\_anchor, 58
- update\_trusted\_token\_issuer, 103
- update\_typed\_link\_facet, 18
- update\_user, 55, 60
- update\_user\_attributes, 31
- update\_user\_pool, 31
- update\_user\_pool\_client, 31
- update\_user\_pool\_domain, 31
- update\_web\_acl, 116, 120, 124
- update\_xss\_match\_set, 116, 120
- upgrade\_applied\_schema, 18
- upgrade\_published\_schema, 18
- upload\_server\_certificate, 55
- upload\_signing\_certificate, 55
- upload\_ssh\_public\_key, 55
- validate\_policy, 6
- validate\_resource\_policy, 84
- verifiedpermissions, 109
- verify, 71
- verify\_mac, 71
- verify\_software\_token, 31
- verify\_trust, 42
- verify\_user\_attribute, 31
- waf, 112
- wafregional, 116
- wafv2, 120