

Package: paws.internet.of.things (via r-universe)

September 4, 2024

Title 'Amazon Web Services' Internet of Things Services

Version 0.7.0

Description Interface to 'Amazon Web Services' internet of things (IoT) services, including data collection, management, and analysis for IoT devices. <<https://aws.amazon.com/iot/>>.

License Apache License (>= 2.0)

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

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

Imports paws.common (>= 0.5.4)

Suggests testthat

Encoding UTF-8

Roxygen list(markdown = TRUE, roclets = c(` `rd", `` namespace", `` collate"))

RoxygenNote 7.1.1

Collate 'greengrass_service.R' 'greengrass_interfaces.R'
'greengrass_operations.R' 'iot1clickdevicesservice_service.R'
'iot1clickdevicesservice_interfaces.R'
'iot1clickdevicesservice_operations.R'
'iot1clickprojects_service.R' 'iot1clickprojects_interfaces.R'
'iot1clickprojects_operations.R' 'iot_service.R'
'iot_interfaces.R' 'iot_operations.R' 'iotanalytics_service.R'
'iotanalytics_interfaces.R' 'iotanalytics_operations.R'
'iotdataplane_service.R' 'iotdataplane_interfaces.R'
'iotdataplane_operations.R' 'iotjobsdataplane_service.R'
'iotjobsdataplane_interfaces.R' 'iotjobsdataplane_operations.R'
'signer_service.R' 'signer_interfaces.R' 'signer_operations.R'

Repository <https://paws-r.r-universe.dev>

RemoteUrl <https://github.com/paws-r/paws>

RemoteRef HEAD

RemoteSha 8ab20b498262e0b343c0153b4f244483aff4987f

Contents

greengrass	2
iot	5
iot1clickdevicesservice	11
iot1clickprojects	12
iotanalytics	14
iotdataplane	16
iotjobsdataplane	17
signer	19
Index	21

greengrass	<i>AWS Greengrass</i>
------------	-----------------------

Description

AWS IoT Greengrass seamlessly extends AWS onto physical devices so they can act locally on the data they generate, while still using the cloud for management, analytics, and durable storage. AWS IoT Greengrass ensures your devices can respond quickly to local events and operate with intermittent connectivity. AWS IoT Greengrass minimizes the cost of transmitting data to the cloud by allowing you to author AWS Lambda functions that execute locally.

Usage

```
greengrass(config = list())
```

Arguments

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

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

```

    ),
    endpoint = "string",
    region = "string"
  )
)

```

Operations

<code>associate_role_to_group</code>	Associates a role with a group
<code>associate_service_role_to_account</code>	Associates a role with your account
<code>create_connector_definition</code>	Creates a connector definition
<code>create_connector_definition_version</code>	Creates a version of a connector definition which has already been defined
<code>create_core_definition</code>	Creates a core definition
<code>create_core_definition_version</code>	Creates a version of a core definition that has already been defined
<code>create_deployment</code>	Creates a deployment
<code>create_device_definition</code>	Creates a device definition
<code>create_device_definition_version</code>	Creates a version of a device definition that has already been defined
<code>create_function_definition</code>	Creates a Lambda function definition which contains a list of Lambda functions and
<code>create_function_definition_version</code>	Creates a version of a Lambda function definition that has already been defined
<code>create_group</code>	Creates a group
<code>create_group_certificate_authority</code>	Creates a CA for the group
<code>create_group_version</code>	Creates a version of a group which has already been defined
<code>create_logger_definition</code>	Creates a logger definition
<code>create_logger_definition_version</code>	Creates a version of a logger definition that has already been defined
<code>create_resource_definition</code>	Creates a resource definition which contains a list of resources to be used in a group
<code>create_resource_definition_version</code>	Creates a version of a resource definition that has already been defined
<code>create_software_update_job</code>	Creates a software update for a core or group of cores (specified as an IoT thing group)
<code>create_subscription_definition</code>	Creates a subscription definition
<code>create_subscription_definition_version</code>	Creates a version of a subscription definition which has already been defined
<code>delete_connector_definition</code>	Deletes a connector definition
<code>delete_core_definition</code>	Deletes a core definition
<code>delete_device_definition</code>	Deletes a device definition
<code>delete_function_definition</code>	Deletes a Lambda function definition
<code>delete_group</code>	Deletes a group
<code>delete_logger_definition</code>	Deletes a logger definition
<code>delete_resource_definition</code>	Deletes a resource definition
<code>delete_subscription_definition</code>	Deletes a subscription definition
<code>disassociate_role_from_group</code>	Disassociates the role from a group
<code>disassociate_service_role_from_account</code>	Disassociates the service role from your account
<code>get_associated_role</code>	Retrieves the role associated with a particular group
<code>get_bulk_deployment_status</code>	Returns the status of a bulk deployment
<code>get_connectivity_info</code>	Retrieves the connectivity information for a core
<code>get_connector_definition</code>	Retrieves information about a connector definition
<code>get_connector_definition_version</code>	Retrieves information about a connector definition version, including the connector
<code>get_core_definition</code>	Retrieves information about a core definition
<code>get_core_definition_version</code>	Retrieves information about a core definition version
<code>get_deployment_status</code>	Returns the status of a deployment
<code>get_device_definition</code>	Retrieves information about a device definition

get_device_definition_version	Retrieves information about a device definition version
get_function_definition	Retrieves information about a Lambda function definition, including its creation time
get_function_definition_version	Retrieves information about a Lambda function definition version, including which resource it is associated with
get_group	Retrieves information about a group
get_group_certificate_authority	Retrieves the CA associated with a group
get_group_certificate_configuration	Retrieves the current configuration for the CA used by the group
get_group_version	Retrieves information about a group version
get_logger_definition	Retrieves information about a logger definition
get_logger_definition_version	Retrieves information about a logger definition version
get_resource_definition	Retrieves information about a resource definition, including its creation time and last updated time
get_resource_definition_version	Retrieves information about a resource definition version, including which resource it is associated with
get_service_role_for_account	Retrieves the service role that is attached to your account
get_subscription_definition	Retrieves information about a subscription definition
get_subscription_definition_version	Retrieves information about a subscription definition version
get_thing_runtime_configuration	Get the runtime configuration of a thing
list_bulk_deployment_detailed_reports	Gets a paginated list of the deployments that have been started in a bulk deployment
list_bulk_deployments	Returns a list of bulk deployments
list_connector_definitions	Retrieves a list of connector definitions
list_connector_definition_versions	Lists the versions of a connector definition, which are containers for connectors
list_core_definitions	Retrieves a list of core definitions
list_core_definition_versions	Lists the versions of a core definition
list_deployments	Returns a history of deployments for the group
list_device_definitions	Retrieves a list of device definitions
list_device_definition_versions	Lists the versions of a device definition
list_function_definitions	Retrieves a list of Lambda function definitions
list_function_definition_versions	Lists the versions of a Lambda function definition
list_group_certificate_authorities	Retrieves the current CAs for a group
list_groups	Retrieves a list of groups
list_group_versions	Lists the versions of a group
list_logger_definitions	Retrieves a list of logger definitions
list_logger_definition_versions	Lists the versions of a logger definition
list_resource_definitions	Retrieves a list of resource definitions
list_resource_definition_versions	Lists the versions of a resource definition
list_subscription_definitions	Retrieves a list of subscription definitions
list_subscription_definition_versions	Lists the versions of a subscription definition
list_tags_for_resource	Retrieves a list of resource tags for a resource arn
reset_deployments	Resets a group's deployments
start_bulk_deployment	Deploys multiple groups in one operation
stop_bulk_deployment	Stops the execution of a bulk deployment
tag_resource	Adds tags to a Greengrass resource
untag_resource	Remove resource tags from a Greengrass Resource
update_connectivity_info	Updates the connectivity information for the core
update_connector_definition	Updates a connector definition
update_core_definition	Updates a core definition
update_device_definition	Updates a device definition
update_function_definition	Updates a Lambda function definition
update_group	Updates a group
update_group_certificate_configuration	Updates the Certificate expiry time for a group

update_logger_definition	Updates a logger definition
update_resource_definition	Updates a resource definition
update_subscription_definition	Updates a subscription definition
update_thing_runtime_configuration	Updates the runtime configuration of a thing

Examples

```
## Not run:
svc <- greengrass()
svc$associate_role_to_group(
  Foo = 123
)

## End(Not run)
```

iot	<i>AWS IoT</i>
-----	----------------

Description

AWS IoT provides secure, bi-directional communication between Internet-connected devices (such as sensors, actuators, embedded devices, or smart appliances) and the AWS cloud. You can discover your custom IoT-Data endpoint to communicate with, configure rules for data processing and integration with other services, organize resources associated with each device (Registry), configure logging, and create and manage policies and credentials to authenticate devices.

The service endpoints that expose this API are listed in [AWS IoT Core Endpoints and Quotas](#). You must use the endpoint for the region that has the resources you want to access.

The service name used by [AWS Signature Version 4](#) to sign the request is: *execute-api*.

For more information about how AWS IoT works, see the [Developer Guide](#).

For information about how to use the credentials provider for AWS IoT, see [Authorizing Direct Calls to AWS Services](#).

Usage

```
iot(config = list())
```

Arguments

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

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 <- iot(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string"
    ),
    endpoint = "string",
    region = "string"
  )
)

```

Operations

accept_certificate_transfer	Accepts a pending certificate transfer
add_thing_to_billing_group	Adds a thing to a billing group
add_thing_to_thing_group	Adds a thing to a thing group
associate_targets_with_job	Associates a group with a continuous job
attach_policy	Attaches a policy to the specified target
attach_principal_policy	Attaches the specified policy to the specified principal (certificate or other creden
attach_security_profile	Associates a Device Defender security profile with a thing group or this account
attach_thing_principal	Attaches the specified principal to the specified thing
cancel_audit_mitigation_actions_task	Cancels a mitigation action task that is in progress
cancel_audit_task	Cancels an audit that is in progress
cancel_certificate_transfer	Cancels a pending transfer for the specified certificate
cancel_detect_mitigation_actions_task	Cancels a Device Defender ML Detect mitigation action
cancel_job	Cancels a job
cancel_job_execution	Cancels the execution of a job for a given thing
clear_default_authorizer	Clears the default authorizer
confirm_topic_rule_destination	Confirms a topic rule destination
create_audit_suppression	Creates a Device Defender audit suppression
create_authorizer	Creates an authorizer
create_billing_group	Creates a billing group
create_certificate_from_csr	Creates an X
create_custom_metric	Use this API to define a Custom Metric published by your devices to Device Defe
create_dimension	Create a dimension that you can use to limit the scope of a metric used in a securi
create_domain_configuration	Creates a domain configuration
create_dynamic_thing_group	Creates a dynamic thing group
create_job	Creates a job
create_keys_and_certificate	Creates a 2048-bit RSA key pair and issues an X
create_mitigation_action	Defines an action that can be applied to audit findings by using StartAuditMitigat
create_ota_update	Creates an AWS IoT OTAUpdate on a target group of things or groups
create_policy	Creates an AWS IoT policy

<code>create_policy_version</code>	Creates a new version of the specified AWS IoT policy
<code>create_provisioning_claim</code>	Creates a provisioning claim
<code>create_provisioning_template</code>	Creates a fleet provisioning template
<code>create_provisioning_template_version</code>	Creates a new version of a fleet provisioning template
<code>create_role_alias</code>	Creates a role alias
<code>create_scheduled_audit</code>	Creates a scheduled audit that is run at a specified time interval
<code>create_security_profile</code>	Creates a Device Defender security profile
<code>create_stream</code>	Creates a stream for delivering one or more large files in chunks over MQTT
<code>create_thing</code>	Creates a thing record in the registry
<code>create_thing_group</code>	Create a thing group
<code>create_thing_type</code>	Creates a new thing type
<code>create_topic_rule</code>	Creates a rule
<code>create_topic_rule_destination</code>	Creates a topic rule destination
<code>delete_account_audit_configuration</code>	Restores the default settings for Device Defender audits for this account
<code>delete_audit_suppression</code>	Deletes a Device Defender audit suppression
<code>delete_authorizer</code>	Deletes an authorizer
<code>delete_billing_group</code>	Deletes the billing group
<code>delete_ca_certificate</code>	Deletes a registered CA certificate
<code>delete_certificate</code>	Deletes the specified certificate
<code>delete_custom_metric</code>	Before you can delete a custom metric, you must first remove the custom metric from the registry
<code>delete_dimension</code>	Removes the specified dimension from your AWS account
<code>delete_domain_configuration</code>	Deletes the specified domain configuration
<code>delete_dynamic_thing_group</code>	Deletes a dynamic thing group
<code>delete_job</code>	Deletes a job and its related job executions
<code>delete_job_execution</code>	Deletes a job execution
<code>delete_mitigation_action</code>	Deletes a defined mitigation action from your AWS account
<code>delete_ota_update</code>	Delete an OTA update
<code>delete_policy</code>	Deletes the specified policy
<code>delete_policy_version</code>	Deletes the specified version of the specified policy
<code>delete_provisioning_template</code>	Deletes a fleet provisioning template
<code>delete_provisioning_template_version</code>	Deletes a fleet provisioning template version
<code>delete_registration_code</code>	Deletes a CA certificate registration code
<code>delete_role_alias</code>	Deletes a role alias
<code>delete_scheduled_audit</code>	Deletes a scheduled audit
<code>delete_security_profile</code>	Deletes a Device Defender security profile
<code>delete_stream</code>	Deletes a stream
<code>delete_thing</code>	Deletes the specified thing
<code>delete_thing_group</code>	Deletes a thing group
<code>delete_thing_type</code>	Deletes the specified thing type
<code>delete_topic_rule</code>	Deletes the rule
<code>delete_topic_rule_destination</code>	Deletes a topic rule destination
<code>delete_v2_logging_level</code>	Deletes a logging level
<code>deprecate_thing_type</code>	Deprecates a thing type
<code>describe_account_audit_configuration</code>	Gets information about the Device Defender audit settings for this account
<code>describe_audit_finding</code>	Gets information about a single audit finding
<code>describe_audit_mitigation_actions_task</code>	Gets information about an audit mitigation task that is used to apply mitigation actions
<code>describe_audit_suppression</code>	Gets information about a Device Defender audit suppression
<code>describe_audit_task</code>	Gets information about a Device Defender audit

<code>describe_authorizer</code>	Describes an authorizer
<code>describe_billing_group</code>	Returns information about a billing group
<code>describe_ca_certificate</code>	Describes a registered CA certificate
<code>describe_certificate</code>	Gets information about the specified certificate
<code>describe_custom_metric</code>	Gets information about a Device Defender detect custom metric
<code>describe_default_authorizer</code>	Describes the default authorizer
<code>describe_detect_mitigation_actions_task</code>	Gets information about a Device Defender ML Detect mitigation action
<code>describe_dimension</code>	Provides details about a dimension that is defined in your AWS account
<code>describe_domain_configuration</code>	Gets summary information about a domain configuration
<code>describe_endpoint</code>	Returns a unique endpoint specific to the AWS account making the call
<code>describe_event_configurations</code>	Describes event configurations
<code>describe_index</code>	Describes a search index
<code>describe_job</code>	Describes a job
<code>describe_job_execution</code>	Describes a job execution
<code>describe_mitigation_action</code>	Gets information about a mitigation action
<code>describe_provisioning_template</code>	Returns information about a fleet provisioning template
<code>describe_provisioning_template_version</code>	Returns information about a fleet provisioning template version
<code>describe_role_alias</code>	Describes a role alias
<code>describe_scheduled_audit</code>	Gets information about a scheduled audit
<code>describe_security_profile</code>	Gets information about a Device Defender security profile
<code>describe_stream</code>	Gets information about a stream
<code>describe_thing</code>	Gets information about the specified thing
<code>describe_thing_group</code>	Describe a thing group
<code>describe_thing_registration_task</code>	Describes a bulk thing provisioning task
<code>describe_thing_type</code>	Gets information about the specified thing type
<code>detach_policy</code>	Detaches a policy from the specified target
<code>detach_principal_policy</code>	Removes the specified policy from the specified certificate
<code>detach_security_profile</code>	Disassociates a Device Defender security profile from a thing group or from this
<code>detach_thing_principal</code>	Detaches the specified principal from the specified thing
<code>disable_topic_rule</code>	Disables the rule
<code>enable_topic_rule</code>	Enables the rule
<code>get_behavior_model_training_summaries</code>	Returns a Device Defender's ML Detect Security Profile training model's status
<code>get_cardinality</code>	Returns the approximate count of unique values that match the query
<code>get_effective_policies</code>	Gets a list of the policies that have an effect on the authorization behavior of the s
<code>get_indexing_configuration</code>	Gets the indexing configuration
<code>get_job_document</code>	Gets a job document
<code>get_logging_options</code>	Gets the logging options
<code>get_ota_update</code>	Gets an OTA update
<code>get_percentiles</code>	Groups the aggregated values that match the query into percentile groupings
<code>get_policy</code>	Gets information about the specified policy with the policy document of the defau
<code>get_policy_version</code>	Gets information about the specified policy version
<code>get_registration_code</code>	Gets a registration code used to register a CA certificate with AWS IoT
<code>get_statistics</code>	Returns the count, average, sum, minimum, maximum, sum of squares, variance,
<code>get_topic_rule</code>	Gets information about the rule
<code>get_topic_rule_destination</code>	Gets information about a topic rule destination
<code>get_v2_logging_options</code>	Gets the fine grained logging options
<code>list_active_violations</code>	Lists the active violations for a given Device Defender security profile
<code>list_attached_policies</code>	Lists the policies attached to the specified thing group

list_audit_findings	Lists the findings (results) of a Device Defender audit or of the audits performed
list_audit_mitigation_actions_executions	Gets the status of audit mitigation action tasks that were executed
list_audit_mitigation_actions_tasks	Gets a list of audit mitigation action tasks that match the specified filters
list_audit_suppressions	Lists your Device Defender audit listings
list_audit_tasks	Lists the Device Defender audits that have been performed during a given time pe
list_authorizers	Lists the authorizers registered in your account
list_billing_groups	Lists the billing groups you have created
list_ca_certificates	Lists the CA certificates registered for your AWS account
list_certificates	Lists the certificates registered in your AWS account
list_certificates_by_ca	List the device certificates signed by the specified CA certificate
list_custom_metrics	Lists your Device Defender detect custom metrics
list_detect_mitigation_actions_executions	Lists mitigation actions executions for a Device Defender ML Detect Security Pro
list_detect_mitigation_actions_tasks	List of Device Defender ML Detect mitigation actions tasks
list_dimensions	List the set of dimensions that are defined for your AWS account
list_domain_configurations	Gets a list of domain configurations for the user
list_indices	Lists the search indices
list_job_executions_for_job	Lists the job executions for a job
list_job_executions_for_thing	Lists the job executions for the specified thing
list_jobs	Lists jobs
list_mitigation_actions	Gets a list of all mitigation actions that match the specified filter criteria
list_ota_updates	Lists OTA updates
list_outgoing_certificates	Lists certificates that are being transferred but not yet accepted
list_policies	Lists your policies
list_policy_principals	Lists the principals associated with the specified policy
list_policy_versions	Lists the versions of the specified policy and identifies the default version
list_principal_policies	Lists the policies attached to the specified principal
list_principal_things	Lists the things associated with the specified principal
list_provisioning_templates	Lists the fleet provisioning templates in your AWS account
list_provisioning_template_versions	A list of fleet provisioning template versions
list_role_aliases	Lists the role aliases registered in your account
list_scheduled_audits	Lists all of your scheduled audits
list_security_profiles	Lists the Device Defender security profiles you've created
list_security_profiles_for_target	Lists the Device Defender security profiles attached to a target (thing group)
list_streams	Lists all of the streams in your AWS account
list_tags_for_resource	Lists the tags (metadata) you have assigned to the resource
list_targets_for_policy	List targets for the specified policy
list_targets_for_security_profile	Lists the targets (thing groups) associated with a given Device Defender security
list_thing_groups	List the thing groups in your account
list_thing_groups_for_thing	List the thing groups to which the specified thing belongs
list_thing_principals	Lists the principals associated with the specified thing
list_thing_registration_task_reports	Information about the thing registration tasks
list_thing_registration_tasks	List bulk thing provisioning tasks
list_things	Lists your things
list_things_in_billing_group	Lists the things you have added to the given billing group
list_things_in_thing_group	Lists the things in the specified group
list_thing_types	Lists the existing thing types
list_topic_rule_destinations	Lists all the topic rule destinations in your AWS account
list_topic_rules	Lists the rules for the specific topic

<code>list_v2_logging_levels</code>	Lists logging levels
<code>list_violation_events</code>	Lists the Device Defender security profile violations discovered during the given
<code>register_ca_certificate</code>	Registers a CA certificate with AWS IoT
<code>register_certificate</code>	Registers a device certificate with AWS IoT
<code>register_certificate_without_ca</code>	Register a certificate that does not have a certificate authority (CA)
<code>register_thing</code>	Provisions a thing in the device registry
<code>reject_certificate_transfer</code>	Rejects a pending certificate transfer
<code>remove_thing_from_billing_group</code>	Removes the given thing from the billing group
<code>remove_thing_from_thing_group</code>	Remove the specified thing from the specified group
<code>replace_topic_rule</code>	Replaces the rule
<code>search_index</code>	The query search index
<code>set_default_authorizer</code>	Sets the default authorizer
<code>set_default_policy_version</code>	Sets the specified version of the specified policy as the policy's default (operative)
<code>set_logging_options</code>	Sets the logging options
<code>set_v2_logging_level</code>	Sets the logging level
<code>set_v2_logging_options</code>	Sets the logging options for the V2 logging service
<code>start_audit_mitigation_actions_task</code>	Starts a task that applies a set of mitigation actions to the specified target
<code>start_detect_mitigation_actions_task</code>	Starts a Device Defender ML Detect mitigation actions task
<code>start_on_demand_audit_task</code>	Starts an on-demand Device Defender audit
<code>start_thing_registration_task</code>	Creates a bulk thing provisioning task
<code>stop_thing_registration_task</code>	Cancel a bulk thing provisioning task
<code>tag_resource</code>	Adds to or modifies the tags of the given resource
<code>test_authorization</code>	Tests if a specified principal is authorized to perform an AWS IoT action on a spe
<code>test_invoke_authorizer</code>	Tests a custom authorization behavior by invoking a specified custom authorizer
<code>transfer_certificate</code>	Transfers the specified certificate to the specified AWS account
<code>untag_resource</code>	Removes the given tags (metadata) from the resource
<code>update_account_audit_configuration</code>	Configures or reconfigures the Device Defender audit settings for this account
<code>update_audit_suppression</code>	Updates a Device Defender audit suppression
<code>update_authorizer</code>	Updates an authorizer
<code>update_billing_group</code>	Updates information about the billing group
<code>update_ca_certificate</code>	Updates a registered CA certificate
<code>update_certificate</code>	Updates the status of the specified certificate
<code>update_custom_metric</code>	Updates a Device Defender detect custom metric
<code>update_dimension</code>	Updates the definition for a dimension
<code>update_domain_configuration</code>	Updates values stored in the domain configuration
<code>update_dynamic_thing_group</code>	Updates a dynamic thing group
<code>update_event_configurations</code>	Updates the event configurations
<code>update_indexing_configuration</code>	Updates the search configuration
<code>update_job</code>	Updates supported fields of the specified job
<code>update_mitigation_action</code>	Updates the definition for the specified mitigation action
<code>update_provisioning_template</code>	Updates a fleet provisioning template
<code>update_role_alias</code>	Updates a role alias
<code>update_scheduled_audit</code>	Updates a scheduled audit, including which checks are performed and how often
<code>update_security_profile</code>	Updates a Device Defender security profile
<code>update_stream</code>	Updates an existing stream
<code>update_thing</code>	Updates the data for a thing
<code>update_thing_group</code>	Update a thing group
<code>update_thing_groups_for_thing</code>	Updates the groups to which the thing belongs

update_topic_rule_destination	Updates a topic rule destination
validate_security_profile_behaviors	Validates a Device Defender security profile behaviors specification

Examples

```
## Not run:
svc <- iot()
svc$accept_certificate_transfer(
  Foo = 123
)

## End(Not run)
```

iot1clickdevicesservice
AWS IoT 1-Click Devices Service

Description

Describes all of the AWS IoT 1-Click device-related API operations for the service. Also provides sample requests, responses, and errors for the supported web services protocols.

Usage

```
iot1clickdevicesservice(config = list())
```

Arguments

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

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 <- iot1clickdevicesservice(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
```

```

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

```

Operations

claim_devices_by_claim_code	Adds device(s) to your account (i
describe_device	Given a device ID, returns a DescribeDeviceResponse object describing the details of the device
finalize_device_claim	Given a device ID, finalizes the claim request for the associated device
get_device_methods	Given a device ID, returns the invocable methods associated with the device
initiate_device_claim	Given a device ID, initiates a claim request for the associated device
invoke_device_method	Given a device ID, issues a request to invoke a named device method (with possible parameters)
list_device_events	Using a device ID, returns a DeviceEventsResponse object containing an array of events for the device
list_devices	Lists the 1-Click compatible devices associated with your AWS account
list_tags_for_resource	Lists the tags associated with the specified resource ARN
tag_resource	Adds or updates the tags associated with the resource ARN
unclaim_device	Disassociates a device from your AWS account using its device ID
untag_resource	Using tag keys, deletes the tags (key/value pairs) associated with the specified resource ARN
update_device_state	Using a Boolean value (true or false), this operation enables or disables the device given a device ID

Examples

```

## Not run:
svc <- iot1clickdevicesservice()
svc$claim_devices_by_claim_code(
  Foo = 123
)

## End(Not run)

```

iot1clickprojects *AWS IoT 1-Click Projects Service*

Description

The AWS IoT 1-Click Projects API Reference

Usage

```
iot1clickprojects(config = list())
```

Arguments

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

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 <- iot1clickprojects(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string"
    ),
    endpoint = "string",
    region = "string"
  )
)
```

Operations

associate_device_with_placement	Associates a physical device with a placement
create_placement	Creates an empty placement
create_project	Creates an empty project with a placement template
delete_placement	Deletes a placement
delete_project	Deletes a project
describe_placement	Describes a placement in a project
describe_project	Returns an object describing a project
disassociate_device_from_placement	Removes a physical device from a placement
get_devices_in_placement	Returns an object enumerating the devices in a placement
list_placements	Lists the placement(s) of a project
list_projects	Lists the AWS IoT 1-Click project(s) associated with your AWS account and region
list_tags_for_resource	Lists the tags (metadata key/value pairs) which you have assigned to the resource
tag_resource	Creates or modifies tags for a resource
untag_resource	Removes one or more tags (metadata key/value pairs) from a resource
update_placement	Updates a placement with the given attributes
update_project	Updates a project associated with your AWS account and region

Examples

```
## Not run:
svc <- iot1clickprojects()
svc$associate_device_with_placement(
  Foo = 123
)

## End(Not run)
```

iotanalytics

AWS IoT Analytics

Description

AWS IoT Analytics allows you to collect large amounts of device data, process messages, and store them. You can then query the data and run sophisticated analytics on it. AWS IoT Analytics enables advanced data exploration through integration with Jupyter Notebooks and data visualization through integration with Amazon QuickSight.

Traditional analytics and business intelligence tools are designed to process structured data. IoT data often comes from devices that record noisy processes (such as temperature, motion, or sound). As a result the data from these devices can have significant gaps, corrupted messages, and false readings that must be cleaned up before analysis can occur. Also, IoT data is often only meaningful in the context of other data from external sources.

AWS IoT Analytics automates the steps required to analyze data from IoT devices. AWS IoT Analytics filters, transforms, and enriches IoT data before storing it in a time-series data store for analysis. You can set up the service to collect only the data you need from your devices, apply mathematical transforms to process the data, and enrich the data with device-specific metadata such as device type and location before storing it. Then, you can analyze your data by running queries using the built-in SQL query engine, or perform more complex analytics and machine learning inference. AWS IoT Analytics includes pre-built models for common IoT use cases so you can answer questions like which devices are about to fail or which customers are at risk of abandoning their wearable devices.

Usage

```
iotanalytics(config = list())
```

Arguments

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

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 <- iotanalytics(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string"
    ),
    endpoint = "string",
    region = "string"
  )
)

```

Operations

batch_put_message	Sends messages to a channel
cancel_pipeline_reprocessing	Cancels the reprocessing of data through the pipeline
create_channel	Creates a channel
create_dataset	Creates a dataset
create_dataset_content	Creates the content of a data set by applying a queryAction (a SQL query) or a containerAction
create_datastore	Creates a data store, which is a repository for messages
create_pipeline	Creates a pipeline
delete_channel	Deletes the specified channel
delete_dataset	Deletes the specified dataset
delete_dataset_content	Deletes the content of the specified dataset
delete_datastore	Deletes the specified data store
delete_pipeline	Deletes the specified pipeline
describe_channel	Retrieves information about a channel
describe_dataset	Retrieves information about a dataset
describe_datastore	Retrieves information about a data store
describe_logging_options	Retrieves the current settings of the AWS IoT Analytics logging options
describe_pipeline	Retrieves information about a pipeline
get_dataset_content	Retrieves the contents of a data set as presigned URIs
list_channels	Retrieves a list of channels
list_dataset_contents	Lists information about data set contents that have been created
list_datasets	Retrieves information about data sets
list_datastores	Retrieves a list of data stores
list_pipelines	Retrieves a list of pipelines
list_tags_for_resource	Lists the tags (metadata) that you have assigned to the resource
put_logging_options	Sets or updates the AWS IoT Analytics logging options
run_pipeline_activity	Simulates the results of running a pipeline activity on a message payload
sample_channel_data	Retrieves a sample of messages from the specified channel ingested during the specified time
start_pipeline_reprocessing	Starts the reprocessing of raw message data through the pipeline
tag_resource	Adds to or modifies the tags of the given resource

<code>untag_resource</code>	Removes the given tags (metadata) from the resource
<code>update_channel</code>	Updates the settings of a channel
<code>update_dataset</code>	Updates the settings of a data set
<code>update_datastore</code>	Updates the settings of a data store
<code>update_pipeline</code>	Updates the settings of a pipeline

Examples

```
## Not run:
svc <- iotanalytics()
svc$batch_put_message(
  Foo = 123
)

## End(Not run)
```

iotdataplane

AWS IoT Data Plane

Description

AWS IoT

AWS IoT-Data enables secure, bi-directional communication between Internet-connected things (such as sensors, actuators, embedded devices, or smart appliances) and the AWS cloud. It implements a broker for applications and things to publish messages over HTTP (Publish) and retrieve, update, and delete shadows. A shadow is a persistent representation of your things and their state in the AWS cloud.

Find the endpoint address for actions in the AWS IoT data plane by running this CLI command:
`aws iot describe-endpoint --endpoint-type iot:Data-ATS`

The service name used by [AWS Signature Version 4](#) to sign requests is: *iotdevicegateway*.

Usage

```
iotdataplane(config = list())
```

Arguments

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

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 <- iotdataplane(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string"
    ),
    endpoint = "string",
    region = "string"
  )
)

```

Operations

delete_thing_shadow	Deletes the shadow for the specified thing
get_thing_shadow	Gets the shadow for the specified thing
list_named_shadows_for_thing	Lists the shadows for the specified thing
publish	Publishes state information
update_thing_shadow	Updates the shadow for the specified thing

Examples

```

## Not run:
svc <- iotdataplane()
svc$delete_thing_shadow(
  Foo = 123
)

## End(Not run)

```

Description

AWS IoT Jobs is a service that allows you to define a set of jobs — remote operations that are sent to and executed on one or more devices connected to AWS IoT. For example, you can define a job that instructs a set of devices to download and install application or firmware updates, reboot, rotate certificates, or perform remote troubleshooting operations.

To create a job, you make a job document which is a description of the remote operations to be performed, and you specify a list of targets that should perform the operations. The targets can be individual things, thing groups or both.

AWS IoT Jobs sends a message to inform the targets that a job is available. The target starts the execution of the job by downloading the job document, performing the operations it specifies, and reporting its progress to AWS IoT. The Jobs service provides commands to track the progress of a job on a specific target and for all the targets of the job

Usage

```
iotjobsdataplane(config = list())
```

Arguments

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

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 <- iotjobsdataplane(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string"
    ),
    endpoint = "string",
    region = "string"
  )
)
```

Operations

describe_job_execution	Gets details of a job execution
get_pending_job_executions	Gets the list of all jobs for a thing that are not in a terminal status
start_next_pending_job_execution	Gets and starts the next pending (status IN_PROGRESS or QUEUED) job execution for
update_job_execution	Updates the status of a job execution

Examples

```
## Not run:
svc <- iotjobsdataplane()
svc$describe_job_execution(
  Foo = 123
)

## End(Not run)
```

signer

AWS Signer

Description

AWS Signer is a fully managed code signing service to help you ensure the trust and integrity of your code.

AWS Signer supports the following applications:

With *code signing for AWS Lambda*, you can sign AWS Lambda deployment packages. Integrated support is provided for Amazon S3, Amazon CloudWatch, and AWS CloudTrail. In order to sign code, you create a signing profile and then use Signer to sign Lambda zip files in S3.

With *code signing for IoT*, you can sign code for any IoT device that is supported by AWS. IoT code signing is available for [Amazon FreeRTOS](#) and [AWS IoT Device Management](#), and is integrated with [AWS Certificate Manager \(ACM\)](#). In order to sign code, you import a third-party code signing certificate using ACM, and use that to sign updates in Amazon FreeRTOS and AWS IoT Device Management.

For more information about AWS Signer, see the [AWS Signer Developer Guide](#).

Usage

```
signer(config = list())
```

Arguments

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

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 <- signer(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string"
    ),
    endpoint = "string",
    region = "string"
  )
)

```

Operations

add_profile_permission	Adds cross-account permissions to a signing profile
cancel_signing_profile	Changes the state of an ACTIVE signing profile to CANCELED
describe_signing_job	Returns information about a specific code signing job
get_signing_platform	Returns information on a specific signing platform
get_signing_profile	Returns information on a specific signing profile
list_profile_permissions	Lists the cross-account permissions associated with a signing profile
list_signing_jobs	Lists all your signing jobs
list_signing_platforms	Lists all signing platforms available in code signing that match the request parameters
list_signing_profiles	Lists all available signing profiles in your AWS account
list_tags_for_resource	Returns a list of the tags associated with a signing profile resource
put_signing_profile	Creates a signing profile
remove_profile_permission	Removes cross-account permissions from a signing profile
revoke_signature	Changes the state of a signing job to REVOKED
revoke_signing_profile	Changes the state of a signing profile to REVOKED
start_signing_job	Initiates a signing job to be performed on the code provided
tag_resource	Adds one or more tags to a signing profile
untag_resource	Removes one or more tags from a signing profile

Examples

```

## Not run:
svc <- signer()
svc$add_profile_permission(
  Foo = 123
)

## End(Not run)

```

Index

accept_certificate_transfer, [6](#)
add_profile_permission, [20](#)
add_thing_to_billing_group, [6](#)
add_thing_to_thing_group, [6](#)
associate_device_with_placement, [13](#)
associate_role_to_group, [3](#)
associate_service_role_to_account, [3](#)
associate_targets_with_job, [6](#)
attach_policy, [6](#)
attach_principal_policy, [6](#)
attach_security_profile, [6](#)
attach_thing_principal, [6](#)

batch_put_message, [15](#)

cancel_audit_mitigation_actions_task, [6](#)
cancel_audit_task, [6](#)
cancel_certificate_transfer, [6](#)
cancel_detect_mitigation_actions_task, [6](#)
cancel_job, [6](#)
cancel_job_execution, [6](#)
cancel_pipeline_reprocessing, [15](#)
cancel_signing_profile, [20](#)
claim_devices_by_claim_code, [12](#)
clear_default_authorizer, [6](#)
confirm_topic_rule_destination, [6](#)
create_audit_suppression, [6](#)
create_authorizer, [6](#)
create_billing_group, [6](#)
create_certificate_from_csr, [6](#)
create_channel, [15](#)
create_connector_definition, [3](#)
create_connector_definition_version, [3](#)
create_core_definition, [3](#)
create_core_definition_version, [3](#)
create_custom_metric, [6](#)
create_dataset, [15](#)
create_dataset_content, [15](#)
create_datastore, [15](#)
create_deployment, [3](#)
create_device_definition, [3](#)
create_device_definition_version, [3](#)
create_dimension, [6](#)
create_domain_configuration, [6](#)
create_dynamic_thing_group, [6](#)
create_function_definition, [3](#)
create_function_definition_version, [3](#)
create_group, [3](#)
create_group_certificate_authority, [3](#)
create_group_version, [3](#)
create_job, [6](#)
create_keys_and_certificate, [6](#)
create_logger_definition, [3](#)
create_logger_definition_version, [3](#)
create_mitigation_action, [6](#)
create_ota_update, [6](#)
create_pipeline, [15](#)
create_placement, [13](#)
create_policy, [6](#)
create_policy_version, [7](#)
create_project, [13](#)
create_provisioning_claim, [7](#)
create_provisioning_template, [7](#)
create_provisioning_template_version, [7](#)
create_resource_definition, [3](#)
create_resource_definition_version, [3](#)
create_role_alias, [7](#)
create_scheduled_audit, [7](#)
create_security_profile, [7](#)
create_software_update_job, [3](#)
create_stream, [7](#)
create_subscription_definition, [3](#)
create_subscription_definition_version, [3](#)
create_thing, [7](#)
create_thing_group, [7](#)

create_thing_type, 7
create_topic_rule, 7
create_topic_rule_destination, 7

delete_account_audit_configuration, 7
delete_audit_suppression, 7
delete_authorizer, 7
delete_billing_group, 7
delete_ca_certificate, 7
delete_certificate, 7
delete_channel, 15
delete_connector_definition, 3
delete_core_definition, 3
delete_custom_metric, 7
delete_dataset, 15
delete_dataset_content, 15
delete_datastore, 15
delete_device_definition, 3
delete_dimension, 7
delete_domain_configuration, 7
delete_dynamic_thing_group, 7
delete_function_definition, 3
delete_group, 3
delete_job, 7
delete_job_execution, 7
delete_logger_definition, 3
delete_mitigation_action, 7
delete_ota_update, 7
delete_pipeline, 15
delete_placement, 13
delete_policy, 7
delete_policy_version, 7
delete_project, 13
delete_provisioning_template, 7
delete_provisioning_template_version, 7
delete_registration_code, 7
delete_resource_definition, 3
delete_role_alias, 7
delete_scheduled_audit, 7
delete_security_profile, 7
delete_stream, 7
delete_subscription_definition, 3
delete_thing, 7
delete_thing_group, 7
delete_thing_shadow, 17
delete_thing_type, 7
delete_topic_rule, 7
delete_topic_rule_destination, 7

delete_v2_logging_level, 7
deprecate_thing_type, 7
describe_account_audit_configuration, 7
describe_audit_finding, 7
describe_audit_mitigation_actions_task, 7
describe_audit_suppression, 7
describe_audit_task, 7
describe_authorizer, 8
describe_billing_group, 8
describe_ca_certificate, 8
describe_certificate, 8
describe_channel, 15
describe_custom_metric, 8
describe_dataset, 15
describe_datastore, 15
describe_default_authorizer, 8
describe_detect_mitigation_actions_task, 8
describe_device, 12
describe_dimension, 8
describe_domain_configuration, 8
describe_endpoint, 8
describe_event_configurations, 8
describe_index, 8
describe_job, 8
describe_job_execution, 8, 18
describe_logging_options, 15
describe_mitigation_action, 8
describe_pipeline, 15
describe_placement, 13
describe_project, 13
describe_provisioning_template, 8
describe_provisioning_template_version, 8
describe_role_alias, 8
describe_scheduled_audit, 8
describe_security_profile, 8
describe_signing_job, 20
describe_stream, 8
describe_thing, 8
describe_thing_group, 8
describe_thing_registration_task, 8
describe_thing_type, 8
detach_policy, 8
detach_principal_policy, 8
detach_security_profile, 8

- detach_thing_principal, 8
- disable_topic_rule, 8
- disassociate_device_from_placement, 13
- disassociate_role_from_group, 3
- disassociate_service_role_from_account, 3
- enable_topic_rule, 8
- finalize_device_claim, 12
- get_associated_role, 3
- get_behavior_model_training_summaries, 8
- get_bulk_deployment_status, 3
- get_cardinality, 8
- get_connectivity_info, 3
- get_connector_definition, 3
- get_connector_definition_version, 3
- get_core_definition, 3
- get_core_definition_version, 3
- get_dataset_content, 15
- get_deployment_status, 3
- get_device_definition, 3
- get_device_definition_version, 4
- get_device_methods, 12
- get_devices_in_placement, 13
- get_effective_policies, 8
- get_function_definition, 4
- get_function_definition_version, 4
- get_group, 4
- get_group_certificate_authority, 4
- get_group_certificate_configuration, 4
- get_group_version, 4
- get_indexing_configuration, 8
- get_job_document, 8
- get_logger_definition, 4
- get_logger_definition_version, 4
- get_logging_options, 8
- get_ota_update, 8
- get_pending_job_executions, 18
- get_percentiles, 8
- get_policy, 8
- get_policy_version, 8
- get_registration_code, 8
- get_resource_definition, 4
- get_resource_definition_version, 4
- get_service_role_for_account, 4
- get_signing_platform, 20
- get_signing_profile, 20
- get_statistics, 8
- get_subscription_definition, 4
- get_subscription_definition_version, 4
- get_thing_runtime_configuration, 4
- get_thing_shadow, 17
- get_topic_rule, 8
- get_topic_rule_destination, 8
- get_v2_logging_options, 8
- greengrass, 2
- initiate_device_claim, 12
- invoke_device_method, 12
- iot, 5
- iot1clickdevicesservice, 11
- iot1clickprojects, 12
- iotanalytics, 14
- iotdataplane, 16
- iotjobsdataplane, 17
- list_active_violations, 8
- list_attached_policies, 8
- list_audit_findings, 9
- list_audit_mitigation_actions_executions, 9
- list_audit_mitigation_actions_tasks, 9
- list_audit_suppressions, 9
- list_audit_tasks, 9
- list_authorizers, 9
- list_billing_groups, 9
- list_bulk_deployment_detailed_reports, 4
- list_bulk_deployments, 4
- list_ca_certificates, 9
- list_certificates, 9
- list_certificates_by_ca, 9
- list_channels, 15
- list_connector_definition_versions, 4
- list_connector_definitions, 4
- list_core_definition_versions, 4
- list_core_definitions, 4
- list_custom_metrics, 9
- list_dataset_contents, 15
- list_datasets, 15
- list_datastores, 15
- list_deployments, 4
- list_detect_mitigation_actions_executions, 9

list_detect_mitigation_actions_tasks, 9

list_device_definition_versions, 4

list_device_definitions, 4

list_device_events, 12

list_devices, 12

list_dimensions, 9

list_domain_configurations, 9

list_function_definition_versions, 4

list_function_definitions, 4

list_group_certificate_authorities, 4

list_group_versions, 4

list_groups, 4

list_indices, 9

list_job_executions_for_job, 9

list_job_executions_for_thing, 9

list_jobs, 9

list_logger_definition_versions, 4

list_logger_definitions, 4

list_mitigation_actions, 9

list_named_shadows_for_thing, 17

list_ota_updates, 9

list_outgoing_certificates, 9

list_pipelines, 15

list_placements, 13

list_policies, 9

list_policy_principals, 9

list_policy_versions, 9

list_principal_policies, 9

list_principal_things, 9

list_profile_permissions, 20

list_projects, 13

list_provisioning_template_versions, 9

list_provisioning_templates, 9

list_resource_definition_versions, 4

list_resource_definitions, 4

list_role_aliases, 9

list_scheduled_audits, 9

list_security_profiles, 9

list_security_profiles_for_target, 9

list_signing_jobs, 20

list_signing_platforms, 20

list_signing_profiles, 20

list_streams, 9

list_subscription_definition_versions, 4

list_subscription_definitions, 4

list_tags_for_resource, 4, 9, 12, 13, 15, 20

list_targets_for_policy, 9

list_targets_for_security_profile, 9

list_thing_groups, 9

list_thing_groups_for_thing, 9

list_thing_principals, 9

list_thing_registration_task_reports, 9

list_thing_registration_tasks, 9

list_thing_types, 9

list_things, 9

list_things_in_billing_group, 9

list_things_in_thing_group, 9

list_topic_rule_destinations, 9

list_topic_rules, 9

list_v2_logging_levels, 10

list_violation_events, 10

publish, 17

put_logging_options, 15

put_signing_profile, 20

register_ca_certificate, 10

register_certificate, 10

register_certificate_without_ca, 10

register_thing, 10

reject_certificate_transfer, 10

remove_profile_permission, 20

remove_thing_from_billing_group, 10

remove_thing_from_thing_group, 10

replace_topic_rule, 10

reset_deployments, 4

revoke_signature, 20

revoke_signing_profile, 20

run_pipeline_activity, 15

sample_channel_data, 15

search_index, 10

set_default_authorizer, 10

set_default_policy_version, 10

set_logging_options, 10

set_v2_logging_level, 10

set_v2_logging_options, 10

signer, 19

start_audit_mitigation_actions_task, 10

start_bulk_deployment, 4

start_detect_mitigation_actions_task, 10

start_next_pending_job_execution, 18

start_on_demand_audit_task, [10](#)
start_pipeline_reprocessing, [15](#)
start_signing_job, [20](#)
start_thing_registration_task, [10](#)
stop_bulk_deployment, [4](#)
stop_thing_registration_task, [10](#)

tag_resource, [4](#), [10](#), [12](#), [13](#), [15](#), [20](#)
test_authorization, [10](#)
test_invoke_authorizer, [10](#)
transfer_certificate, [10](#)

unclaim_device, [12](#)
untag_resource, [4](#), [10](#), [12](#), [13](#), [16](#), [20](#)
update_account_audit_configuration, [10](#)
update_audit_suppression, [10](#)
update_authorizer, [10](#)
update_billing_group, [10](#)
update_ca_certificate, [10](#)
update_certificate, [10](#)
update_channel, [16](#)
update_connectivity_info, [4](#)
update_connector_definition, [4](#)
update_core_definition, [4](#)
update_custom_metric, [10](#)
update_dataset, [16](#)
update_datastore, [16](#)
update_device_definition, [4](#)
update_device_state, [12](#)
update_dimension, [10](#)
update_domain_configuration, [10](#)
update_dynamic_thing_group, [10](#)
update_event_configurations, [10](#)
update_function_definition, [4](#)
update_group, [4](#)
update_group_certificate_configuration,
[4](#)
update_indexing_configuration, [10](#)
update_job, [10](#)
update_job_execution, [18](#)
update_logger_definition, [5](#)
update_mitigation_action, [10](#)
update_pipeline, [16](#)
update_placement, [13](#)
update_project, [13](#)
update_provisioning_template, [10](#)
update_resource_definition, [5](#)
update_role_alias, [10](#)
update_scheduled_audit, [10](#)
update_security_profile, [10](#)
update_stream, [10](#)
update_subscription_definition, [5](#)
update_thing, [10](#)
update_thing_group, [10](#)
update_thing_groups_for_thing, [10](#)
update_thing_runtime_configuration, [5](#)
update_thing_shadow, [17](#)
update_topic_rule_destination, [11](#)
validate_security_profile_behaviors,
[11](#)