>

Feedback Preferences 📀

Service Authorization < Reference

Service Authorization Reference

Actions, resources, and condition keys for AWS IAM Identity Center (successor to AWS Single Sign-On)

PDF

Documentation > Service Authorization Reference > Service Authorization Reference

AWS IAM Identity Center (successor to AWS Single Sign-On) (service prefix: sso) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS IAM Identity
 Center (successor to AWS Single Sign-On)
- Resource types defined by AWS IAM Identity Center (successor to AWS Single Sign-On)
- Condition keys for AWS IAM Identity Center (successor to AWS Single Sign-On)

Actions defined by AWS IAM Identity Center (successor to AWS Single Sign-On)

You can specify the following actions in the Action element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single

On this page

Actions

Resource types

Q

Contact Us

Create an AWS Account

Feedback 📮

Preferences 📀

Documentation > Service Authorization Reference > Service Authorization Reference rne <mark>kesource types</mark> column or the Actions

> table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the Resource element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's Condition element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

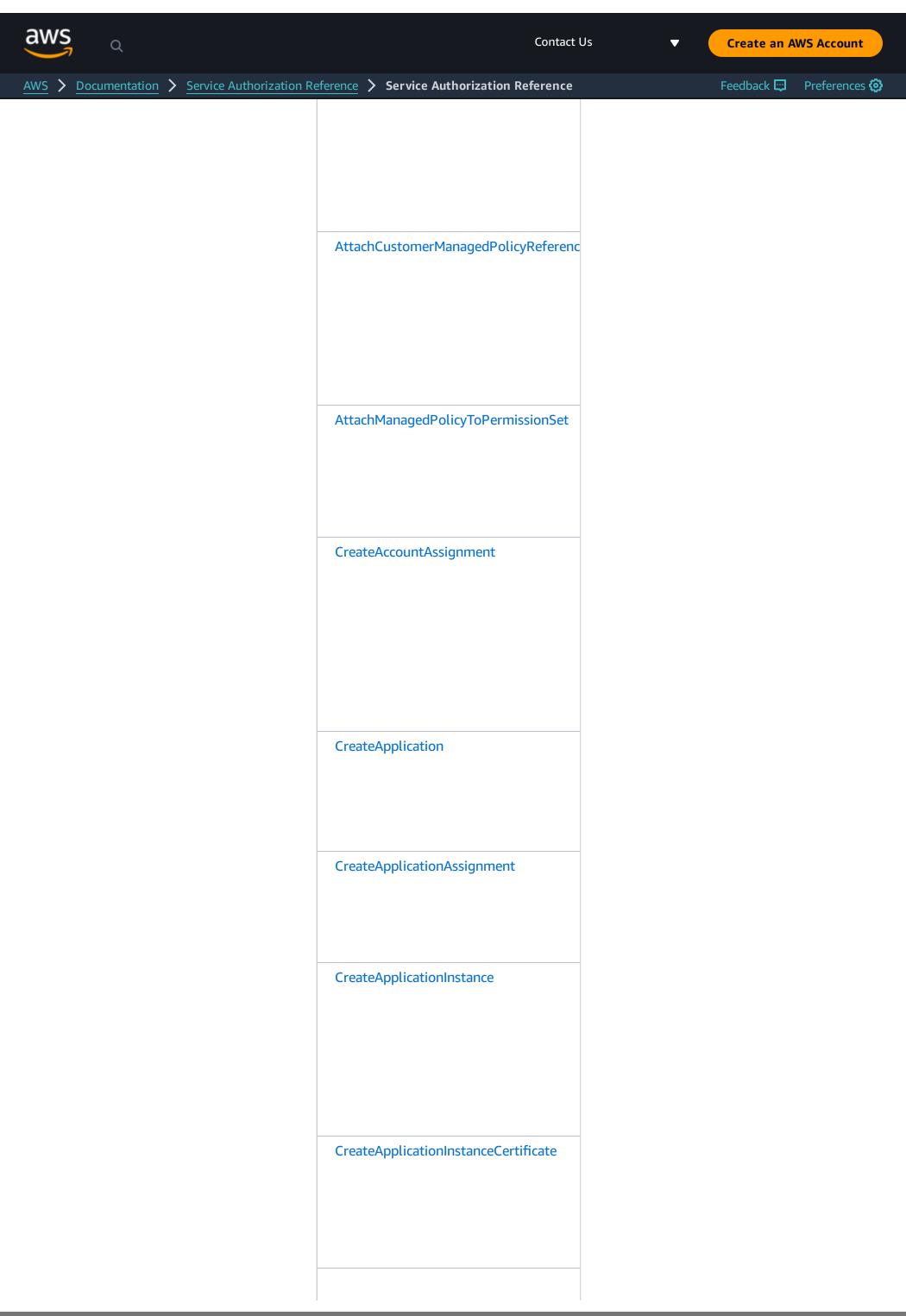
Note

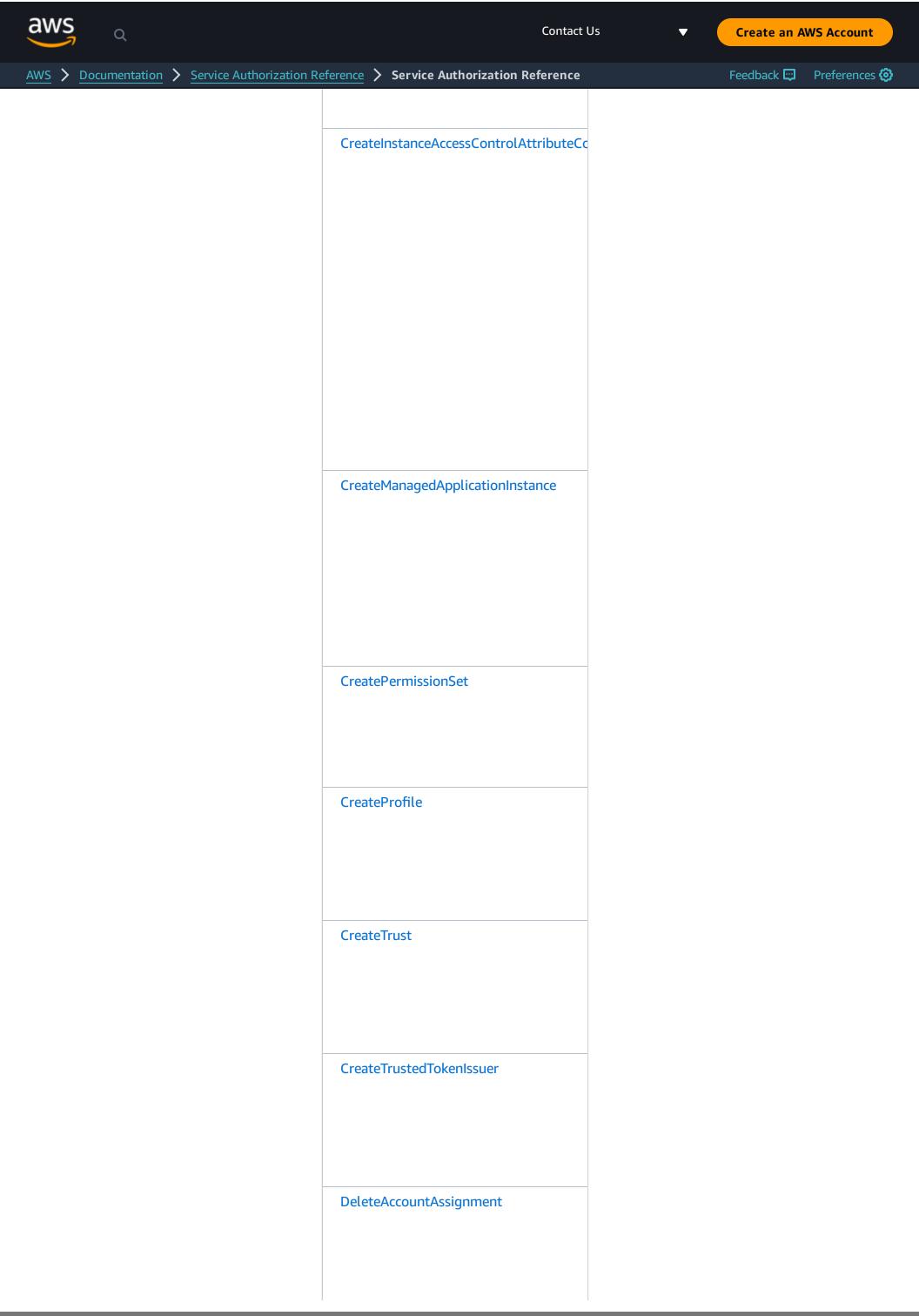
Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types** (*required) column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

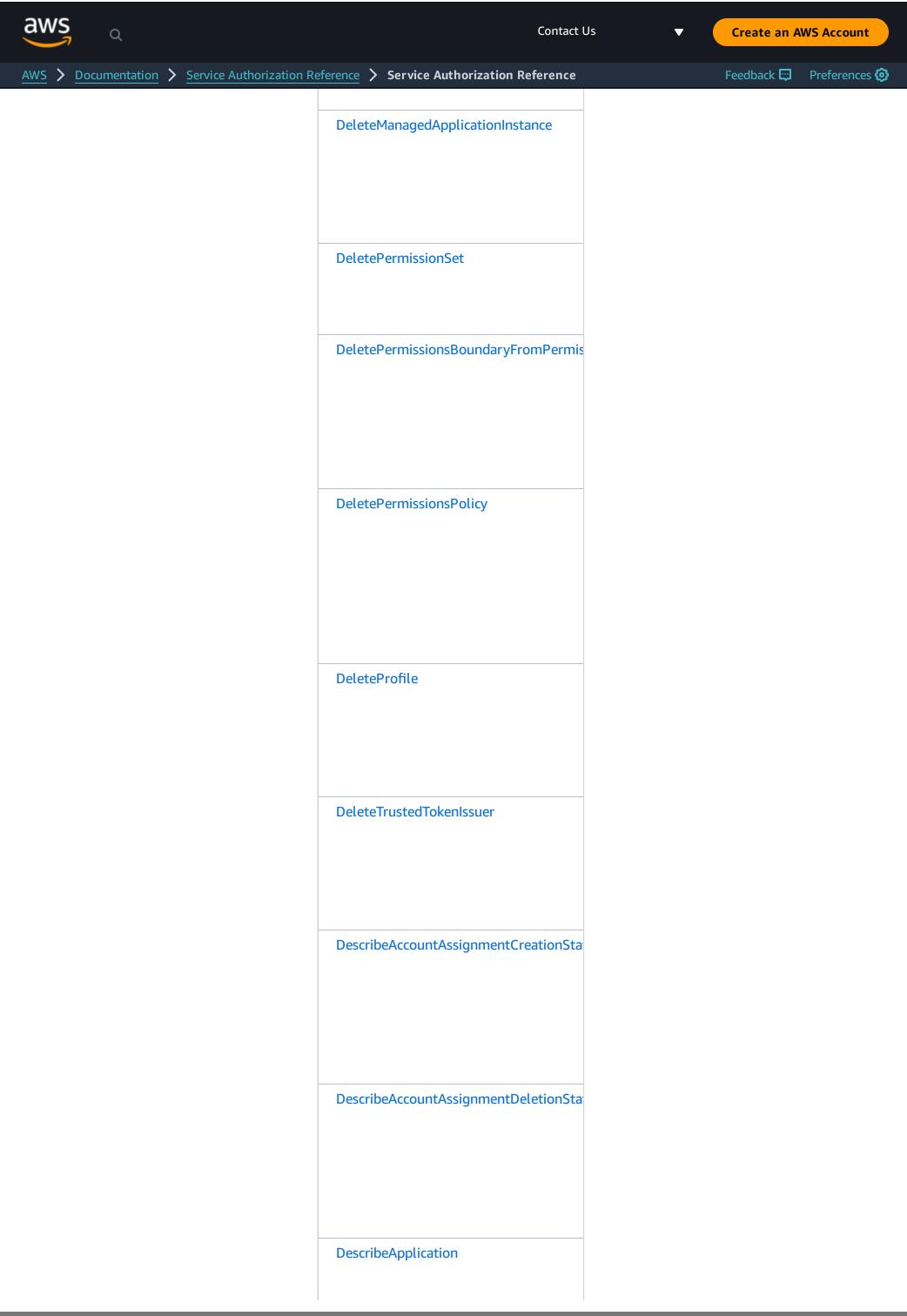
Actions

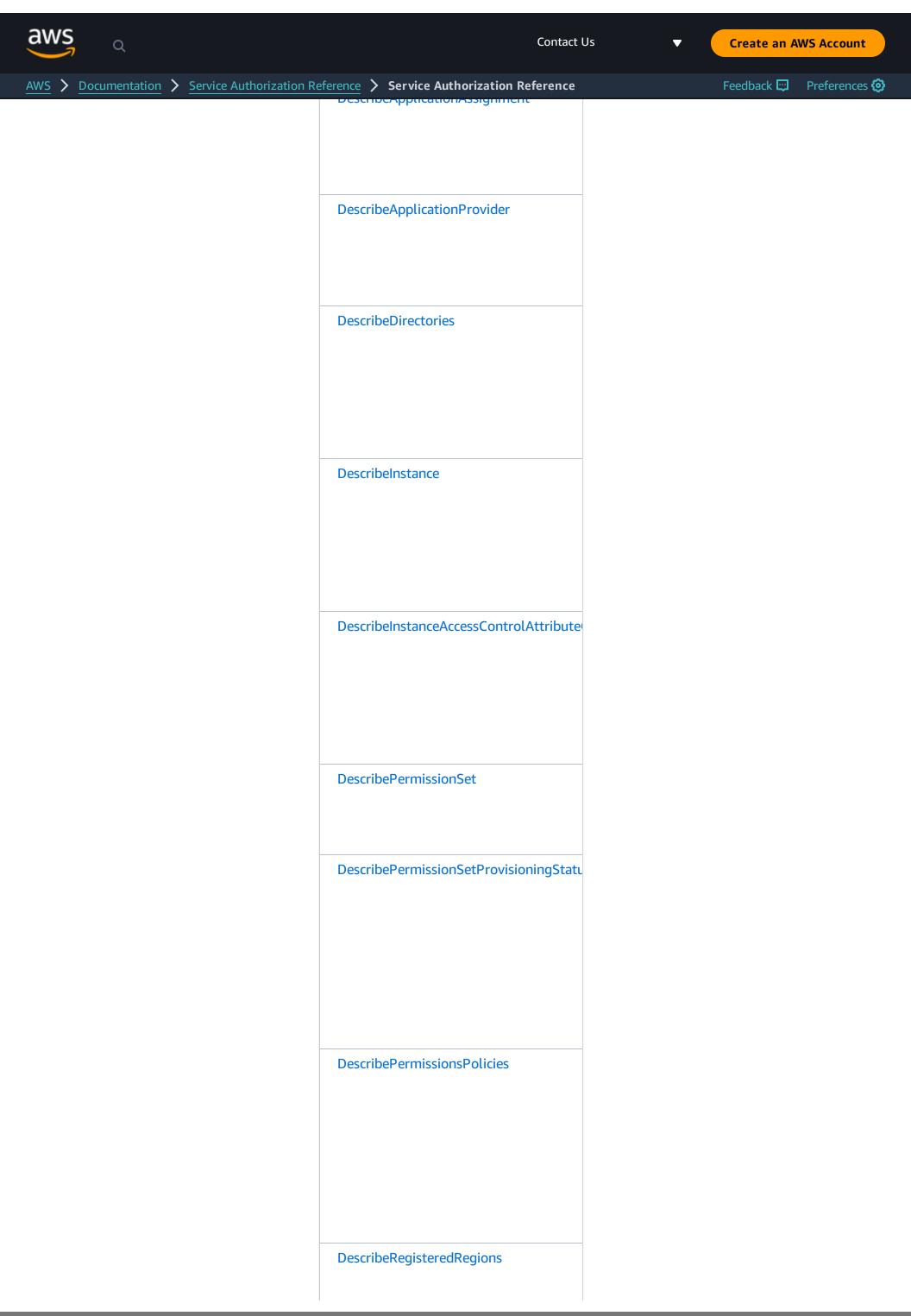
AssociateDirectory

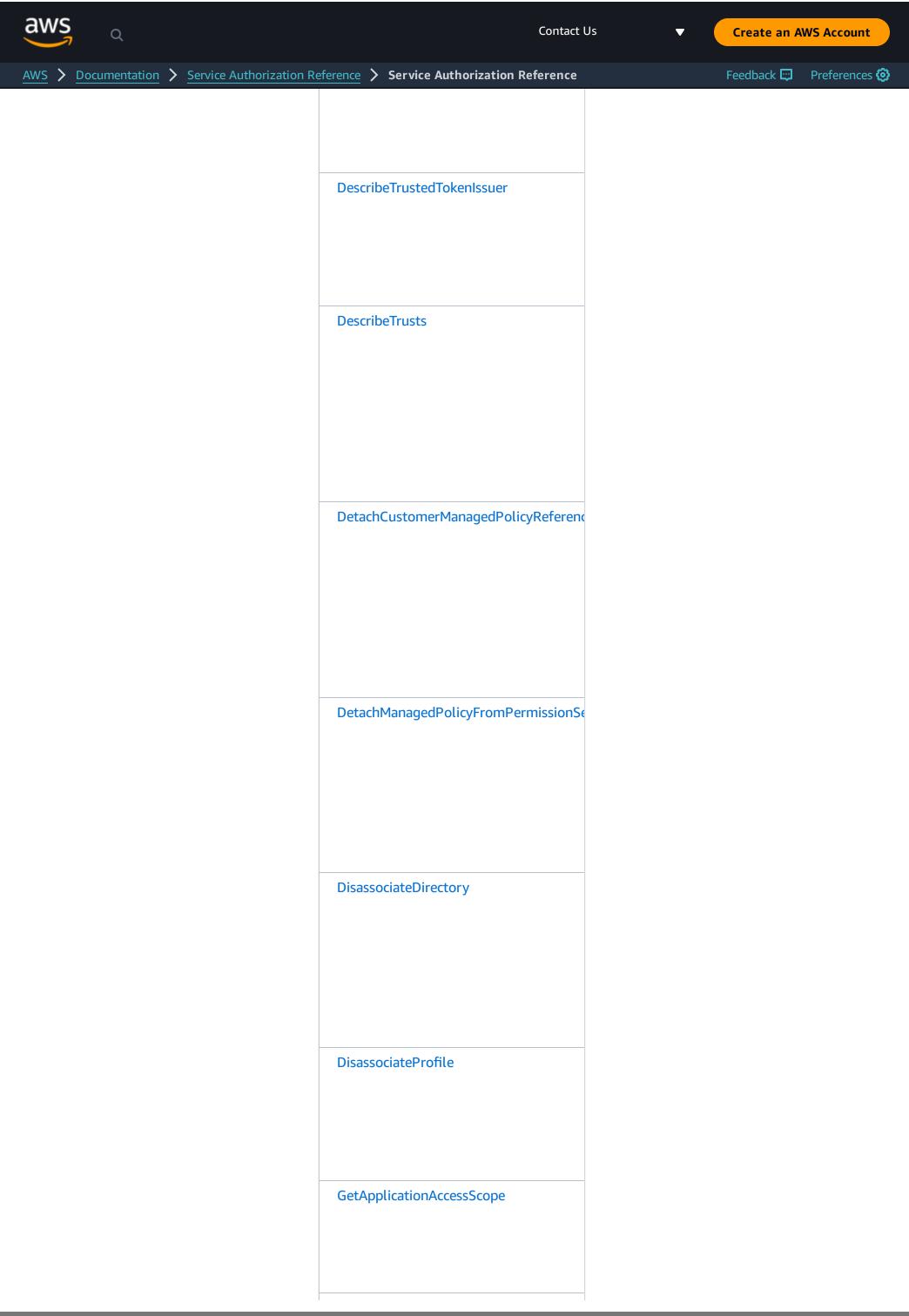


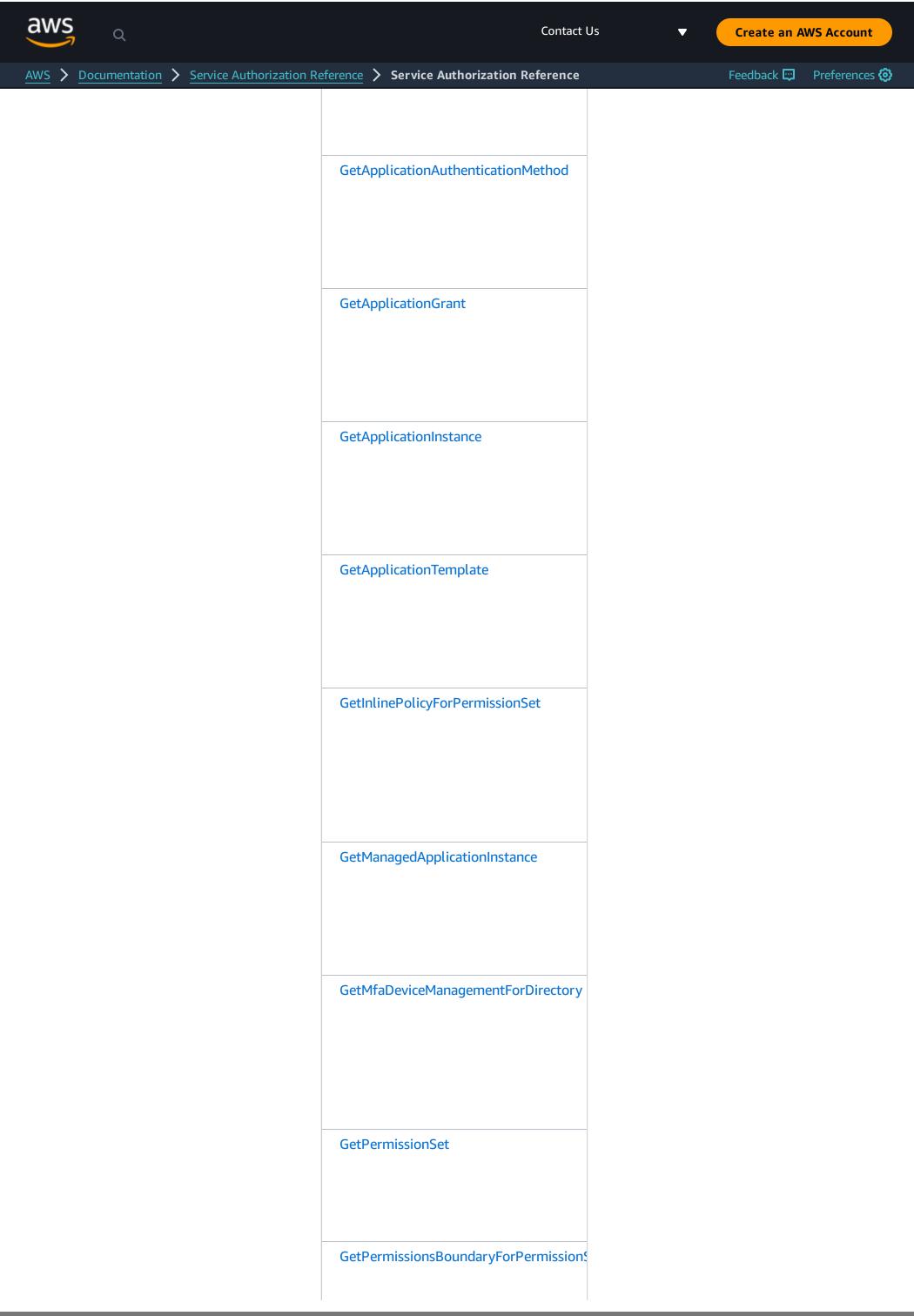


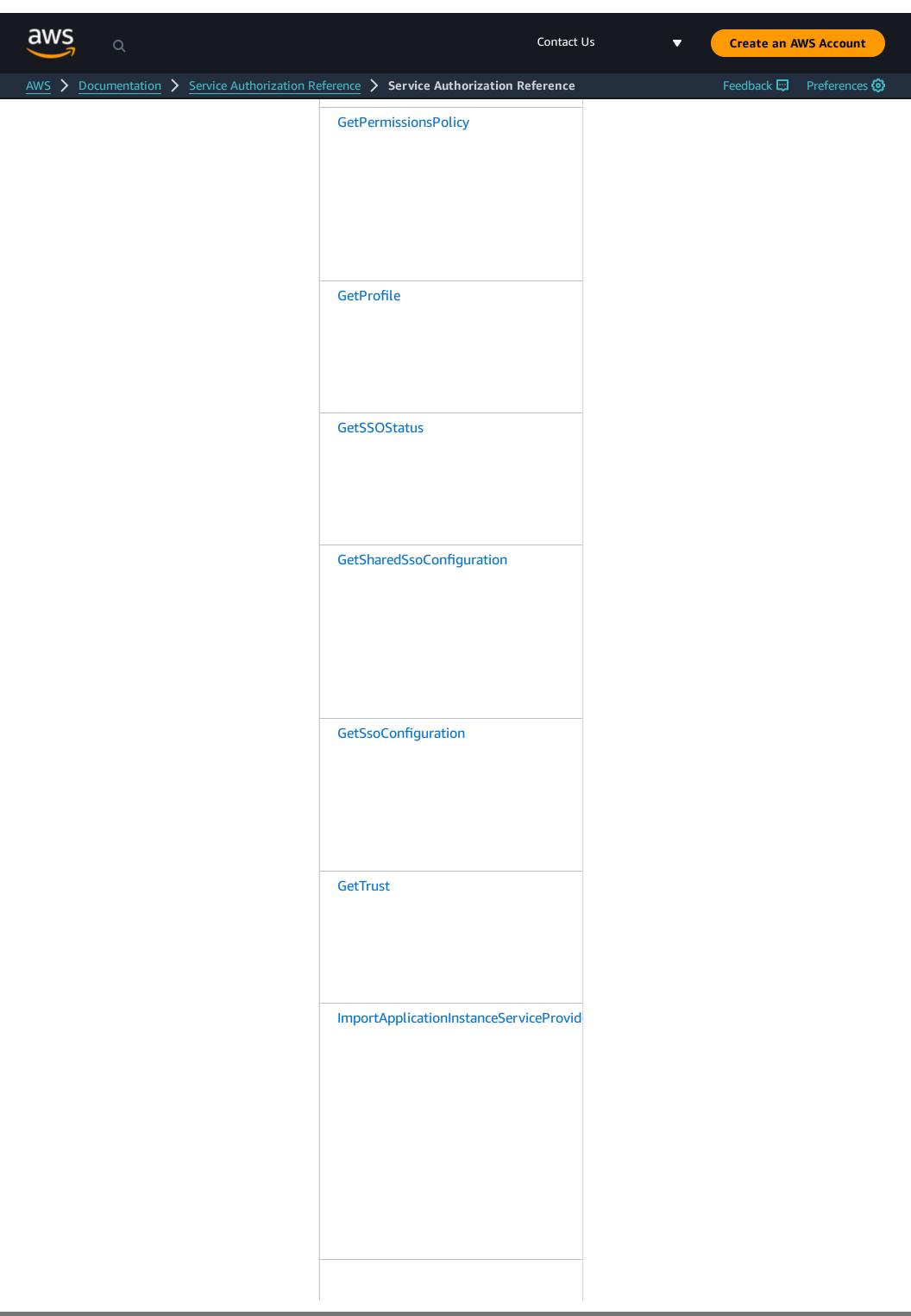


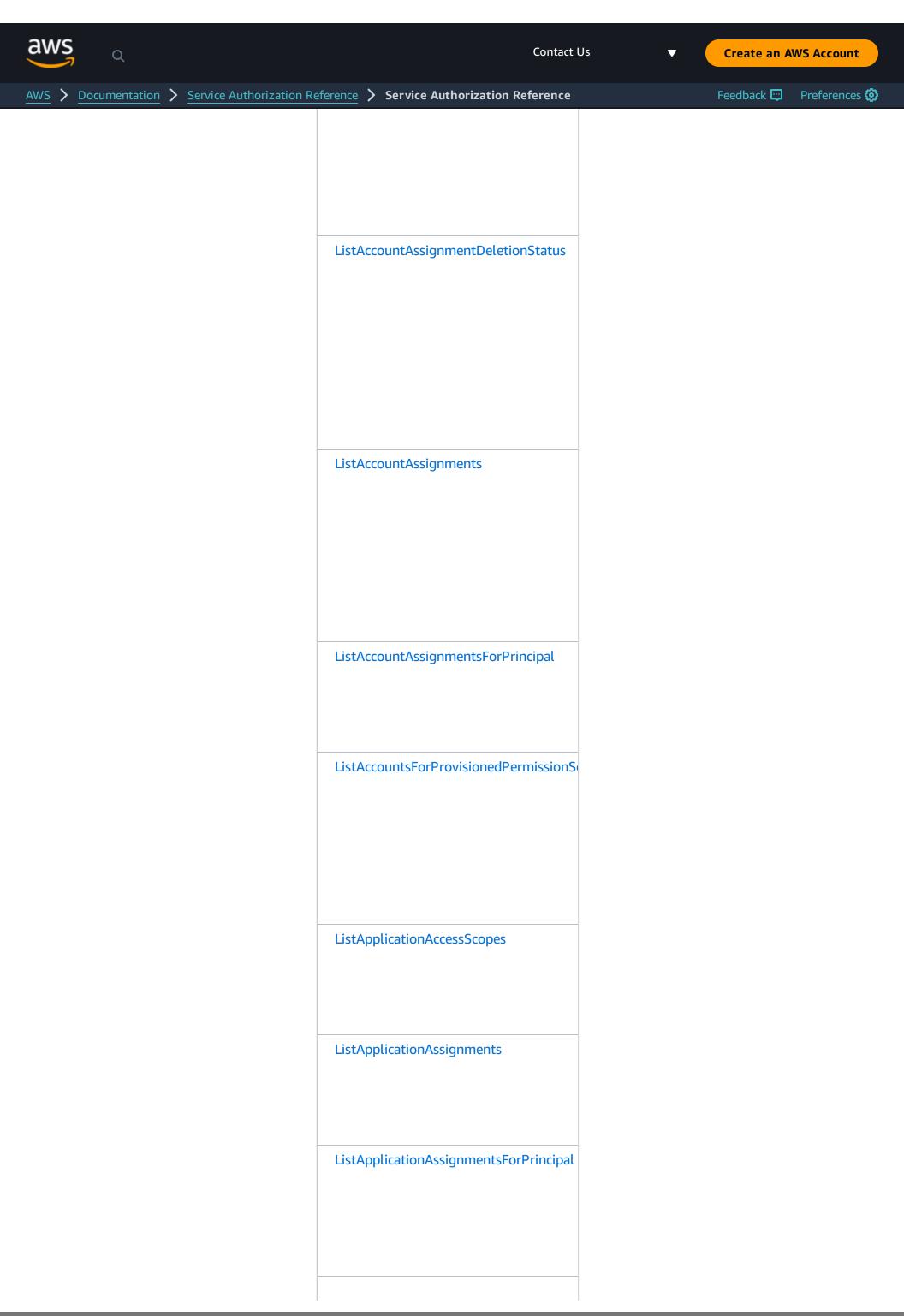


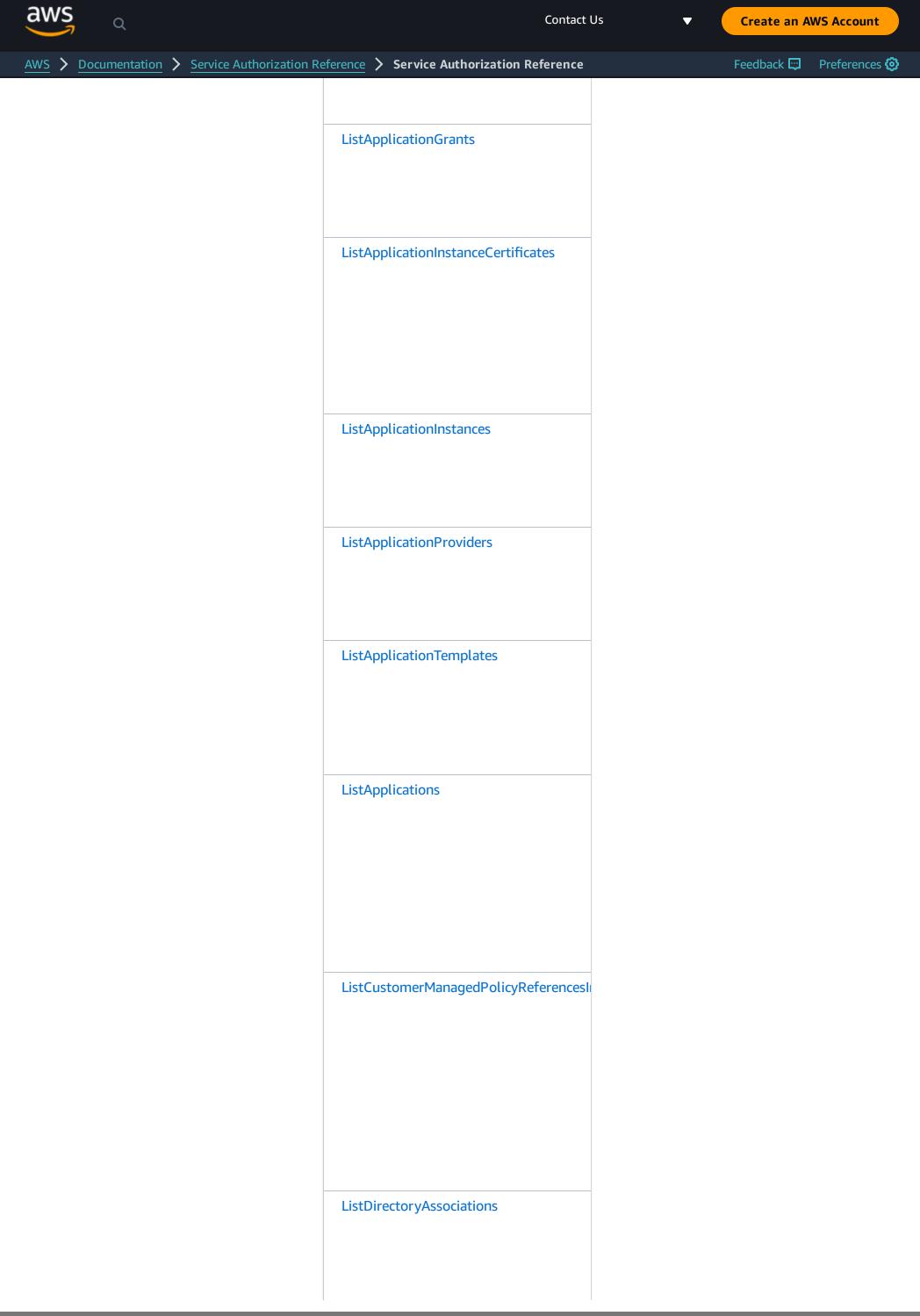


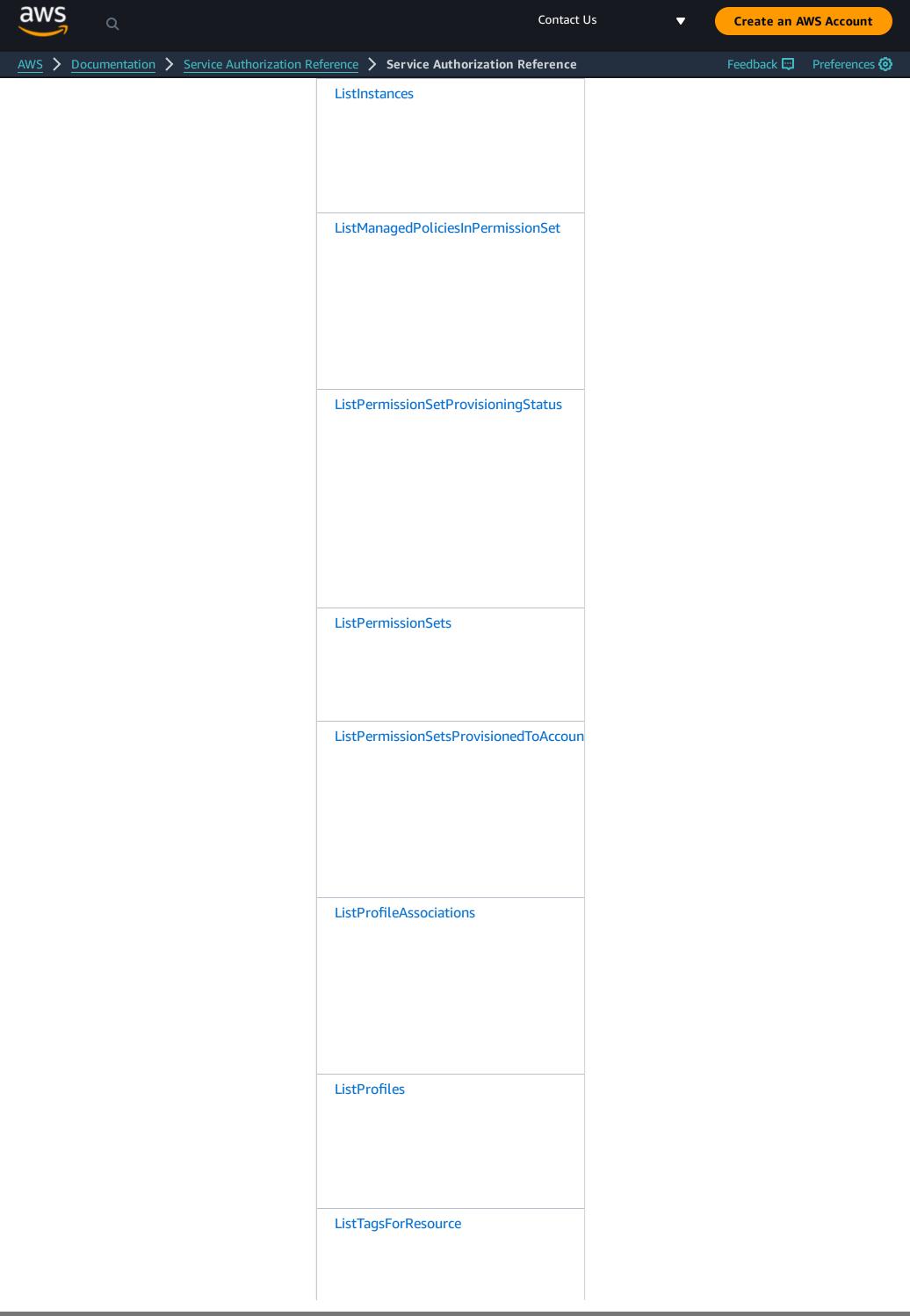


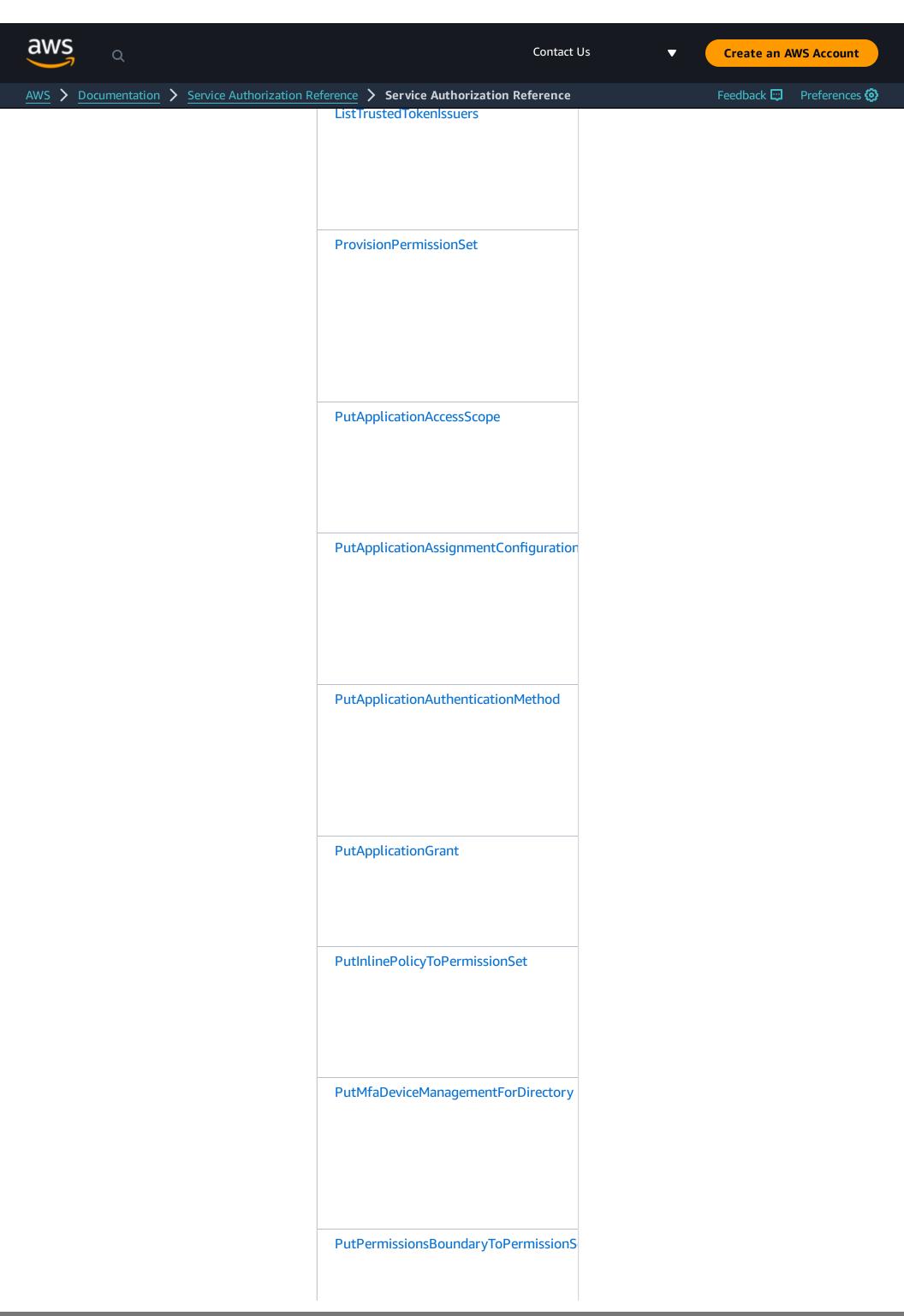


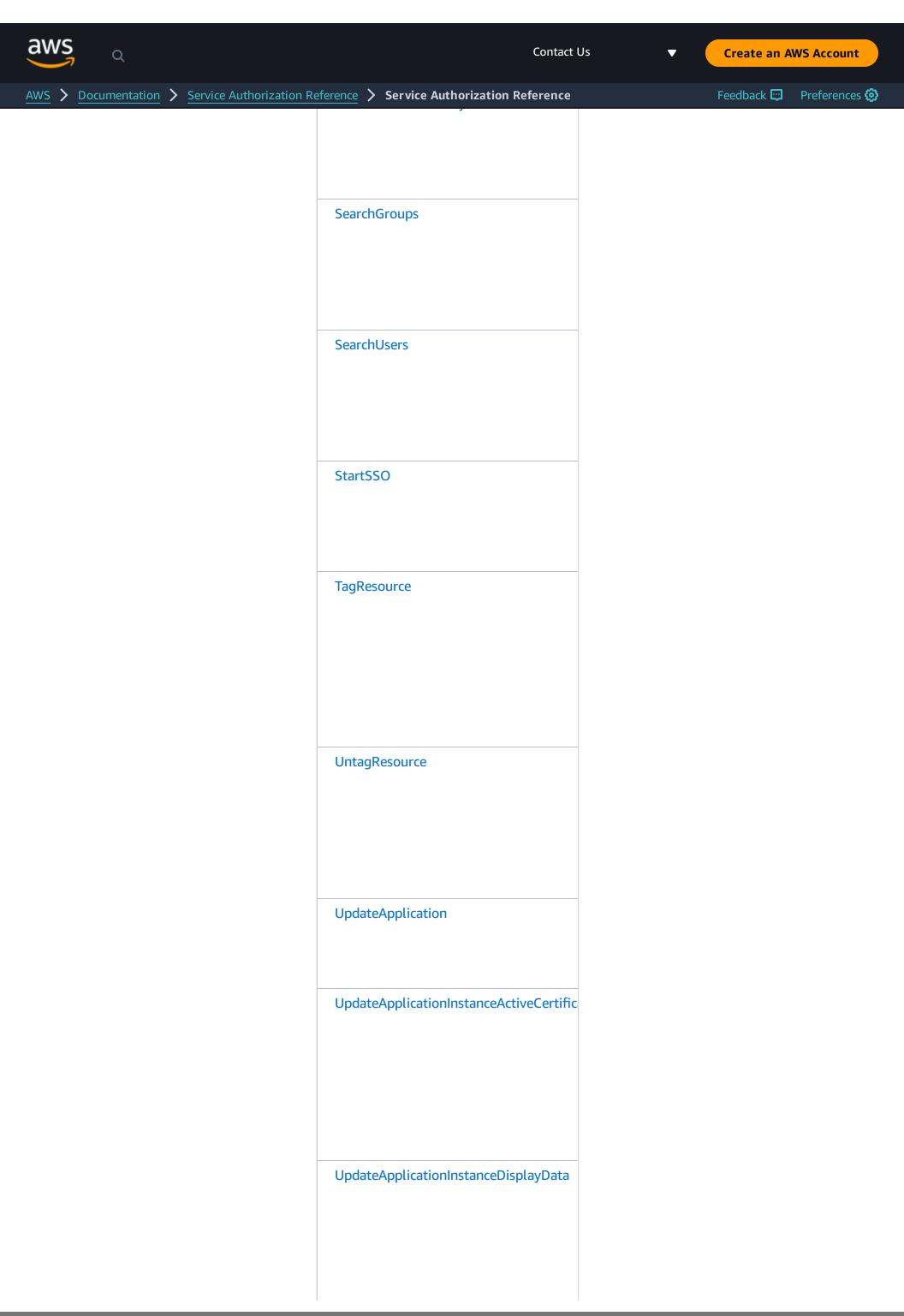




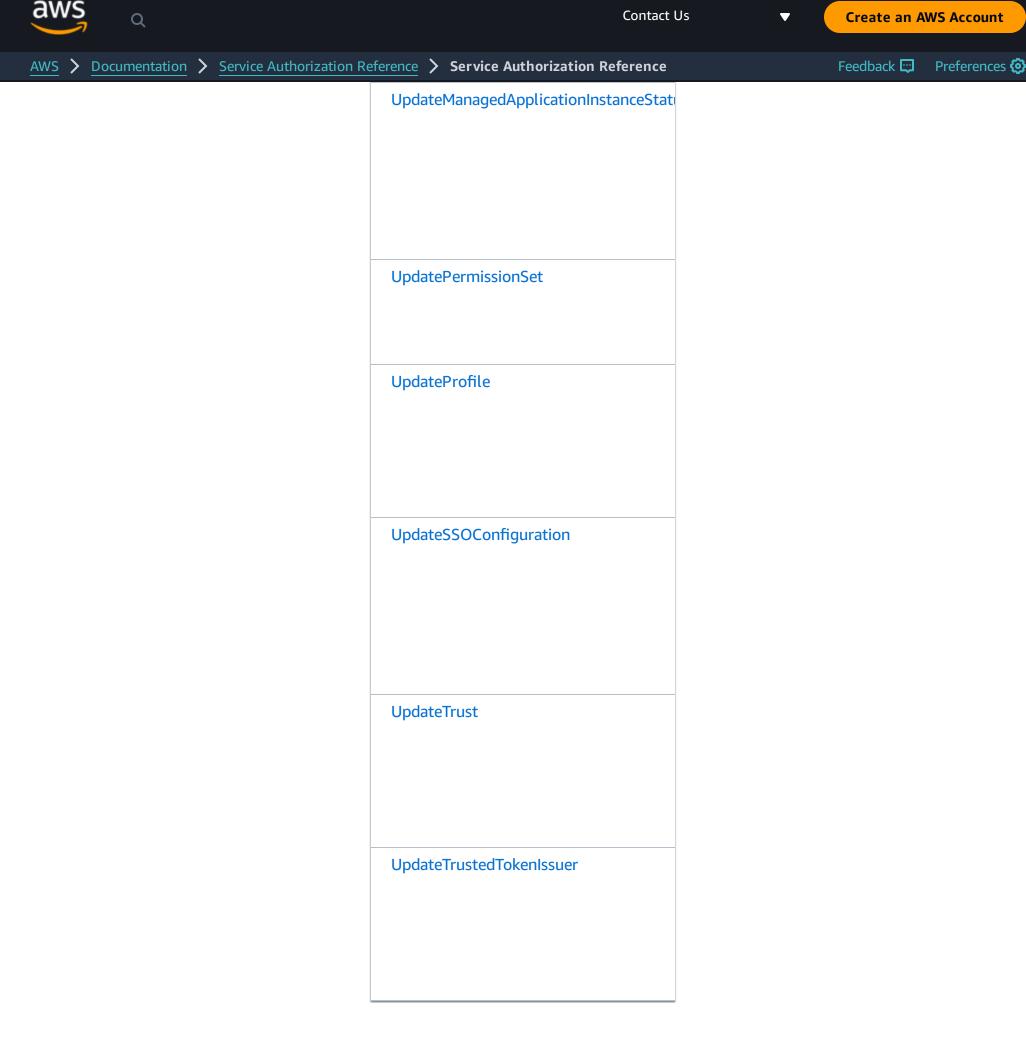












Resource types defined by AWS IAM Identity Center (successor to AWS Single Sign-On)

The following resource types are defined by this service and can be used in the Resource element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details

Contact Us

Create an AWS Account

Feedback Preferences 📀

AWS > Documentation > Service Authorization Reference > Service Authorization Reference		
	Resource types	71111
	PermissionSet	arn:\${Parti1
	Account	arn:\${Parti1
	Instance	arn:\${Partit
	Application	arn:\${Partit
	TrustedTokenIssuer	arn:\${Partit
	ApplicationProvider	arn:\${Partit

Condition keys for AWS IAM Identity Center (successor to AWS Single Sign-On)

AWS IAM Identity Center (successor to AWS Single Sign-On) defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see Available global condition keys.

Condition keys	Descr
aws:RequestTag/\${TagKey}	Filters access the ta that a passed the re
aws:ResourceTag/\${TagKey}	Filters access the ta associ with t resou
aws:TagKeys	Filters access the ta that a passed the re
sso:ApplicationAccount	Filters access the ac

Did this page help you?

AWS > Documentation > Service Authorization Reference > Service Authorization Reference



Provide feedback

Next

topic: AWS

Feedback 📮

Preferences 📀

IAM Identity

Center

(successor to AWS Single

Sign-On) directory

Previous

topic: AWS IAM Access Analyzer

Need help?

- Try AWS re:Post ☑
- Connect with an AWS IQ expert

Privacy | Site terms | Cookie preferences | © 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.