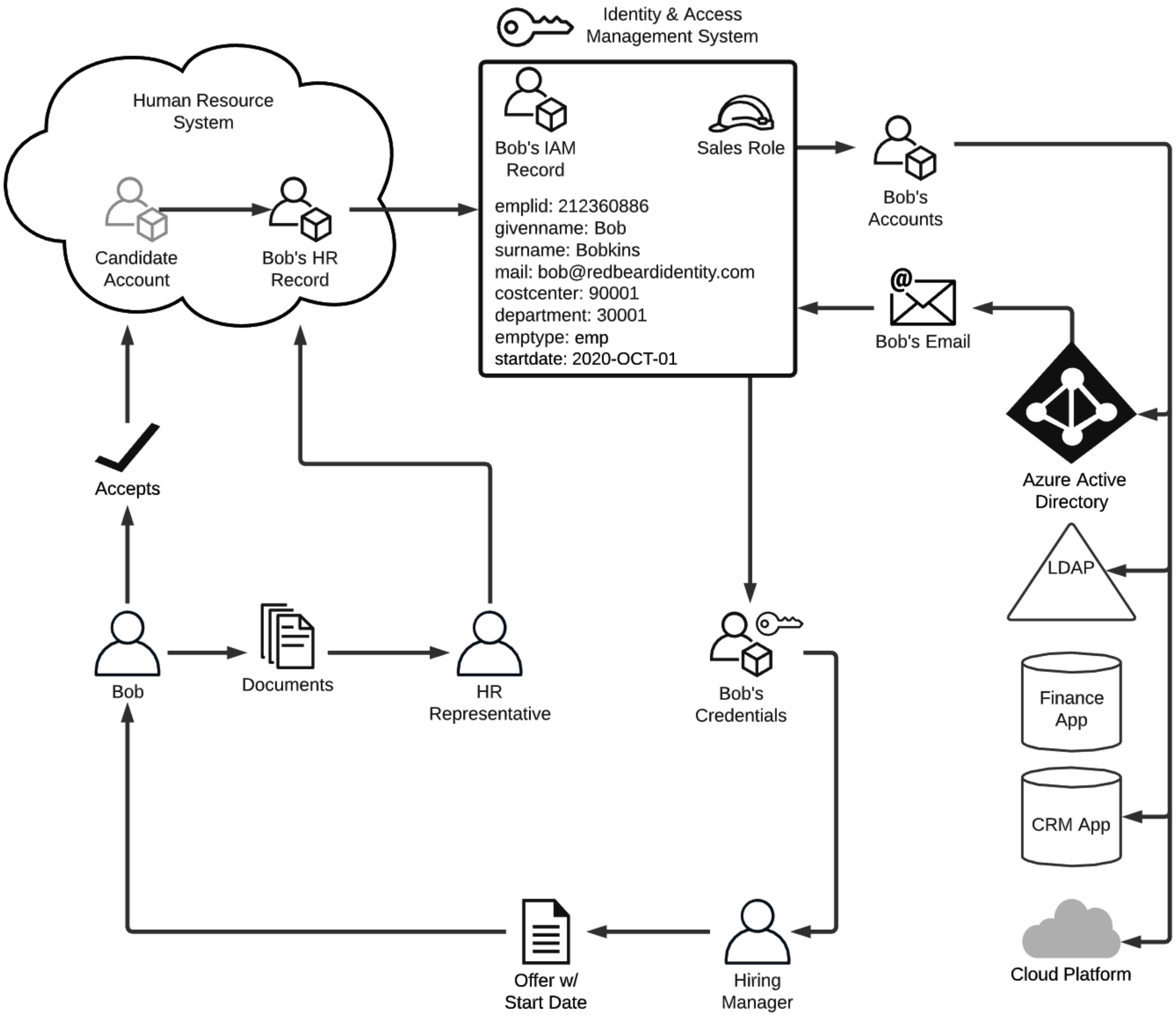
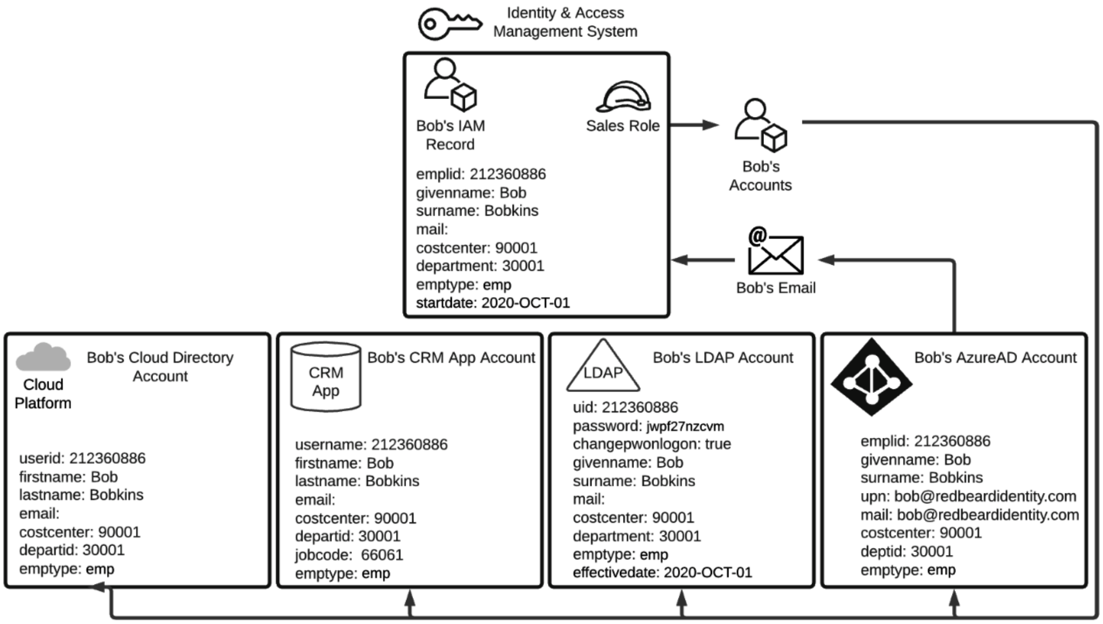
Chapter 1: An Introduction to IAM and AWS IAM Concepts



emplid: 212360886
givenname: Bob
surname: Bobkins
mail: bob@redbeardidentity.com
costcenter: 90001
department: 30001
emptype: emp
startdate: 2020-OCT-01



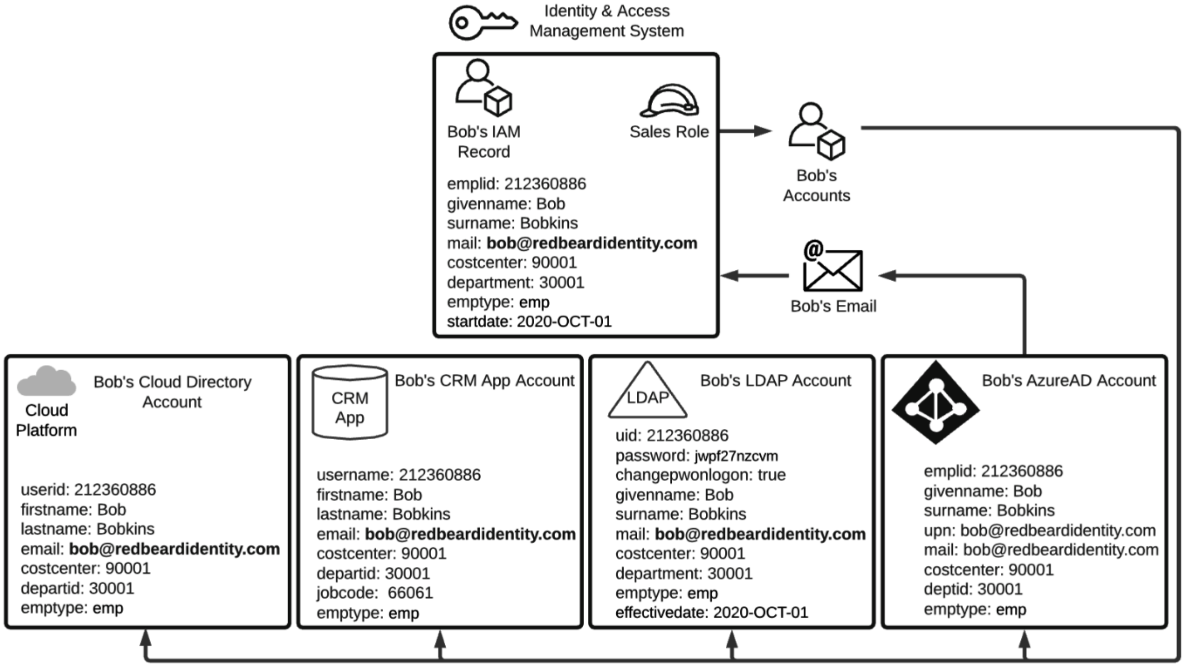
emplid: 212360886
givenname: Bob
surname: Bobkins
mail:
costcenter: 90001
department: 30001
emptype: emp
startdate: 2020-OCT-01

userid: 212360886
firstname: Bob
lastname: Bobkins
email:
costcenter: 90001
departid: 30001
emptype: emp

username: 212360886
firstname: Bob
lastname: Bobkins
email:
costcenter: 90001
departid: 30001
jobcode: 66061
emptype: emp

uid: 212360886
password: jwpf27nzcvm
changepwonlogon: true
givenname: Bob
surname: Bobkins
mail:
costcenter: 90001
department: 30001
emptype: emp
effectivedate: 2020-OCT-01

emplid: 212360886
givenname: Bob
surname: Bobkins
upn: bob@redbeardidentity.com
mail: bob@redbeardidentity.com
costcenter: 90001
deptid: 30001
emptype: emp



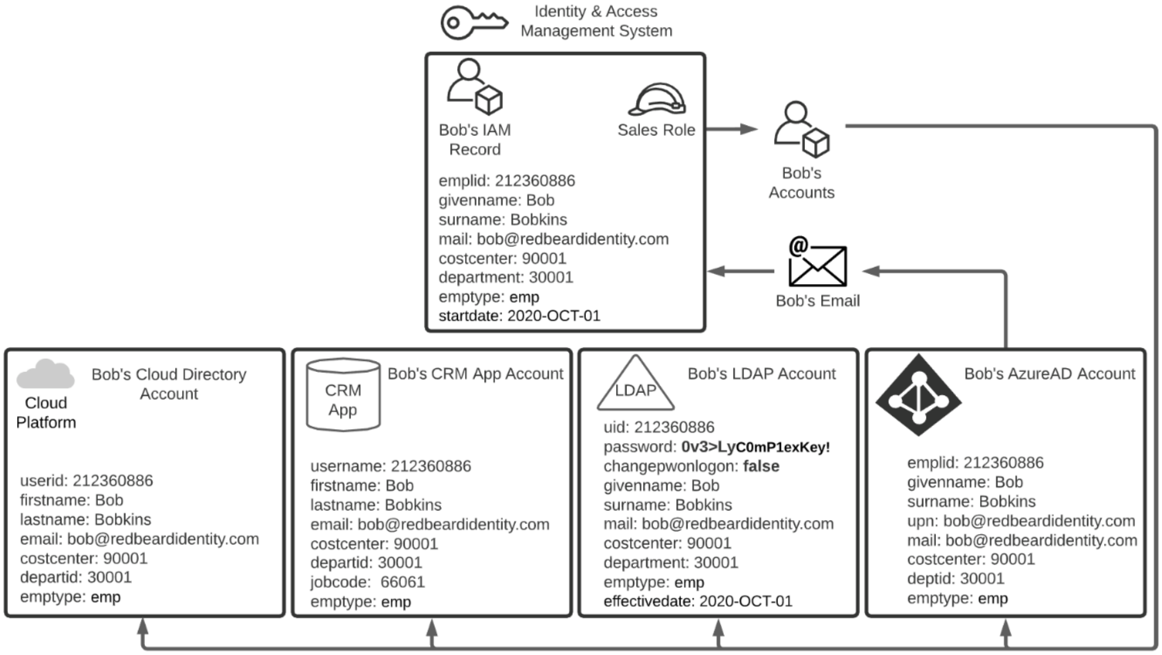
emplid: 212360886
givenname: Bob
surname: Bobkins
mail: **bob@redbeardidentity.com**
costcenter: 90001
department: 30001
emptype: emp
startdate: 2020-OCT-01

userid: 212360886
firstname: Bob
lastname: Bobkins
email: **bob@redbeardidentity.com**
costcenter: 90001
departid: 30001
emptype: emp

username: 212360886
firstname: Bob
lastname: Bobkins
email: **bob@redbeardidentity.com**
costcenter: 90001
departid: 30001
jobcode: 66061
emptype: emp

uid: 212360886
password: jwpf27nzcvm
changepwonlogon: true
givenname: Bob
surname: Bobkins
mail: **bob@redbeardidentity.com**
costcenter: 90001
department: 30001
emptype: emp
effectivedate: 2020-OCT-01

emplid: 212360886
givenname: Bob
surname: Bobkins
upn: bob@redbeardidentity.com
mail: bob@redbeardidentity.com
costcenter: 90001
deptid: 30001
emptype: emp



Bob's IAM Record

emplid: 212360886
givenname: Bob
surname: Bobkins
mail: bob@redbeardidentity.com
costcenter: 90001
department: 30001
emptype: emp
startdate: 2020-OCT-01

Bob's Cloud Directory Account

userid: 212360886
firstname: Bob
lastname: Bobkins
email: bob@redbeardidentity.com
costcenter: 90001
departid: 30001
emptype: emp

Bob's CRM App Account

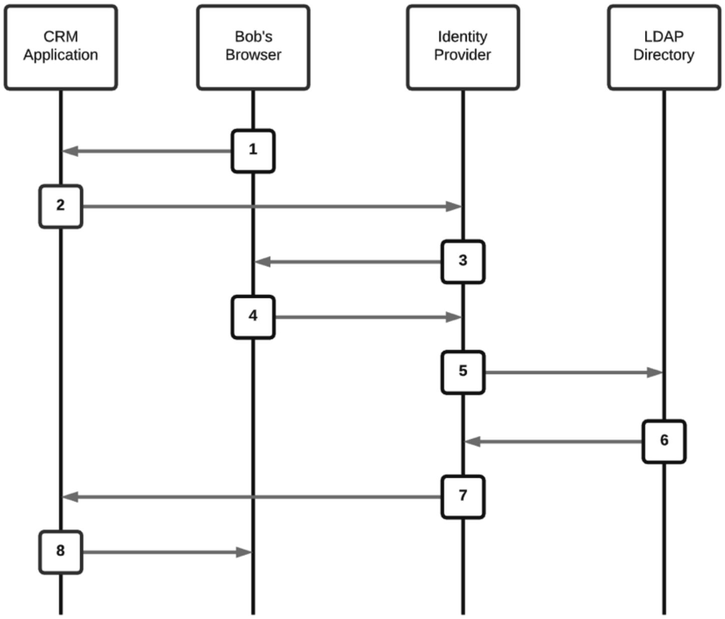
username: 212360886
firstname: Bob
lastname: Bobkins
email: bob@redbeardidentity.com
costcenter: 90001
departid: 30001
jobcode: 66061
emptype: emp

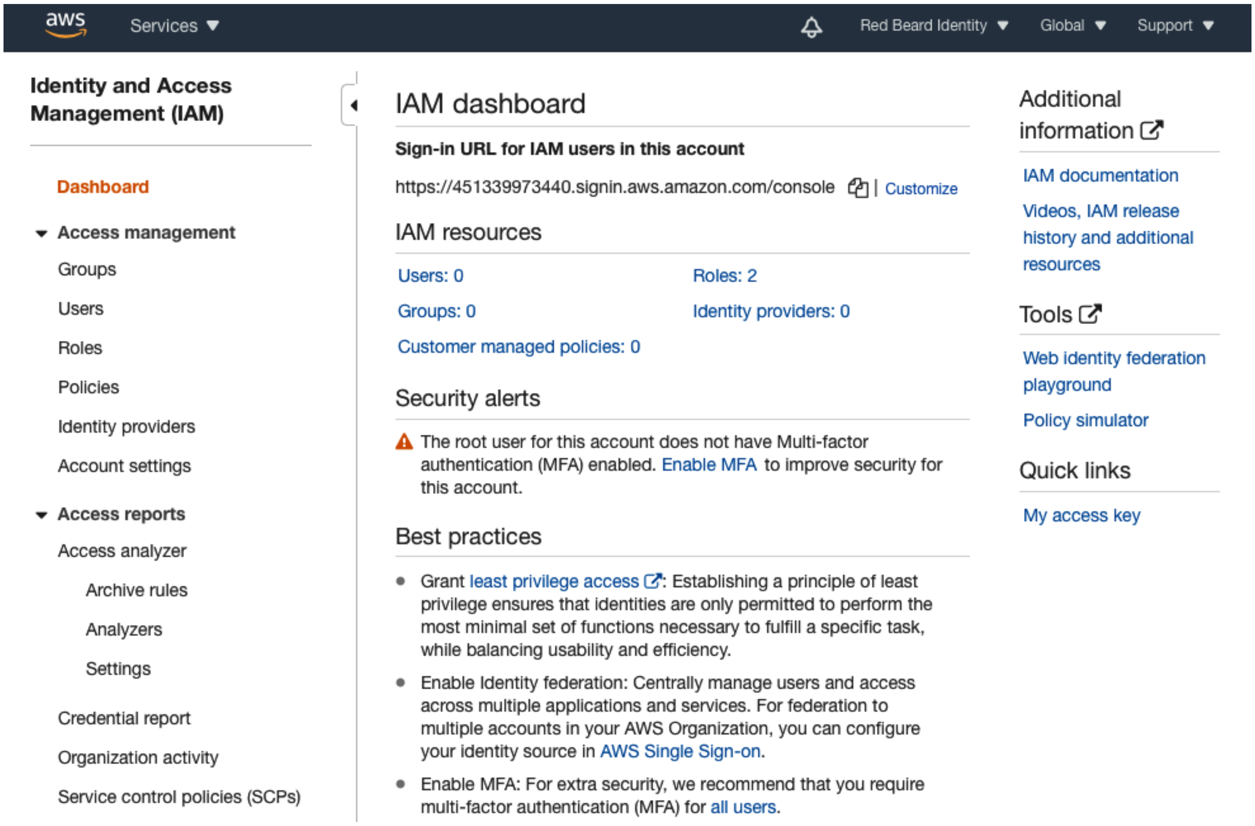
Bob's LDAP Account

uid: 212360886
password: **0v3>LyC0mP1exKey!**
changepwonlogon: **false**
givenname: Bob
surname: Bobkins
mail: bob@redbeardidentity.com
costcenter: 90001
department: 30001
emptype: emp
effectivedate: 2020-OCT-01

Bob's AzureAD Account

emplid: 212360886
givenname: Bob
surname: Bobkins
upn: bob@redbeardidentity.com
mail: bob@redbeardidentity.com
costcenter: 90001
deptid: 30001
emptype: emp





IAM dashboard

Sign-in URL for IAM users in this account

https://451339973440.signin.aws.amazon.com/console | Customize

IAM resources

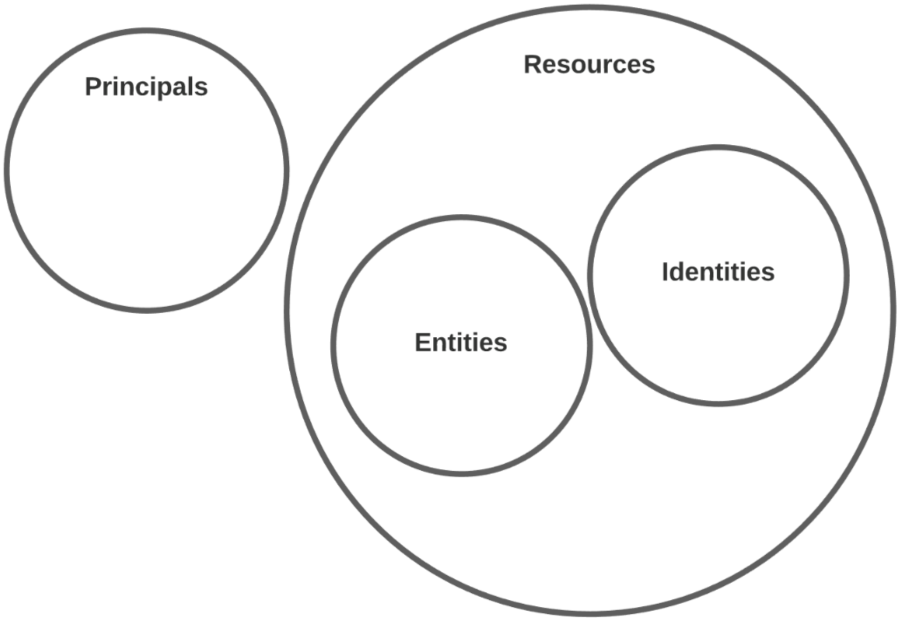
Users: 0	Roles: 2
Groups: 0	Identity providers: 0
Customer managed policies: 0	

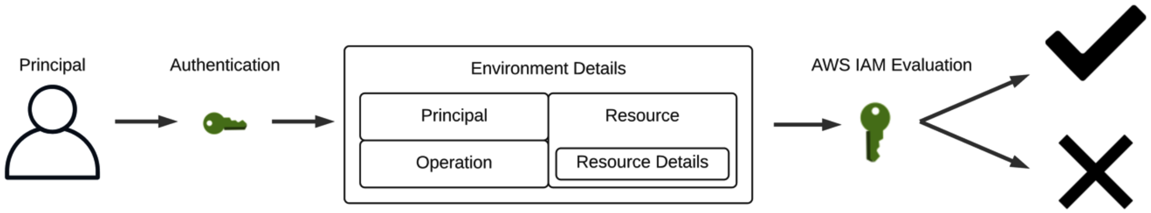
Security alerts

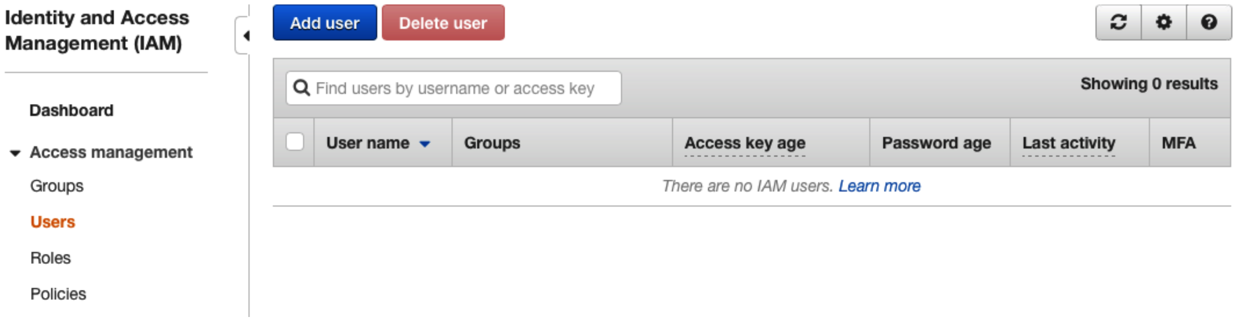
The root user for this account does not have Multi-factor authentication (MFA) enabled. Enable MFA to improve security for this account.

Best practices

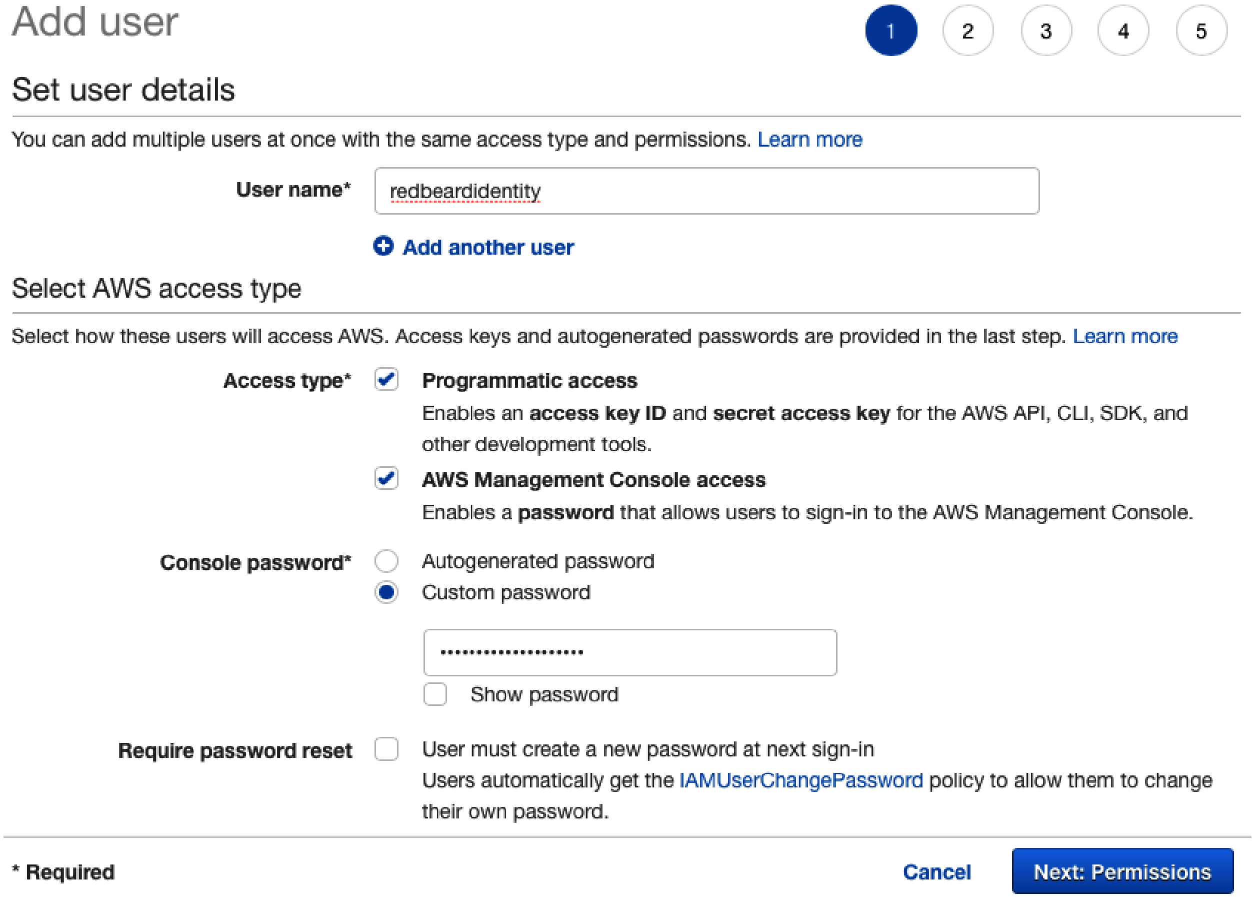
- Grant least privilege access: Establishing a principle of least privilege ensures that identities are only permitted to perform the most minimal set of functions necessary to fulfill a specific task, while balancing usability and efficiency.
- Enable Identity federation: Centrally manage users and access across multiple applications and services. For federation to multiple accounts in your AWS Organization, you can configure your identity source in AWS Single Sign-on.
- Enable MFA: For extra security, we recommend that you require multi-factor authentication (MFA) for all users.







There are no IAM users. Learn more



Add user

Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* redbeardidentity

⊕ Add another user

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

Access type* ☑ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☑ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

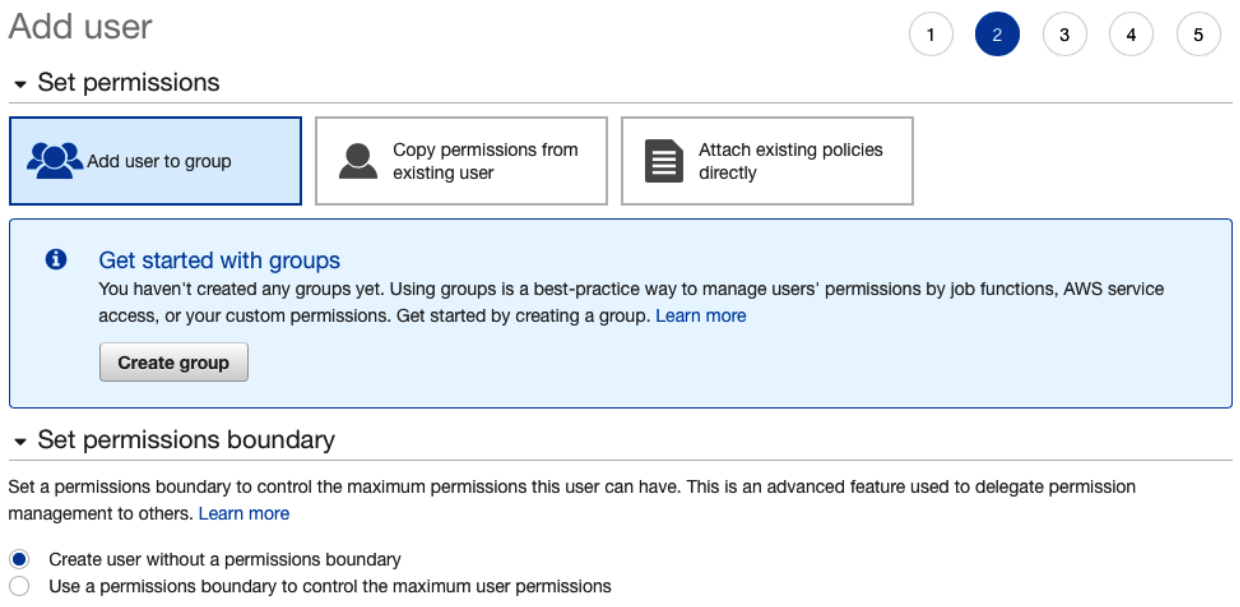
Console password* ○ Autogenerated password
● Custom password

••••••••••••••••••••

□ Show password

Require password reset □ User must create a new password at next sign-in
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

*** Required**



Add user

Set permissions

Add user to group
Copy permissions from existing user
Attach existing policies directly

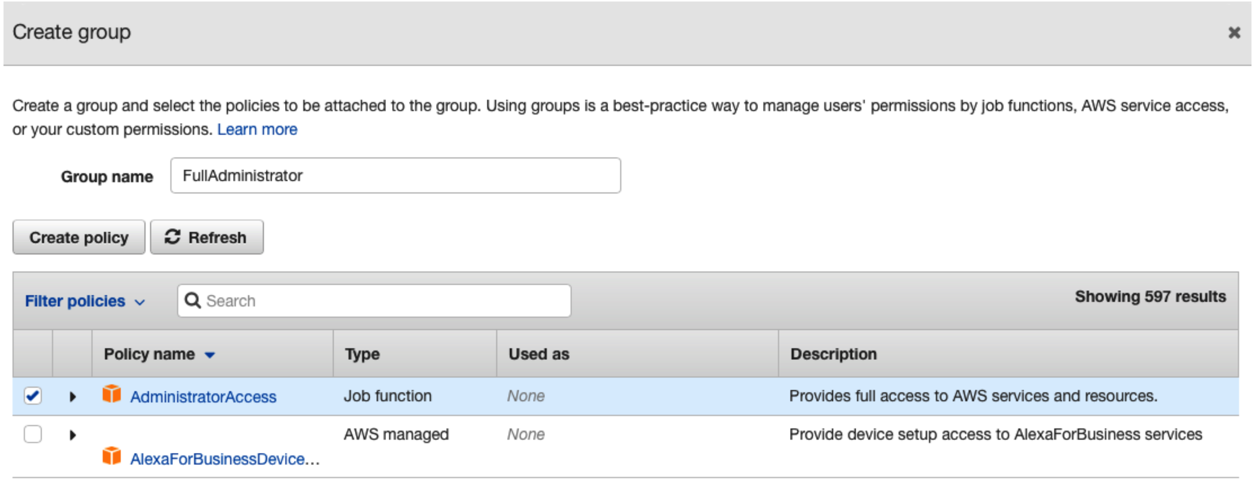
Get started with groups

You haven't created any groups yet. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Get started by creating a group. Learn more

Set permissions boundary

Set a permissions boundary to control the maximum permissions this user can have. This is an advanced feature used to delegate permission management to others. Learn more

● Create user without a permissions boundary
○ Use a permissions boundary to control the maximum user permissions



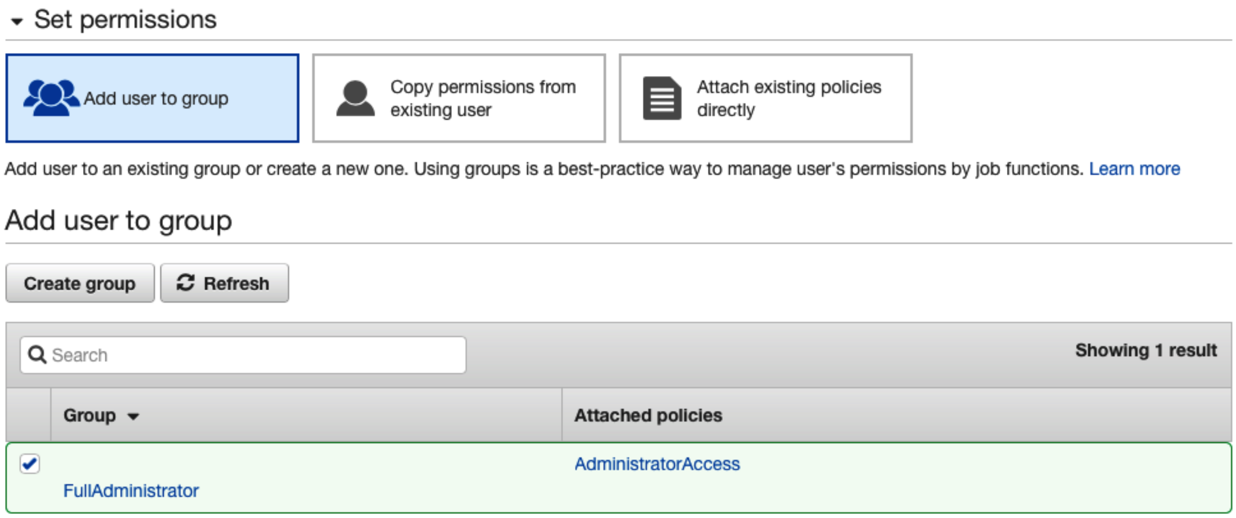
Create group

Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Learn more

Group name FullAdministrator

Showing 597 results

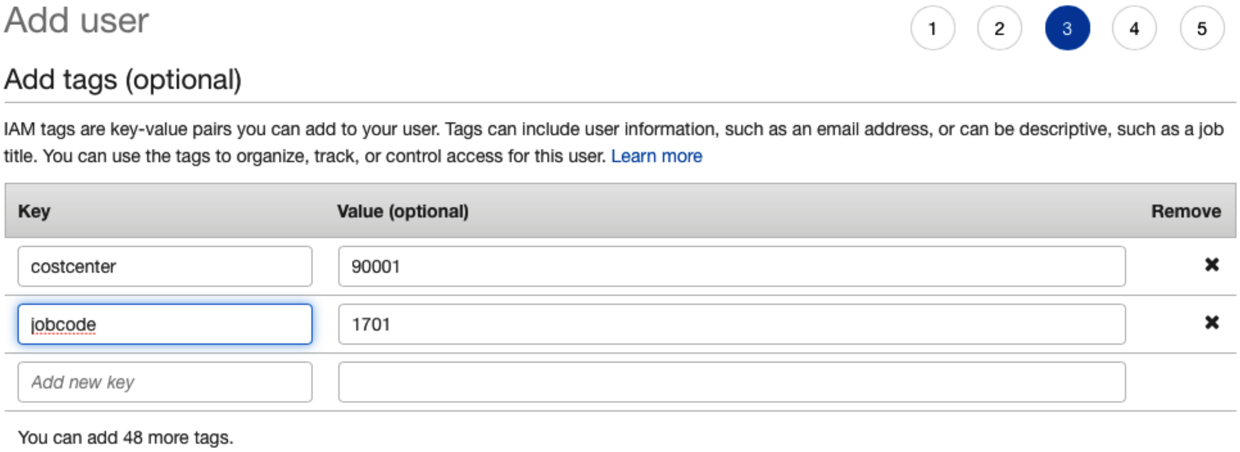
		Policy name	Type	Used as	Description
☑	▸	AdministratorAccess	Job function	*None*	Provides full access to AWS services and resources.
□	▸	AlexaForBusinessDevice…	AWS managed	*None*	Provide device setup access to AlexaForBusiness services


▾ Set permissions
Add user to group
Copy permissions from existing user
Attach existing policies directly

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Add user to group

	Group ▾	Attached policies
☑	FullAdministrator	AdministratorAccess

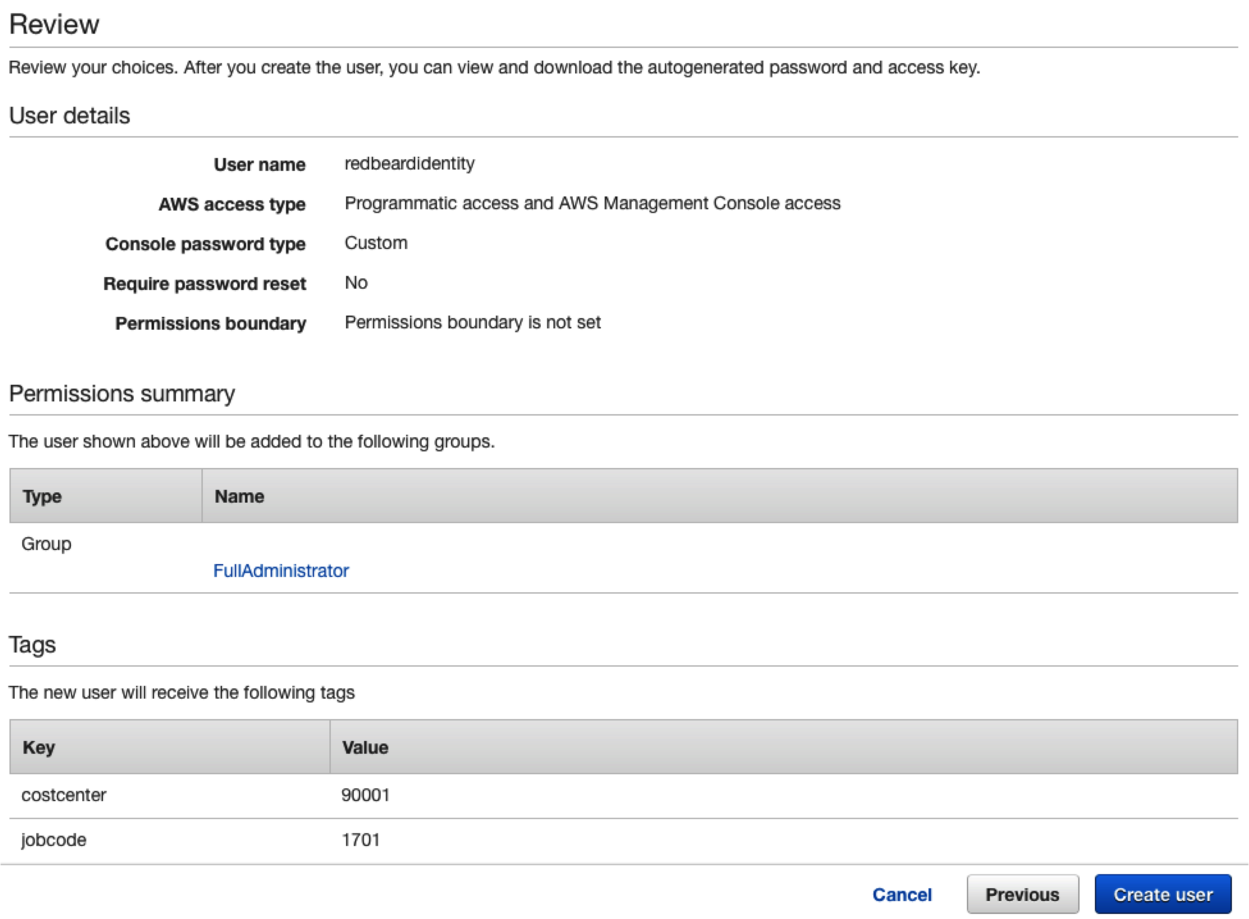


Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. Learn more

Key	Value (optional)	Remove
costcenter	90001	✖
jobcode	1701	✖
Add new key		

You can add 48 more tags.



Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	redbeardidentity
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	No
Permissions boundary	Permissions boundary is not set

Permissions summary

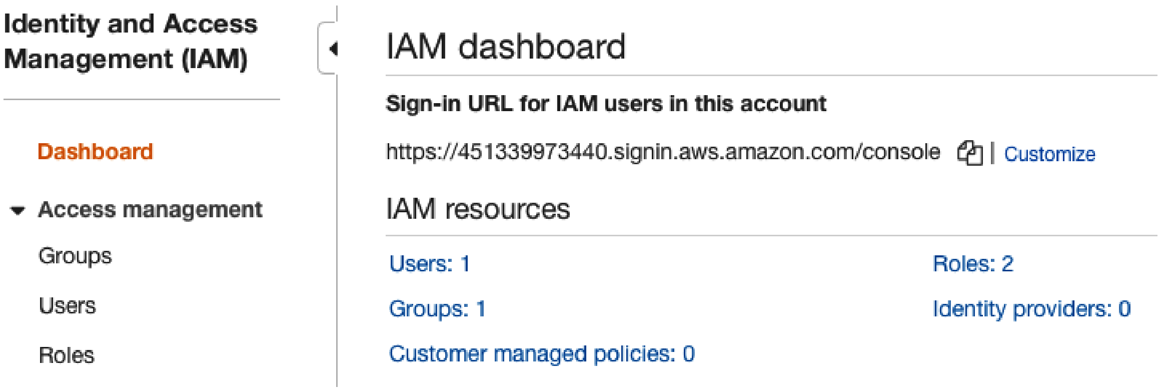
The user shown above will be added to the following groups.

Type	Name
Group	FullAdministrator

Tags

The new user will receive the following tags

Key	Value
costcenter	90001
jobcode	1701



IAM dashboard

Sign-in URL for IAM users in this account

https://451339973440.signin.aws.amazon.com/console

IAM resources

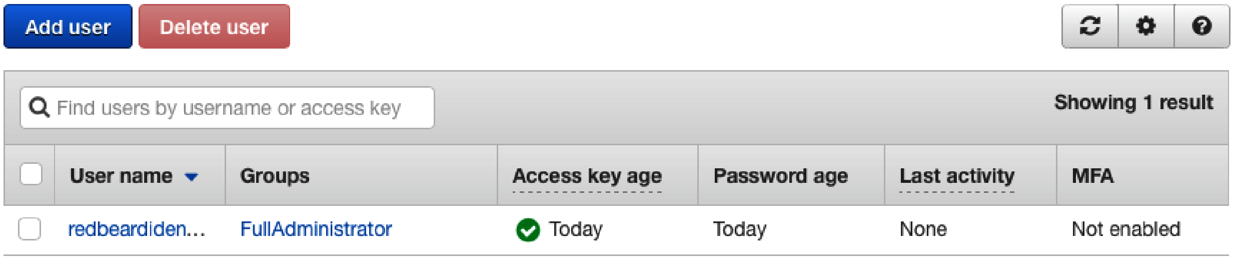
Users: 1

Roles: 2

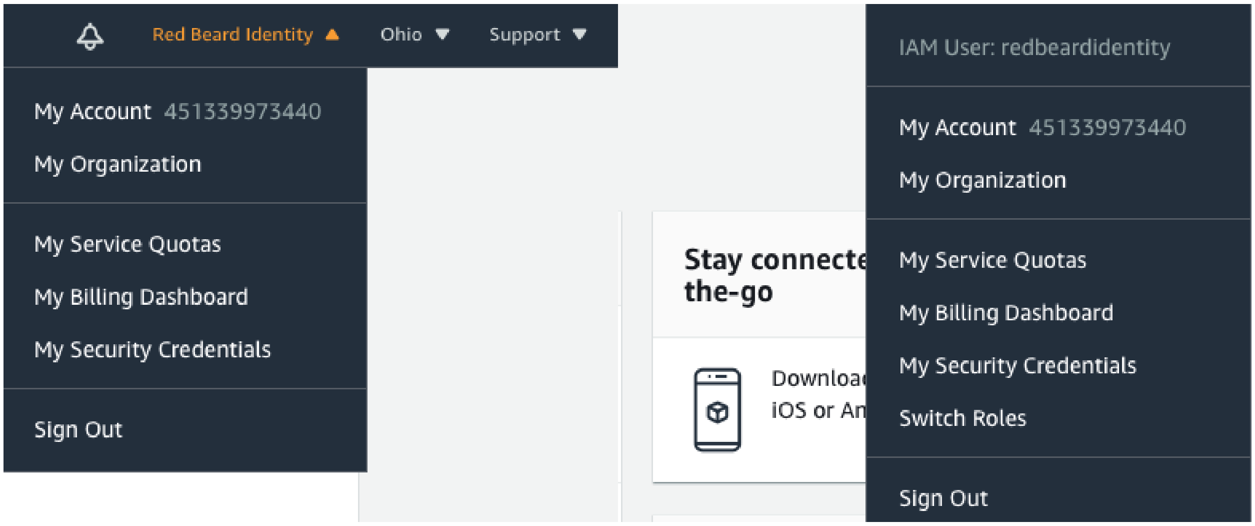
Groups: 1

Identity providers: 0

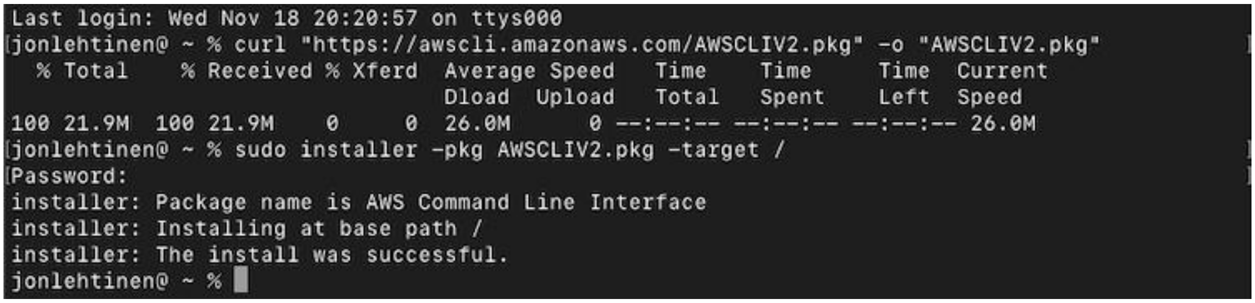
Customer managed policies: 0



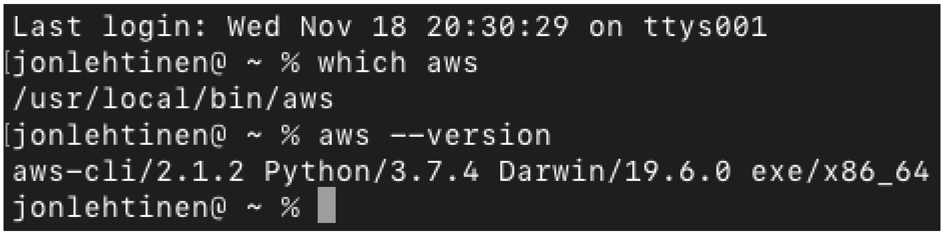
□	User name ▾	Groups	Access key age	Password age	Last activity	MFA
□	redbeardiden…	FullAdministrator	✓ Today	Today	None	Not enabled



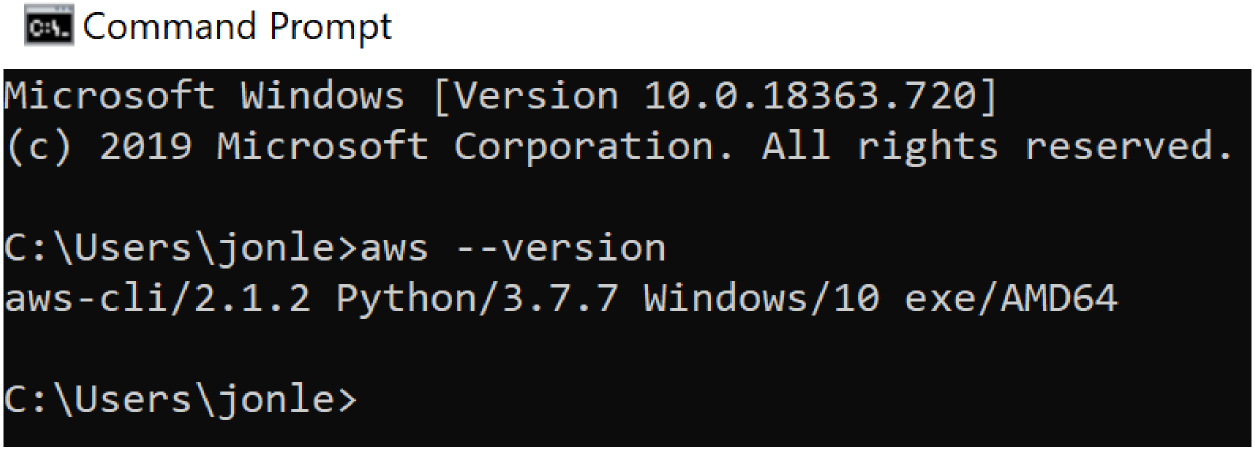
Chapter 2: An Introduction to the AWS CLI



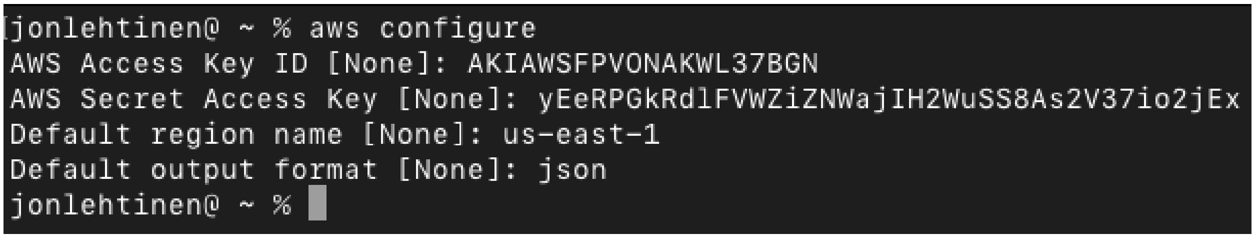
```
Last login: Wed Nov 18 20:20:57 on ttys000
[jonlehtinen@ ~ % curl "https://awscli.amazonaws.com/AWSCLIV2.pkg" -o "AWSCLIV2.pkg"
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 21.9M  100 21.9M    0     0  26.0M      0 --:--:-- --:--:-- --:--:-- 26.0M
[jonlehtinen@ ~ % sudo installer -pkg AWSCLIV2.pkg -target /
[Password:
installer: Package name is AWS Command Line Interface
installer: Installing at base path /
installer: The install was successful.
jonlehtinen@ ~ %
```



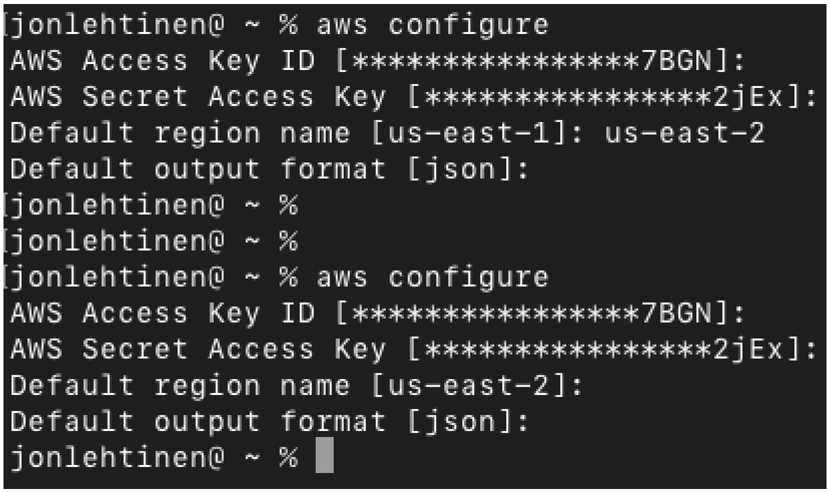
```
Last login: Wed Nov 18 20:30:29 on ttys001
[jonlehtinen@ ~ % which aws
/usr/local/bin/aws
[jonlehtinen@ ~ % aws --version
aws-cli/2.1.2 Python/3.7.4 Darwin/19.6.0 exe/x86_64
jonlehtinen@ ~ %
```



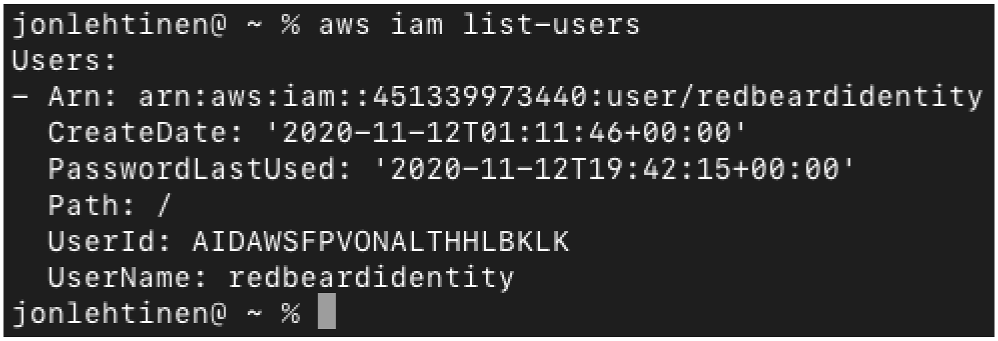
```
Microsoft Windows [Version 10.0.18363.720]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\jonle>aws --version
aws-cli/2.1.2 Python/3.7.7 Windows/10 exe/AMD64

C:\Users\jonle>
```



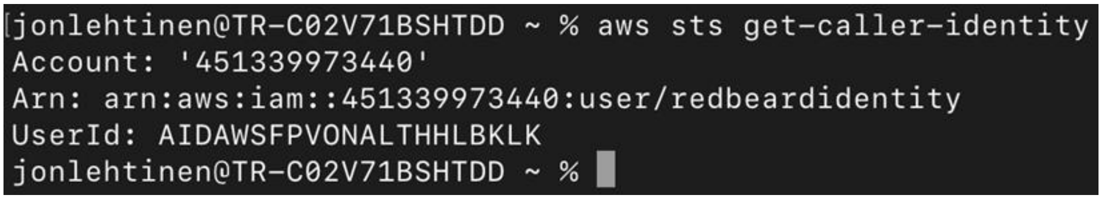
```
[jonlehtinen@ ~ % aws configure
AWS Access Key ID [None]: AKIAWSFPVONAKWL37BGN
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-1
Default output format [None]: json
jonlehtinen@ ~ %
```



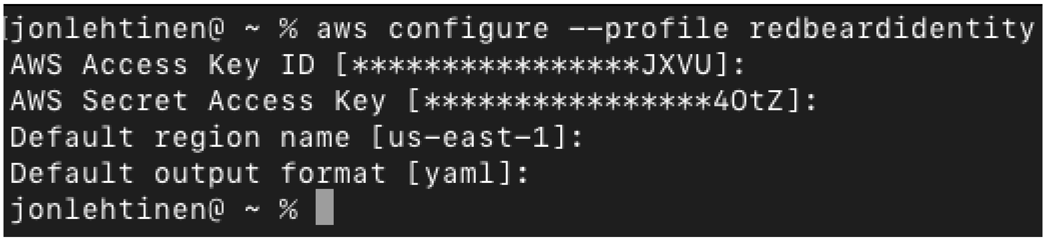
```
[jonlehtinen@ ~ % aws configure
 AWS Access Key ID [****************7BGN]:
 AWS Secret Access Key [****************2jEx]:
 Default region name [us-east-1]: us-east-2
 Default output format [json]:
[jonlehtinen@ ~ %
[jonlehtinen@ ~ %
[jonlehtinen@ ~ % aws configure
 AWS Access Key ID [****************7BGN]:
 AWS Secret Access Key [****************2jEx]:
 Default region name [us-east-2]:
 Default output format [json]:
 jonlehtinen@ ~ %
```



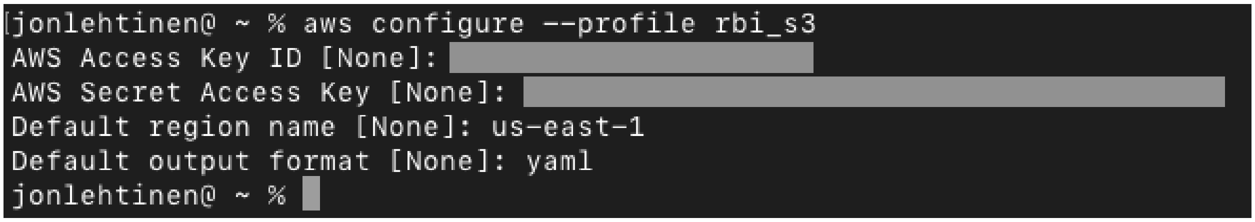
```
jonlehtinen@ ~ % aws iam list-users
Users:
- Arn: arn:aws:iam::451339973440:user/redbeardidentity
  CreateDate: '2020-11-12T01:11:46+00:00'
  PasswordLastUsed: '2020-11-12T19:42:15+00:00'
  Path: /
  UserId: AIDAWSFPVONALTHHLBKLK
  UserName: redbeardidentity
jonlehtinen@ ~ %
```



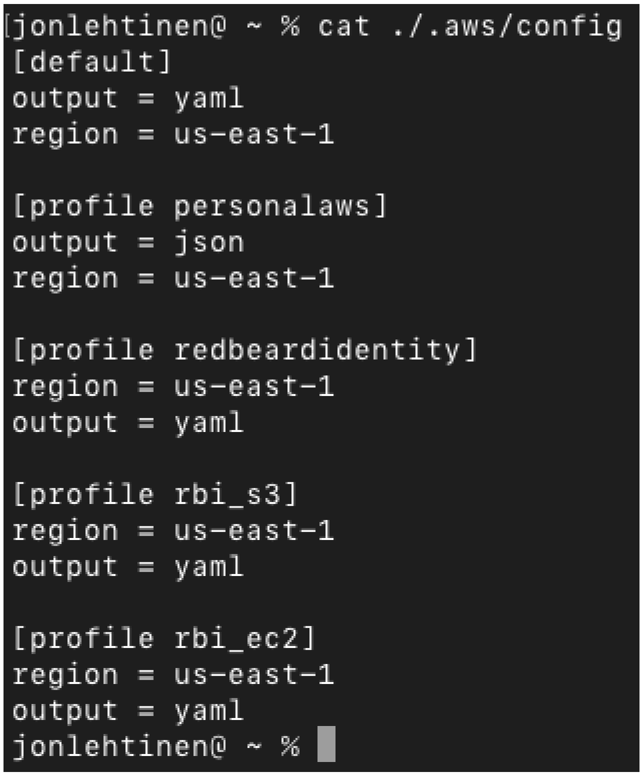
```
[jonlehtinen@TR-C02V71BSHTDD ~ % aws sts get-caller-identity
 Account: '451339973440'
 Arn: arn:aws:iam::451339973440:user/redbeardidentity
 UserId: AIDAWSFPVONALTHHLBKLK
 jonlehtinen@TR-C02V71BSHTDD ~ %
```



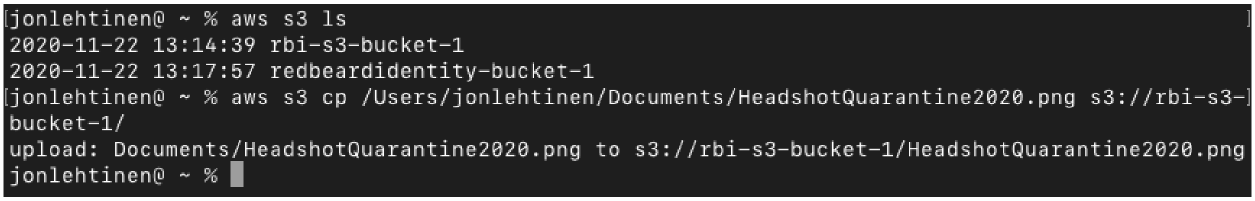
```
[jonlehtinen@ ~ % aws configure --profile redbeardidentity
 AWS Access Key ID [****************JXVU]:
 AWS Secret Access Key [****************4OtZ]:
 Default region name [us-east-1]:
 Default output format [yaml]:
 jonlehtinen@ ~ %
```



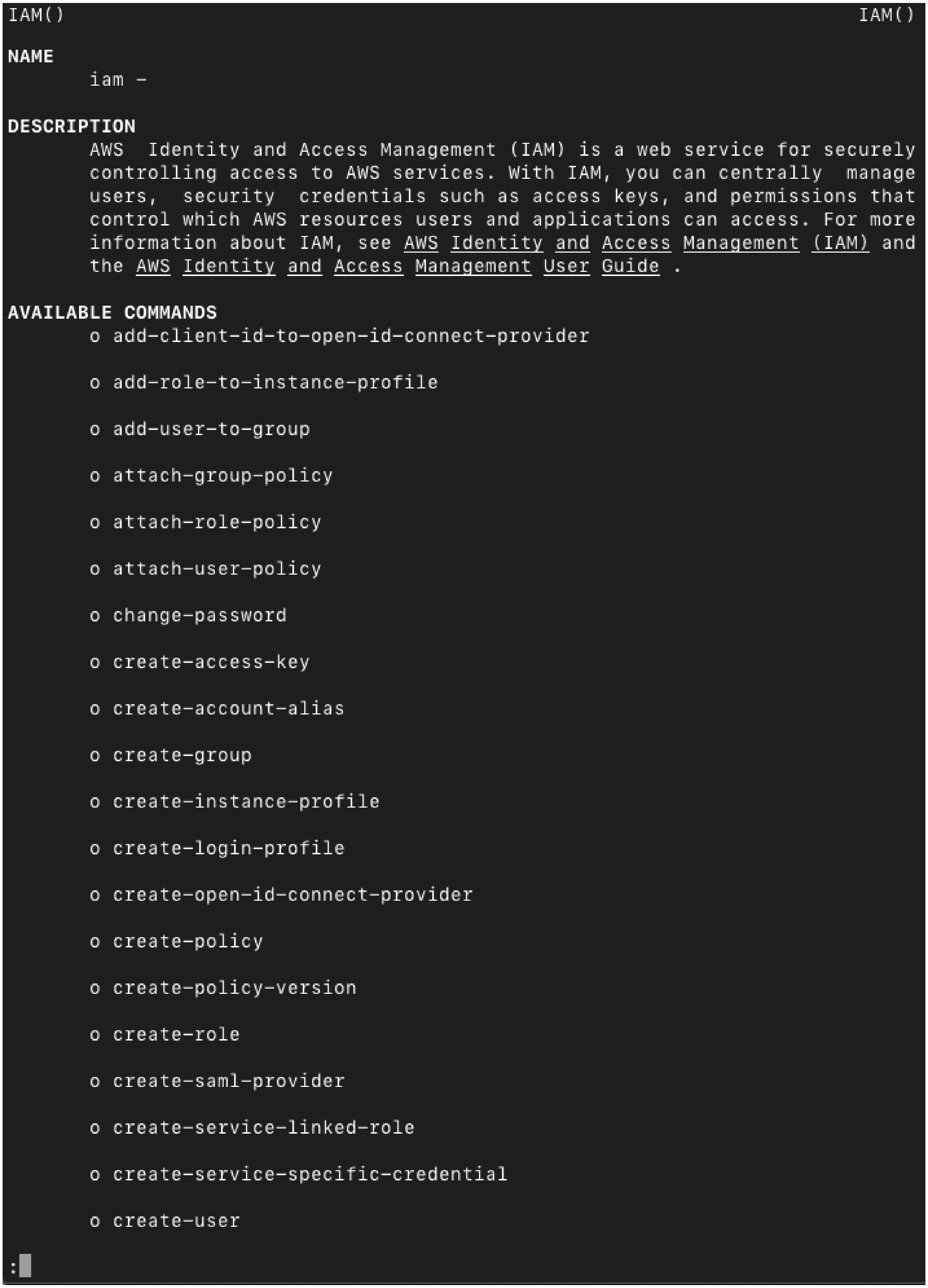
```
jonlehtinen@ ~ % aws configure --profile rbi_s3
AWS Access Key ID [None]: [redacted]
AWS Secret Access Key [None]: [redacted]
Default region name [None]: us-east-1
Default output format [None]: yaml
jonlehtinen@ ~ %
```



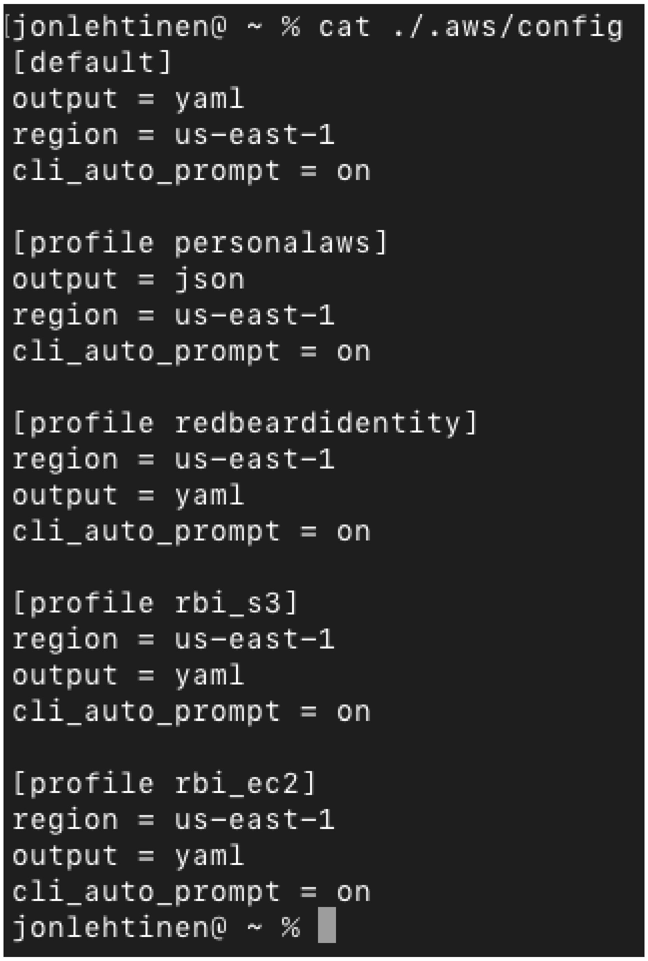
```
jonlehtinen@ ~ % cat ./.aws/config
[default]
output = yaml
region = us-east-1

[profile personalaws]
output = json
region = us-east-1

[profile redbeardidentity]
region = us-east-1
output = yaml

[profile rbi_s3]
region = us-east-1
output = yaml

[profile rbi_ec2]
region = us-east-1
output = yaml
jonlehtinen@ ~ %
```



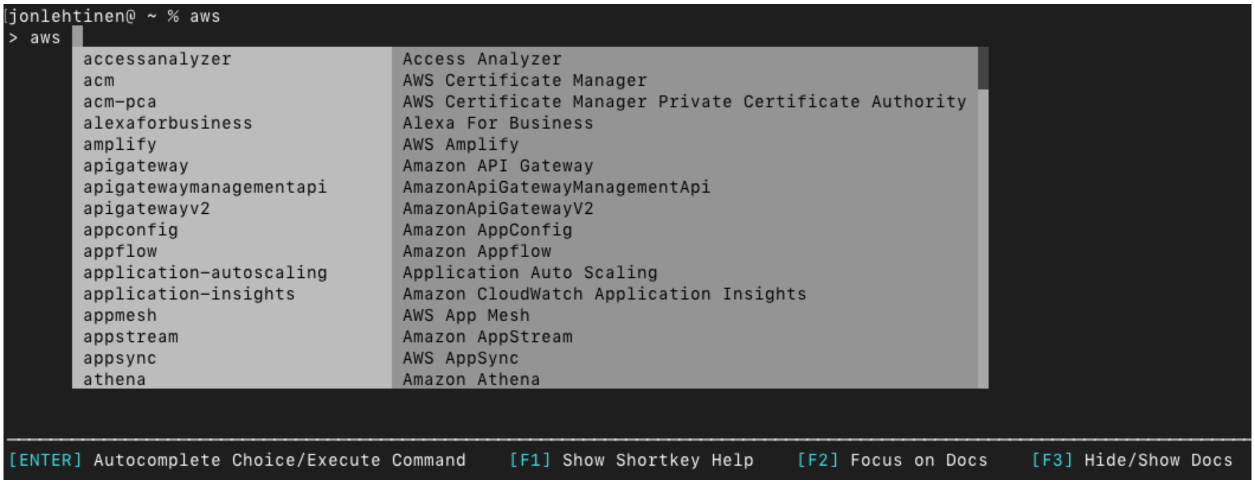
```
jonlehtinen@ ~ % aws s3 ls
2020-11-22 13:14:39 rbi-s3-bucket-1
2020-11-22 13:17:57 redbeardidentity-bucket-1
jonlehtinen@ ~ % aws s3 cp /Users/jonlehtinen/Documents/HeadshotQuarantine2020.png s3://rbi-s3-
bucket-1/
upload: Documents/HeadshotQuarantine2020.png to s3://rbi-s3-bucket-1/HeadshotQuarantine2020.png
jonlehtinen@ ~ %
```



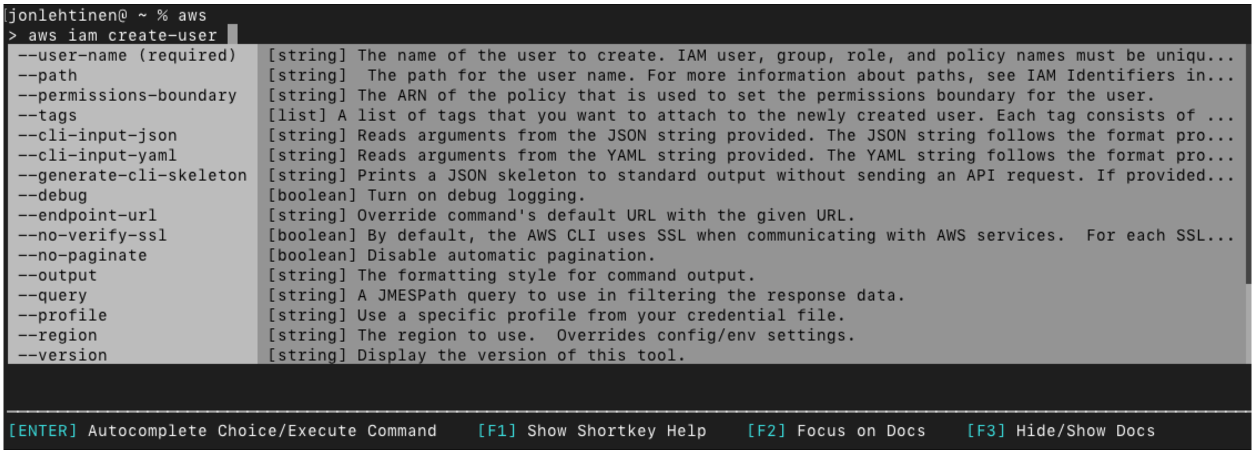
```
IAM()                                                                  IAM()

NAME
       iam -

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

AVAILABLE COMMANDS
       o add-client-id-to-open-id-connect-provider

       o add-role-to-instance-profile

       o add-user-to-group

       o attach-group-policy

       o attach-role-policy

       o attach-user-policy

       o change-password

       o create-access-key

       o create-account-alias

       o create-group

       o create-instance-profile

       o create-login-profile

       o create-open-id-connect-provider

       o create-policy

       o create-policy-version

       o create-role

       o create-saml-provider

       o create-service-linked-role

       o create-service-specific-credential

       o create-user

:
```



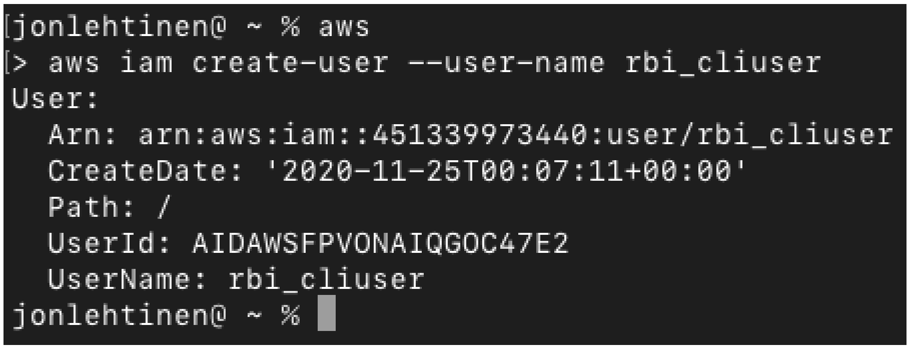
```
[jonlehtinen@ ~ % cat ./.aws/config
[default]
output = yaml
region = us-east-1
cli_auto_prompt = on

[profile personalaws]
output = json
region = us-east-1
cli_auto_prompt = on

[profile redbeardidentity]
region = us-east-1
output = yaml
cli_auto_prompt = on

[profile rbi_s3]
region = us-east-1
output = yaml
cli_auto_prompt = on

[profile rbi_ec2]
region = us-east-1
output = yaml
cli_auto_prompt = on
jonlehtinen@ ~ %
```



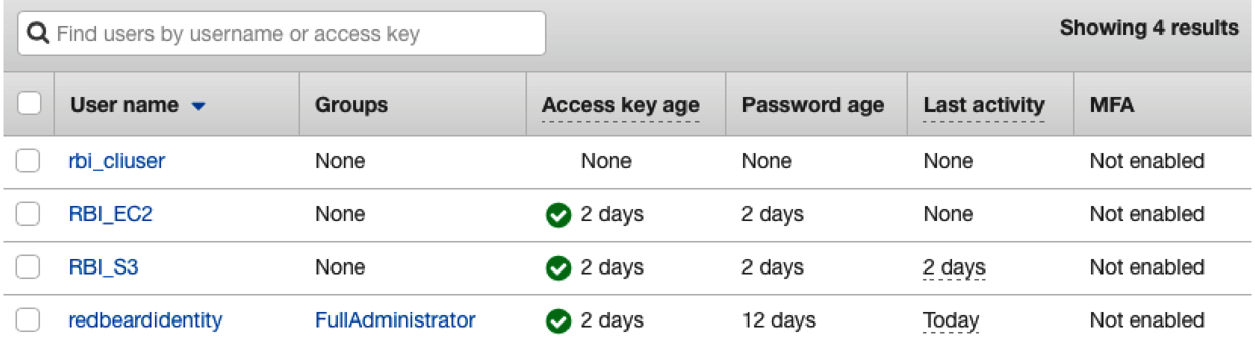
```
[jonlehtinen@ ~ % aws
> aws
      accessanalyzer               Access Analyzer
      acm                          AWS Certificate Manager
      acm-pca                      AWS Certificate Manager Private Certificate Authority
      alexaforbusiness             Alexa For Business
      amplify                      AWS Amplify
      apigateway                   Amazon API Gateway
      apigatewaymanagementapi      AmazonApiGatewayManagementApi
      apigatewayv2                 AmazonApiGatewayV2
      appconfig                    Amazon AppConfig
      appflow                      Amazon Appflow
      application-autoscaling      Application Auto Scaling
      application-insights         Amazon CloudWatch Application Insights
      appmesh                      AWS App Mesh
      appstream                    Amazon AppStream
      appsync                      AWS AppSync
      athena                       Amazon Athena

[ENTER] Autocomplete Choice/Execute Command    [F1] Show Shortkey Help    [F2] Focus on Docs    [F3] Hide/Show Docs
```



```
jonlehtinen@ ~ % aws
> aws iam create-user
 --user-name (required)    [string] The name of the user to create. IAM user, group, role, and policy names must be uniqu...
 --path                    [string]  The path for the user name. For more information about paths, see IAM Identifiers in...
 --permissions-boundary    [string] The ARN of the policy that is used to set the permissions boundary for the user.
 --tags                    [list] A list of tags that you want to attach to the newly created user. Each tag consists of ...
 --cli-input-json          [string] Reads arguments from the JSON string provided. The JSON string follows the format pro...
 --cli-input-yaml          [string] Reads arguments from the YAML string provided. The YAML string follows the format pro...
 --generate-cli-skeleton   [string] Prints a JSON skeleton to standard output without sending an API request. If provided...
 --debug                   [boolean] Turn on debug logging.
 --endpoint-url            [string] Override command's default URL with the given URL.
 --no-verify-ssl           [boolean] By default, the AWS CLI uses SSL when communicating with AWS services.  For each SSL...
 --no-paginate             [boolean] Disable automatic pagination.
 --output                  [string] The formatting style for command output.
 --query                   [string] A JMESPath query to use in filtering the response data.
 --profile                 [string] Use a specific profile from your credential file.
 --region                  [string] The region to use.  Overrides config/env settings.
 --version                 [string] Display the version of this tool.

[ENTER] Autocomplete Choice/Execute Command    [F1] Show Shortkey Help    [F2] Focus on Docs    [F3] Hide/Show Docs
```



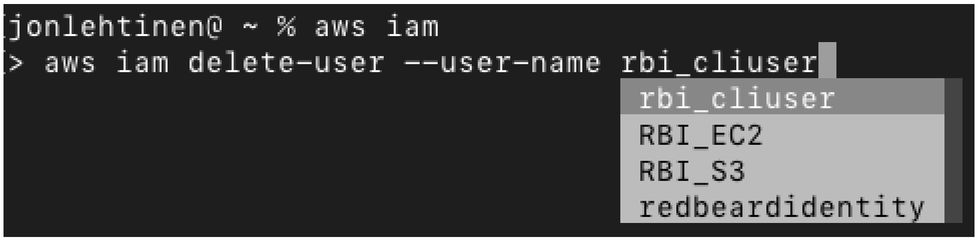
```
jonlehtinen@ ~ % aws
> aws iam create-user --user-name rbi_cliuser
User:
  Arn: arn:aws:iam::451339973440:user/rbi_cliuser
  CreateDate: '2020-11-25T00:07:11+00:00'
  Path: /
  UserId: AIDAWSFPVONAIQGOC47E2
  UserName: rbi_cliuser
jonlehtinen@ ~ %
```



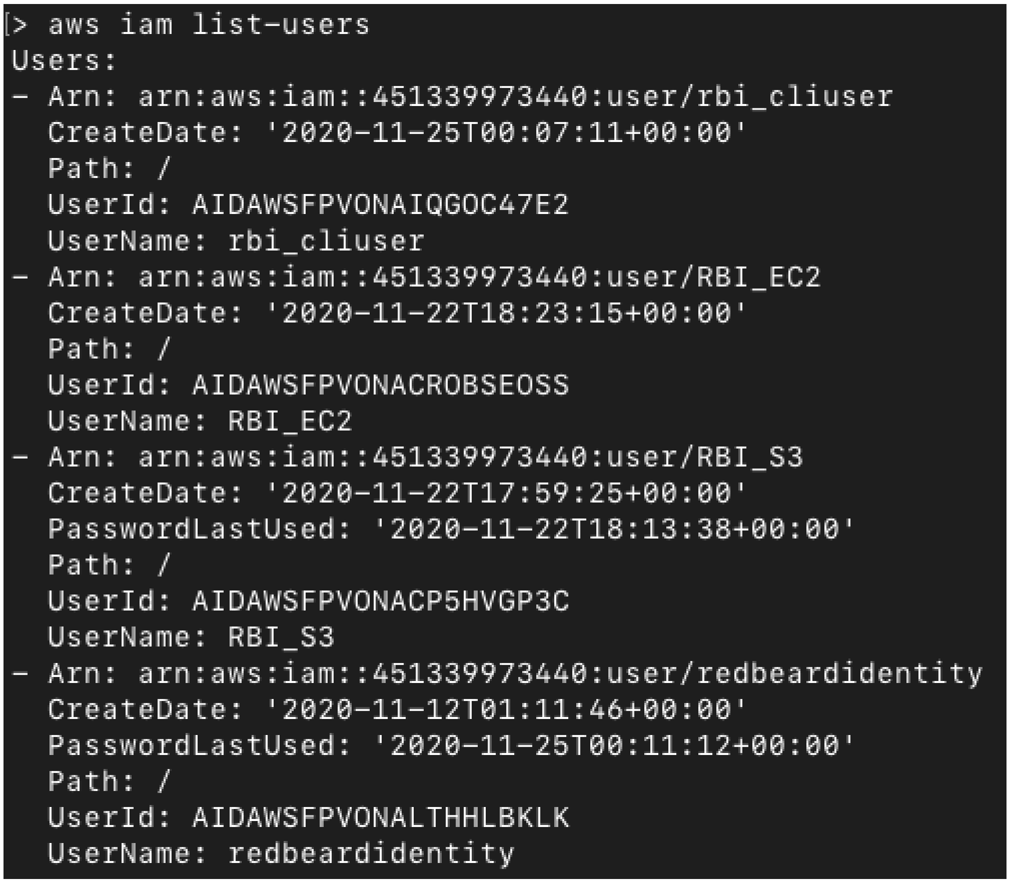
Find users by username or access key

Showing 4 results

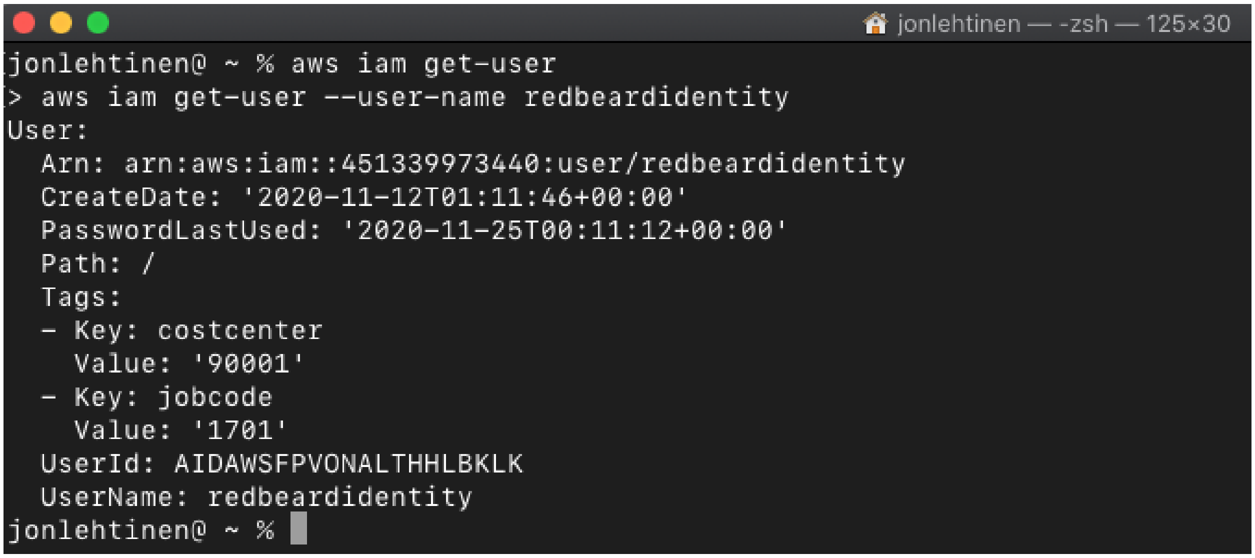
□	User name	Groups	Access key age	Password age	Last activity	MFA
□	rbi_cliuser	None	None	None	None	Not enabled
□	RBI_EC2	None	✓ 2 days	2 days	None	Not enabled
□	RBI_S3	None	✓ 2 days	2 days	2 days	Not enabled
□	redbeardidentity	FullAdministrator	✓ 2 days	12 days	Today	Not enabled



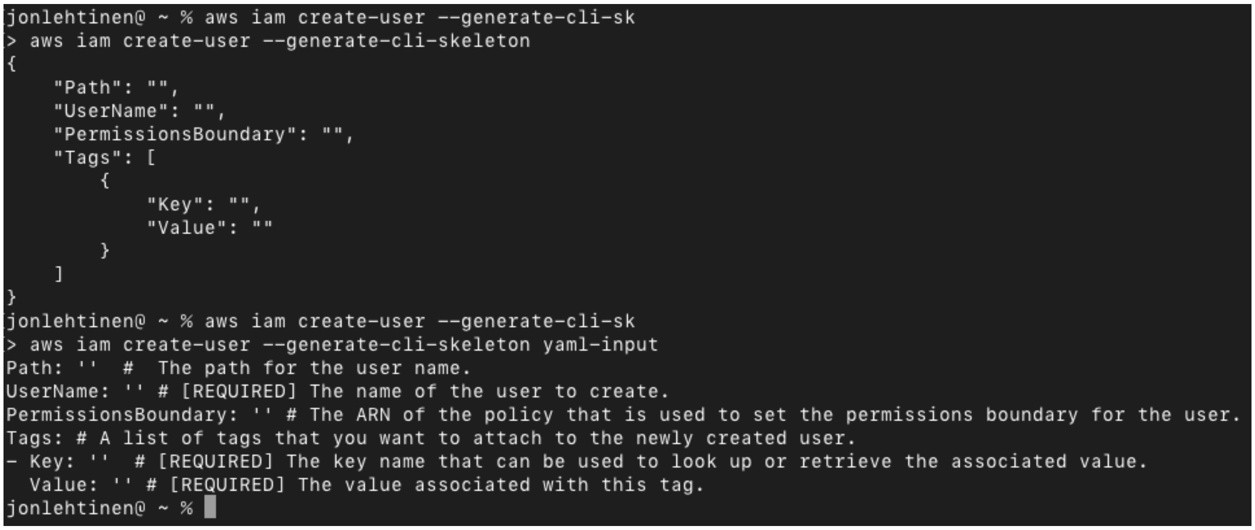
```
jonlehtinen@ ~ % aws iam
> aws iam delete-user --user-name rbi_cliuser
                                  rbi_cliuser
                                  RBI_EC2
                                  RBI_S3
                                  redbeardidentity
```



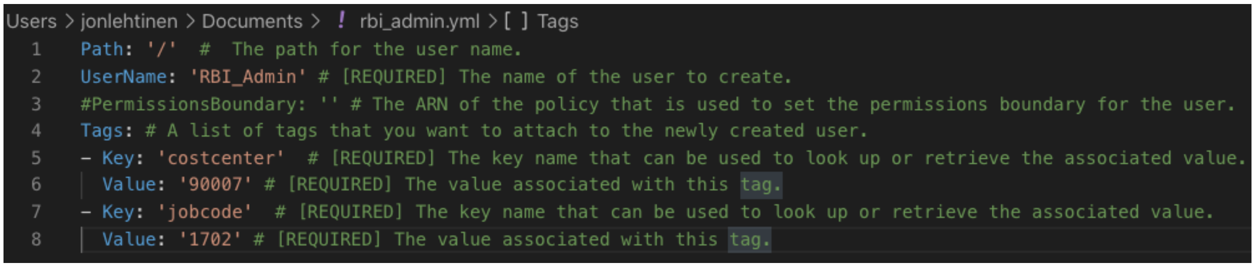
```
[> aws iam list-users
Users:
- Arn: arn:aws:iam::451339973440:user/rbi_cliuser
  CreateDate: '2020-11-25T00:07:11+00:00'
  Path: /
  UserId: AIDAWSFPVONAIQGOC47E2
  UserName: rbi_cliuser
- Arn: arn:aws:iam::451339973440:user/RBI_EC2
  CreateDate: '2020-11-22T18:23:15+00:00'
  Path: /
  UserId: AIDAWSFPVONACROBSEOSS
  UserName: RBI_EC2
- Arn: arn:aws:iam::451339973440:user/RBI_S3
  CreateDate: '2020-11-22T17:59:25+00:00'
  PasswordLastUsed: '2020-11-22T18:13:38+00:00'
  Path: /
  UserId: AIDAWSFPVONACP5HVGP3C
  UserName: RBI_S3
- Arn: arn:aws:iam::451339973440:user/redbeardidentity
  CreateDate: '2020-11-12T01:11:46+00:00'
  PasswordLastUsed: '2020-11-25T00:11:12+00:00'
  Path: /
  UserId: AIDAWSFPVONALTHHLBKLK
  UserName: redbeardidentity
```



```
[jonlehtinen@ ~ % aws iam get-user
[> aws iam get-user --user-name redbeardidentity
User:
  Arn: arn:aws:iam::451339973440:user/redbeardidentity
  CreateDate: '2020-11-12T01:11:46+00:00'
  PasswordLastUsed: '2020-11-25T00:11:12+00:00'
  Path: /
  Tags:
  - Key: costcenter
    Value: '90001'
  - Key: jobcode
    Value: '1701'
  UserId: AIDAWSFPVONALTHHLBKLK
  UserName: redbeardidentity
jonlehtinen@ ~ %
```

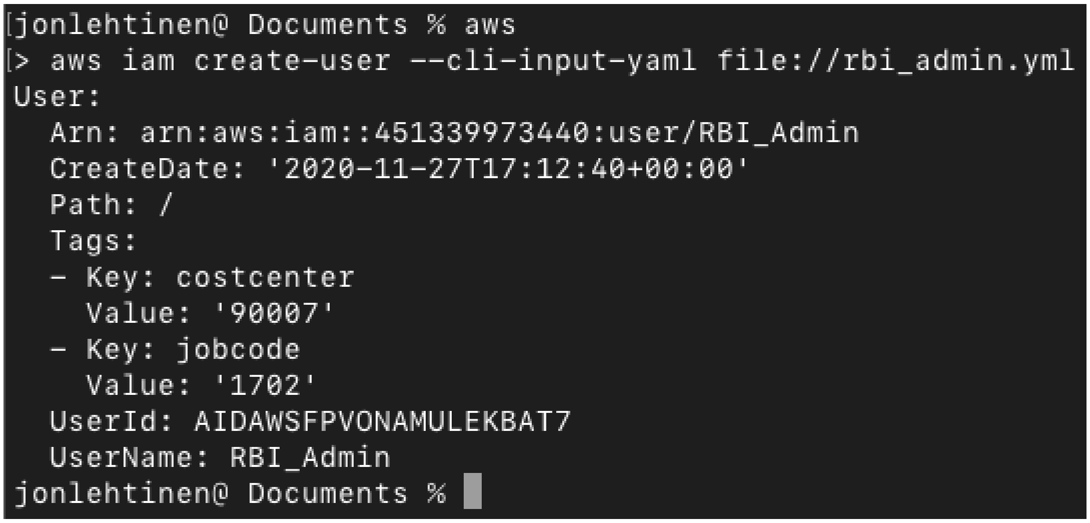


```
jonlehtinen@ ~ % aws iam create-user --generate-cli-sk
> aws iam create-user --generate-cli-skeleton
{
    "Path": "",
    "UserName": "",
    "PermissionsBoundary": "",
    "Tags": [
        {
            "Key": "",
            "Value": ""
        }
    ]
}
jonlehtinen@ ~ % aws iam create-user --generate-cli-sk
> aws iam create-user --generate-cli-skeleton yaml-input
Path: ''  #  The path for the user name.
UserName: '' # [REQUIRED] The name of the user to create.
PermissionsBoundary: '' # The ARN of the policy that is used to set the permissions boundary for the user.
Tags: # A list of tags that you want to attach to the newly created user.
- Key: ''  # [REQUIRED] The key name that can be used to look up or retrieve the associated value.
  Value: '' # [REQUIRED] The value associated with this tag.
jonlehtinen@ ~ %
```

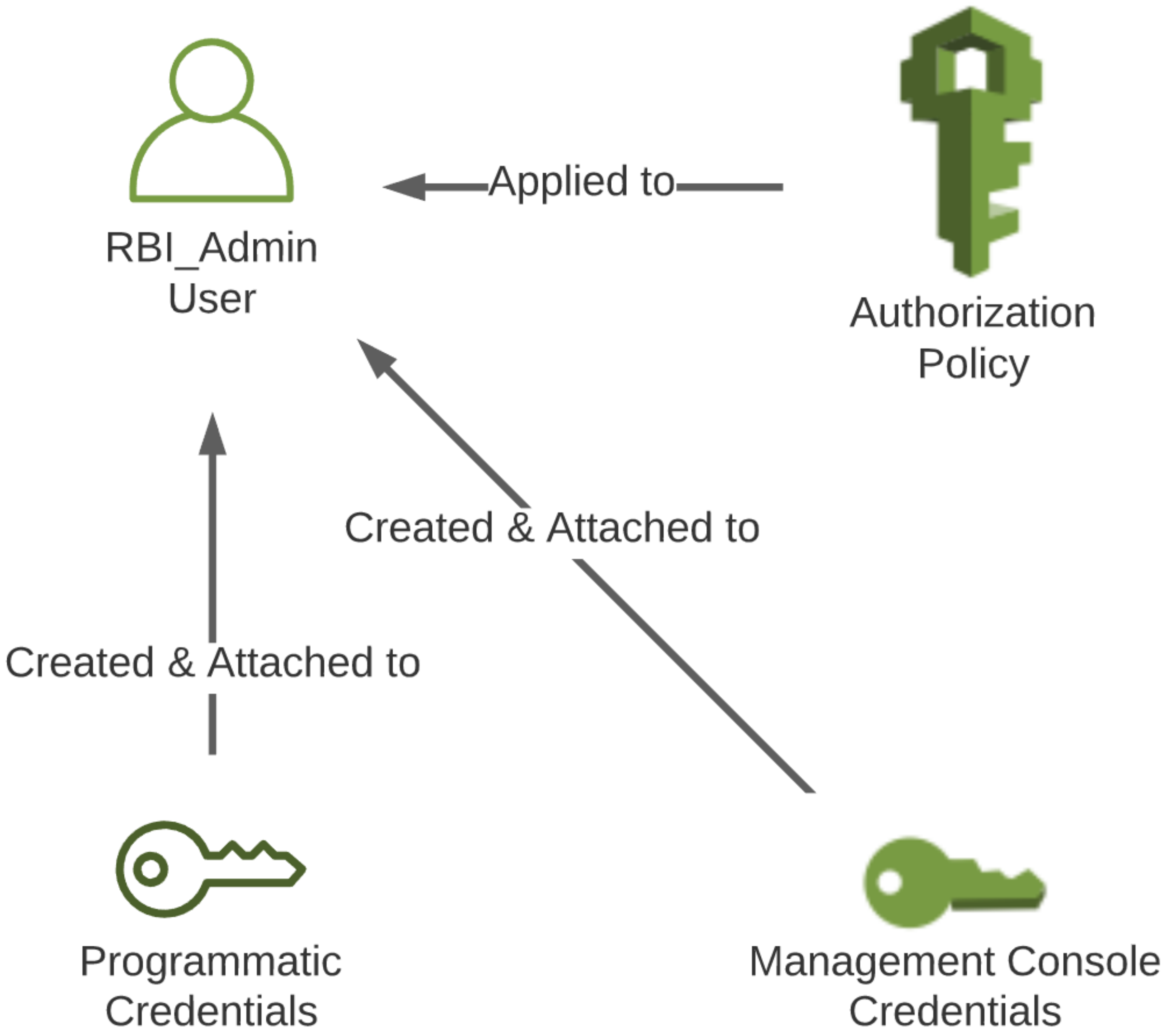


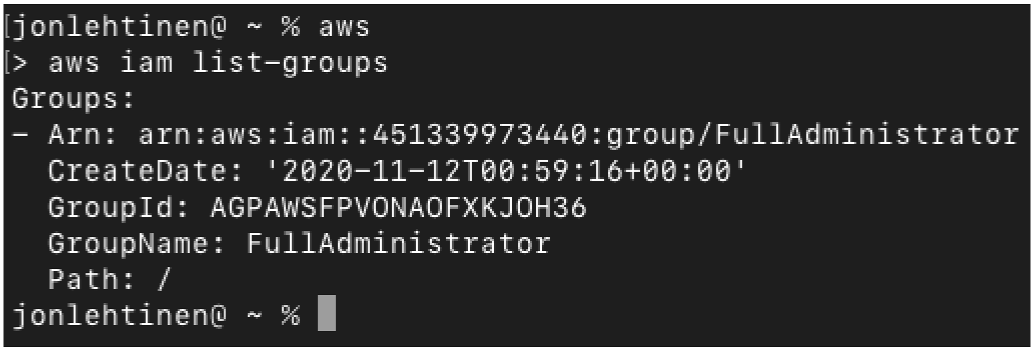
Users > jonlehtinen > Documents > ! rbi_admin.yml > [ ] Tags

```
Path: '/'  #  The path for the user name.
UserName: 'RBI_Admin' # [REQUIRED] The name of the user to create.
#PermissionsBoundary: '' # The ARN of the policy that is used to set the permissions boundary for the user.
Tags: # A list of tags that you want to attach to the newly created user.
- Key: 'costcenter'  # [REQUIRED] The key name that can be used to look up or retrieve the associated value.
  Value: '90007' # [REQUIRED] The value associated with this tag.
- Key: 'jobcode'  # [REQUIRED] The key name that can be used to look up or retrieve the associated value.
  Value: '1702' # [REQUIRED] The value associated with this tag.
```

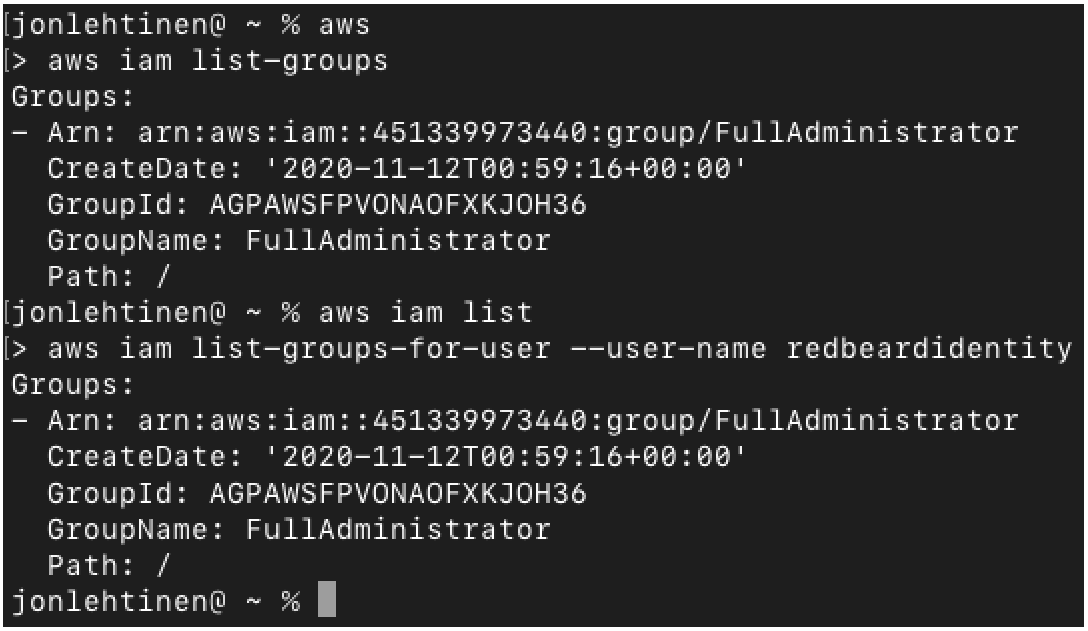


```
[jonlehtinen@ Documents % aws
[> aws iam create-user --cli-input-yaml file://rbi_admin.yml
User:
  Arn: arn:aws:iam::451339973440:user/RBI_Admin
  CreateDate: '2020-11-27T17:12:40+00:00'
  Path: /
  Tags:
  - Key: costcenter
    Value: '90007'
  - Key: jobcode
    Value: '1702'
  UserId: AIDAWSFPVONAMULEKBAT7
  UserName: RBI_Admin
jonlehtinen@ Documents %
```

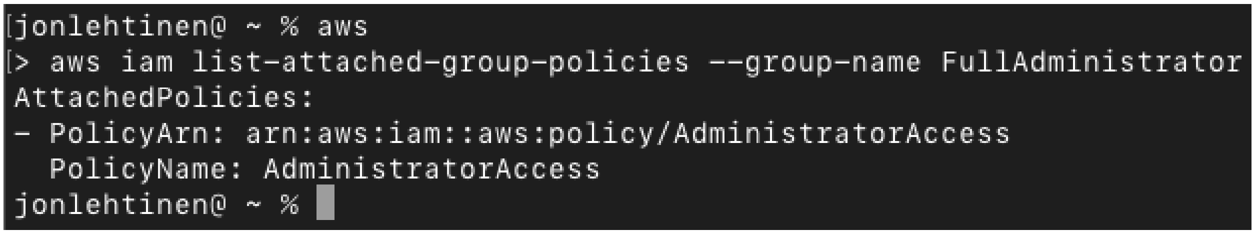




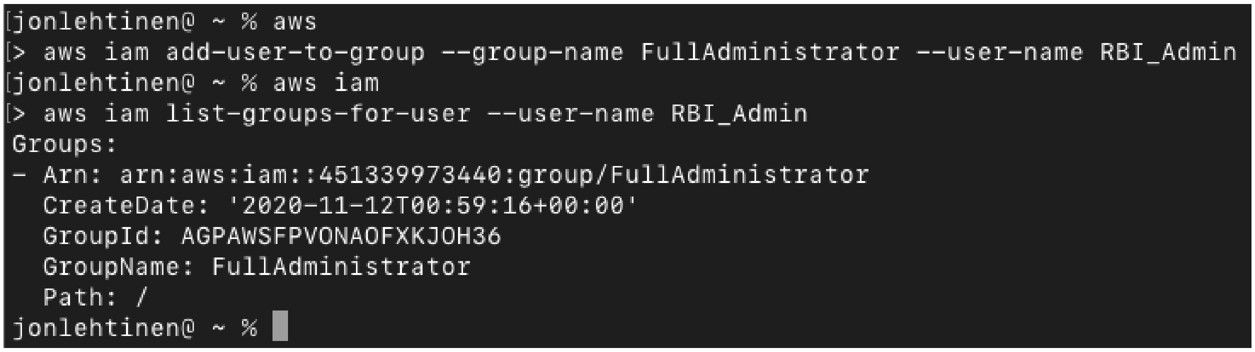
```
[jonlehtinen@ ~ % aws
[> aws iam list-groups
Groups:
- Arn: arn:aws:iam::451339973440:group/FullAdministrator
  CreateDate: '2020-11-12T00:59:16+00:00'
  GroupId: AGPAWSFPVONAOFXKJOH36
  GroupName: FullAdministrator
  Path: /
jonlehtinen@ ~ %
```



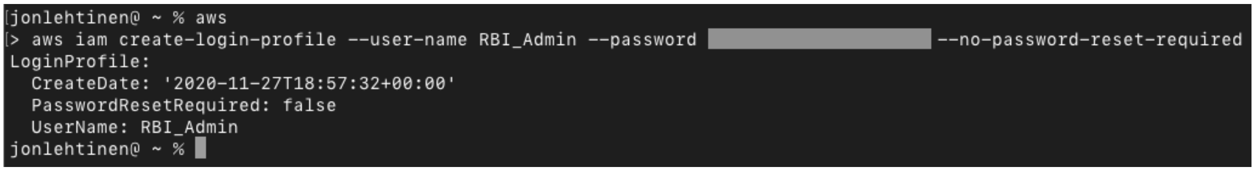
```
[jonlehtinen@ ~ % aws
[> aws iam list-groups
Groups:
- Arn: arn:aws:iam::451339973440:group/FullAdministrator
  CreateDate: '2020-11-12T00:59:16+00:00'
  GroupId: AGPAWSFPVONAOFXKJOH36
  GroupName: FullAdministrator
  Path: /
[jonlehtinen@ ~ % aws iam list
[> aws iam list-groups-for-user --user-name redbeardidentity
Groups:
- Arn: arn:aws:iam::451339973440:group/FullAdministrator
  CreateDate: '2020-11-12T00:59:16+00:00'
  GroupId: AGPAWSFPVONAOFXKJOH36
  GroupName: FullAdministrator
  Path: /
jonlehtinen@ ~ %
```



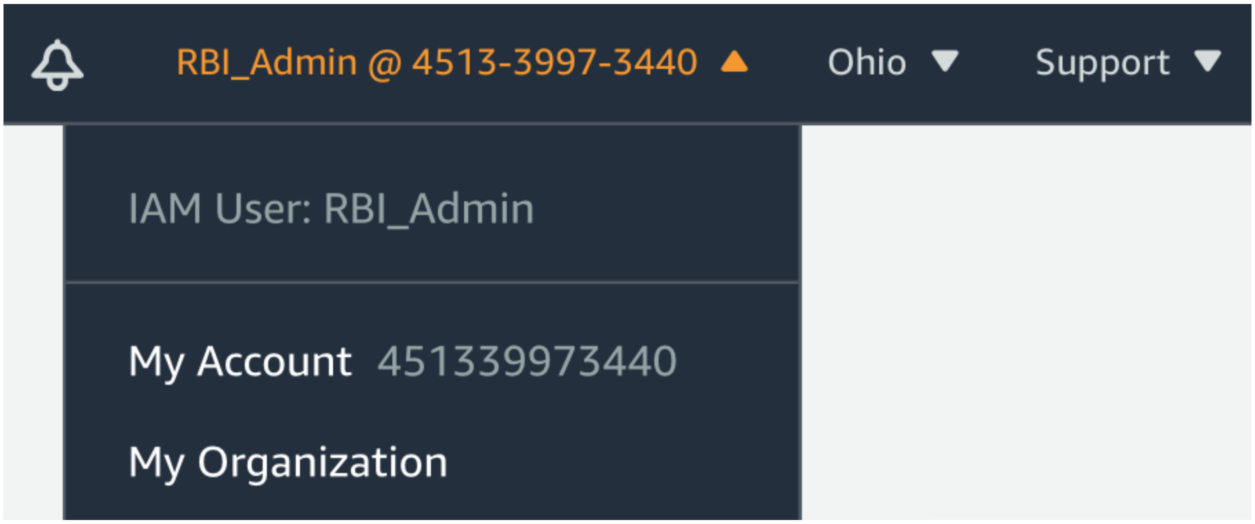
```
[jonlehtinen@ ~ % aws
[> aws iam list-attached-group-policies --group-name FullAdministrator
AttachedPolicies:
- PolicyArn: arn:aws:iam::aws:policy/AdministratorAccess
  PolicyName: AdministratorAccess
jonlehtinen@ ~ %
```

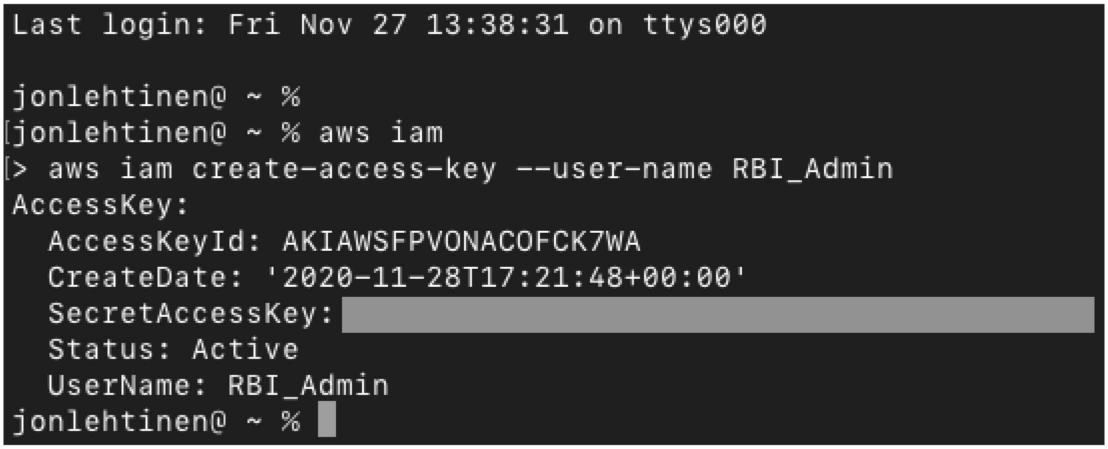


```
[jonlehtinen@ ~ % aws
[> aws iam add-user-to-group --group-name FullAdministrator --user-name RBI_Admin
[jonlehtinen@ ~ % aws iam
[> aws iam list-groups-for-user --user-name RBI_Admin
Groups:
- Arn: arn:aws:iam::451339973440:group/FullAdministrator
  CreateDate: '2020-11-12T00:59:16+00:00'
  GroupId: AGPAWSFPVONAOFXKJOH36
  GroupName: FullAdministrator
  Path: /
jonlehtinen@ ~ %
```

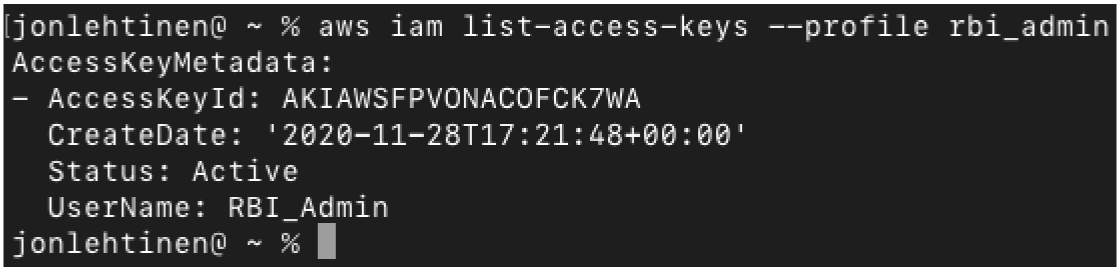


```
[jonlehtinen@ ~ % aws
[> aws iam create-login-profile --user-name RBI_Admin --password [redacted] --no-password-reset-required
LoginProfile:
  CreateDate: '2020-11-27T18:57:32+00:00'
  PasswordResetRequired: false
  UserName: RBI_Admin
jonlehtinen@ ~ %
```

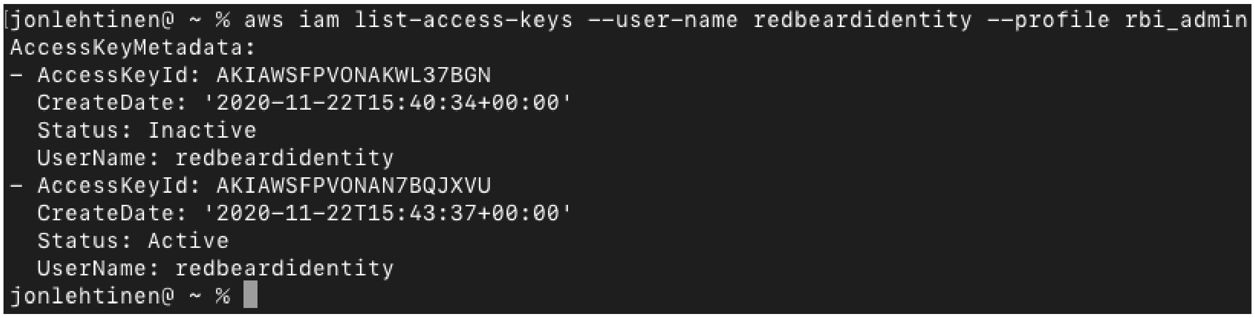




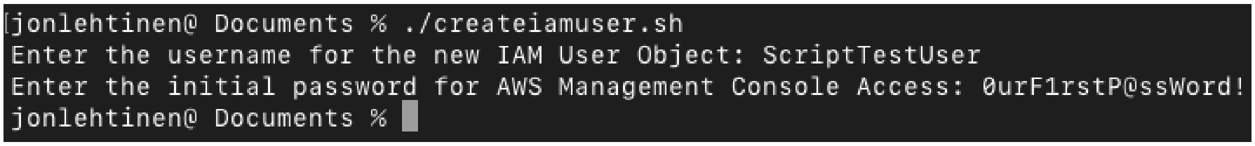
```
Last login: Fri Nov 27 13:38:31 on ttys000

jonlehtinen@ ~ %
[jonlehtinen@ ~ % aws iam
[> aws iam create-access-key --user-name RBI_Admin
AccessKey:
  AccessKeyId: AKIAWSFPVONACOFCK7WA
  CreateDate: '2020-11-28T17:21:48+00:00'
  SecretAccessKey: [redacted]
  Status: Active
  UserName: RBI_Admin
jonlehtinen@ ~ %
```



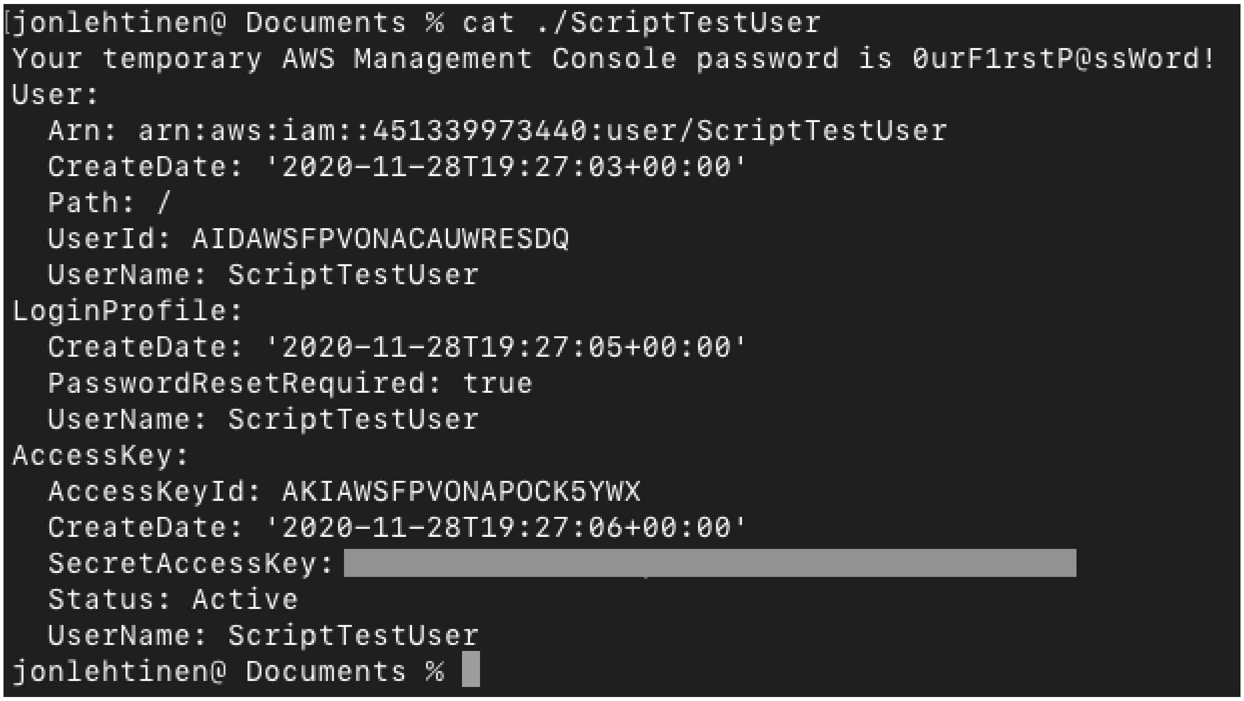
```
[jonlehtinen@ ~ % aws iam list-access-keys --profile rbi_admin
AccessKeyMetadata:
- AccessKeyId: AKIAWSFPVONACOFCK7WA
  CreateDate: '2020-11-28T17:21:48+00:00'
  Status: Active
  UserName: RBI_Admin
jonlehtinen@ ~ %
```



```
[jonlehtinen@ ~ % aws iam list-access-keys --user-name redbeardidentity --profile rbi_admin
AccessKeyMetadata:
- AccessKeyId: AKIAWSFPVONAKWL37BGN
  CreateDate: '2020-11-22T15:40:34+00:00'
  Status: Inactive
  UserName: redbeardidentity
- AccessKeyId: AKIAWSFPVONAN7BQJXVU
  CreateDate: '2020-11-22T15:43:37+00:00'
  Status: Active
  UserName: redbeardidentity
jonlehtinen@ ~ %
```

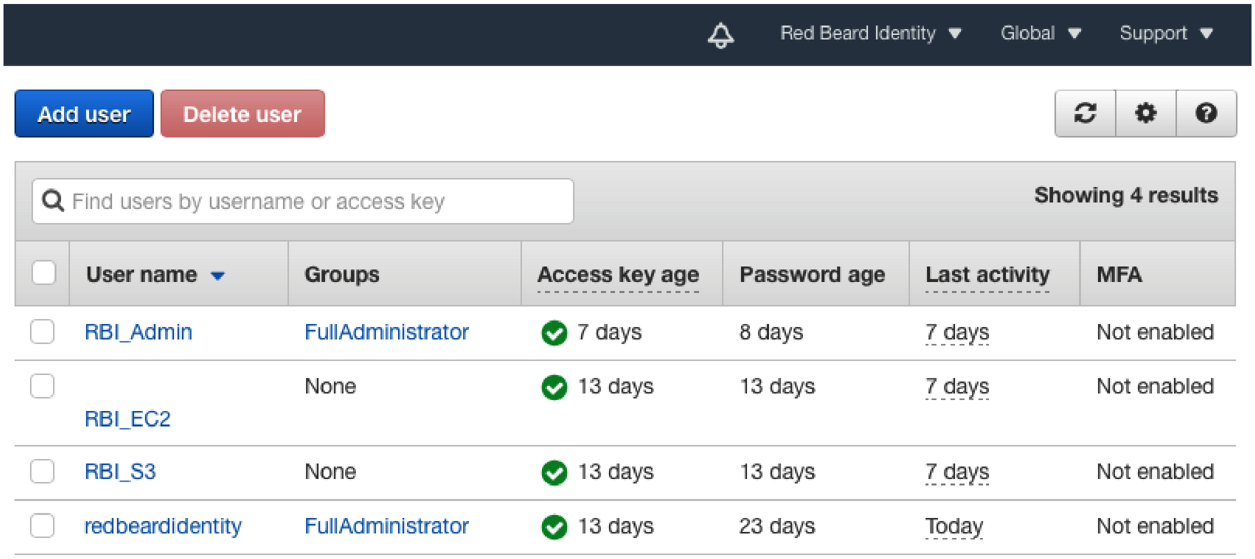


```
[jonlehtinen@ Documents % ./createiamuser.sh
Enter the username for the new IAM User Object: ScriptTestUser
Enter the initial password for AWS Management Console Access: 0urF1rstP@ssWord!
jonlehtinen@ Documents %
```



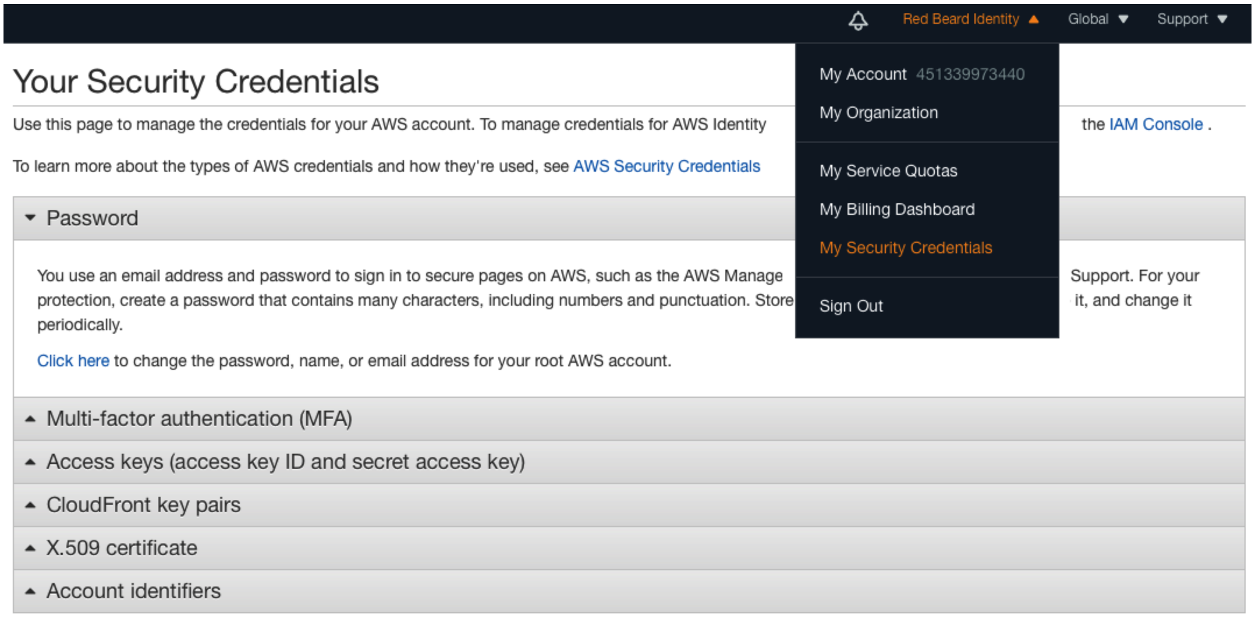
```
[jonlehtinen@ Documents % cat ./ScriptTestUser
Your temporary AWS Management Console password is 0urF1rstP@ssWord!
User:
  Arn: arn:aws:iam::451339973440:user/ScriptTestUser
  CreateDate: '2020-11-28T19:27:03+00:00'
  Path: /
  UserId: AIDAWSFPVONACAUWRESDQ
  UserName: ScriptTestUser
LoginProfile:
  CreateDate: '2020-11-28T19:27:05+00:00'
  PasswordResetRequired: true
  UserName: ScriptTestUser
AccessKey:
  AccessKeyId: AKIAWSFPVONAPOCK5YWX
  CreateDate: '2020-11-28T19:27:06+00:00'
  SecretAccessKey: [redacted]
  Status: Active
  UserName: ScriptTestUser
jonlehtinen@ Documents %
```

Chapter 3: IAM User Management



Showing 4 results

□	User name ▼	Groups	Access key age	Password age	Last activity	MFA
□	RBI_Admin	FullAdministrator	✓ 7 days	8 days	7 days	Not enabled
□	RBI_EC2	None	✓ 13 days	13 days	7 days	Not enabled
□	RBI_S3	None	✓ 13 days	13 days	7 days	Not enabled
□	redbeardidentity	FullAdministrator	✓ 13 days	23 days	Today	Not enabled



Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity the IAM Console .

To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials

▾ Password

You use an email address and password to sign in to secure pages on AWS, such as the AWS Manage Support. For your protection, create a password that contains many characters, including numbers and punctuation. Store it, and change it periodically.

Click here to change the password, name, or email address for your root AWS account.

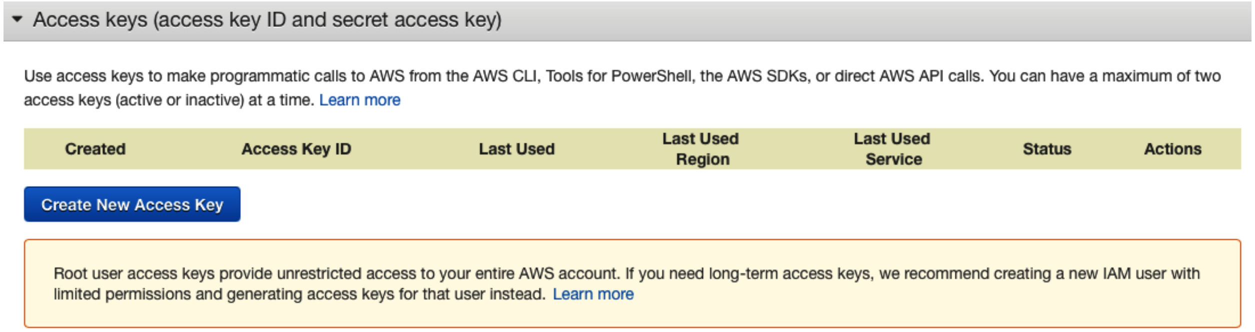
▸ Multi-factor authentication (MFA)

▸ Access keys (access key ID and secret access key)

▸ CloudFront key pairs

▸ X.509 certificate

▸ Account identifiers

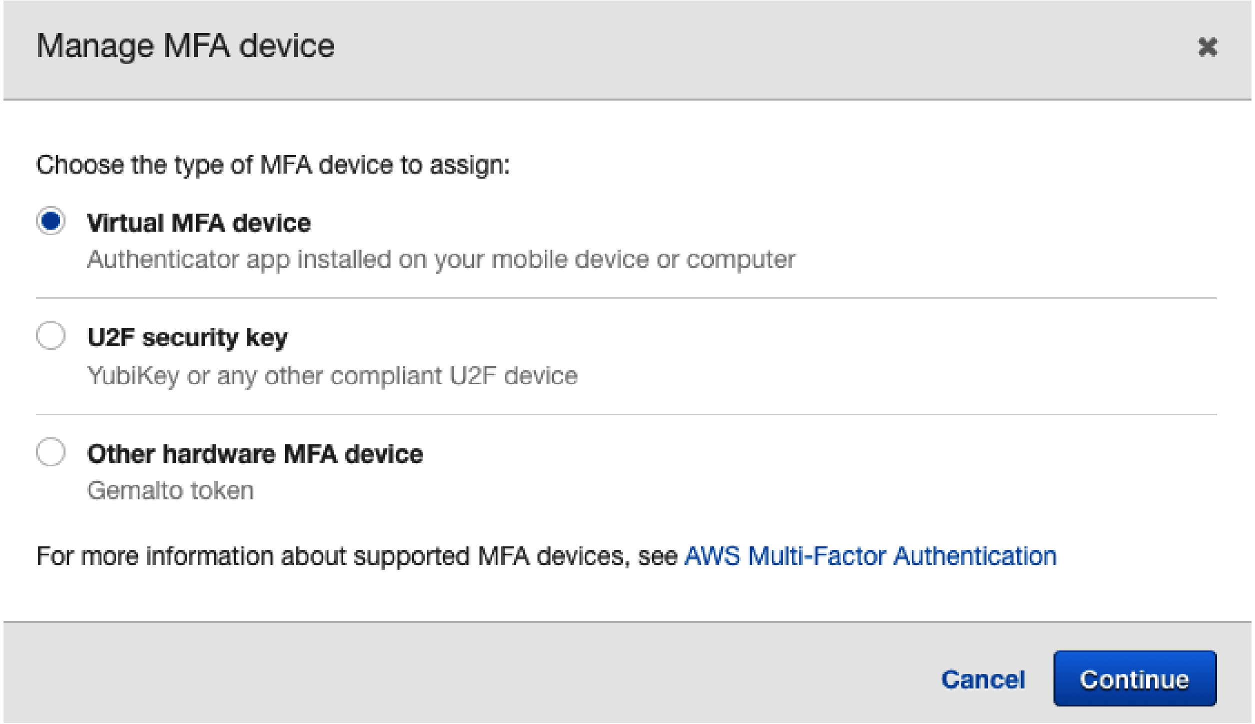


▾ Access keys (access key ID and secret access key)

Use access keys to make programmatic calls to AWS from the AWS CLI, Tools for PowerShell, the AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more

Created	Access Key ID	Last Used	Last Used Region	Last Used Service	Status	Actions

Root user access keys provide unrestricted access to your entire AWS account. If you need long-term access keys, we recommend creating a new IAM user with limited permissions and generating access keys for that user instead. Learn more



Manage MFA device

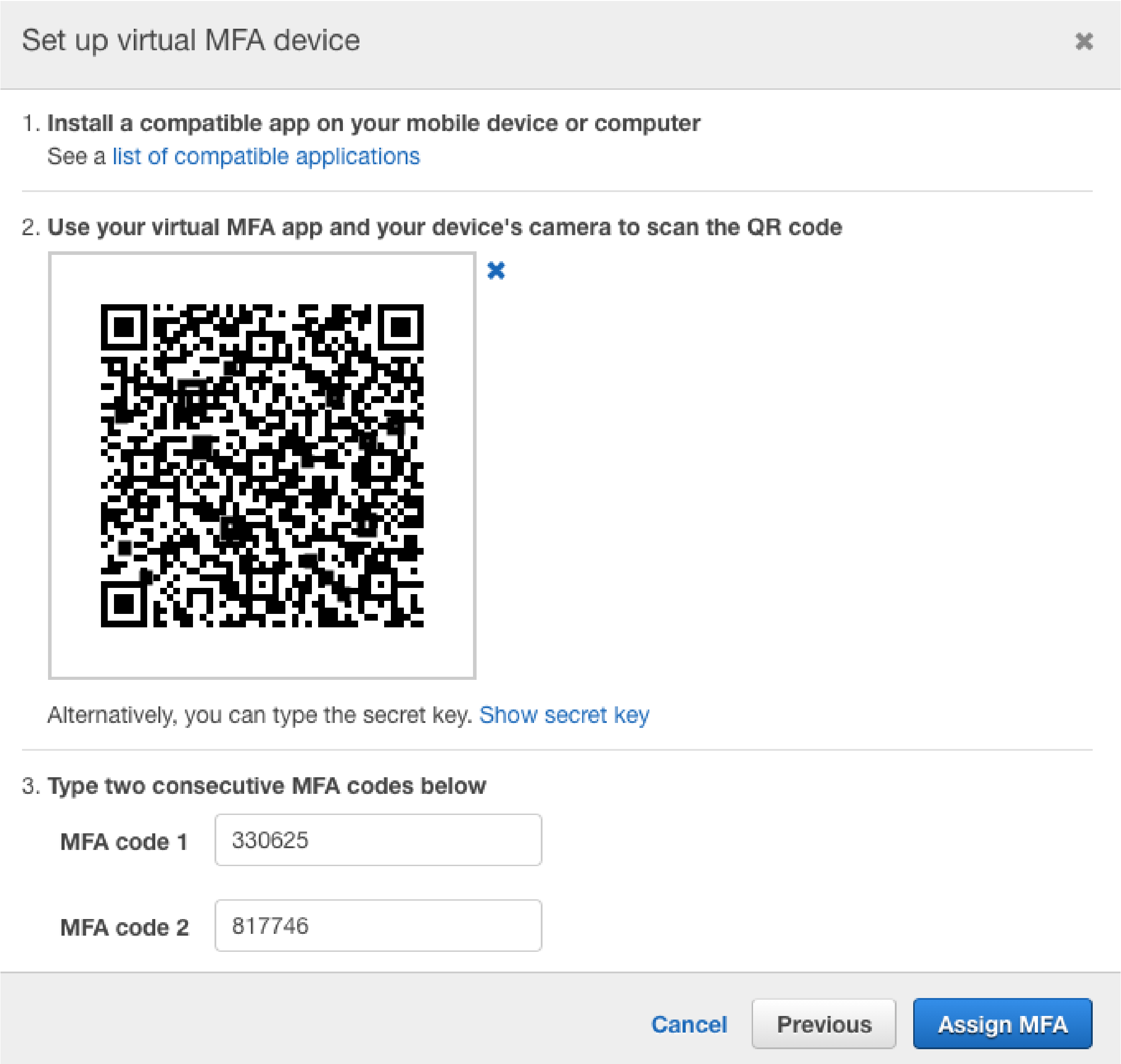
Choose the type of MFA device to assign:

● **Virtual MFA device**
Authenticator app installed on your mobile device or computer

○ **U2F security key**
YubiKey or any other compliant U2F device

○ **Other hardware MFA device**
Gemalto token

For more information about supported MFA devices, see AWS Multi-Factor Authentication



Set up virtual MFA device ✖

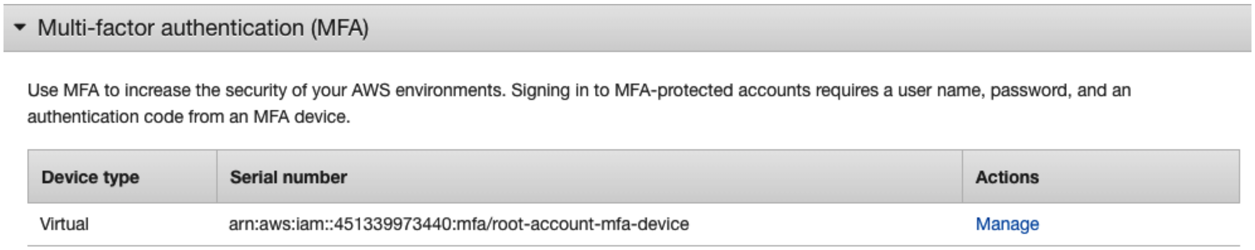
1. **Install a compatible app on your mobile device or computer**
   See a list of compatible applications

2. **Use your virtual MFA app and your device's camera to scan the QR code** ✖

   Alternatively, you can type the secret key. Show secret key

3. **Type two consecutive MFA codes below**

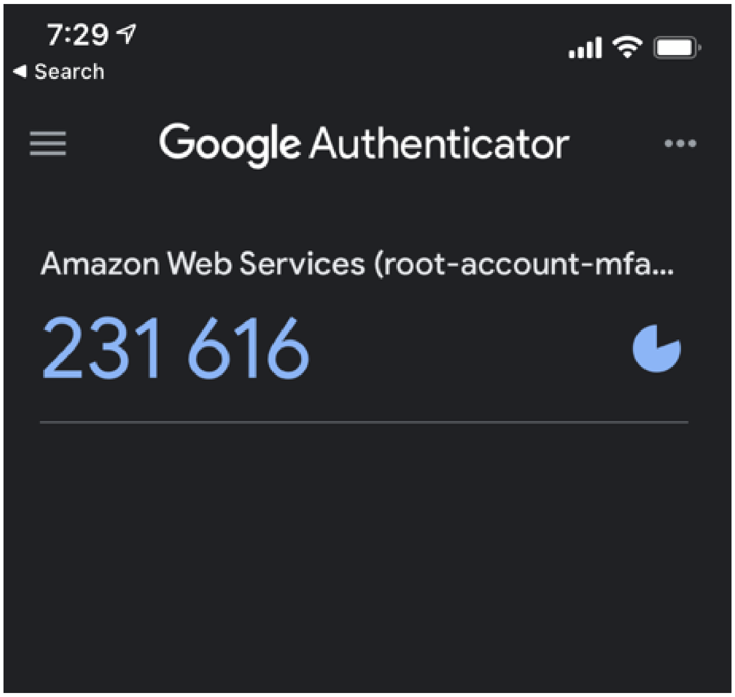
MFA code 1	330625
MFA code 2	817746



▾ Multi-factor authentication (MFA)

Use MFA to increase the security of your AWS environments. Signing in to MFA-protected accounts requires a user name, password, and an authentication code from an MFA device.

Device type	Serial number	Actions
Virtual	arn:aws:iam::451339973440:mfa/root-account-mfa-device	Manage



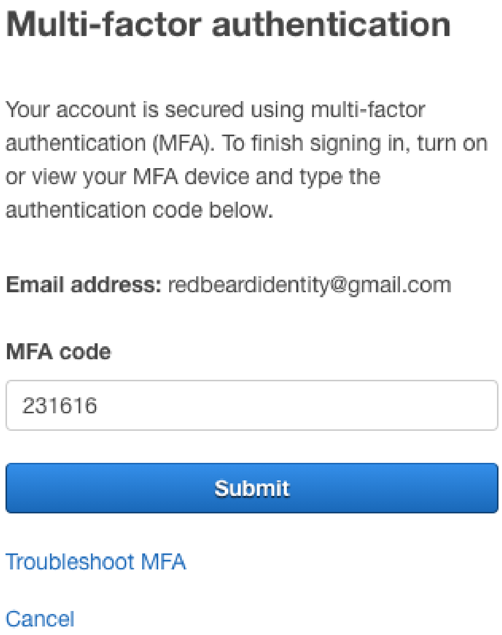
7:29

◂ Search

Google Authenticator

Amazon Web Services (root-account-mfa...

231 616



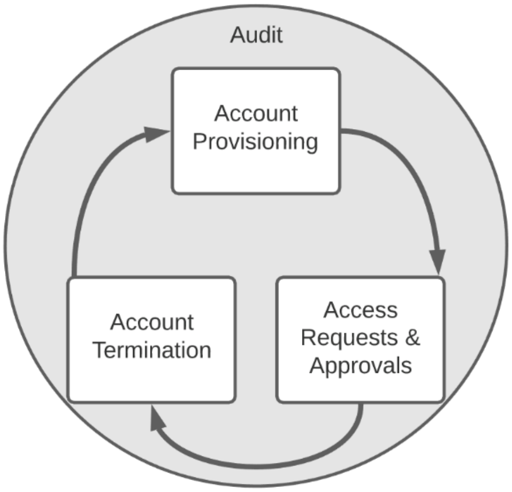
Multi-factor authentication

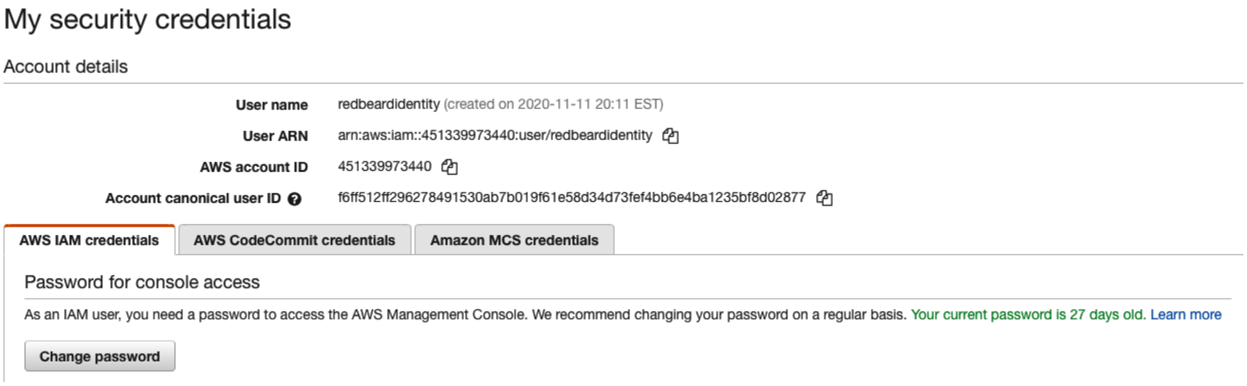
Your account is secured using multi-factor authentication (MFA). To finish signing in, turn on or view your MFA device and type the authentication code below.

Email address: redbeardidentity@gmail.com

MFA code

231616





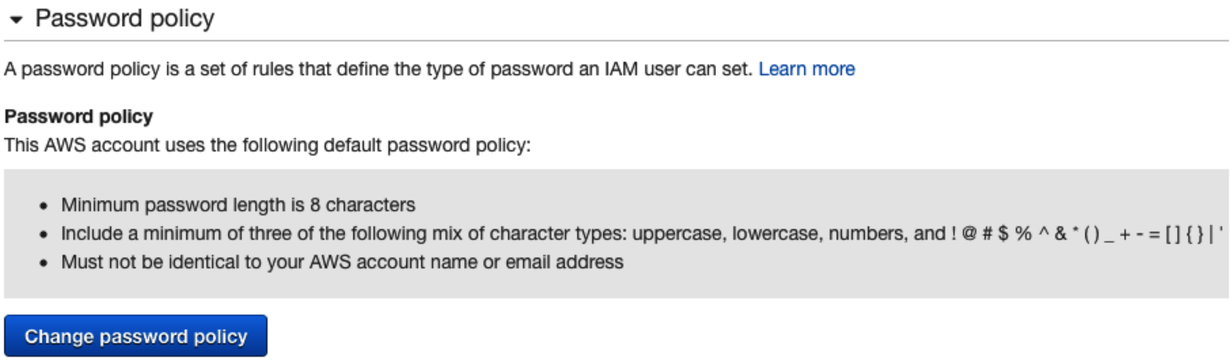
My security credentials

Account details

User name	redbeardidentity (created on 2020-11-11 20:11 EST)
User ARN	arn:aws:iam::451339973440:user/redbeardidentity
AWS account ID	451339973440
Account canonical user ID	f6ff512ff296278491530ab7b019f61e58d34d73fef4bb6e4ba1235bf8d02877

Password for console access

As an IAM user, you need a password to access the AWS Management Console. We recommend changing your password on a regular basis. Your current password is 27 days old. Learn more



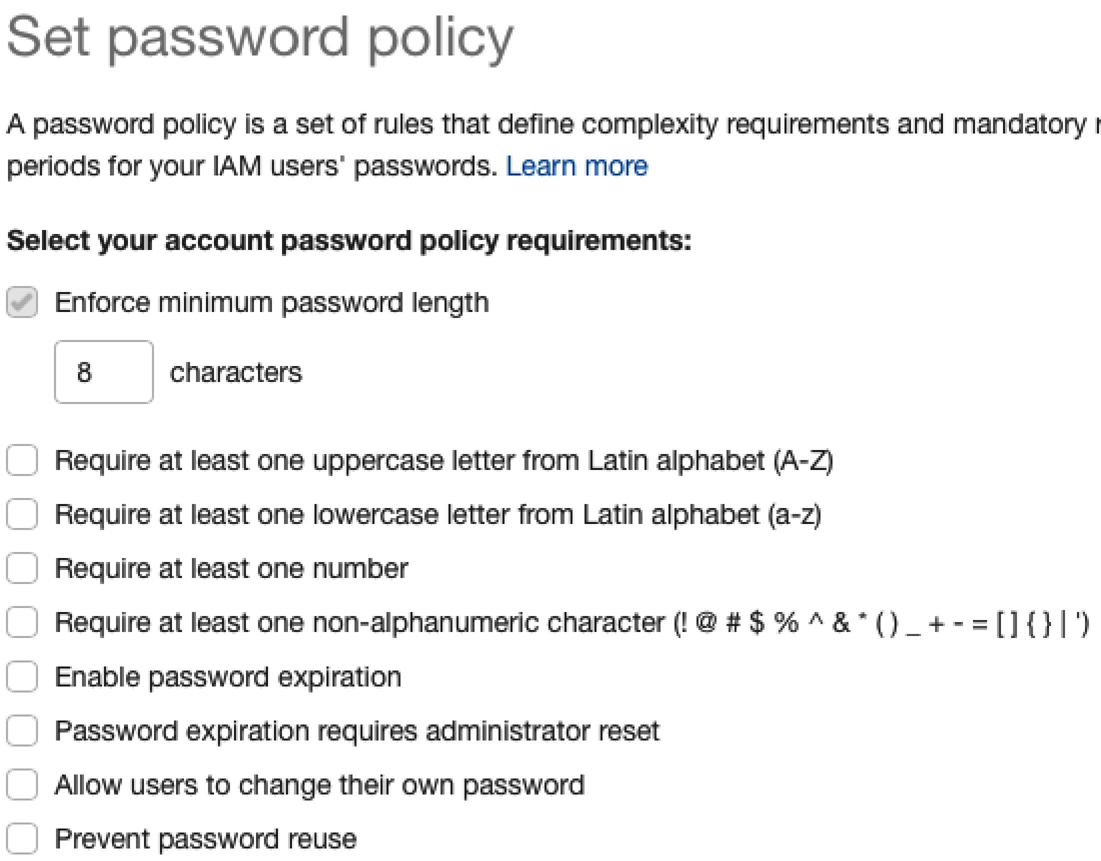
Password policy

A password policy is a set of rules that define the type of password an IAM user can set. Learn more

Password policy

This AWS account uses the following default password policy:

- Minimum password length is 8 characters
- Include a minimum of three of the following mix of character types: uppercase, lowercase, numbers, and ! @ # $ % ^ & * ( ) _ + - = [ ] { } | '
- Must not be identical to your AWS account name or email address



Set password policy

A password policy is a set of rules that define complexity requirements and mandatory rotation periods for your IAM users' passwords. Learn more

Select your account password policy requirements:

☑ Enforce minimum password length

8 characters

☐ Require at least one uppercase letter from Latin alphabet (A-Z)

☐ Require at least one lowercase letter from Latin alphabet (a-z)

☐ Require at least one number

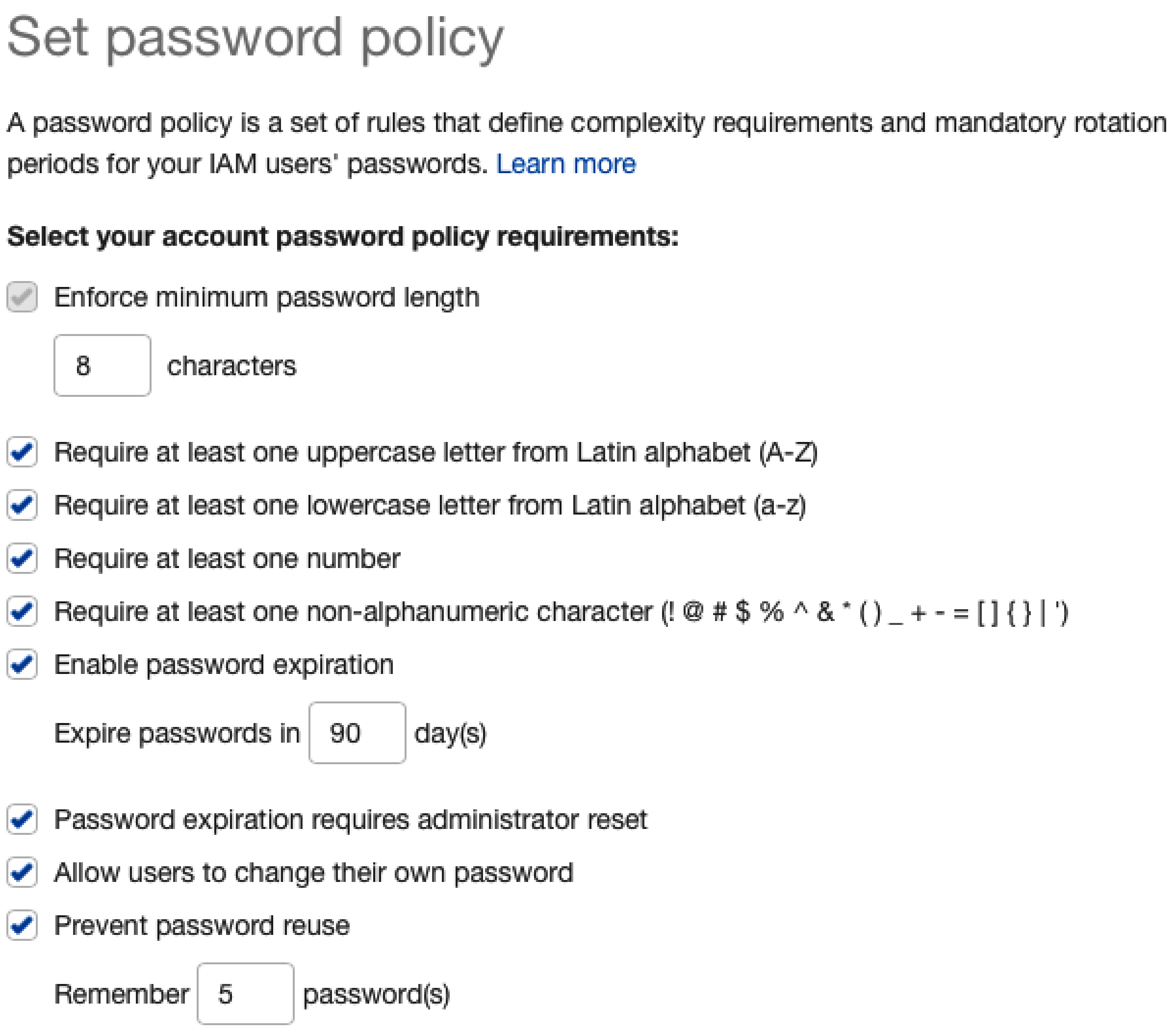
☐ Require at least one non-alphanumeric character (! @ # $ % ^ & * ( ) _ + - = [ ] { } | ')

☐ Enable password expiration

☐ Password expiration requires administrator reset

☐ Allow users to change their own password

☐ Prevent password reuse



Set password policy

A password policy is a set of rules that define complexity requirements and mandatory rotation periods for your IAM users' passwords. Learn more

Select your account password policy requirements:

☑ Enforce minimum password length

8 characters

☑ Require at least one uppercase letter from Latin alphabet (A-Z)

☑ Require at least one lowercase letter from Latin alphabet (a-z)

☑ Require at least one number

☑ Require at least one non-alphanumeric character (! @ # $ % ^ & * ( ) _ + - = [ ] { } | ')

☑ Enable password expiration

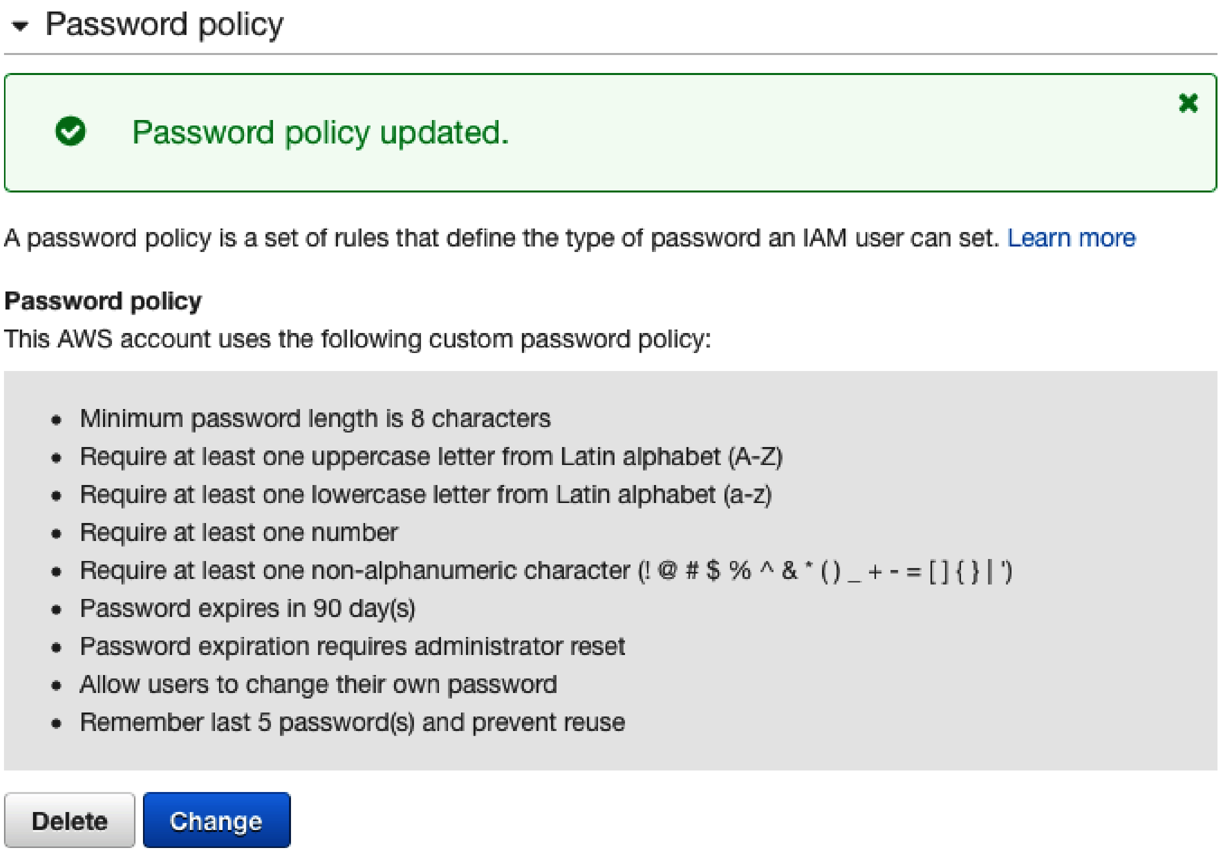
Expire passwords in 90 day(s)

☑ Password expiration requires administrator reset

☑ Allow users to change their own password

☑ Prevent password reuse

Remember 5 password(s)



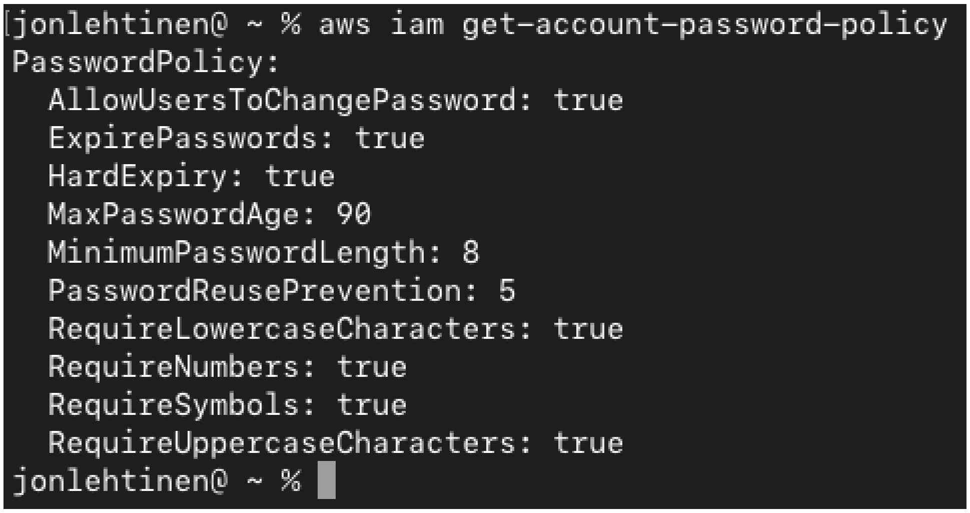
✓ Password policy updated. ✖

A password policy is a set of rules that define the type of password an IAM user can set. Learn more

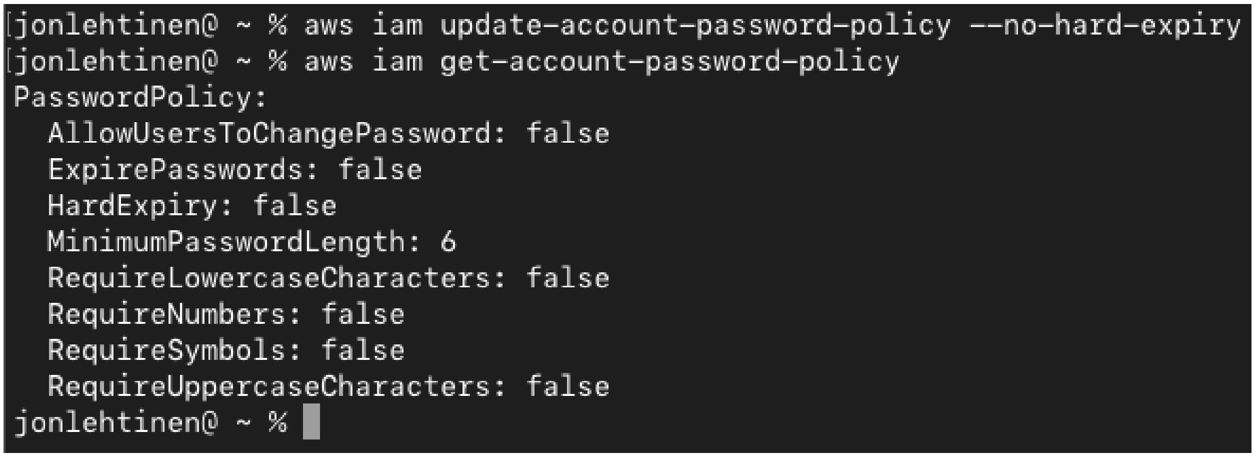
Password policy

This AWS account uses the following custom password policy:

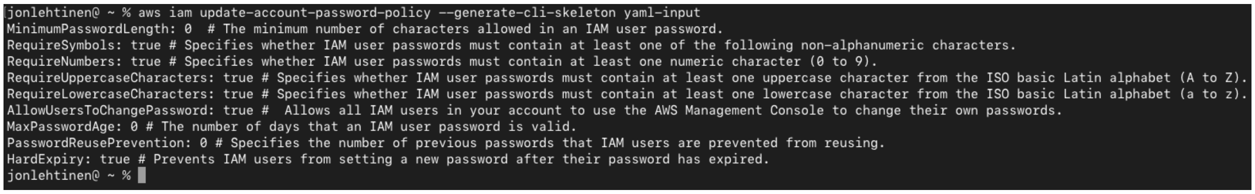
- Minimum password length is 8 characters
- Require at least one uppercase letter from Latin alphabet (A-Z)
- Require at least one lowercase letter from Latin alphabet (a-z)
- Require at least one number
- Require at least one non-alphanumeric character (! @ # $ % ^ & * ( ) _ + - = [ ] { } | ')
- Password expires in 90 day(s)
- Password expiration requires administrator reset
- Allow users to change their own password
- Remember last 5 password(s) and prevent reuse



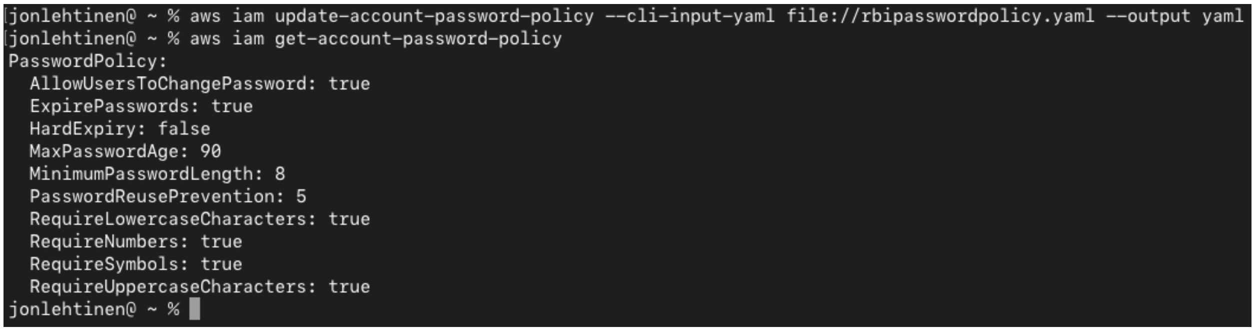
```
[jonlehtinen@ ~ % aws iam get-account-password-policy
PasswordPolicy:
  AllowUsersToChangePassword: true
  ExpirePasswords: true
  HardExpiry: true
  MaxPasswordAge: 90
  MinimumPasswordLength: 8
  PasswordReusePrevention: 5
  RequireLowercaseCharacters: true
  RequireNumbers: true
  RequireSymbols: true
  RequireUppercaseCharacters: true
jonlehtinen@ ~ %
```



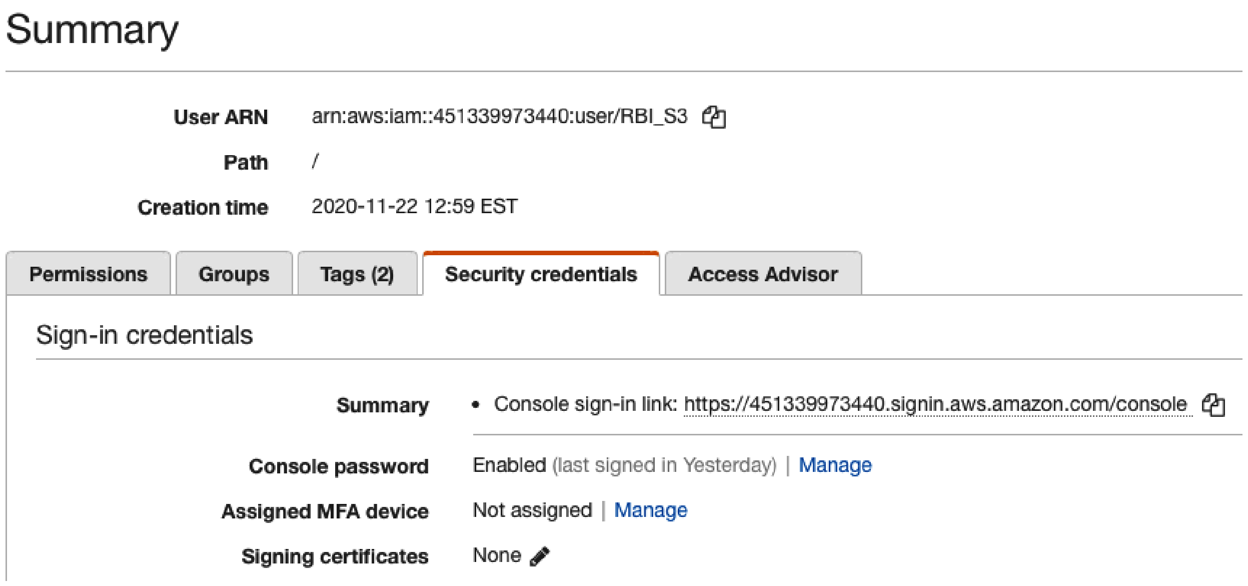
```
[jonlehtinen@ ~ % aws iam update-account-password-policy --no-hard-expiry
[jonlehtinen@ ~ % aws iam get-account-password-policy
PasswordPolicy:
  AllowUsersToChangePassword: false
  ExpirePasswords: false
  HardExpiry: false
  MinimumPasswordLength: 6
  RequireLowercaseCharacters: false
  RequireNumbers: false
  RequireSymbols: false
  RequireUppercaseCharacters: false
jonlehtinen@ ~ %
```



```
[jonlehtinen@ ~ % aws iam update-account-password-policy --generate-cli-skeleton yaml-input
MinimumPasswordLength: 0  # The minimum number of characters allowed in an IAM user password.
RequireSymbols: true # Specifies whether IAM user passwords must contain at least one of the following non-alphanumeric characters.
RequireNumbers: true # Specifies whether IAM user passwords must contain at least one numeric character (0 to 9).
RequireUppercaseCharacters: true # Specifies whether IAM user passwords must contain at least one uppercase character from the ISO basic Latin alphabet (A to Z).
RequireLowercaseCharacters: true # Specifies whether IAM user passwords must contain at least one lowercase character from the ISO basic Latin alphabet (a to z).
AllowUsersToChangePassword: true #  Allows all IAM users in your account to use the AWS Management Console to change their own passwords.
MaxPasswordAge: 0 # The number of days that an IAM user password is valid.
PasswordReusePrevention: 0 # Specifies the number of previous passwords that IAM users are prevented from reusing.
HardExpiry: true # Prevents IAM users from setting a new password after their password has expired.
jonlehtinen@ ~ %
```



```
[jonlehtinen@ ~ % aws iam update-account-password-policy --cli-input-yaml file://rbipasswordpolicy.yaml --output yaml
[jonlehtinen@ ~ % aws iam get-account-password-policy
PasswordPolicy:
  AllowUsersToChangePassword: true
  ExpirePasswords: true
  HardExpiry: false
  MaxPasswordAge: 90
  MinimumPasswordLength: 8
  PasswordReusePrevention: 5
  RequireLowercaseCharacters: true
  RequireNumbers: true
  RequireSymbols: true
  RequireUppercaseCharacters: true
jonlehtinen@ ~ %
```



Summary

User ARN arn:aws:iam::451339973440:user/RBI_S3

Path /

Creation time 2020-11-22 12:59 EST

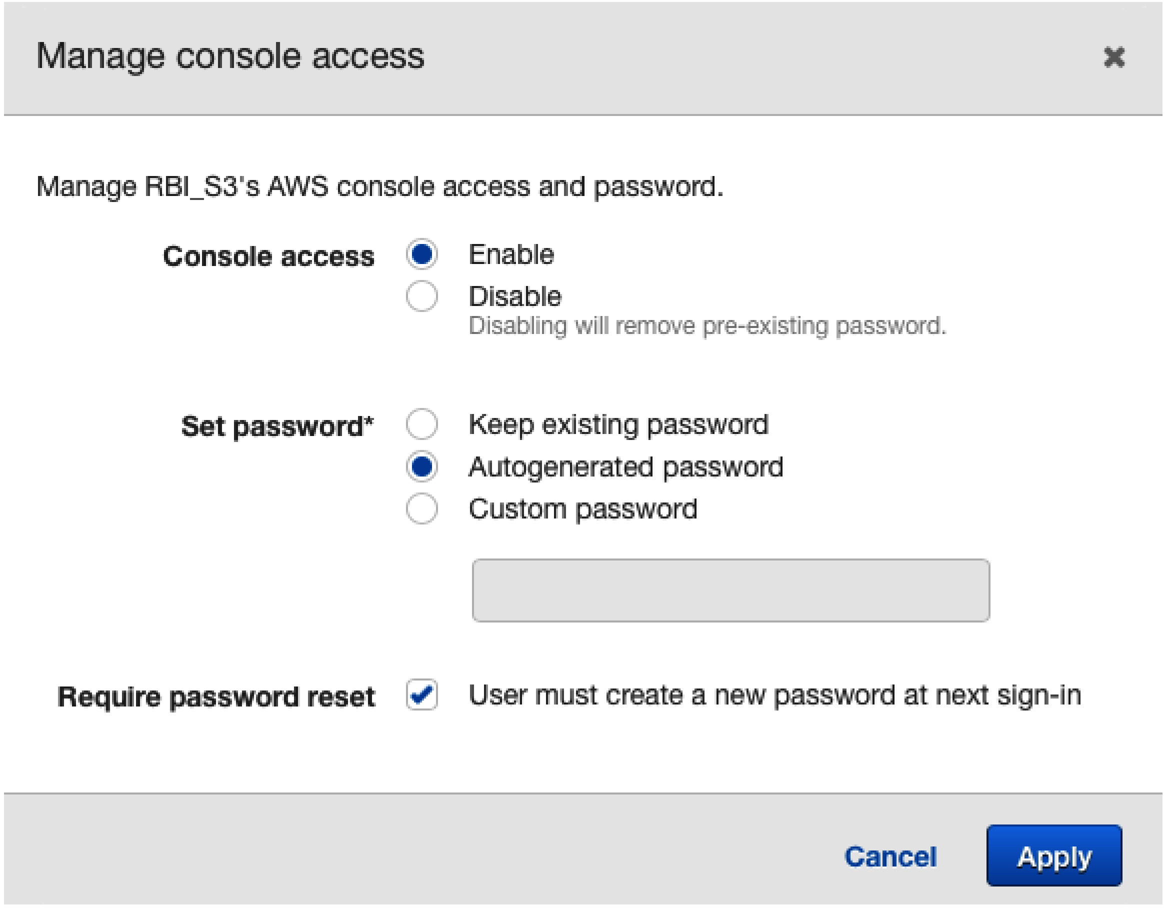
Sign-in credentials

Summary
- Console sign-in link: https://451339973440.signin.aws.amazon.com/console

Console password Enabled (last signed in Yesterday) | Manage

Assigned MFA device Not assigned | Manage

Signing certificates None



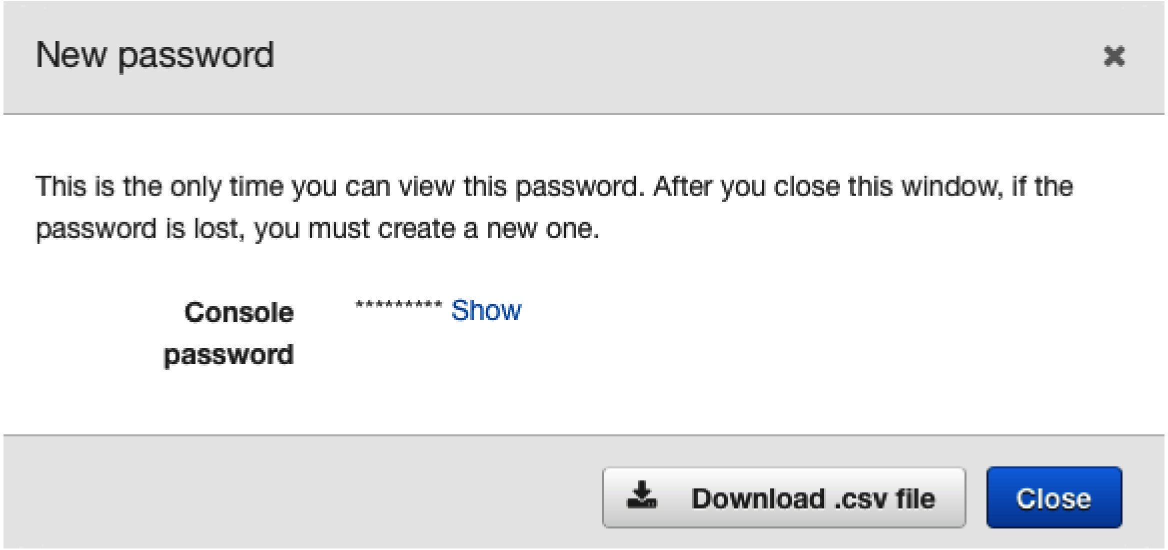
Manage console access

Manage RBI_S3's AWS console access and password.

Console access
● Enable
○ Disable
Disabling will remove pre-existing password.

Set password*
○ Keep existing password
● Autogenerated password
○ Custom password

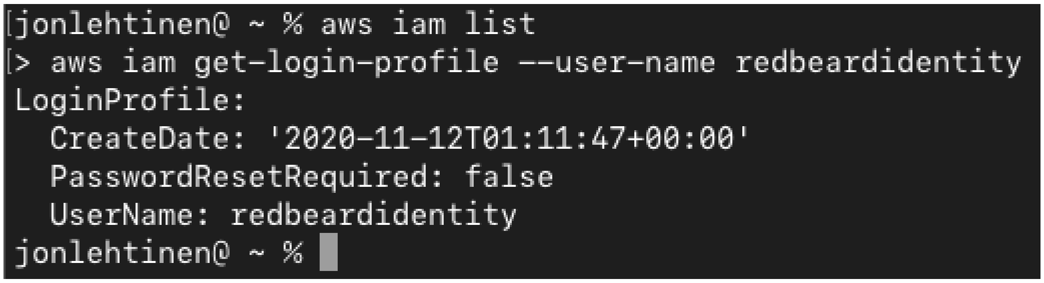
Require password reset ☑ User must create a new password at next sign-in



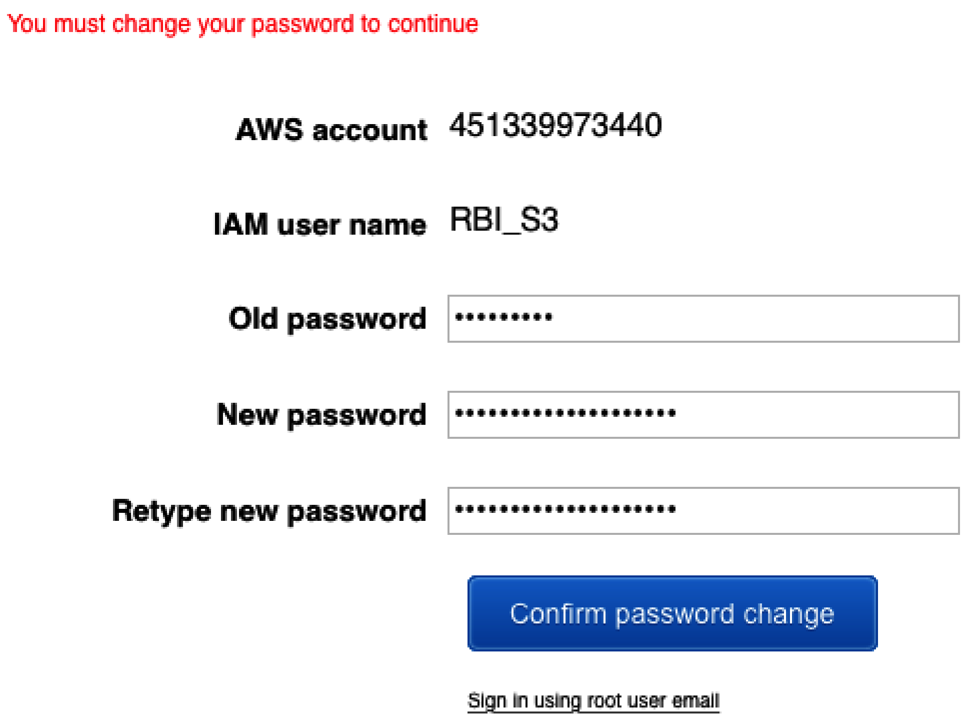
New password

This is the only time you can view this password. After you close this window, if the password is lost, you must create a new one.

Console password ********* Show

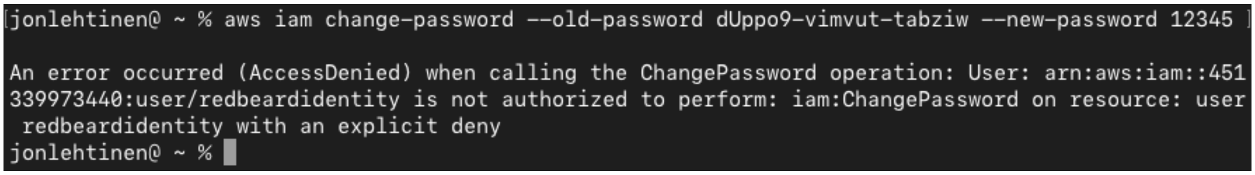


```
[jonlehtinen@ ~ % aws iam list
[> aws iam get-login-profile --user-name redbeardidentity
LoginProfile:
  CreateDate: '2020-11-12T01:11:47+00:00'
  PasswordResetRequired: false
  UserName: redbeardidentity
jonlehtinen@ ~ %
```

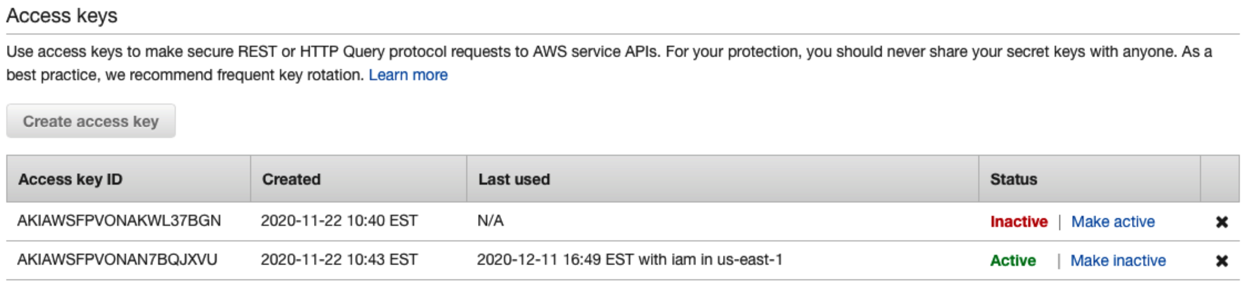


You must change your password to continue

AWS account	451339973440
IAM user name	RBI_S3
Old password	•••••••••
New password	••••••••••••••••••••
Retype new password	••••••••••••••••••••



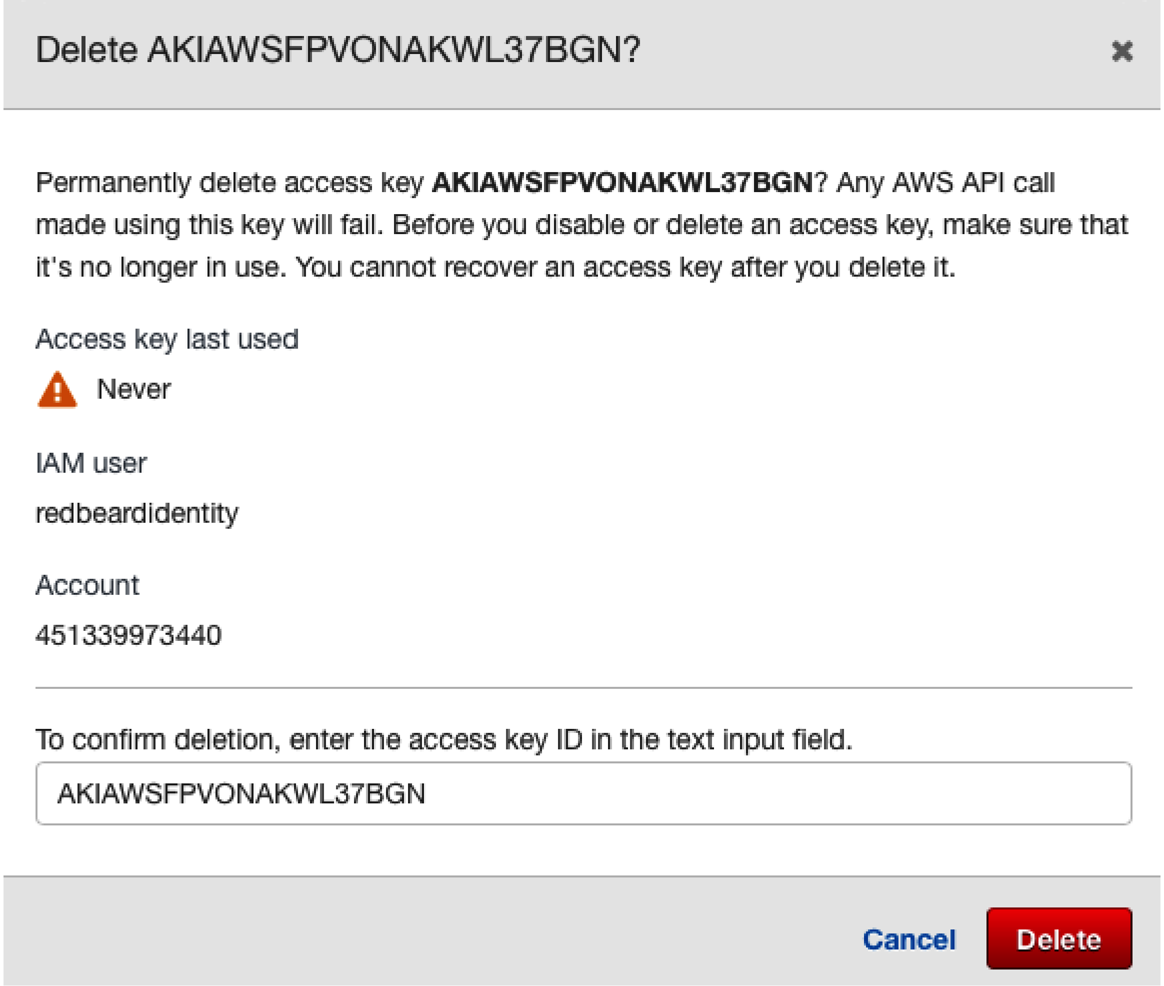
```
[jonlehtinen@ ~ % aws iam change-password --old-password dUppo9-vimvut-tabziw --new-password 12345 ]

An error occurred (AccessDenied) when calling the ChangePassword operation: User: arn:aws:iam::451
339973440:user/redbeardidentity is not authorized to perform: iam:ChangePassword on resource: user
 redbeardidentity with an explicit deny
jonlehtinen@ ~ % █
```



Access keys

Use access keys to make secure REST or HTTP Query protocol requests to AWS service APIs. For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation. Learn more

Access key ID	Created	Last used	Status	
AKIAWSFPVONAKWL37BGN	2020-11-22 10:40 EST	N/A	Inactive | Make active	✖
AKIAWSFPVONAN7BQJXVU	2020-11-22 10:43 EST	2020-12-11 16:49 EST with iam in us-east-1	Active | Make inactive	✖



Delete AKIAWSFPVONAKWL37BGN?

Permanently delete access key **AKIAWSFPVONAKWL37BGN**? Any AWS API call made using this key will fail. Before you disable or delete an access key, make sure that it's no longer in use. You cannot recover an access key after you delete it.

Access key last used

⚠ Never

IAM user

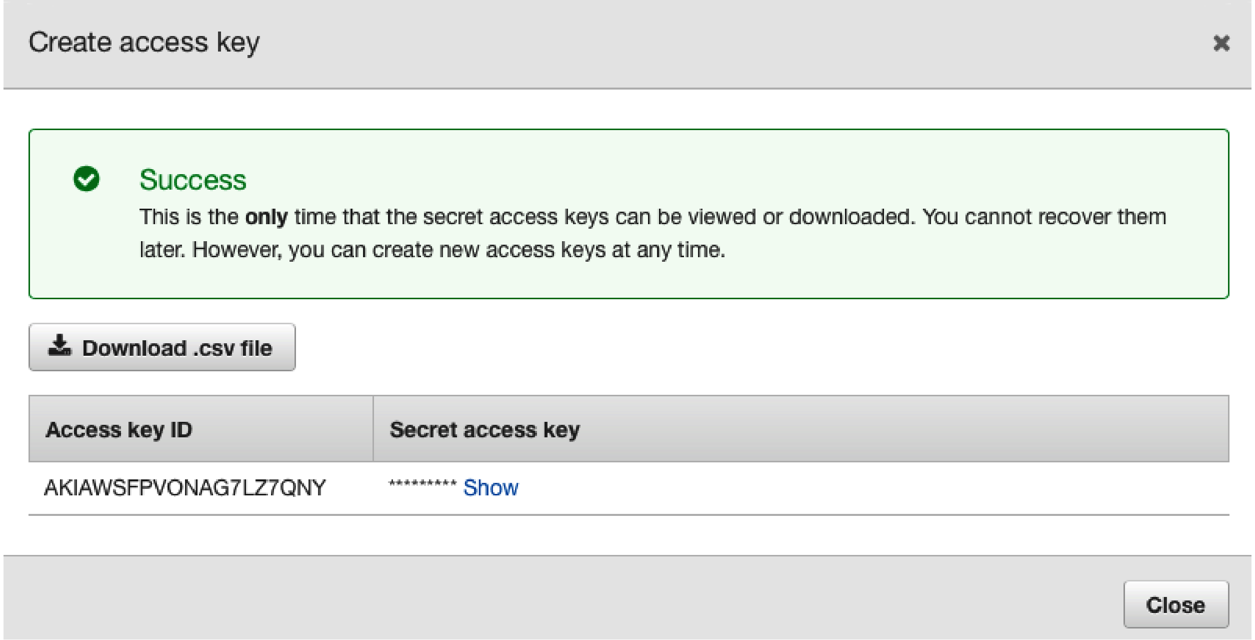
redbeardidentity

Account

451339973440

To confirm deletion, enter the access key ID in the text input field.

AKIAWSFPVONAKWL37BGN

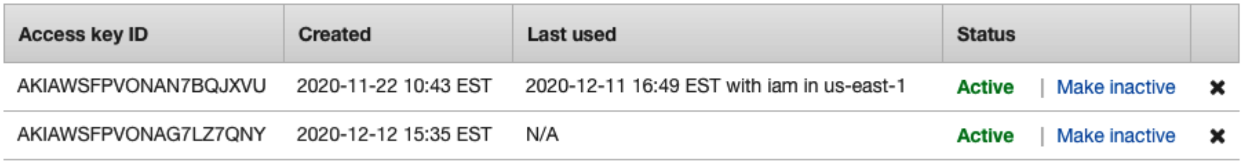


Create access key

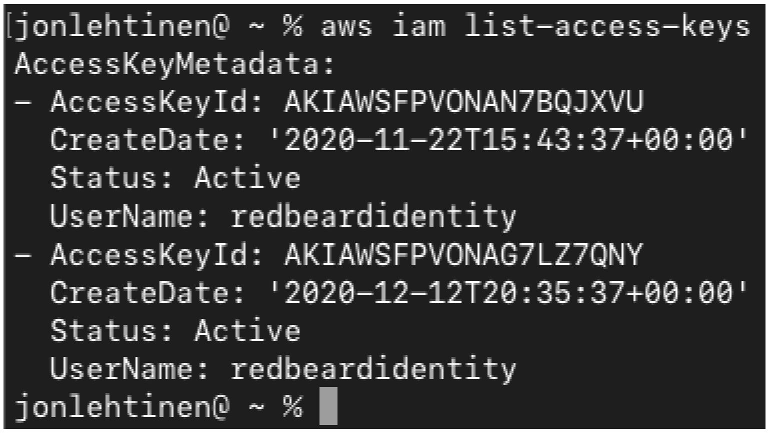
Success

This is the **only** time that the secret access keys can be viewed or downloaded. You cannot recover them later. However, you can create new access keys at any time.

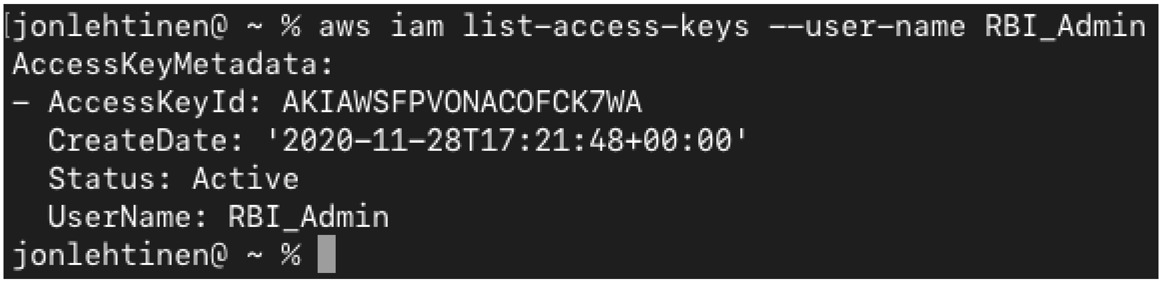
Access key ID	Secret access key
AKIAWSFPVONAG7LZ7QNY	********* Show



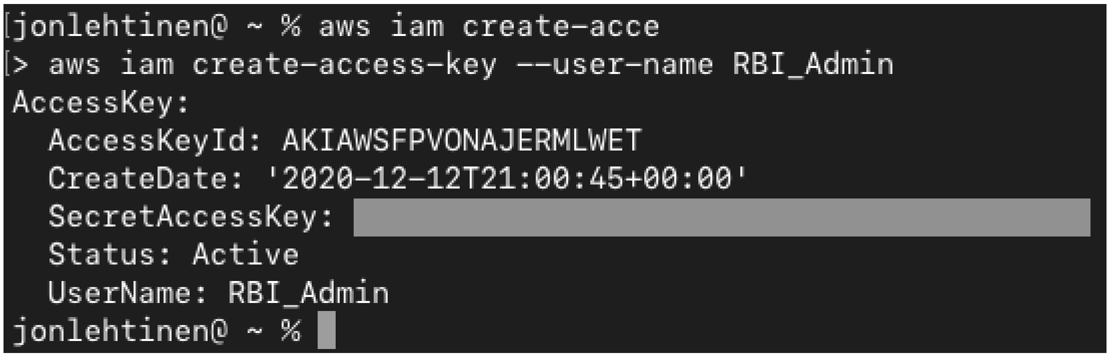
Access key ID	Created	Last used	Status	
AKIAWSFPVONAN7BQJXVU	2020-11-22 10:43 EST	2020-12-11 16:49 EST with iam in us-east-1	Active | Make inactive	✖
AKIAWSFPVONAG7LZ7QNY	2020-12-12 15:35 EST	N/A	Active | Make inactive	✖



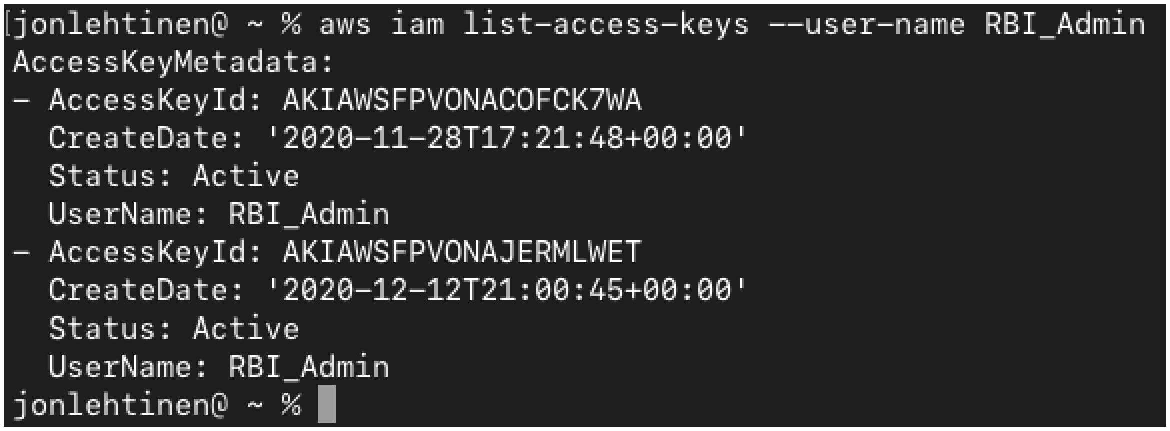
```
[jonlehtinen@ ~ % aws iam list-access-keys
AccessKeyMetadata:
- AccessKeyId: AKIAWSFPVONAN7BQJXVU
  CreateDate: '2020-11-22T15:43:37+00:00'
  Status: Active
  UserName: redbeardidentity
- AccessKeyId: AKIAWSFPVONAG7LZ7QNY
  CreateDate: '2020-12-12T20:35:37+00:00'
  Status: Active
  UserName: redbeardidentity
jonlehtinen@ ~ %
```



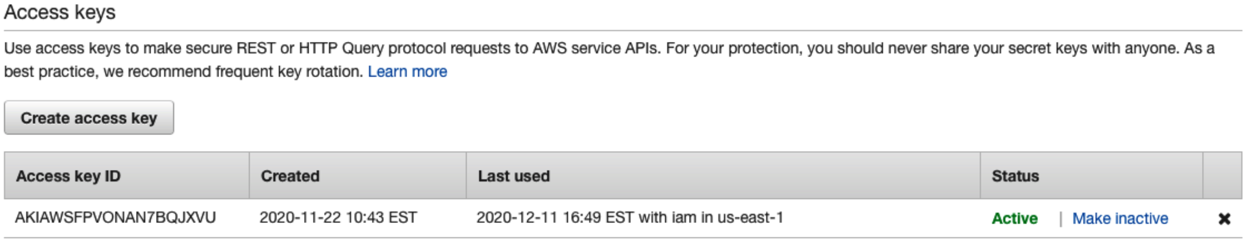
```
[jonlehtinen@ ~ % aws iam list-access-keys --user-name RBI_Admin
AccessKeyMetadata:
- AccessKeyId: AKIAWSFPVONACOFCK7WA
  CreateDate: '2020-11-28T17:21:48+00:00'
  Status: Active
  UserName: RBI_Admin
jonlehtinen@ ~ %
```



```
[jonlehtinen@ ~ % aws iam create-acce
[> aws iam create-access-key --user-name RBI_Admin
AccessKey:
  AccessKeyId: AKIAWSFPVONAJERMLWET
  CreateDate: '2020-12-12T21:00:45+00:00'
  SecretAccessKey: [redacted]
  Status: Active
  UserName: RBI_Admin
jonlehtinen@ ~ %
```



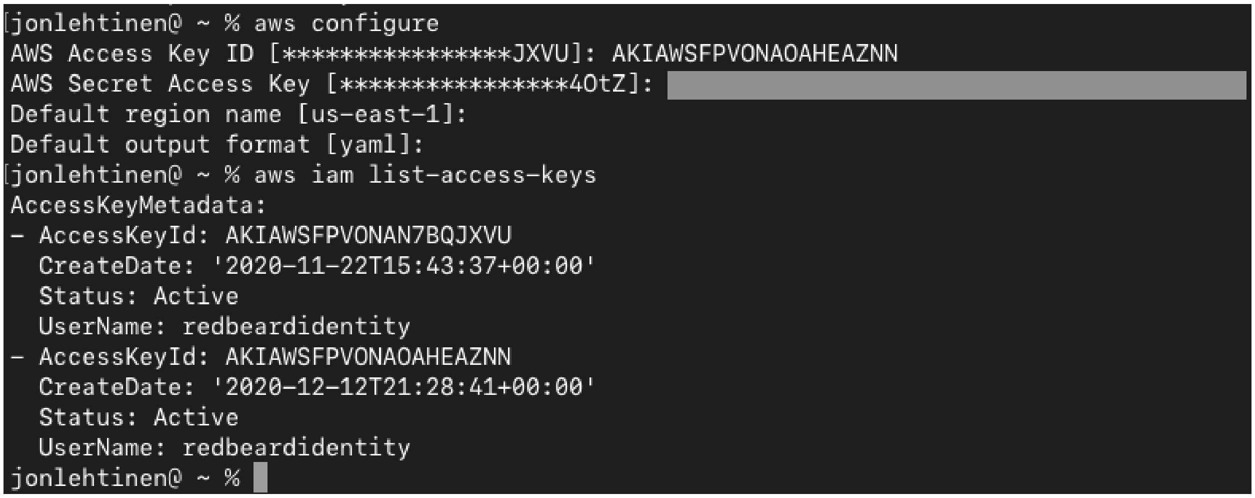
```
[jonlehtinen@ ~ % aws iam list-access-keys --user-name RBI_Admin
AccessKeyMetadata:
- AccessKeyId: AKIAWSFPVONACOFCK7WA
  CreateDate: '2020-11-28T17:21:48+00:00'
  Status: Active
  UserName: RBI_Admin
- AccessKeyId: AKIAWSFPVONAJERMLWET
  CreateDate: '2020-12-12T21:00:45+00:00'
  Status: Active
  UserName: RBI_Admin
jonlehtinen@ ~ %
```



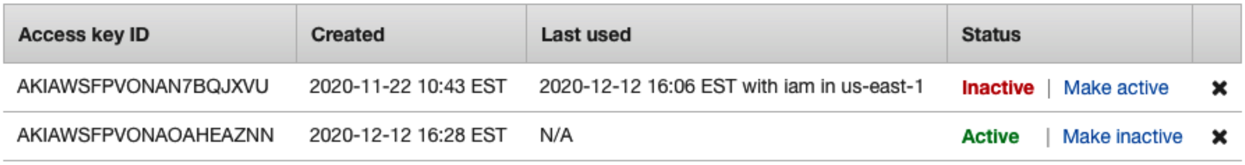
Access keys

Use access keys to make secure REST or HTTP Query protocol requests to AWS service APIs. For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation. Learn more

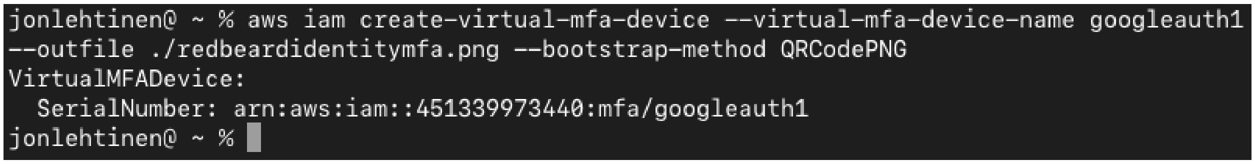
Access key ID	Created	Last used	Status	
AKIAWSFPVONAN7BQJXVU	2020-11-22 10:43 EST	2020-12-11 16:49 EST with iam in us-east-1	Active | Make inactive	✖



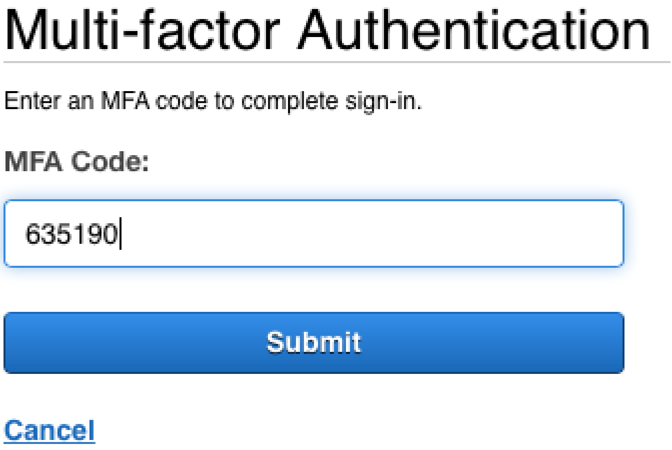
```
[jonlehtinen@ ~ % aws configure
AWS Access Key ID [****************JXVU]: AKIAWSFPVONAOAHEAZNN
AWS Secret Access Key [****************4OtZ]: [redacted]
Default region name [us-east-1]:
Default output format [yaml]:
[jonlehtinen@ ~ % aws iam list-access-keys
AccessKeyMetadata:
- AccessKeyId: AKIAWSFPVONAN7BQJXVU
  CreateDate: '2020-11-22T15:43:37+00:00'
  Status: Active
  UserName: redbeardidentity
- AccessKeyId: AKIAWSFPVONAOAHEAZNN
  CreateDate: '2020-12-12T21:28:41+00:00'
  Status: Active
  UserName: redbeardidentity
jonlehtinen@ ~ %
```



Access key ID	Created	Last used	Status	
AKIAWSFPVONAN7BQJXVU	2020-11-22 10:43 EST	2020-12-12 16:06 EST with iam in us-east-1	Inactive | Make active	✖
AKIAWSFPVONAOAHEAZNN	2020-12-12 16:28 EST	N/A	Active | Make inactive	✖



```
jonlehtinen@ ~ % aws iam create-virtual-mfa-device --virtual-mfa-device-name googleauth1
--outfile ./redbeardidentitymfa.png --bootstrap-method QRCodePNG
VirtualMFADevice:
  SerialNumber: arn:aws:iam::451339973440:mfa/googleauth1
jonlehtinen@ ~ %
```

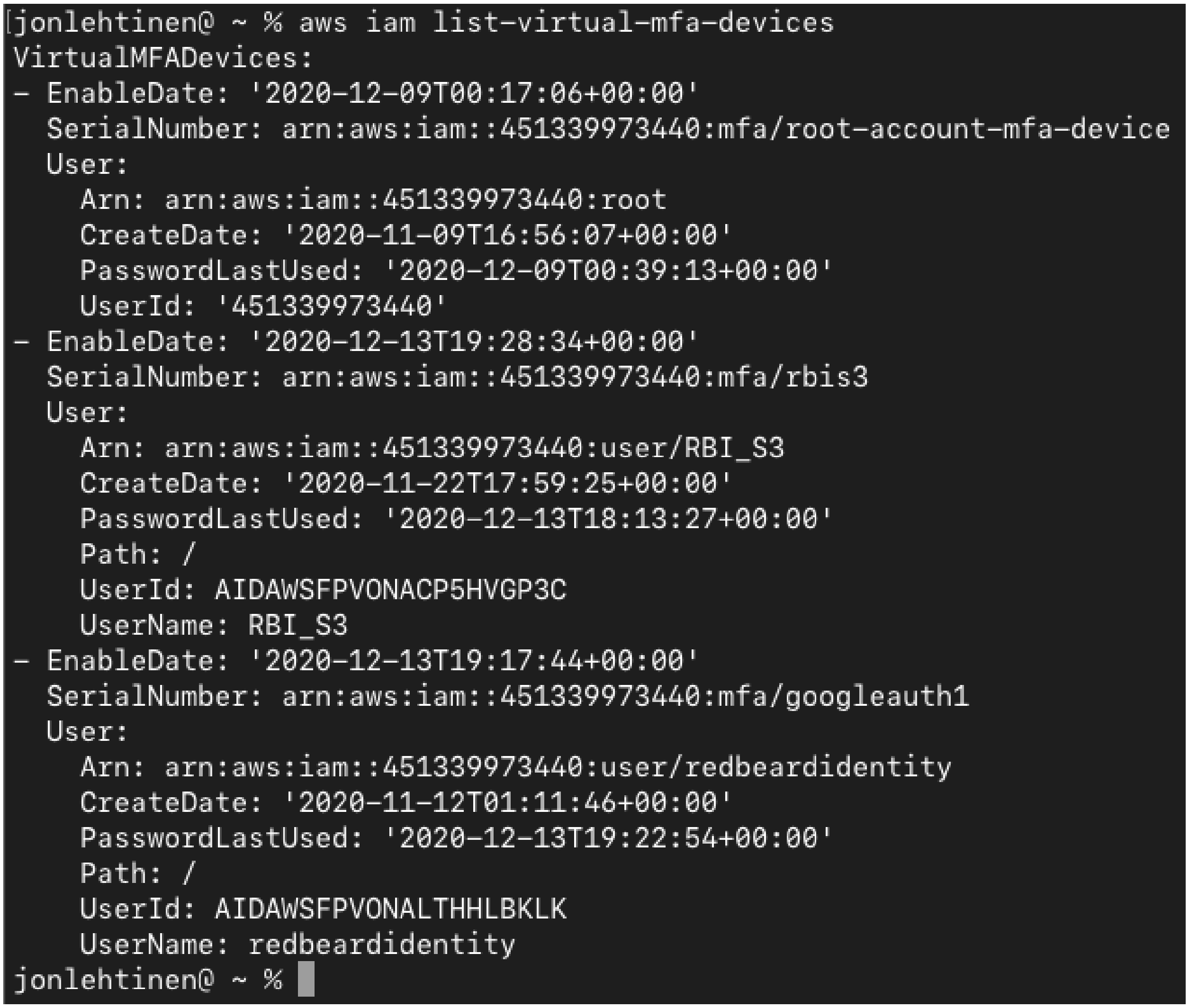


Multi-factor Authentication

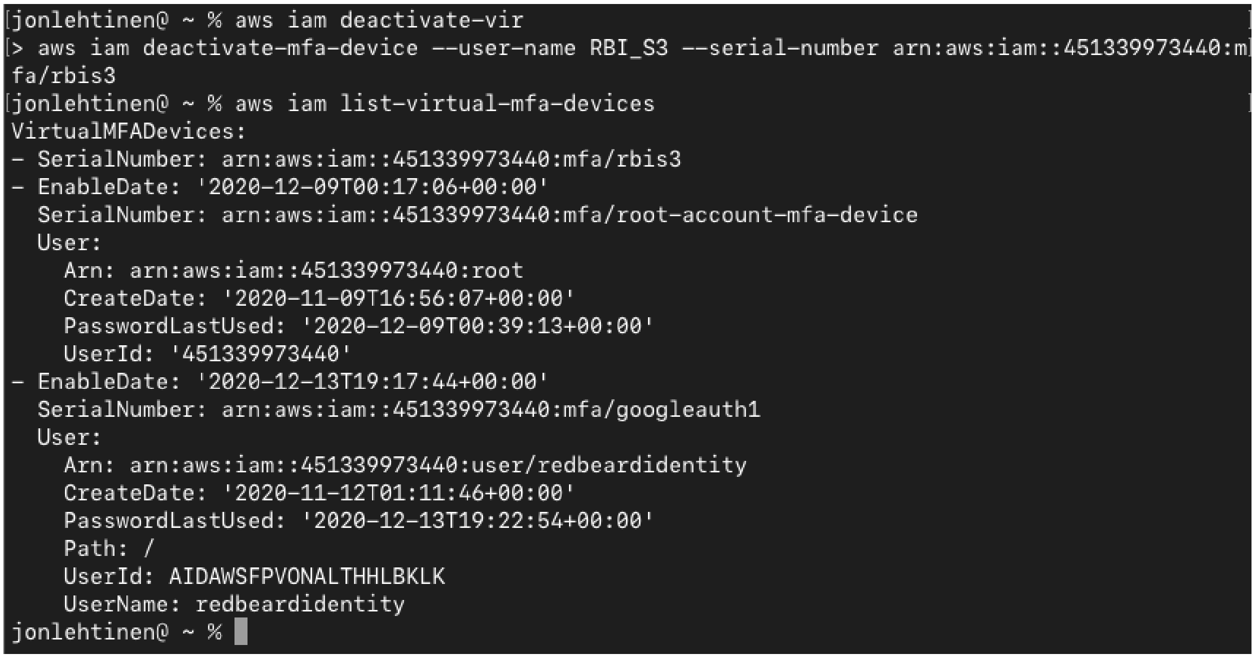
Enter an MFA code to complete sign-in.

MFA Code:

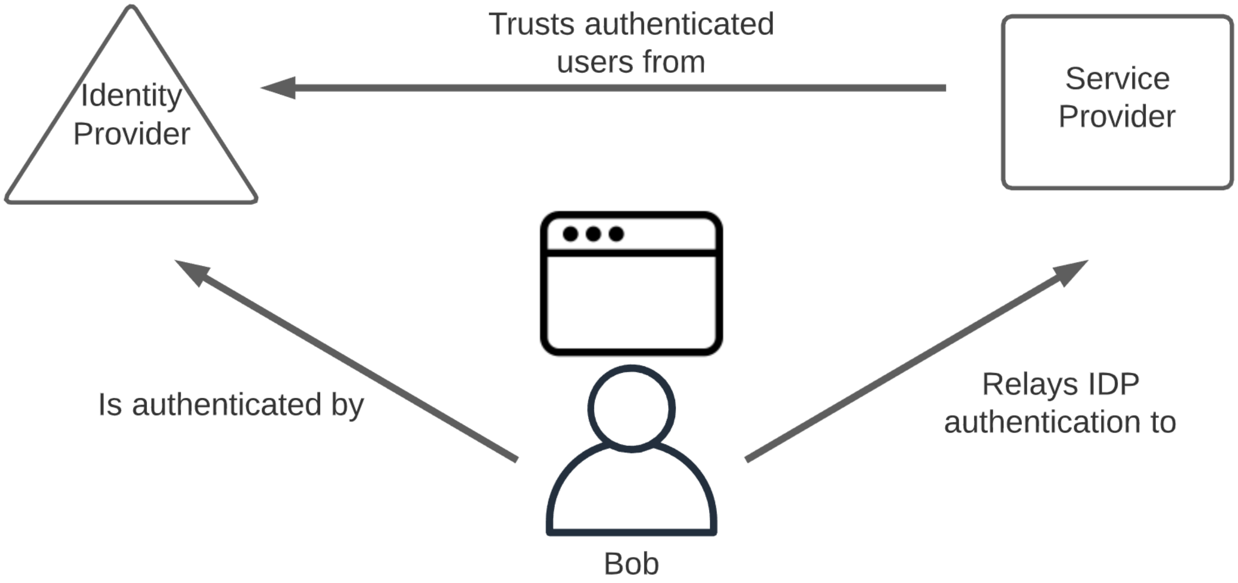
635190

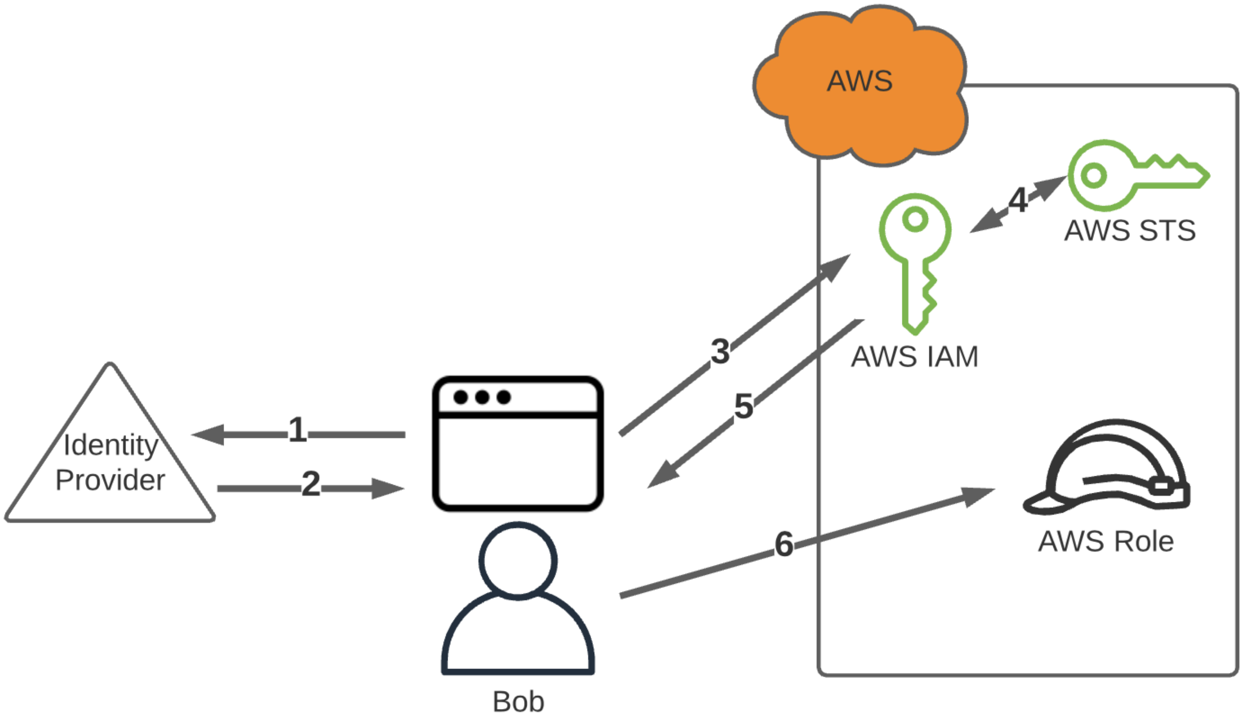


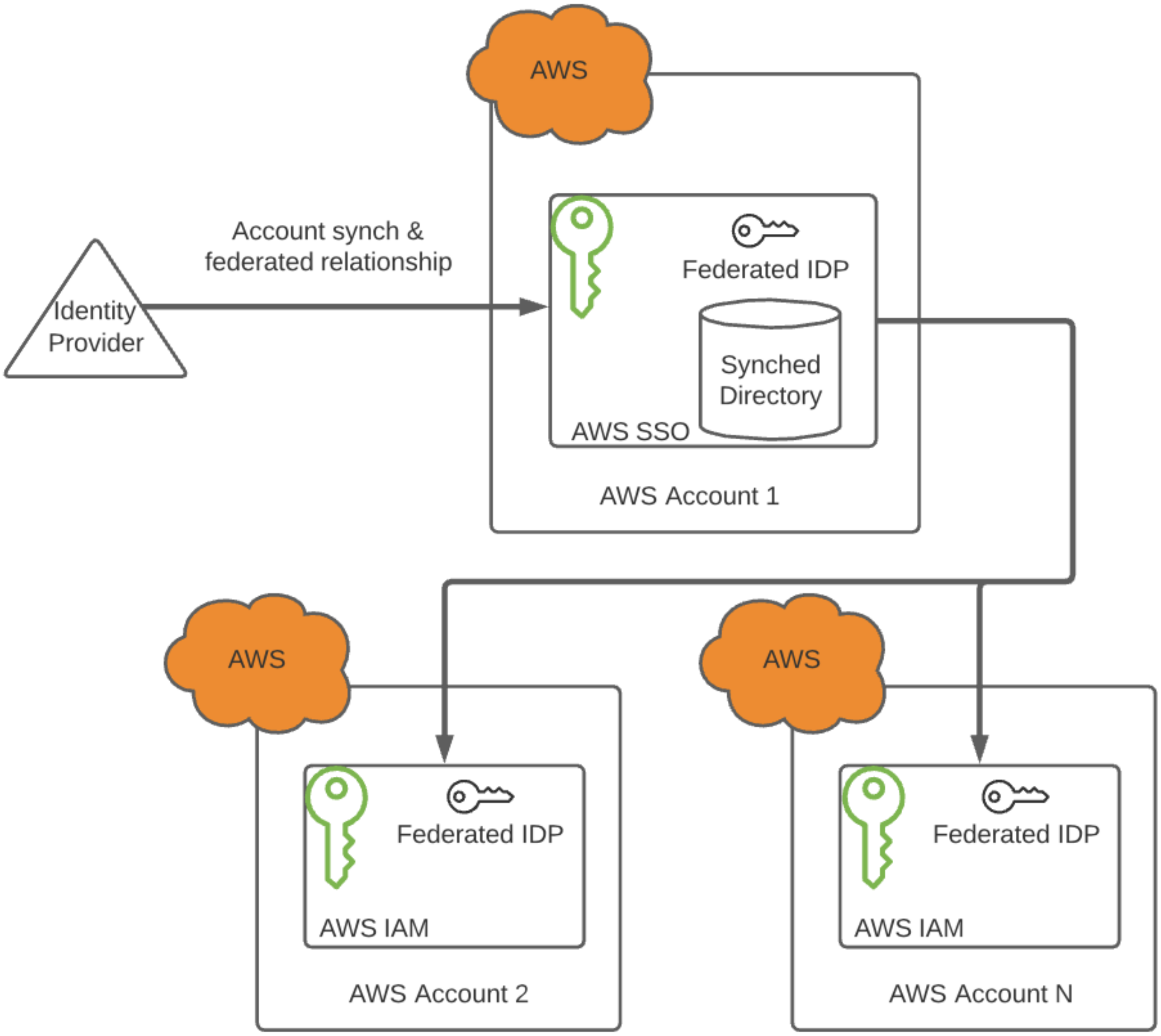
```
[jonlehtinen@ ~ % aws iam list-virtual-mfa-devices
VirtualMFADevices:
- EnableDate: '2020-12-09T00:17:06+00:00'
  SerialNumber: arn:aws:iam::451339973440:mfa/root-account-mfa-device
  User:
    Arn: arn:aws:iam::451339973440:root
    CreateDate: '2020-11-09T16:56:07+00:00'
    PasswordLastUsed: '2020-12-09T00:39:13+00:00'
    UserId: '451339973440'
- EnableDate: '2020-12-13T19:28:34+00:00'
  SerialNumber: arn:aws:iam::451339973440:mfa/rbis3
  User:
    Arn: arn:aws:iam::451339973440:user/RBI_S3
    CreateDate: '2020-11-22T17:59:25+00:00'
    PasswordLastUsed: '2020-12-13T18:13:27+00:00'
    Path: /
    UserId: AIDAWSFPVONACP5HVGP3C
    UserName: RBI_S3
- EnableDate: '2020-12-13T19:17:44+00:00'
  SerialNumber: arn:aws:iam::451339973440:mfa/googleauth1
  User:
    Arn: arn:aws:iam::451339973440:user/redbeardidentity
    CreateDate: '2020-11-12T01:11:46+00:00'
    PasswordLastUsed: '2020-12-13T19:22:54+00:00'
    Path: /
    UserId: AIDAWSFPVONALTHHLBKLK
    UserName: redbeardidentity
jonlehtinen@ ~ %
```



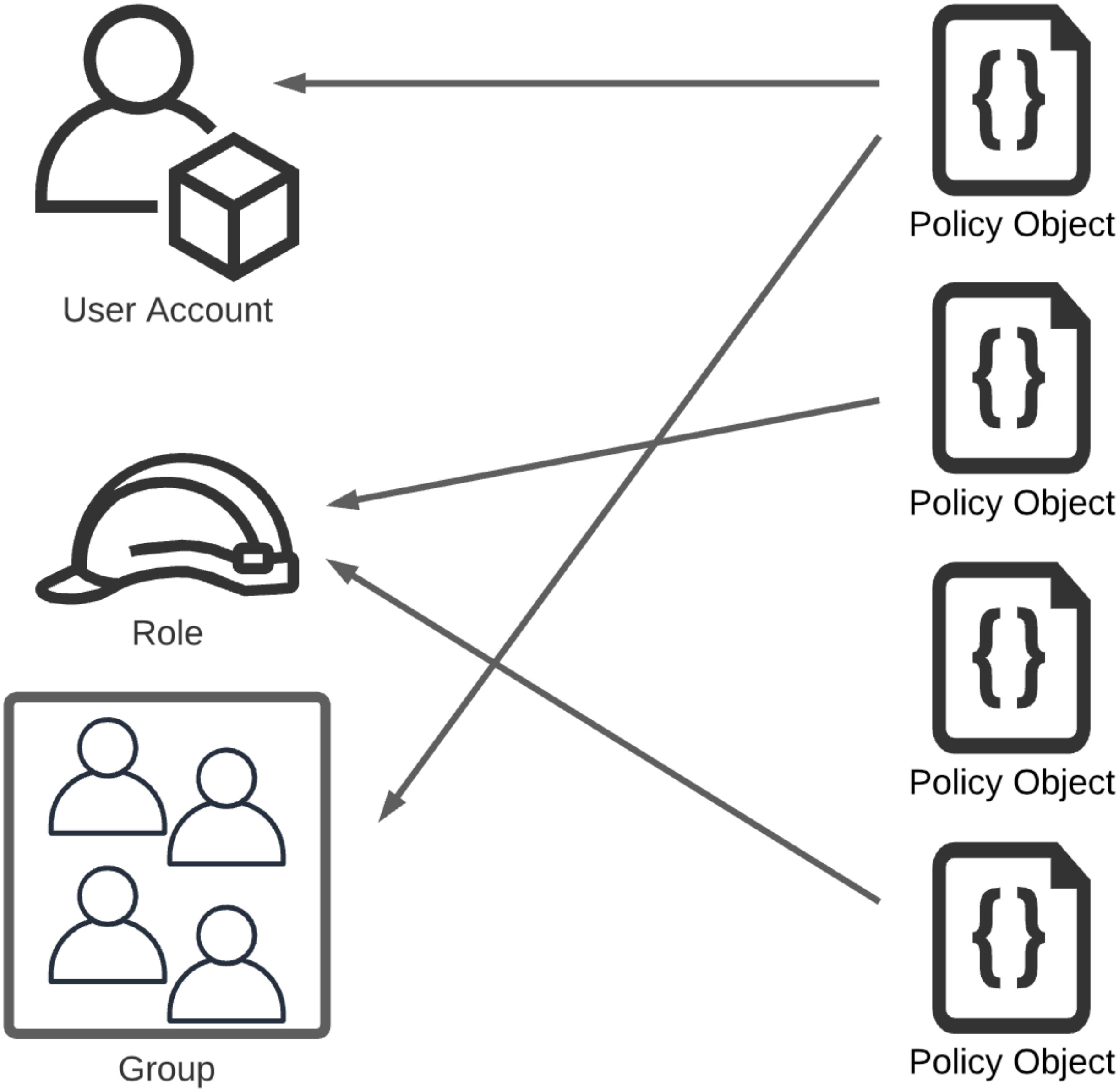
```
[jonlehtinen@ ~ % aws iam deactivate-vir
[> aws iam deactivate-mfa-device --user-name RBI_S3 --serial-number arn:aws:iam::451339973440:m
fa/rbis3
[jonlehtinen@ ~ % aws iam list-virtual-mfa-devices
VirtualMFADevices:
- SerialNumber: arn:aws:iam::451339973440:mfa/rbis3
- EnableDate: '2020-12-09T00:17:06+00:00'
  SerialNumber: arn:aws:iam::451339973440:mfa/root-account-mfa-device
  User:
    Arn: arn:aws:iam::451339973440:root
    CreateDate: '2020-11-09T16:56:07+00:00'
    PasswordLastUsed: '2020-12-09T00:39:13+00:00'
    UserId: '451339973440'
- EnableDate: '2020-12-13T19:17:44+00:00'
  SerialNumber: arn:aws:iam::451339973440:mfa/googleauth1
  User:
    Arn: arn:aws:iam::451339973440:user/redbeardidentity
    CreateDate: '2020-11-12T01:11:46+00:00'
    PasswordLastUsed: '2020-12-13T19:22:54+00:00'
    Path: /
    UserId: AIDAWSFPVONALTHHLBKLK
    UserName: redbeardidentity
jonlehtinen@ ~ %
```

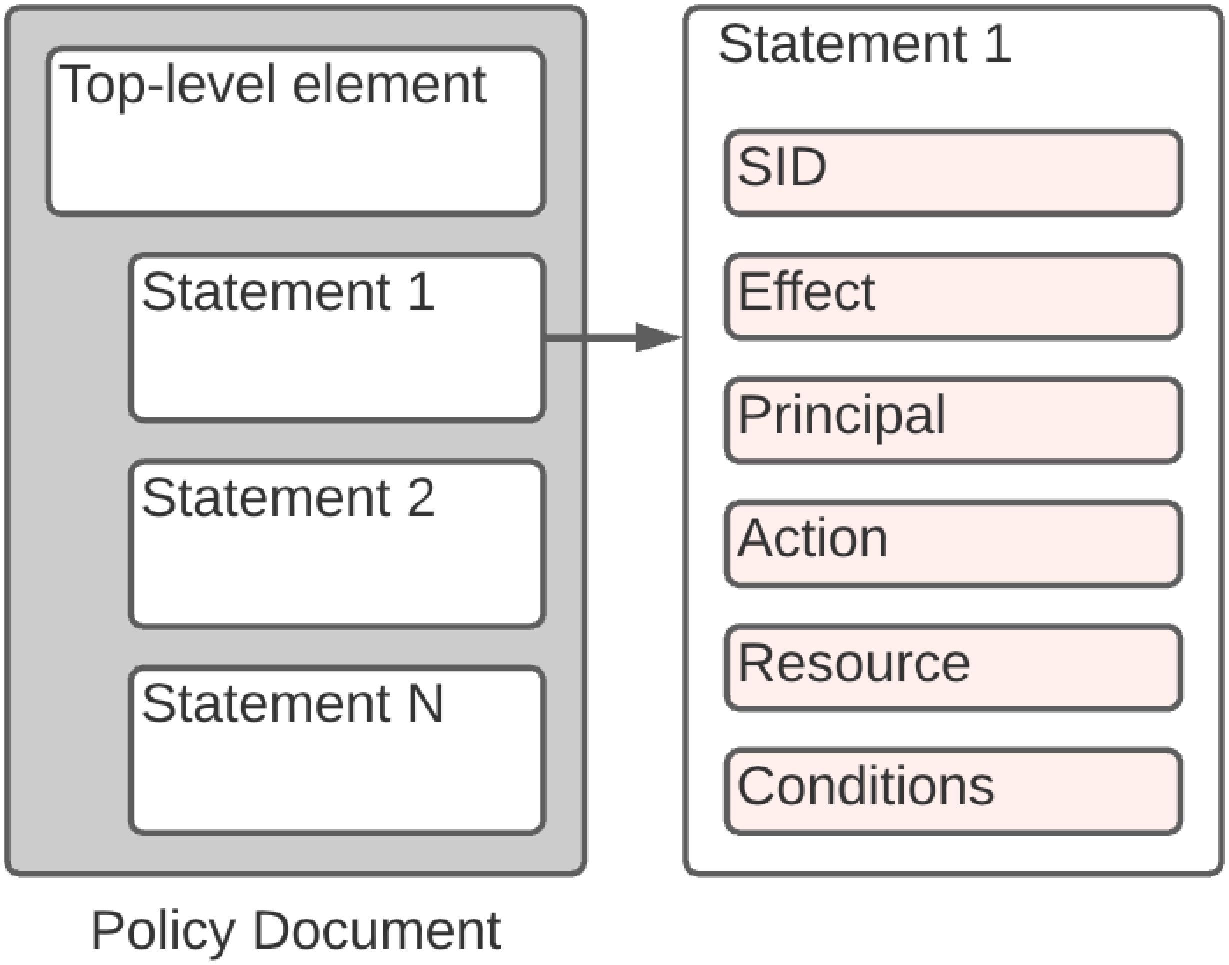


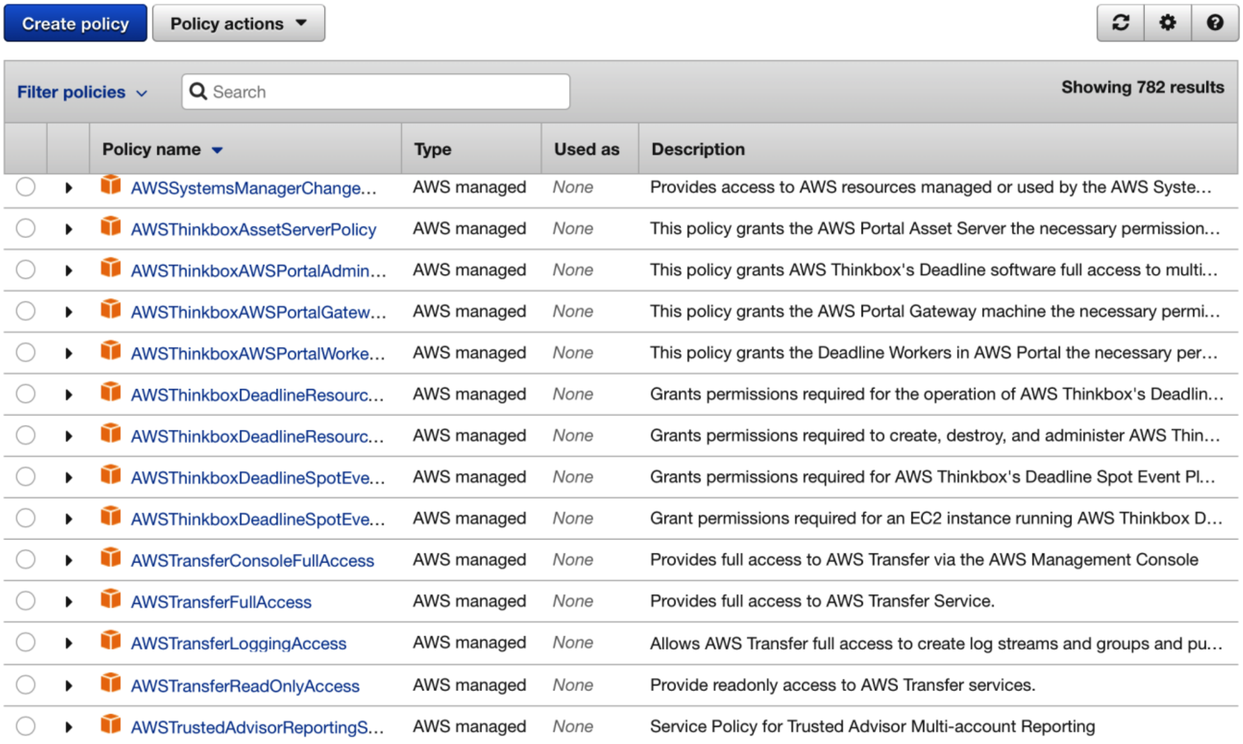

AWS
AWS STS
4
AWS IAM
3
5
Identity Provider
1
2
AWS Role
6
Bob


AWS
Account synch &
federated relationship
Identity
Provider
Federated IDP
Synched
Directory
AWS SSO
AWS Account 1
AWS
AWS
Federated IDP
AWS IAM
AWS Account 2
Federated IDP
AWS IAM
AWS Account N

Chapter 4: Access Management, Policies, and Permissions

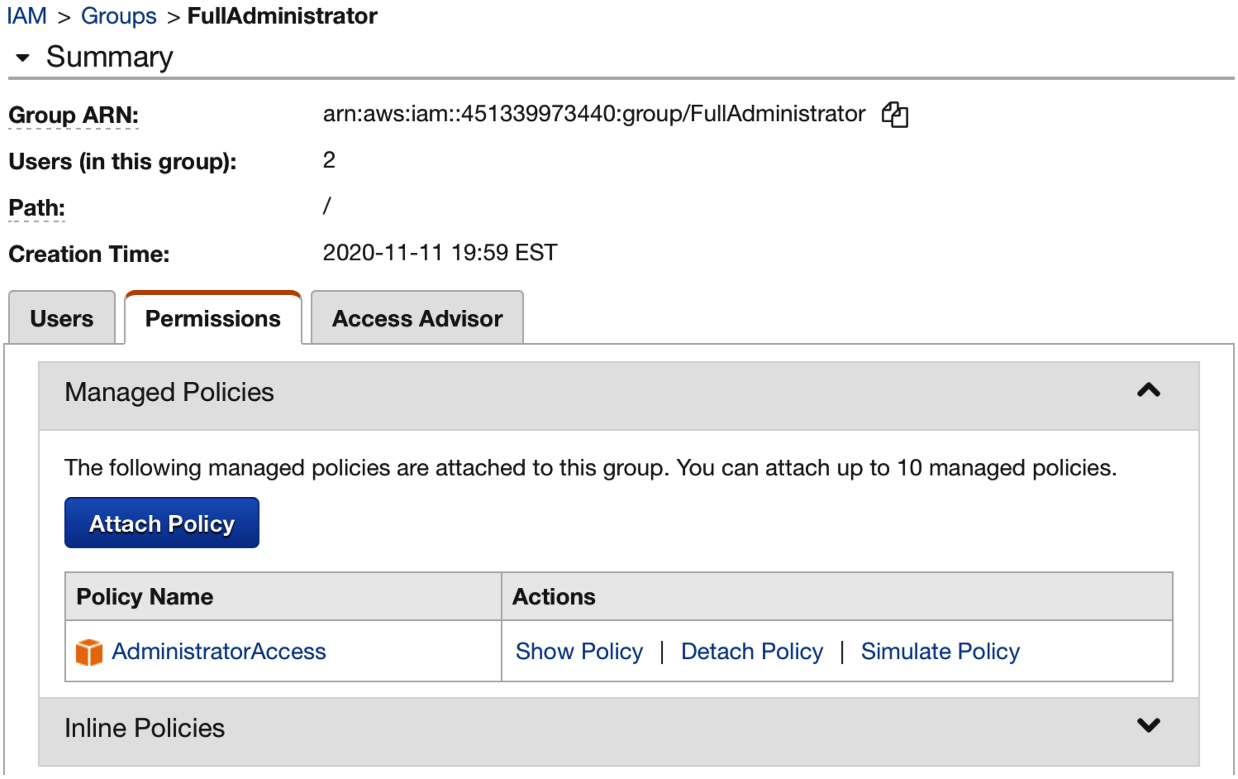



Top-level element
Statement 1
Statement 2
Statement N
Policy Document
Statement 1
SID
Effect
Principal
Action
Resource
Conditions



Showing 782 results

		Policy name ▾	Type	Used as	Description
○	▸	AWSSystemsManagerChange...	AWS managed	*None*	Provides access to AWS resources managed or used by the AWS Syste...
○	▸	AWSThinkboxAssetServerPolicy	AWS managed	*None*	This policy grants the AWS Portal Asset Server the necessary permission...
○	▸	AWSThinkboxAWSPortalAdmin...	AWS managed	*None*	This policy grants AWS Thinkbox's Deadline software full access to multi...
○	▸	AWSThinkboxAWSPortalGatew...	AWS managed	*None*	This policy grants the AWS Portal Gateway machine the necessary permi...
○	▸	AWSThinkboxAWSPortalWorke...	AWS managed	*None*	This policy grants the Deadline Workers in AWS Portal the necessary per...
○	▸	AWSThinkboxDeadlineResourc...	AWS managed	*None*	Grants permissions required for the operation of AWS Thinkbox's Deadlin...
○	▸	AWSThinkboxDeadlineResourc...	AWS managed	*None*	Grants permissions required to create, destroy, and administer AWS Thin...
○	▸	AWSThinkboxDeadlineSpotEve...	AWS managed	*None*	Grants permissions required for AWS Thinkbox's Deadline Spot Event Pl...
○	▸	AWSThinkboxDeadlineSpotEve...	AWS managed	*None*	Grant permissions required for an EC2 instance running AWS Thinkbox D...
○	▸	AWSTransferConsoleFullAccess	AWS managed	*None*	Provides full access to AWS Transfer via the AWS Management Console
○	▸	AWSTransferFullAccess	AWS managed	*None*	Provides full access to AWS Transfer Service.
○	▸	AWSTransferLoggingAccess	AWS managed	*None*	Allows AWS Transfer full access to create log streams and groups and pu...
○	▸	AWSTransferReadOnlyAccess	AWS managed	*None*	Provide readonly access to AWS Transfer services.
○	▸	AWSTrustedAdvisorReportingS...	AWS managed	*None*	Service Policy for Trusted Advisor Multi-account Reporting



IAM > Groups > **FullAdministrator**

▾ Summary

Group ARN: arn:aws:iam::451339973440:group/FullAdministrator

Users (in this group): 2

Path: /

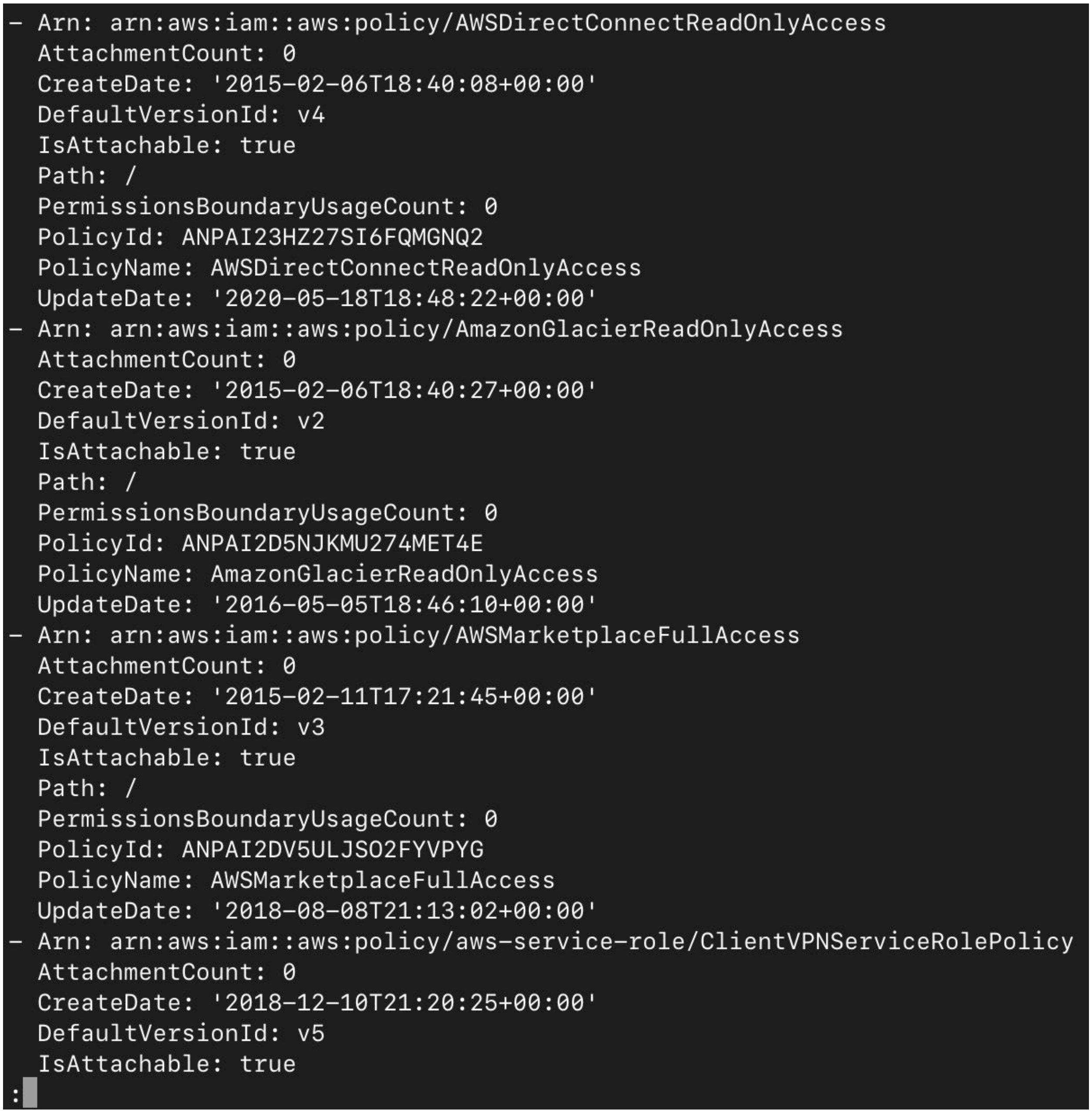
Creation Time: 2020-11-11 19:59 EST

Managed Policies

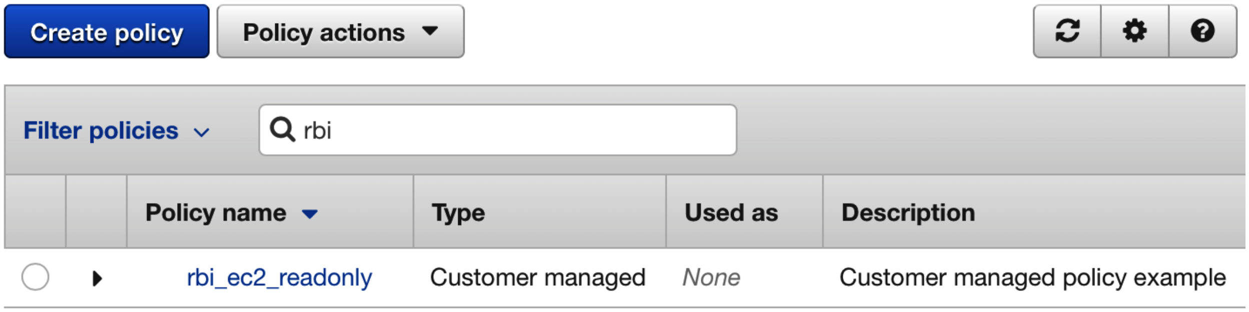
The following managed policies are attached to this group. You can attach up to 10 managed policies.

Policy Name	Actions
AdministratorAccess	Show Policy | Detach Policy | Simulate Policy

Inline Policies

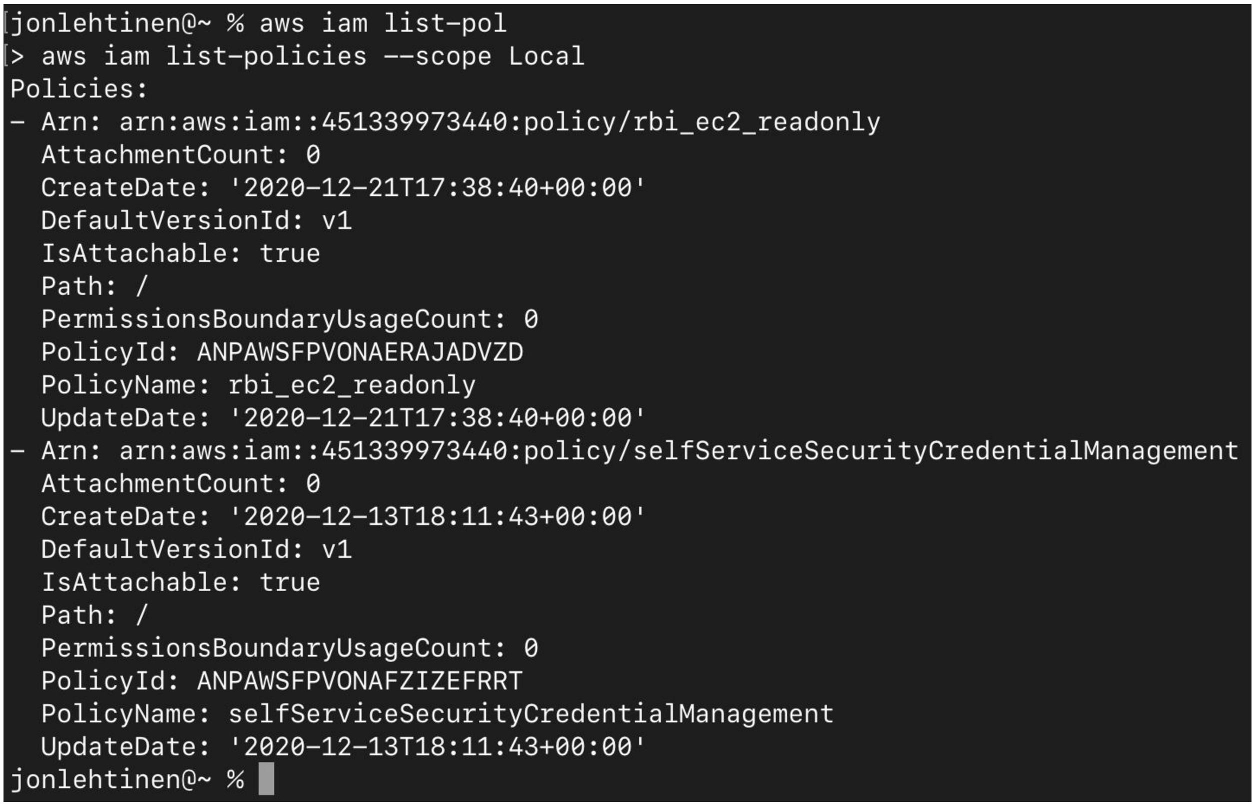


```
- Arn: arn:aws:iam::aws:policy/AWSDirectConnectReadOnlyAccess
  AttachmentCount: 0
  CreateDate: '2015-02-06T18:40:08+00:00'
  DefaultVersionId: v4
  IsAttachable: true
  Path: /
  PermissionsBoundaryUsageCount: 0
  PolicyId: ANPAI23HZ27SI6FQMGNQ2
  PolicyName: AWSDirectConnectReadOnlyAccess
  UpdateDate: '2020-05-18T18:48:22+00:00'
- Arn: arn:aws:iam::aws:policy/AmazonGlacierReadOnlyAccess
  AttachmentCount: 0
  CreateDate: '2015-02-06T18:40:27+00:00'
  DefaultVersionId: v2
  IsAttachable: true
  Path: /
  PermissionsBoundaryUsageCount: 0
  PolicyId: ANPAI2D5NJKMU274MET4E
  PolicyName: AmazonGlacierReadOnlyAccess
  UpdateDate: '2016-05-05T18:46:10+00:00'
- Arn: arn:aws:iam::aws:policy/AWSMarketplaceFullAccess
  AttachmentCount: 0
  CreateDate: '2015-02-11T17:21:45+00:00'
  DefaultVersionId: v3
  IsAttachable: true
  Path: /
  PermissionsBoundaryUsageCount: 0
  PolicyId: ANPAI2DV5ULJSO2FYVPYG
  PolicyName: AWSMarketplaceFullAccess
  UpdateDate: '2018-08-08T21:13:02+00:00'
- Arn: arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceRolePolicy
  AttachmentCount: 0
  CreateDate: '2018-12-10T21:20:25+00:00'
  DefaultVersionId: v5
  IsAttachable: true
:
```

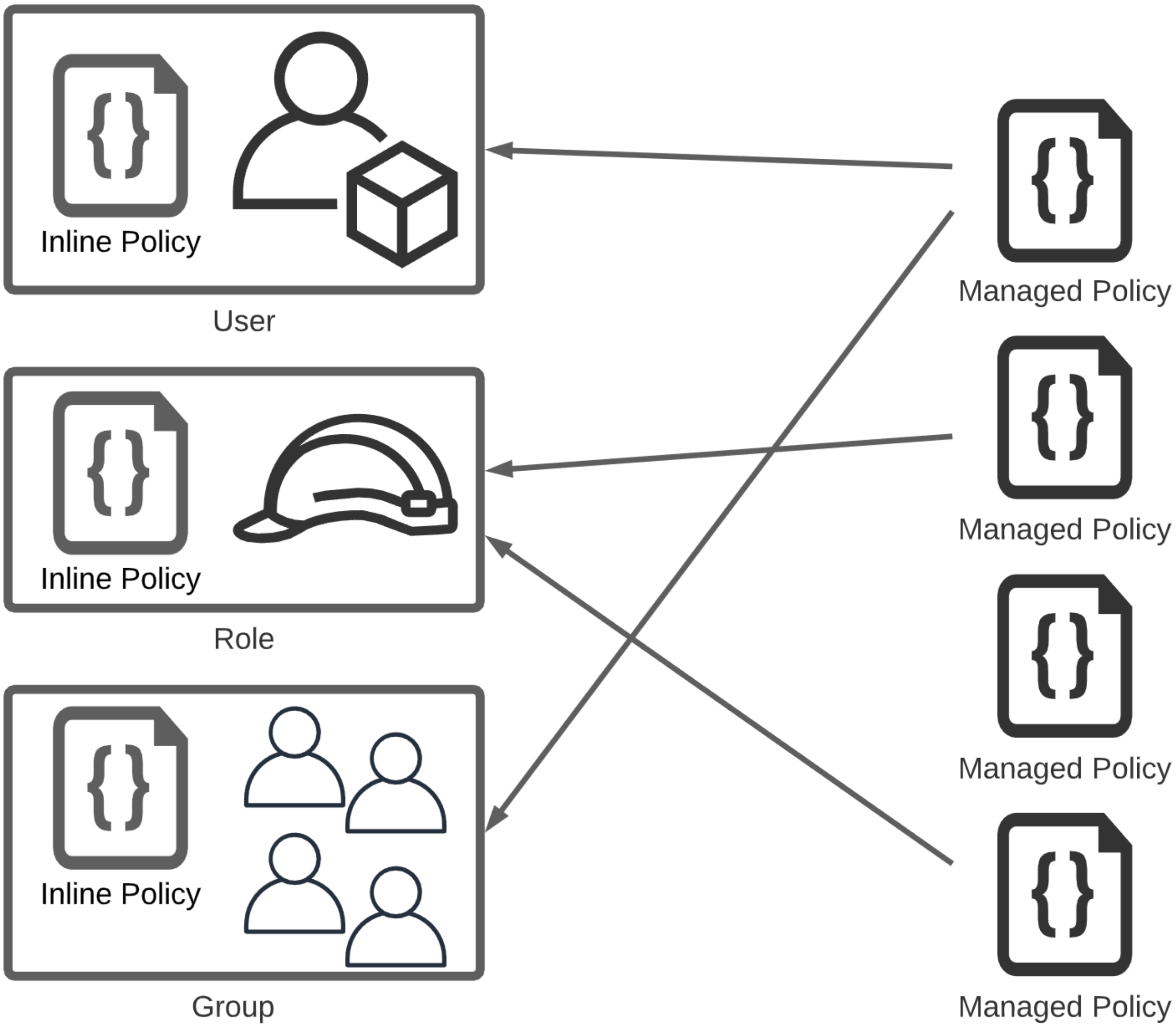


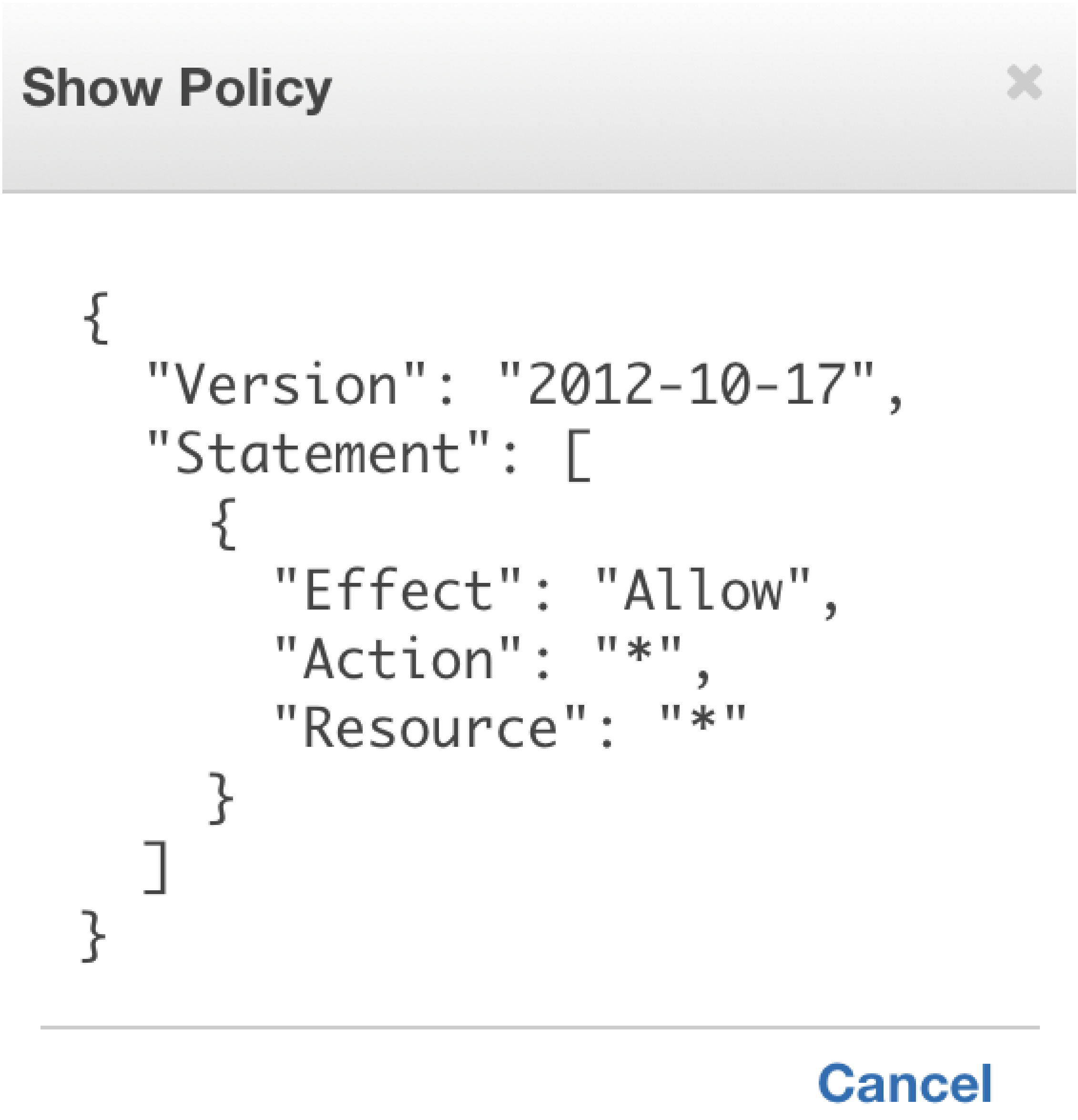
🔍 rbi

		Policy name ▼	Type	Used as	Description
○	▸	rbi_ec2_readonly	Customer managed	*None*	Customer managed policy example

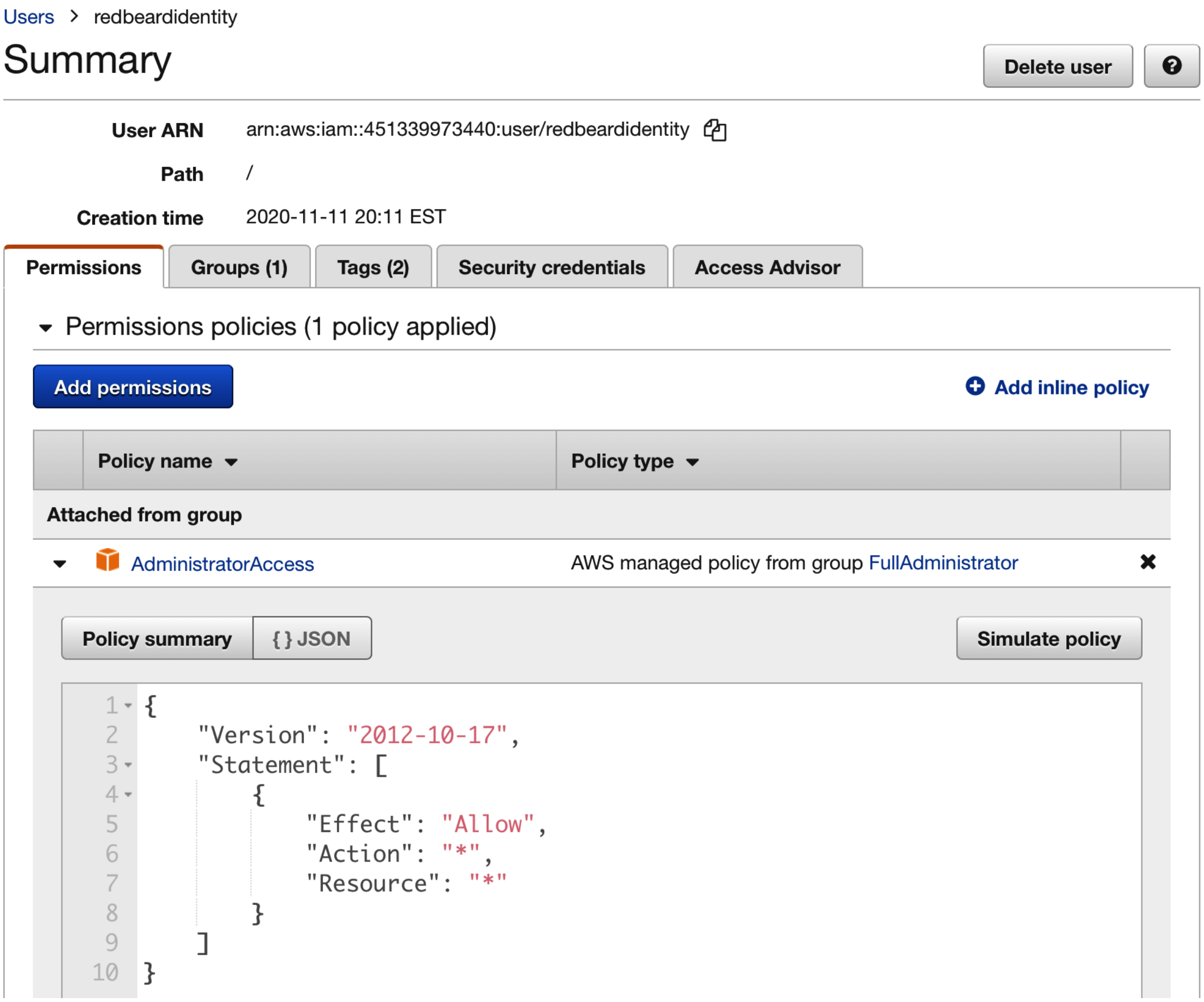


```
[jonlehtinen@~ % aws iam list-pol
[> aws iam list-policies --scope Local
Policies:
- Arn: arn:aws:iam::451339973440:policy/rbi_ec2_readonly
  AttachmentCount: 0
  CreateDate: '2020-12-21T17:38:40+00:00'
  DefaultVersionId: v1
  IsAttachable: true
  Path: /
  PermissionsBoundaryUsageCount: 0
  PolicyId: ANPAWSFPVONAERAJADVZD
  PolicyName: rbi_ec2_readonly
  UpdateDate: '2020-12-21T17:38:40+00:00'
- Arn: arn:aws:iam::451339973440:policy/selfServiceSecurityCredentialManagement
  AttachmentCount: 0
  CreateDate: '2020-12-13T18:11:43+00:00'
  DefaultVersionId: v1
  IsAttachable: true
  Path: /
  PermissionsBoundaryUsageCount: 0
  PolicyId: ANPAWSFPVONAFZIZEFRRT
  PolicyName: selfServiceSecurityCredentialManagement
  UpdateDate: '2020-12-13T18:11:43+00:00'
jonlehtinen@~ %
```


Inline Policy
User
Inline Policy
Role
Inline Policy
Group
Managed Policy
Managed Policy
Managed Policy
Managed Policy



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*"
    }
  ]
}
```

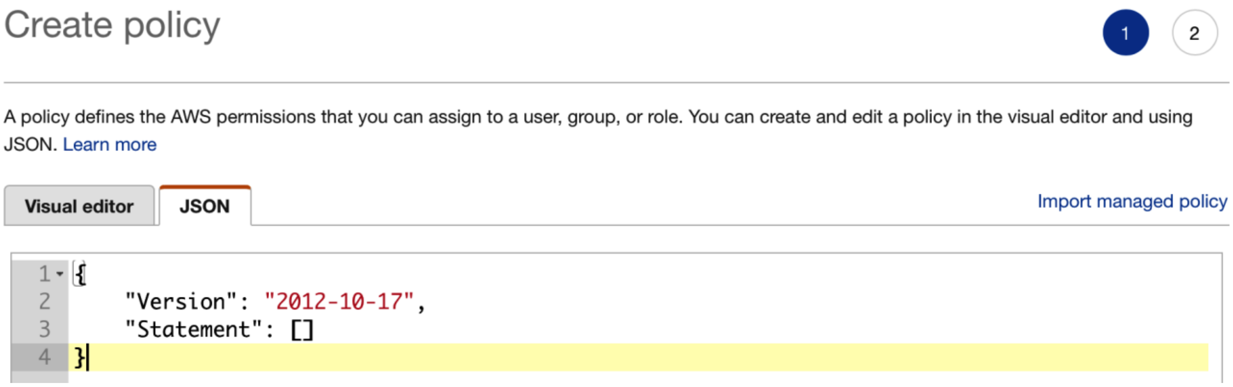


User ARN	arn:aws:iam::451339973440:user/redbeardidentity
Path	/
Creation time	2020-11-11 20:11 EST

Permissions policies (1 policy applied)

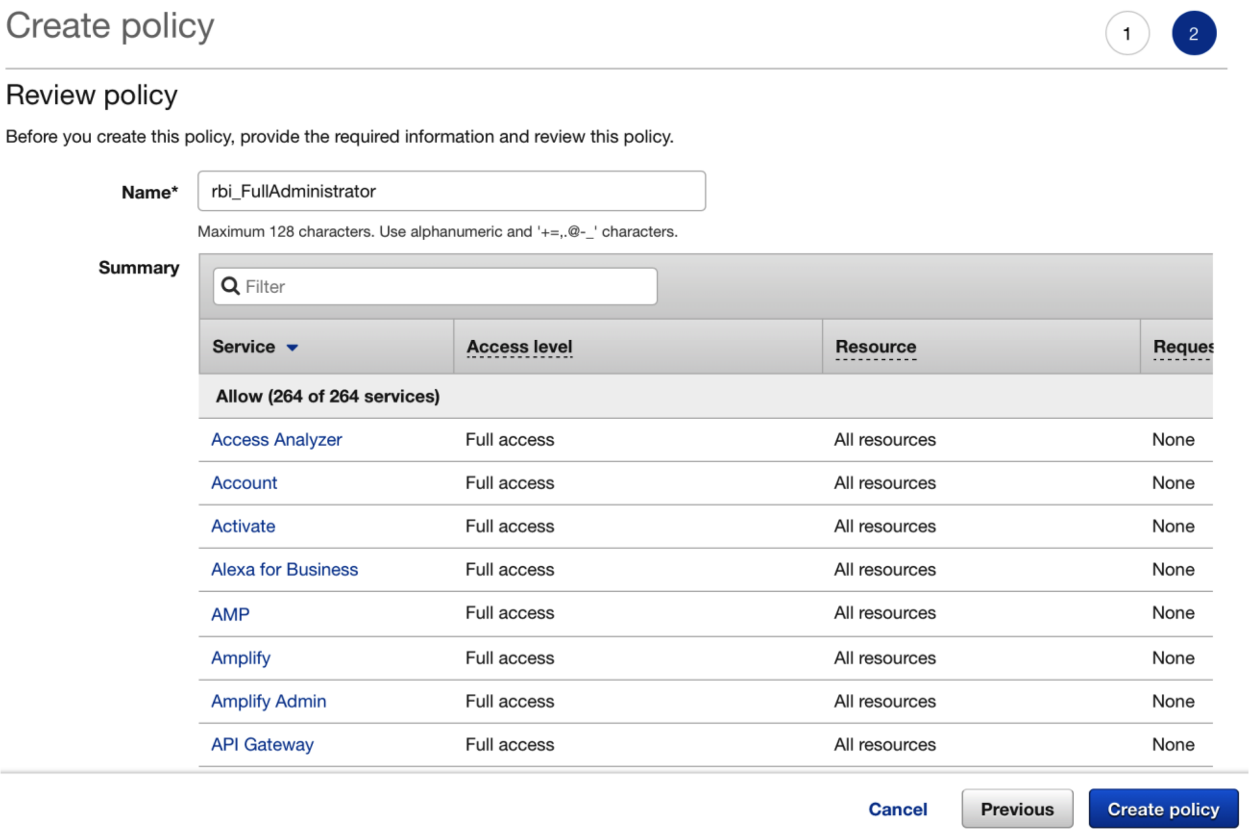
Policy name	Policy type
Attached from group	
AdministratorAccess	AWS managed policy from group FullAdministrator

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```



A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

```
{
    "Version": "2012-10-17",
    "Statement": []
}
```



Create policy

Review policy

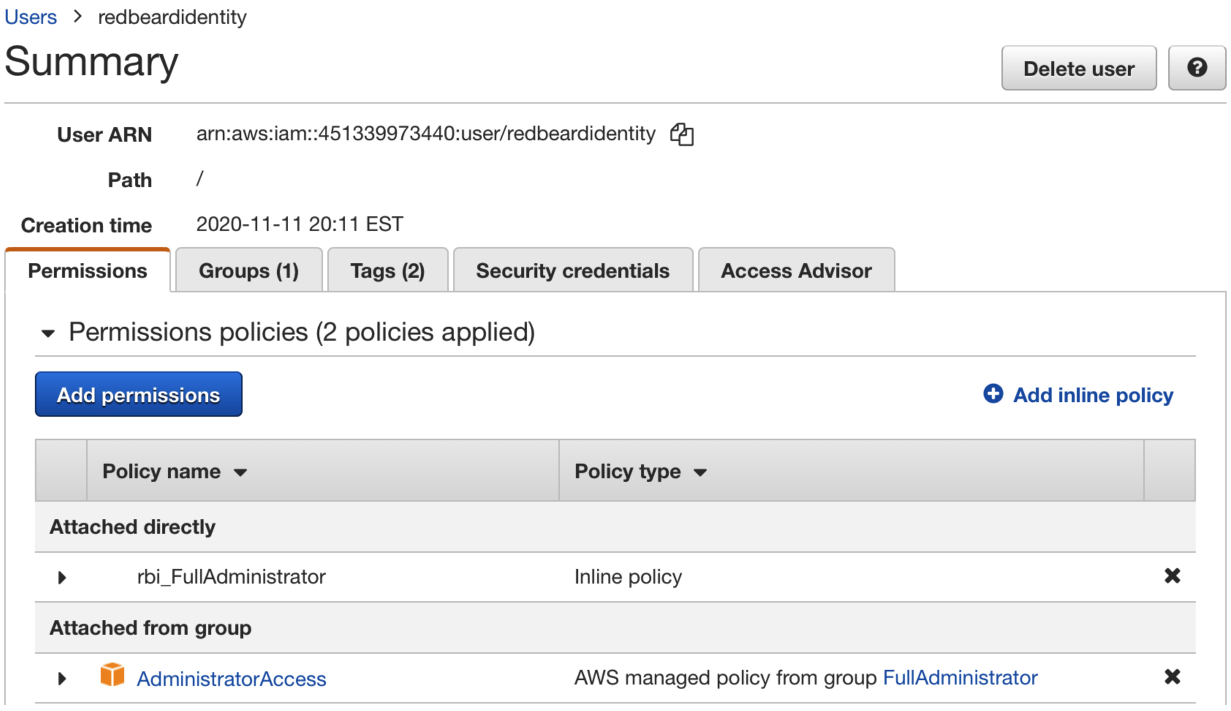
Before you create this policy, provide the required information and review this policy.

Name* rbi_FullAdministrator

Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Summary

Service ▼	Access level	Resource	Reques
Allow (264 of 264 services)			
Access Analyzer	Full access	All resources	None
Account	Full access	All resources	None
Activate	Full access	All resources	None
Alexa for Business	Full access	All resources	None
AMP	Full access	All resources	None
Amplify	Full access	All resources	None
Amplify Admin	Full access	All resources	None
API Gateway	Full access	All resources	None



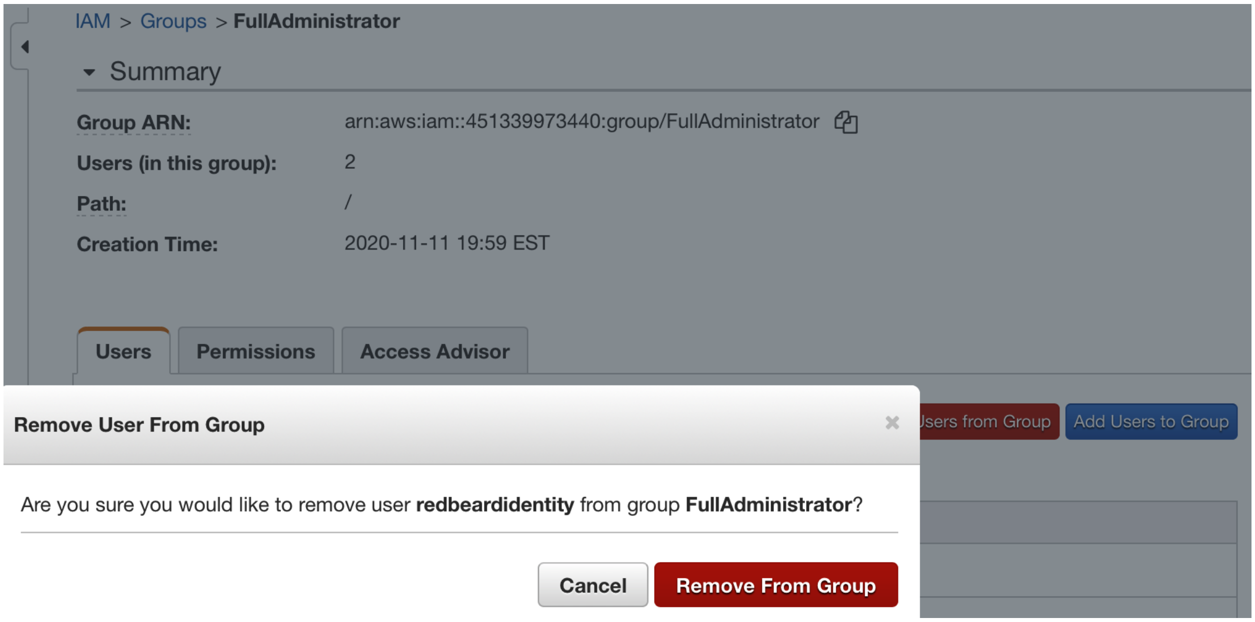
Users > redbeardidentity

Summary

User ARN	arn:aws:iam::451339973440:user/redbeardidentity
Path	/
Creation time	2020-11-11 20:11 EST

▾ Permissions policies (2 policies applied)

Policy name ▼	Policy type ▼	
Attached directly		
▸ rbi_FullAdministrator	Inline policy	✖
Attached from group		
▸ AdministratorAccess	AWS managed policy from group FullAdministrator	✖



Group ARN: arn:aws:iam::451339973440:group/FullAdministrator

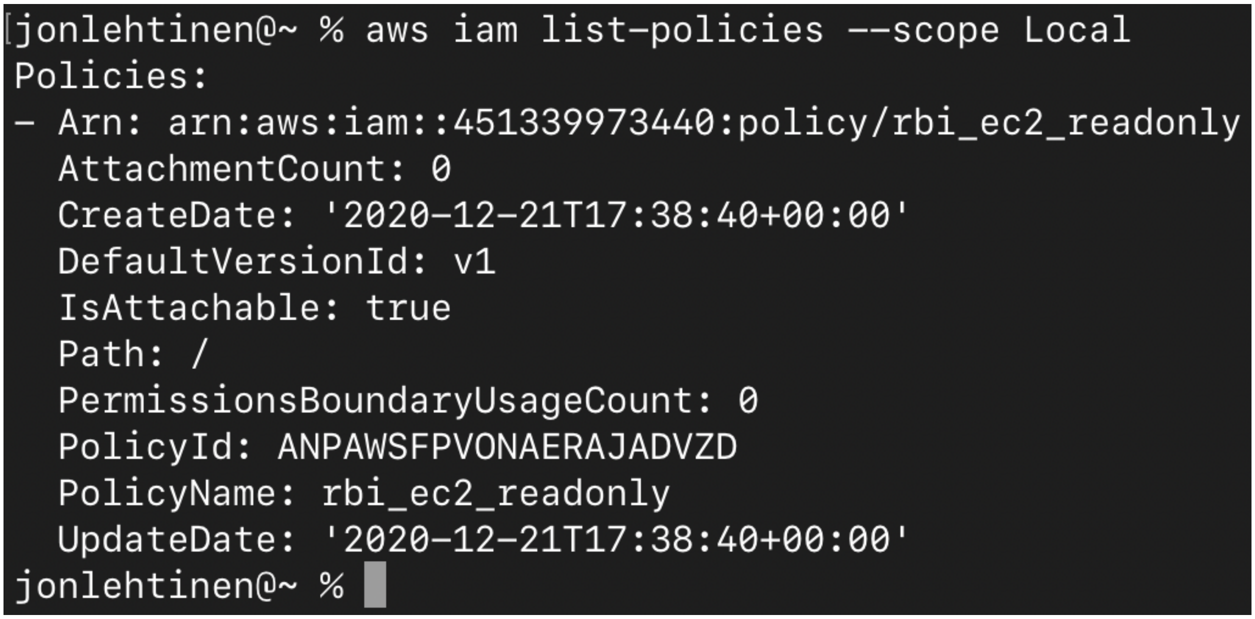
Users (in this group): 2

Path: /

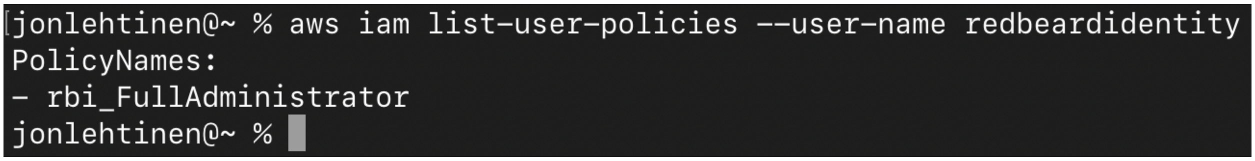
Creation Time: 2020-11-11 19:59 EST

Remove User From Group

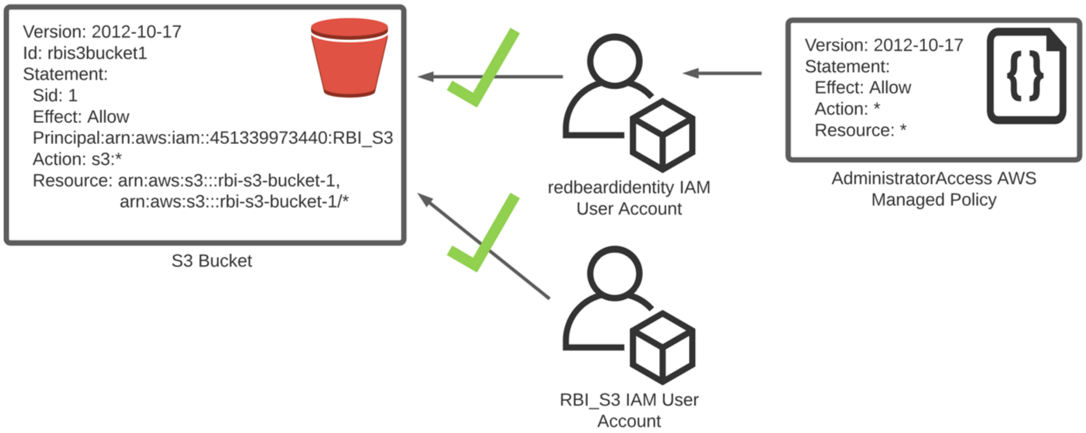
Are you sure you would like to remove user **redbeardidentity** from group **FullAdministrator**?



```
[jonlehtinen@~ % aws iam list-policies --scope Local
Policies:
- Arn: arn:aws:iam::451339973440:policy/rbi_ec2_readonly
  AttachmentCount: 0
  CreateDate: '2020-12-21T17:38:40+00:00'
  DefaultVersionId: v1
  IsAttachable: true
  Path: /
  PermissionsBoundaryUsageCount: 0
  PolicyId: ANPAWSFPVONAERAJADVZD
  PolicyName: rbi_ec2_readonly
  UpdateDate: '2020-12-21T17:38:40+00:00'
jonlehtinen@~ %
```



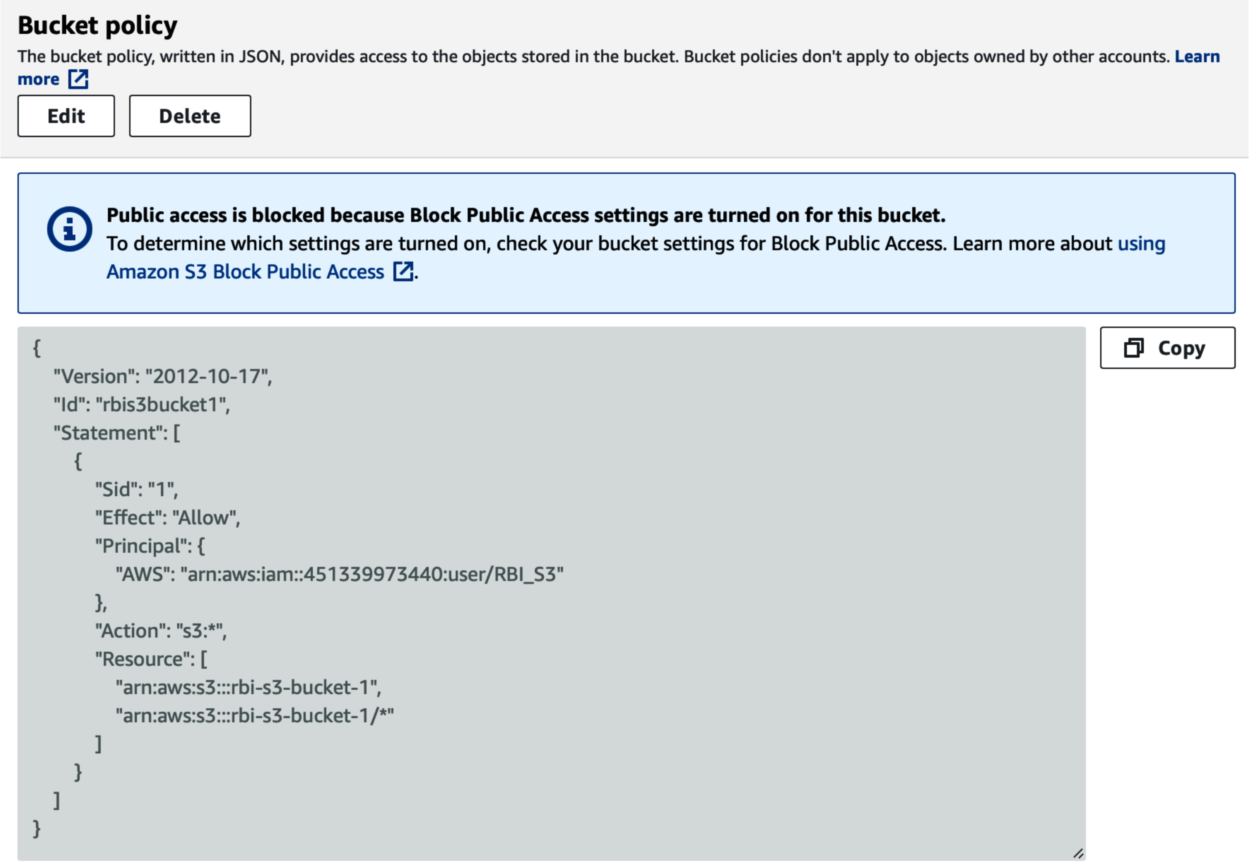
```
[jonlehtinen@~ % aws iam list-user-policies --user-name redbeardidentity
PolicyNames:
- rbi_FullAdministrator
jonlehtinen@~ %
```



Version: 2012-10-17
Id: rbis3bucket1
Statement:
Sid: 1
Effect: Allow
Principal:arn:aws:iam::451339973440:RBI_S3
Action: s3:*
Resource: arn:aws:s3:::rbi-s3-bucket-1,
arn:aws:s3:::rbi-s3-bucket-1/*

Version: 2012-10-17
Statement:
Effect: Allow
Action: *
Resource: *

S3 Bucket
redbeardidentity IAM User Account
AdministratorAccess AWS Managed Policy
RBI_S3 IAM User Account

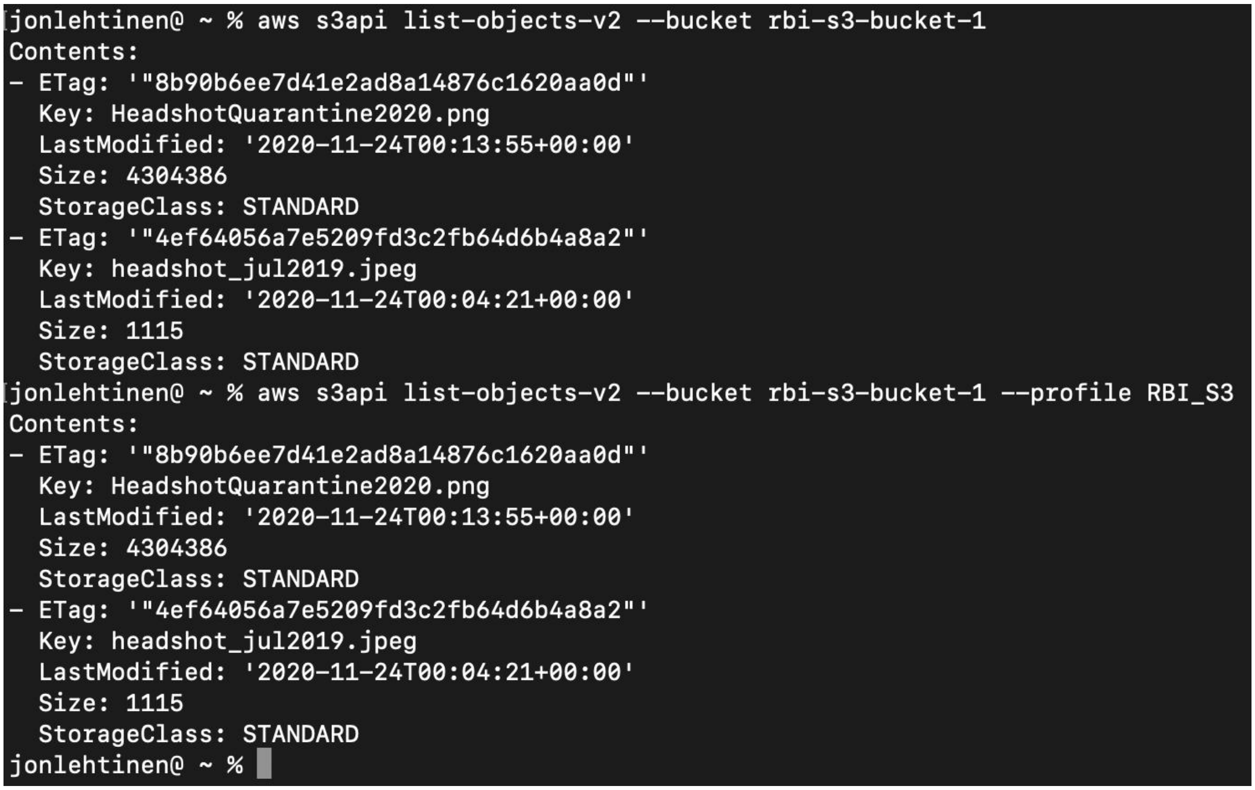


Bucket policy

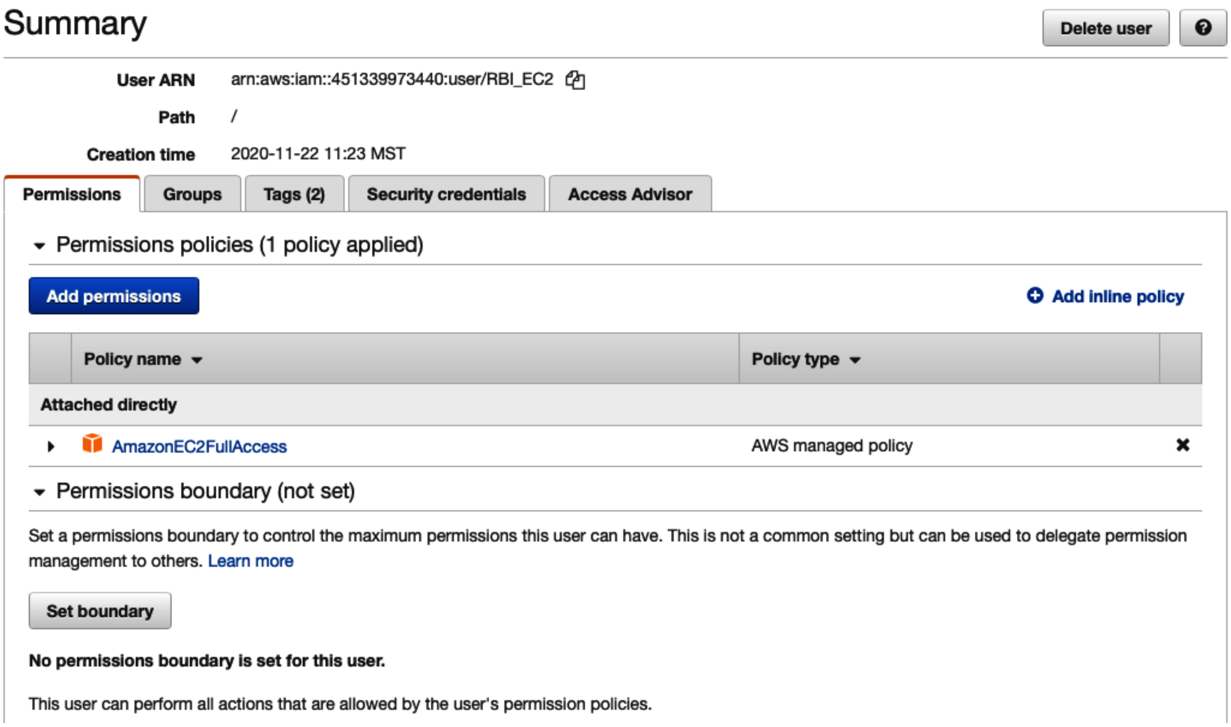
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

Public access is blocked because Block Public Access settings are turned on for this bucket.
To determine which settings are turned on, check your bucket settings for Block Public Access. Learn more about using Amazon S3 Block Public Access.

```
{
  "Version": "2012-10-17",
  "Id": "rbis3bucket1",
  "Statement": [
    {
      "Sid": "1",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::451339973440:user/RBI_S3"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::rbi-s3-bucket-1",
        "arn:aws:s3:::rbi-s3-bucket-1/*"
      ]
    }
  ]
}
```



```
jonlehtinen@ ~ % aws s3api list-objects-v2 --bucket rbi-s3-bucket-1
Contents:
- ETag: '"8b90b6ee7d41e2ad8a14876c1620aa0d"'
  Key: HeadshotQuarantine2020.png
  LastModified: '2020-11-24T00:13:55+00:00'
  Size: 4304386
  StorageClass: STANDARD
- ETag: '"4ef64056a7e5209fd3c2fb64d6b4a8a2"'
  Key: headshot_jul2019.jpeg
  LastModified: '2020-11-24T00:04:21+00:00'
  Size: 1115
  StorageClass: STANDARD
jonlehtinen@ ~ % aws s3api list-objects-v2 --bucket rbi-s3-bucket-1 --profile RBI_S3
Contents:
- ETag: '"8b90b6ee7d41e2ad8a14876c1620aa0d"'
  Key: HeadshotQuarantine2020.png
  LastModified: '2020-11-24T00:13:55+00:00'
  Size: 4304386
  StorageClass: STANDARD
- ETag: '"4ef64056a7e5209fd3c2fb64d6b4a8a2"'
  Key: headshot_jul2019.jpeg
  LastModified: '2020-11-24T00:04:21+00:00'
  Size: 1115
  StorageClass: STANDARD
jonlehtinen@ ~ %
```



Summary

User ARN arn:aws:iam::451339973440:user/RBI_EC2

Path /

Creation time 2020-11-22 11:23 MST

▾ Permissions policies (1 policy applied)

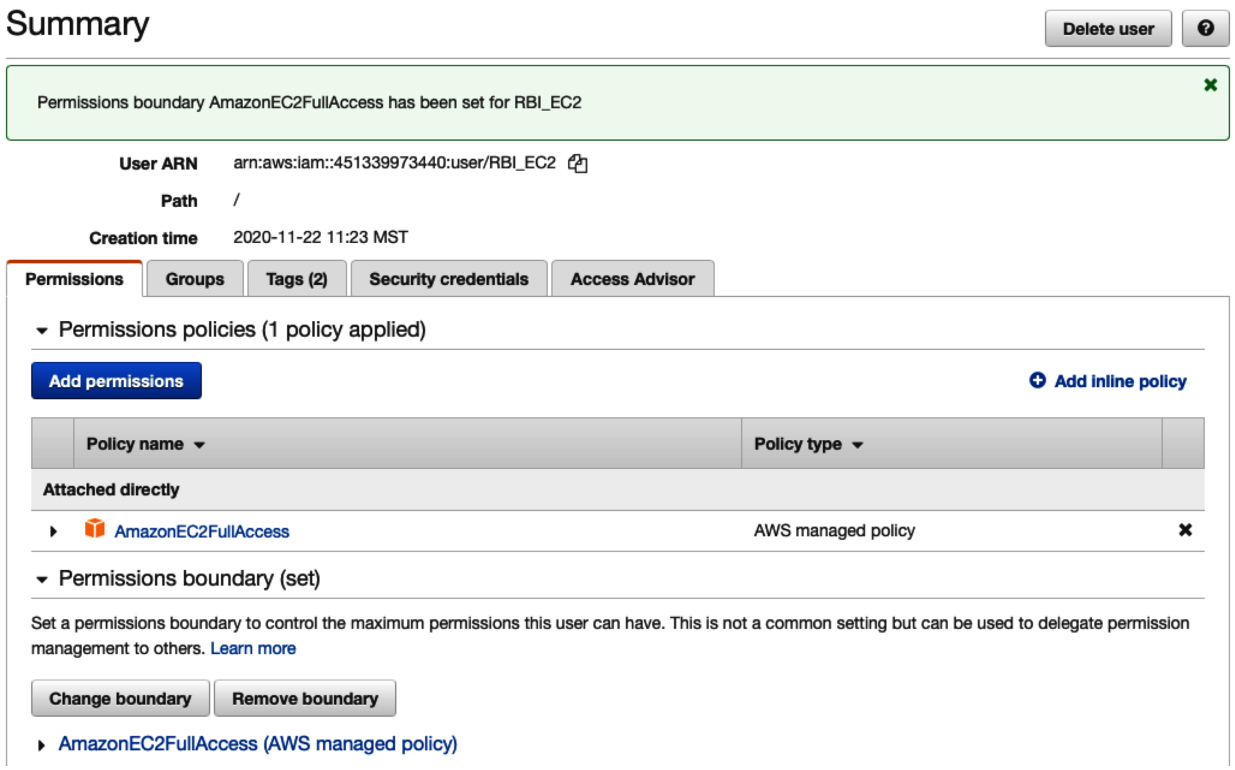
Policy name ▾	Policy type ▾
Attached directly	
AmazonEC2FullAccess	AWS managed policy

▾ Permissions boundary (not set)

Set a permissions boundary to control the maximum permissions this user can have. This is not a common setting but can be used to delegate permission management to others. Learn more

No permissions boundary is set for this user.

This user can perform all actions that are allowed by the user's permission policies.



Summary

Permissions boundary AmazonEC2FullAccess has been set for RBI_EC2

User ARN	arn:aws:iam::451339973440:user/RBI_EC2
Path	/
Creation time	2020-11-22 11:23 MST

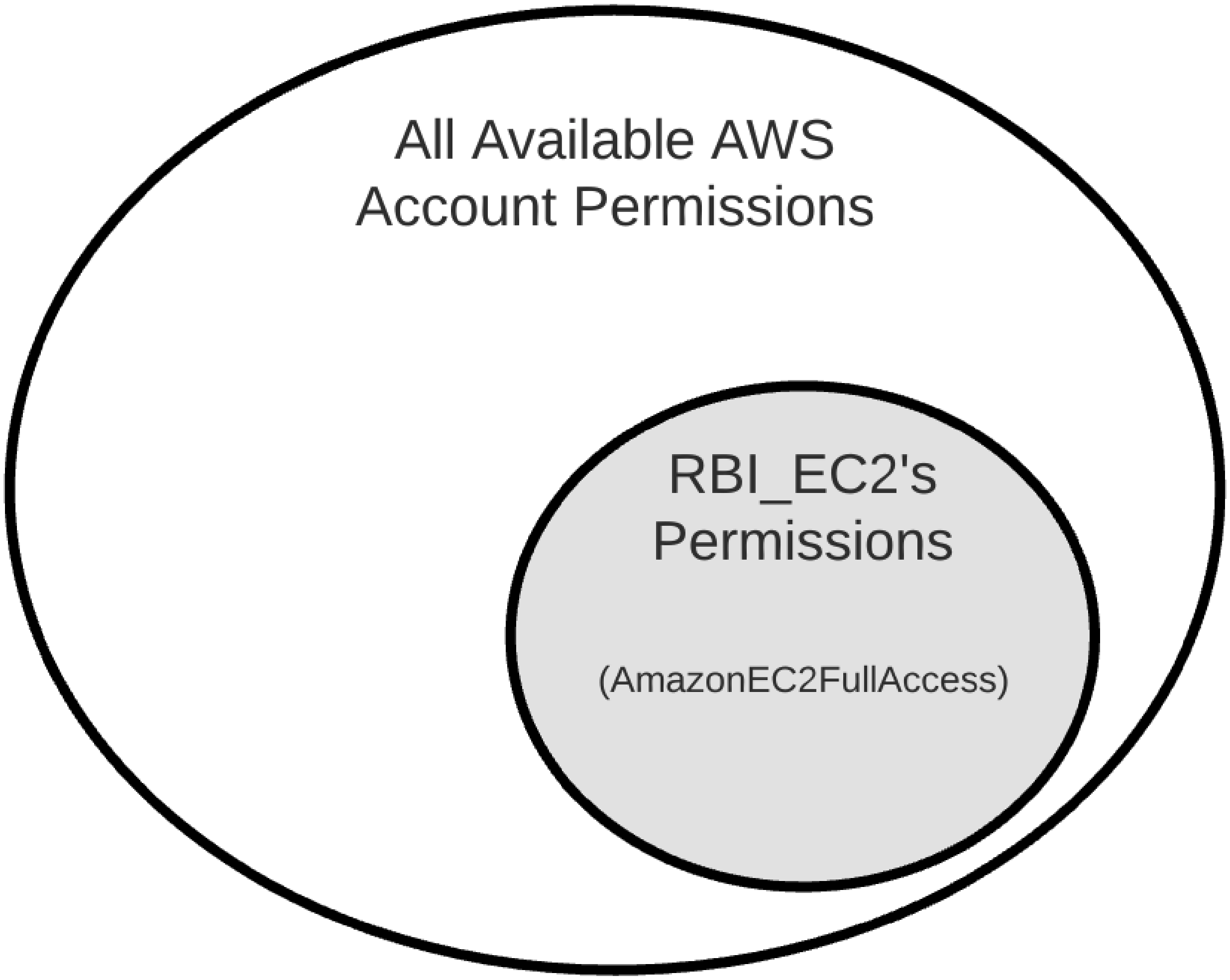
Permissions policies (1 policy applied)

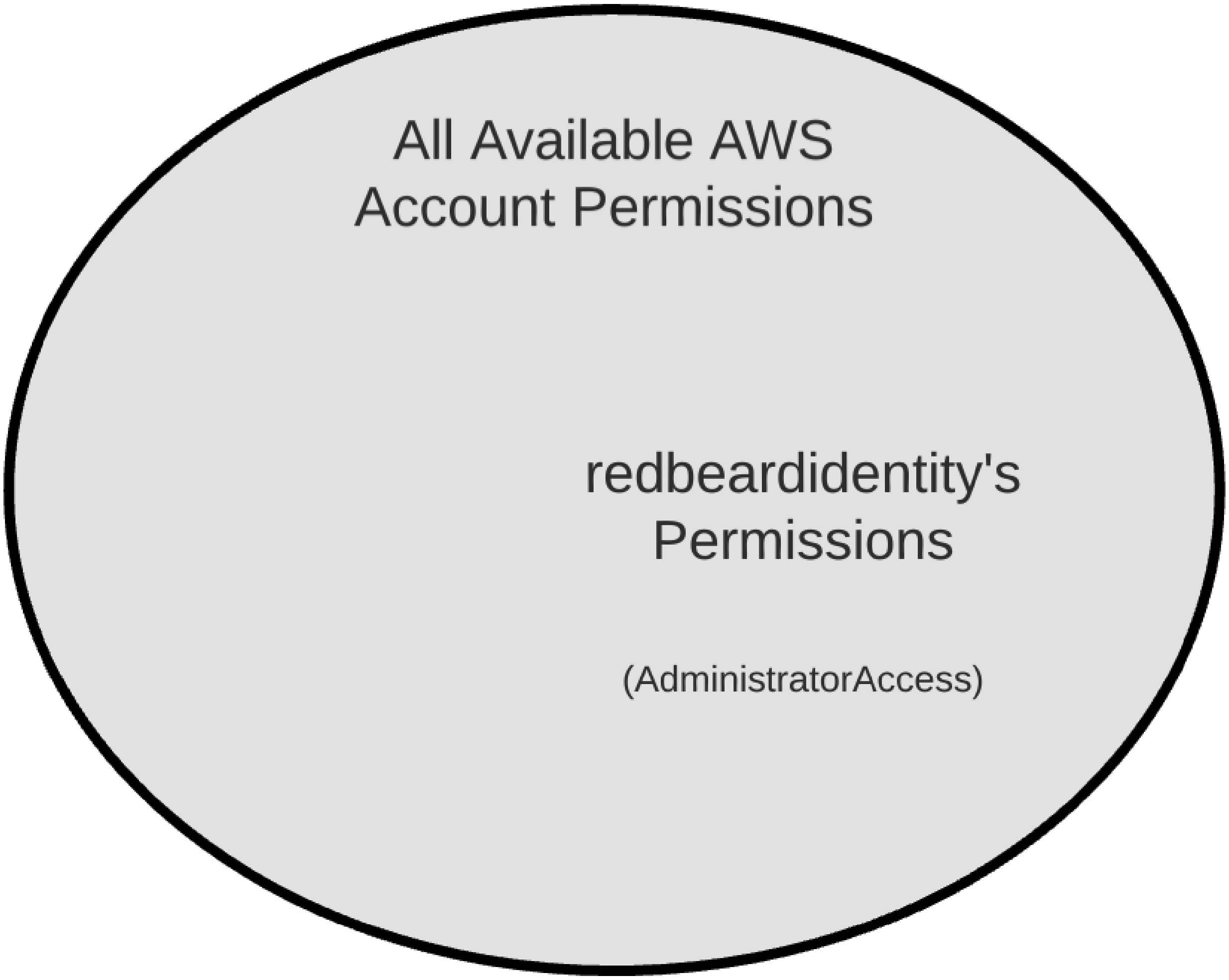
Policy name	Policy type
Attached directly	
AmazonEC2FullAccess	AWS managed policy

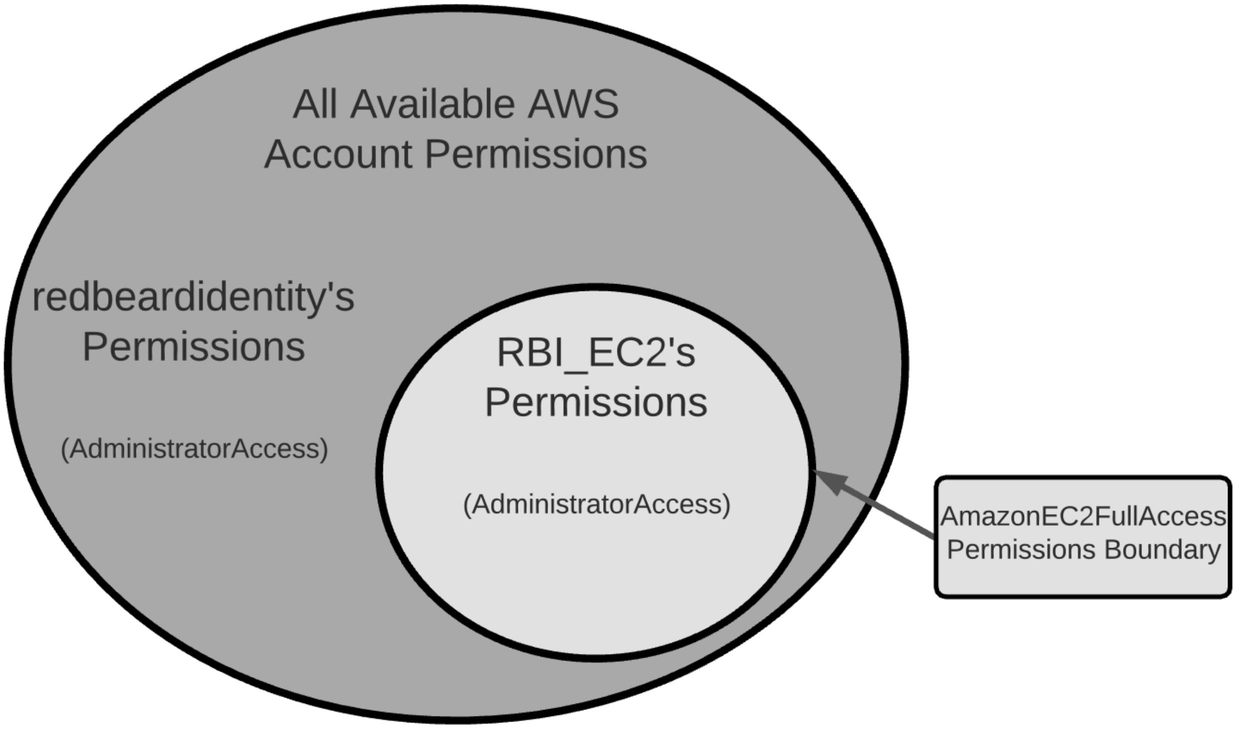
Permissions boundary (set)

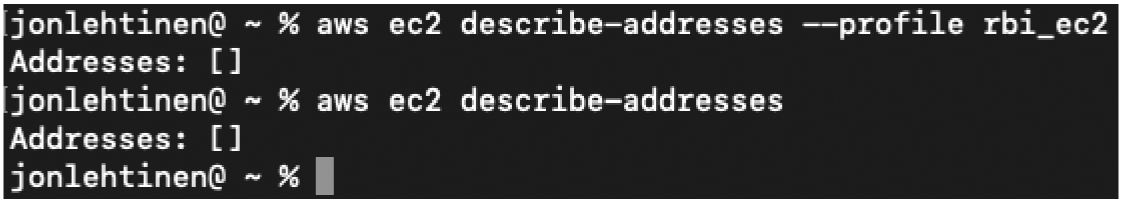
Set a permissions boundary to control the maximum permissions this user can have. This is not a common setting but can be used to delegate permission management to others. Learn more

AmazonEC2FullAccess (AWS managed policy)

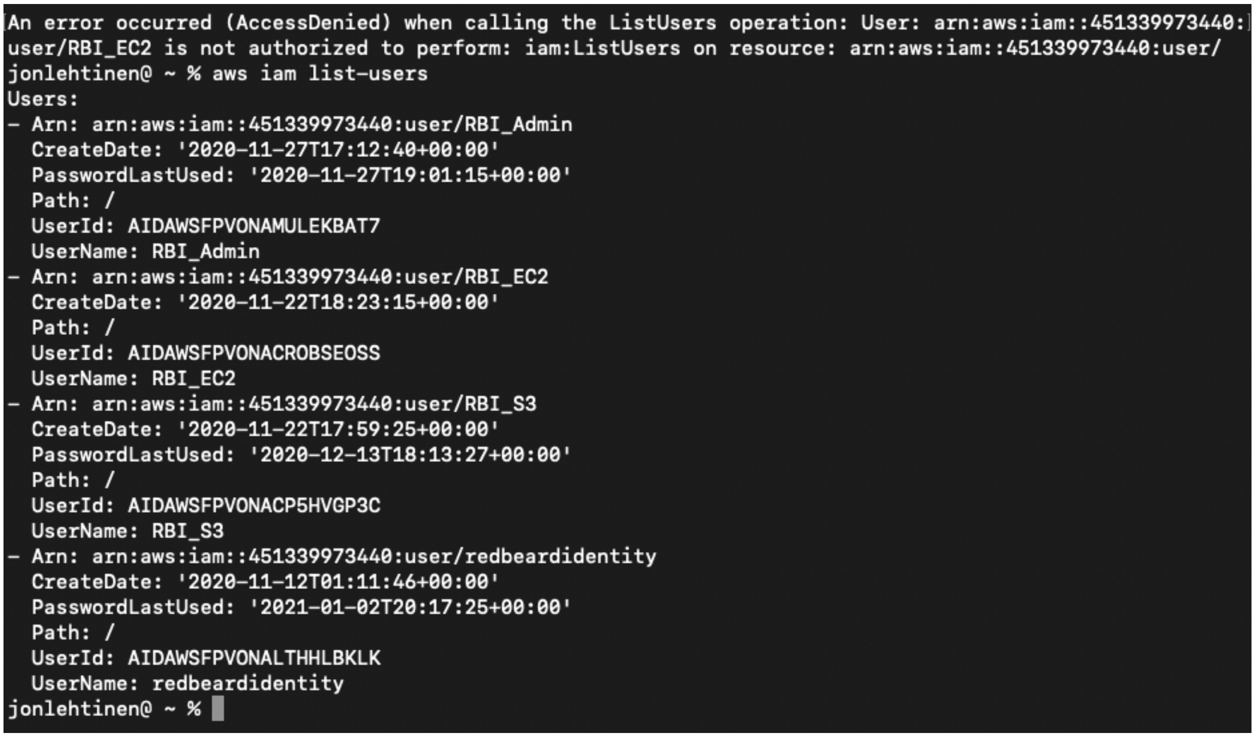

All Available AWS
Account Permissions
RBI_EC2's
Permissions
(AmazonEC2FullAccess)


All Available AWS Account Permissions
redbeardidentity's Permissions
(AdministratorAccess)

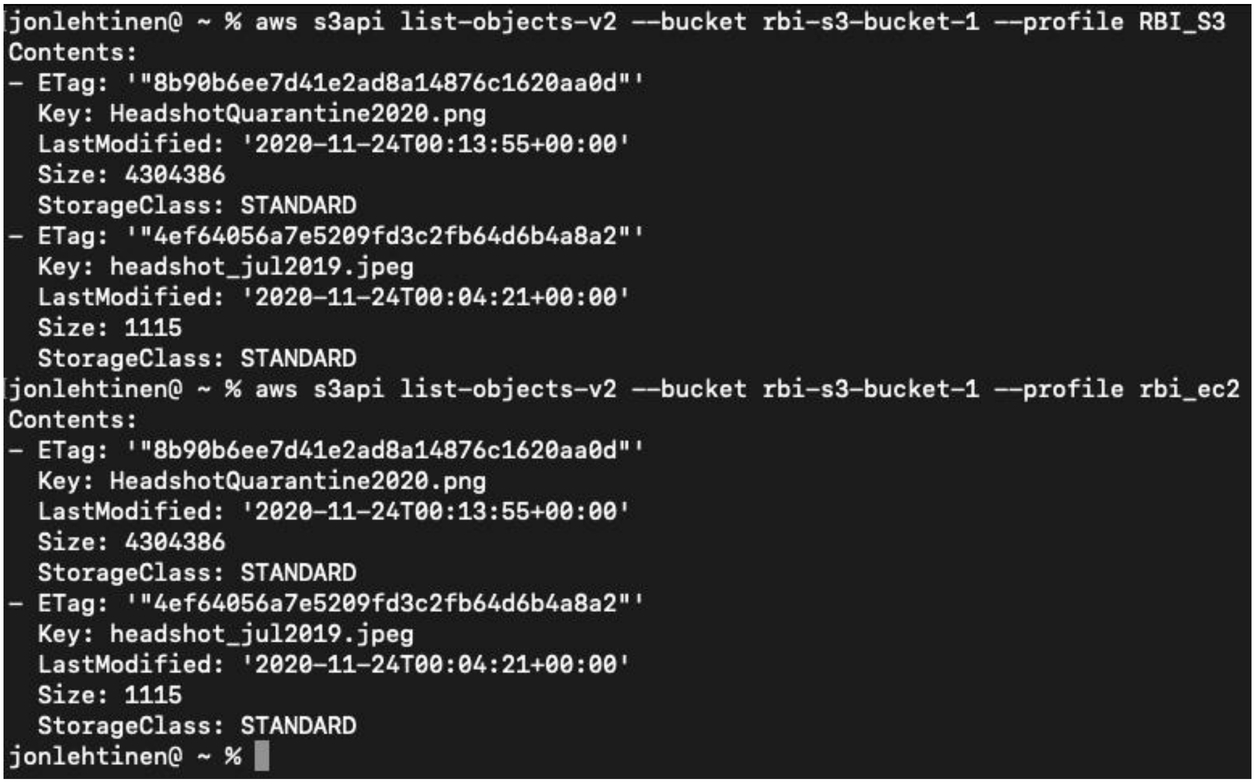

All Available AWS Account Permissions
redbeardidentity's Permissions
(AdministratorAccess)
RBI_EC2's Permissions
(AdministratorAccess)
AmazonEC2FullAccess Permissions Boundary



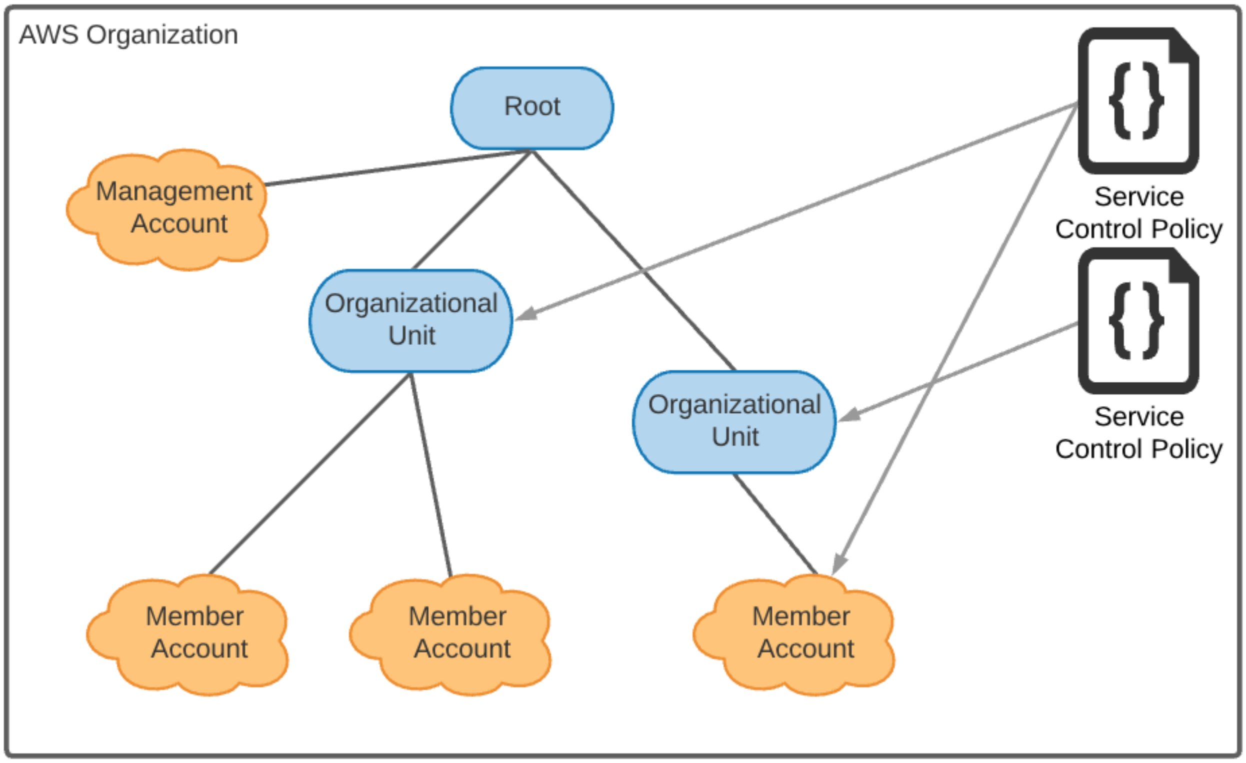
```
[jonlehtinen@ ~ % aws ec2 describe-addresses --profile rbi_ec2
Addresses: []
[jonlehtinen@ ~ % aws ec2 describe-addresses
Addresses: []
jonlehtinen@ ~ %
```

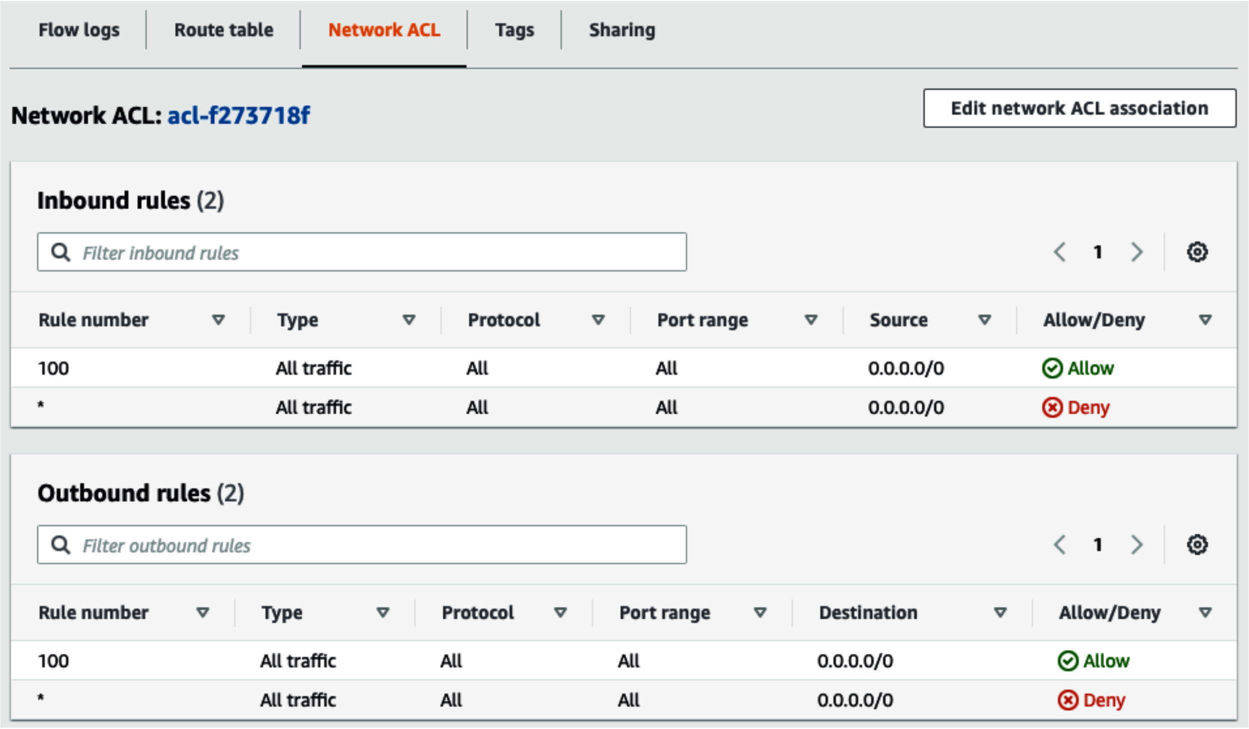


```
An error occurred (AccessDenied) when calling the ListUsers operation: User: arn:aws:iam::451339973440:
user/RBI_EC2 is not authorized to perform: iam:ListUsers on resource: arn:aws:iam::451339973440:user/
jonlehtinen@ ~ % aws iam list-users
Users:
- Arn: arn:aws:iam::451339973440:user/RBI_Admin
  CreateDate: '2020-11-27T17:12:40+00:00'
  PasswordLastUsed: '2020-11-27T19:01:15+00:00'
  Path: /
  UserId: AIDAWSFPVONAMULEKBAT7
  UserName: RBI_Admin
- Arn: arn:aws:iam::451339973440:user/RBI_EC2
  CreateDate: '2020-11-22T18:23:15+00:00'
  Path: /
  UserId: AIDAWSFPVONACROBSEOSS
  UserName: RBI_EC2
- Arn: arn:aws:iam::451339973440:user/RBI_S3
  CreateDate: '2020-11-22T17:59:25+00:00'
  PasswordLastUsed: '2020-12-13T18:13:27+00:00'
  Path: /
  UserId: AIDAWSFPVONACP5HVGP3C
  UserName: RBI_S3
- Arn: arn:aws:iam::451339973440:user/redbeardidentity
  CreateDate: '2020-11-12T01:11:46+00:00'
  PasswordLastUsed: '2021-01-02T20:17:25+00:00'
  Path: /
  UserId: AIDAWSFPVONALTHHLBKLK
  UserName: redbeardidentity
jonlehtinen@ ~ %
```



```
jonlehtinen@ ~ % aws s3api list-objects-v2 --bucket rbi-s3-bucket-1 --profile RBI_S3
Contents:
- ETag: '"8b90b6ee7d41e2ad8a14876c1620aa0d"'
  Key: HeadshotQuarantine2020.png
  LastModified: '2020-11-24T00:13:55+00:00'
  Size: 4304386
  StorageClass: STANDARD
- ETag: '"4ef64056a7e5209fd3c2fb64d6b4a8a2"'
  Key: headshot_jul2019.jpeg
  LastModified: '2020-11-24T00:04:21+00:00'
  Size: 1115
  StorageClass: STANDARD
jonlehtinen@ ~ % aws s3api list-objects-v2 --bucket rbi-s3-bucket-1 --profile rbi_ec2
Contents:
- ETag: '"8b90b6ee7d41e2ad8a14876c1620aa0d"'
  Key: HeadshotQuarantine2020.png
  LastModified: '2020-11-24T00:13:55+00:00'
  Size: 4304386
  StorageClass: STANDARD
- ETag: '"4ef64056a7e5209fd3c2fb64d6b4a8a2"'
  Key: headshot_jul2019.jpeg
  LastModified: '2020-11-24T00:04:21+00:00'
  Size: 1115
  StorageClass: STANDARD
jonlehtinen@ ~ %
```





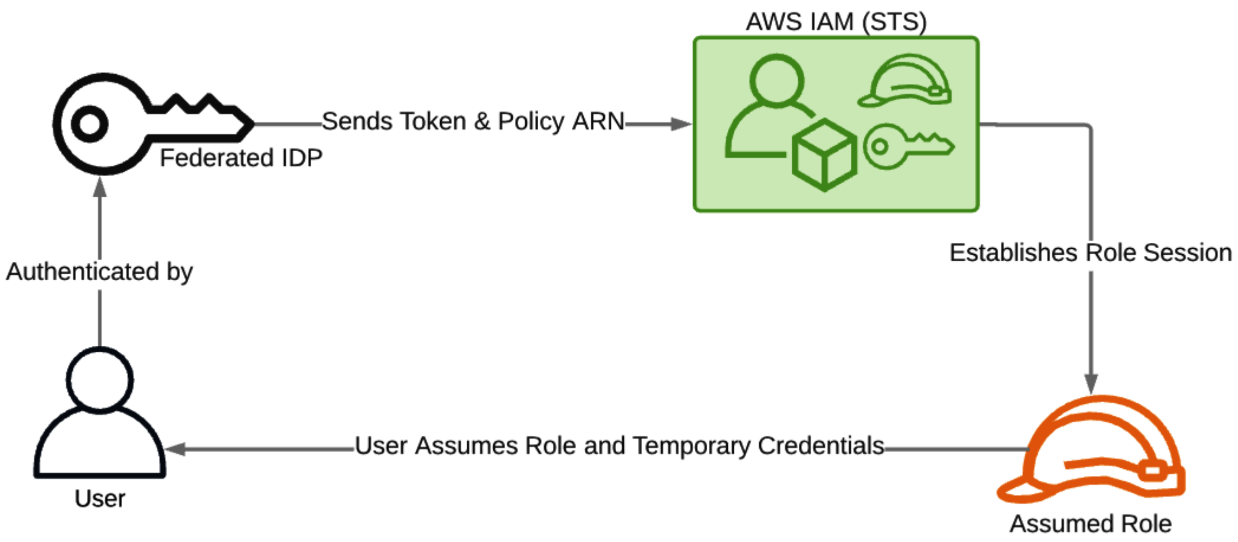
Network ACL: acl-f273718f

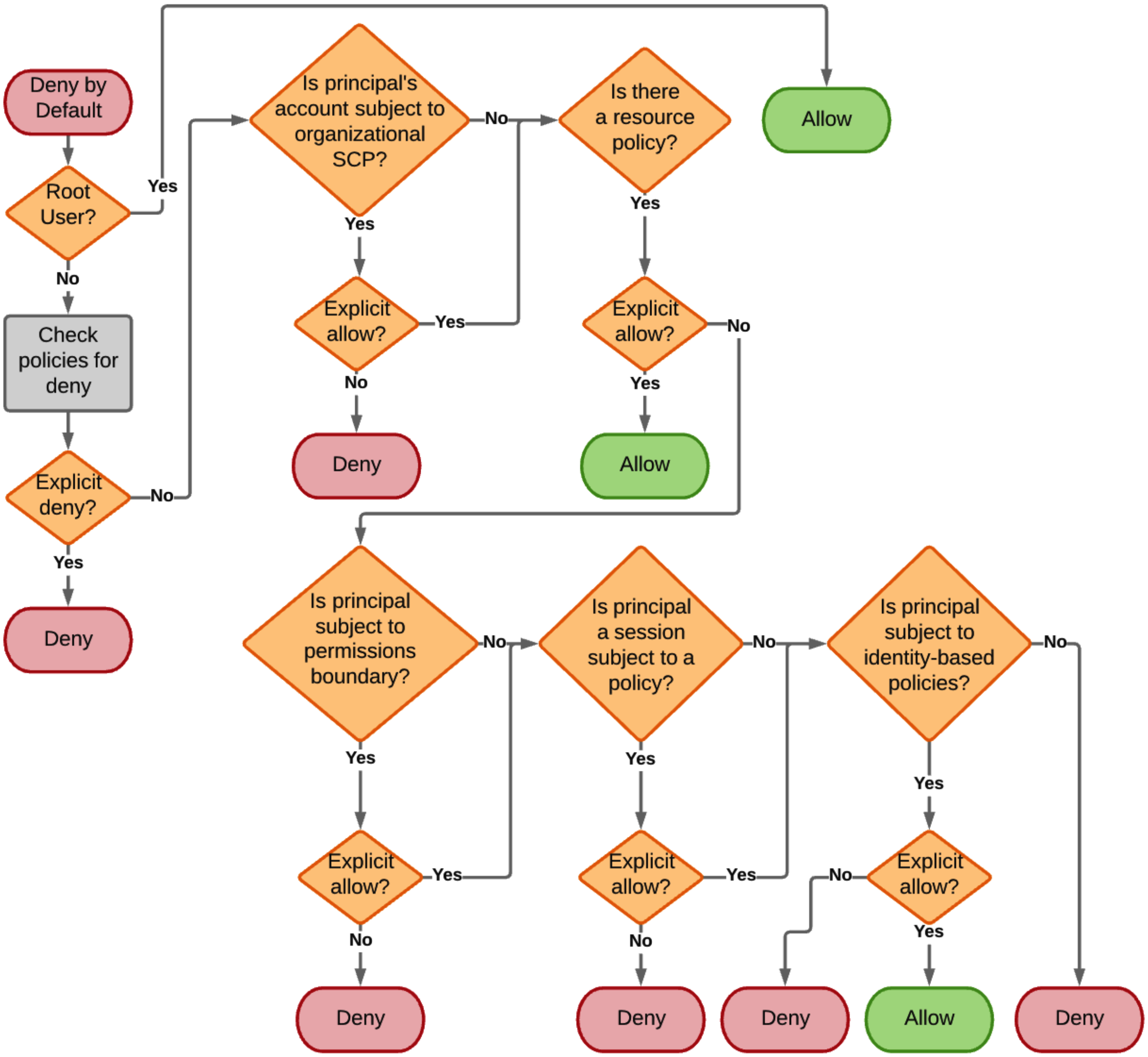
Inbound rules (2)

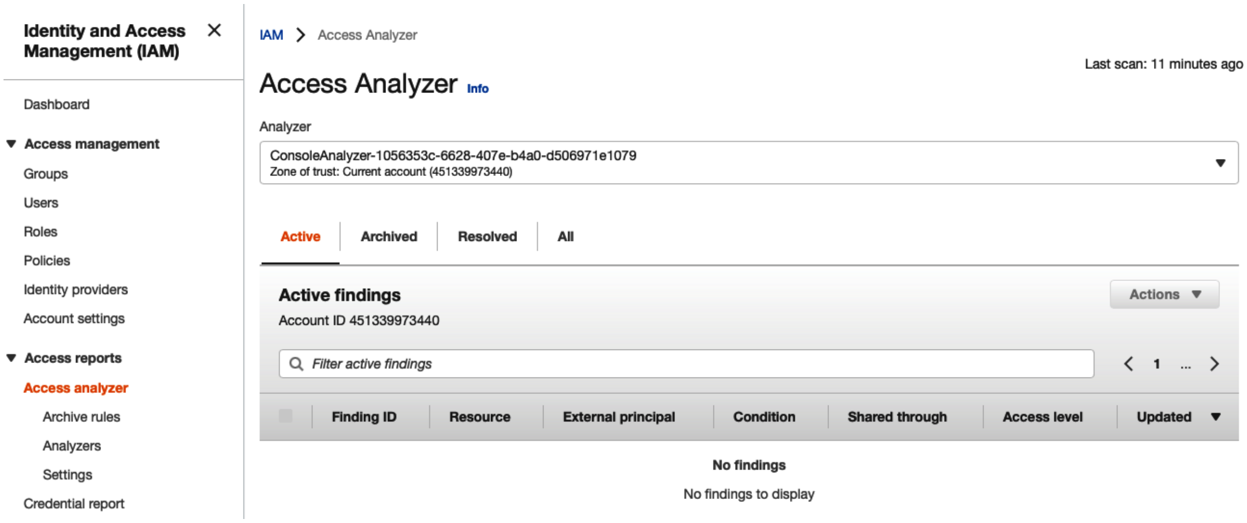
Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	✓ Allow
*	All traffic	All	All	0.0.0.0/0	⊗ Deny

Outbound rules (2)

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	✓ Allow
*	All traffic	All	All	0.0.0.0/0	⊗ Deny


AWS IAM (STS)
Sends Token & Policy ARN
Federated IDP
Authenticated by
Establishes Role Session
User
User Assumes Role and Temporary Credentials
Assumed Role


Deny by Default
Root User?
Yes
No
Check policies for deny
Explicit deny?
No
Yes
Deny
Is principal's account subject to organizational SCP?
No
Yes
Explicit allow?
Yes
No
Deny
Is there a resource policy?
Yes
Explicit allow?
No
Yes
Allow
Allow
Is principal subject to permissions boundary?
No
Yes
Explicit allow?
Yes
No
Deny
Is principal a session subject to a policy?
No
Yes
Explicit allow?
Yes
No
Deny
Is principal subject to identity-based policies?
No
Yes
Explicit allow?
No
Yes
Deny
Allow
Deny



Last scan: 11 minutes ago

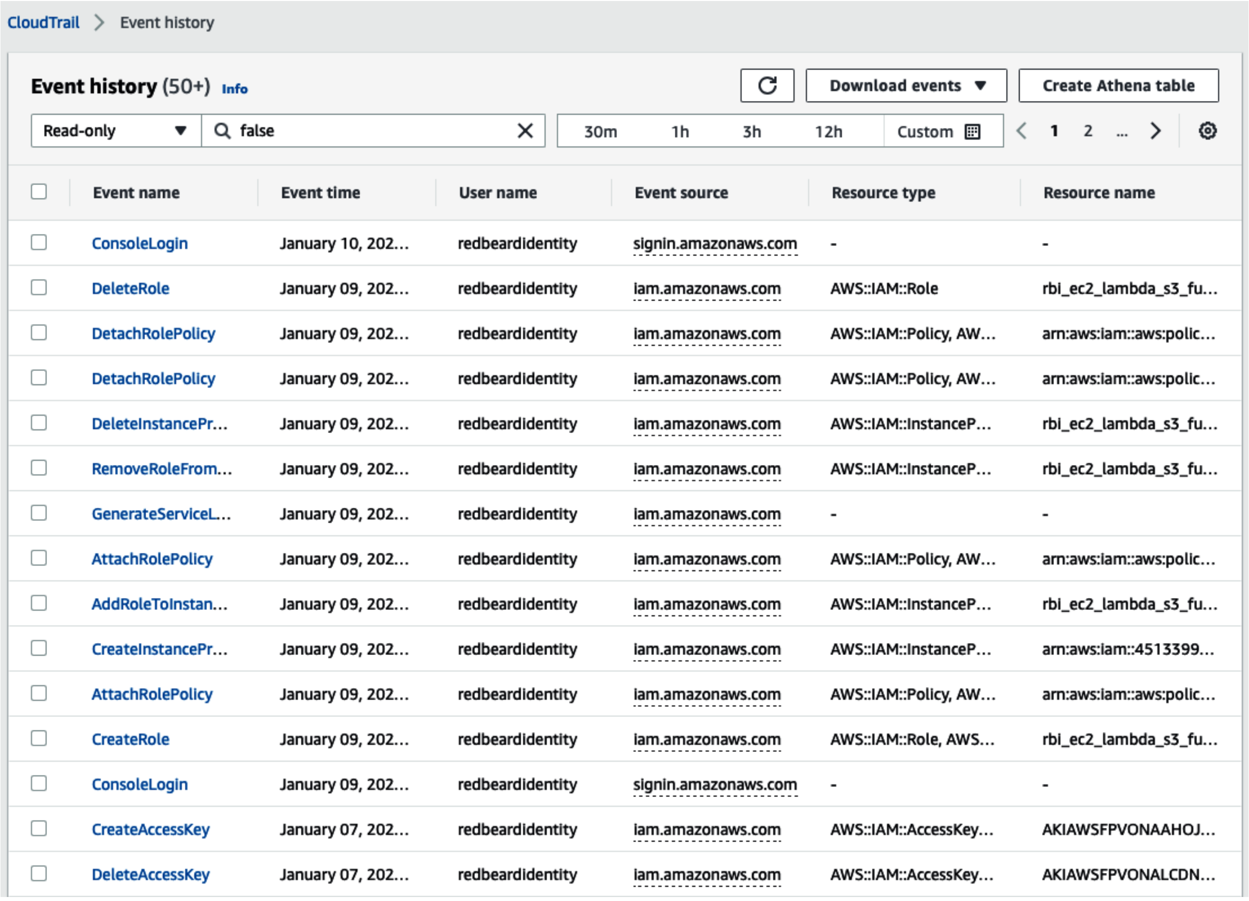
Access Analyzer

Analyzer: ConsoleAnalyzer-1056353c-6628-407e-b4a0-d506971e1079
Zone of trust: Current account (451339973440)

Active findings
Account ID 451339973440

Finding ID	Resource	External principal	Condition	Shared through	Access level	Updated

No findings
No findings to display

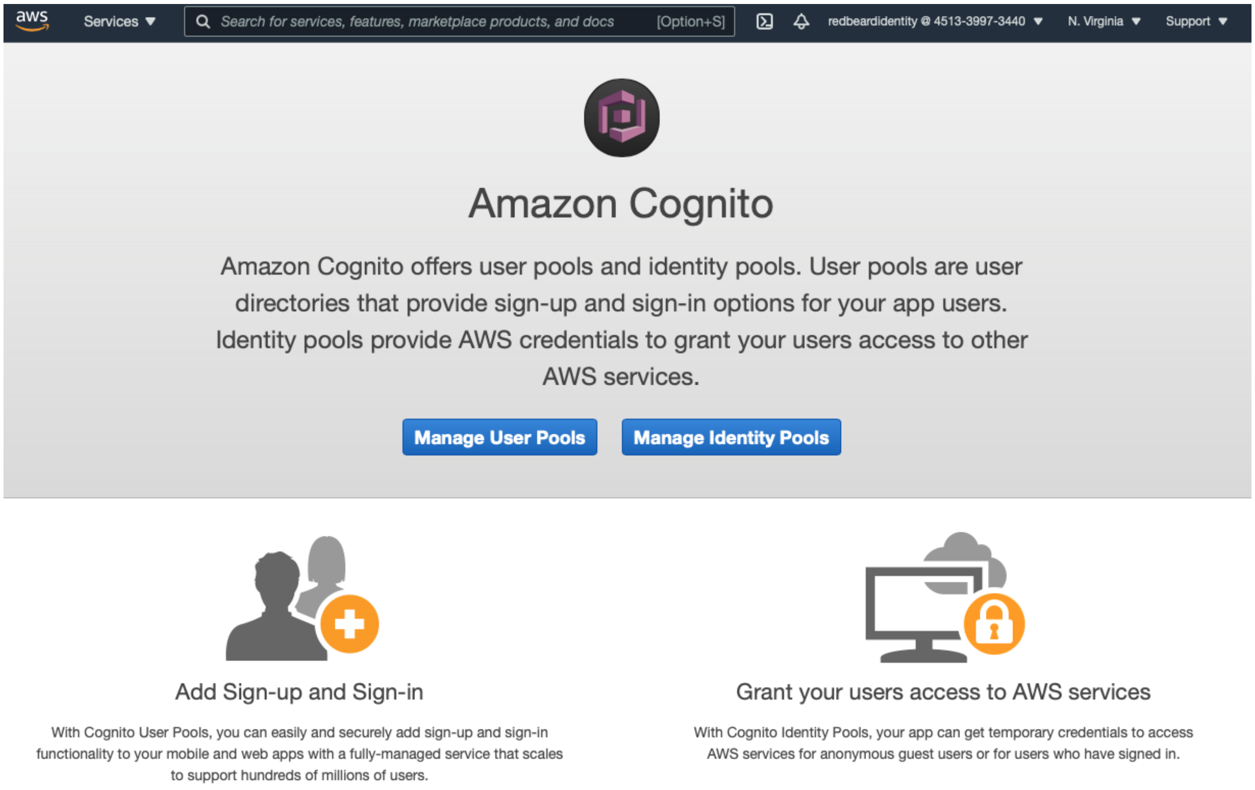


Event history (50+)

Read-only ▼ false

☐	Event name	Event time	User name	Event source	Resource type	Resource name
☐	ConsoleLogin	January 10, 202...	redbeardidentity	signin.amazonaws.com	-	-
☐	DeleteRole	January 09, 202...	redbeardidentity	iam.amazonaws.com	AWS::IAM::Role	rbi_ec2_lambda_s3_fu...
☐	DetachRolePolicy	January 09, 202...	redbeardidentity	iam.amazonaws.com	AWS::IAM::Policy, AW...	arn:aws:iam::aws:polic...
☐	DetachRolePolicy	January 09, 202...	redbeardidentity	iam.amazonaws.com	AWS::IAM::Policy, AW...	arn:aws:iam::aws:polic...
☐	DeleteInstancePr...	January 09, 202...	redbeardidentity	iam.amazonaws.com	AWS::IAM::InstanceP...	rbi_ec2_lambda_s3_fu...
☐	RemoveRoleFrom...	January 09, 202...	redbeardidentity	iam.amazonaws.com	AWS::IAM::InstanceP...	rbi_ec2_lambda_s3_fu...
☐	GenerateServiceL...	January 09, 202...	redbeardidentity	iam.amazonaws.com	-	-
☐	AttachRolePolicy	January 09, 202...	redbeardidentity	iam.amazonaws.com	AWS::IAM::Policy, AW...	arn:aws:iam::aws:polic...
☐	AddRoleToInstan...	January 09, 202...	redbeardidentity	iam.amazonaws.com	AWS::IAM::InstanceP...	rbi_ec2_lambda_s3_fu...
☐	CreateInstancePr...	January 09, 202...	redbeardidentity	iam.amazonaws.com	AWS::IAM::InstanceP...	arn:aws:iam::4513399...
☐	AttachRolePolicy	January 09, 202...	redbeardidentity	iam.amazonaws.com	AWS::IAM::Policy, AW...	arn:aws:iam::aws:polic...
☐	CreateRole	January 09, 202...	redbeardidentity	iam.amazonaws.com	AWS::IAM::Role, AWS...	rbi_ec2_lambda_s3_fu...
☐	ConsoleLogin	January 09, 202...	redbeardidentity	signin.amazonaws.com	-	-
☐	CreateAccessKey	January 07, 202...	redbeardidentity	iam.amazonaws.com	AWS::IAM::AccessKey...	AKIAWSFPVONAAHOJ...
☐	DeleteAccessKey	January 07, 202...	redbeardidentity	iam.amazonaws.com	AWS::IAM::AccessKey...	AKIAWSFPVONALCDN...

Chapter 5: Introducing Amazon Cognito


aws
Services ▼
Search for services, features, marketplace products, and docs [Option+S]
redbeardidentity @ 4513-3997-3440 ▼
N. Virginia ▼
Support ▼

Amazon Cognito

Amazon Cognito offers user pools and identity pools. User pools are user directories that provide sign-up and sign-in options for your app users. Identity pools provide AWS credentials to grant your users access to other AWS services.

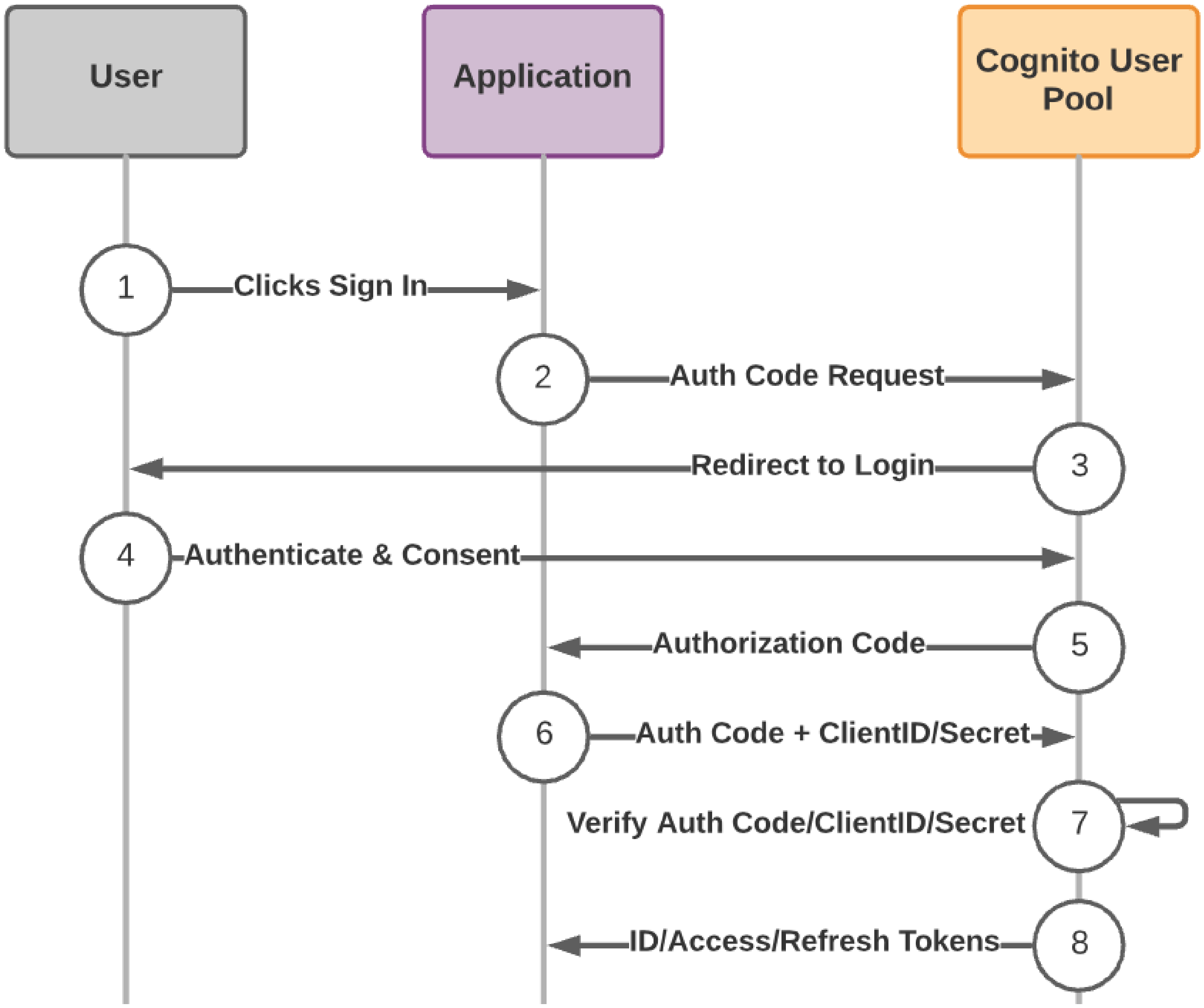
Manage User Pools
Manage Identity Pools

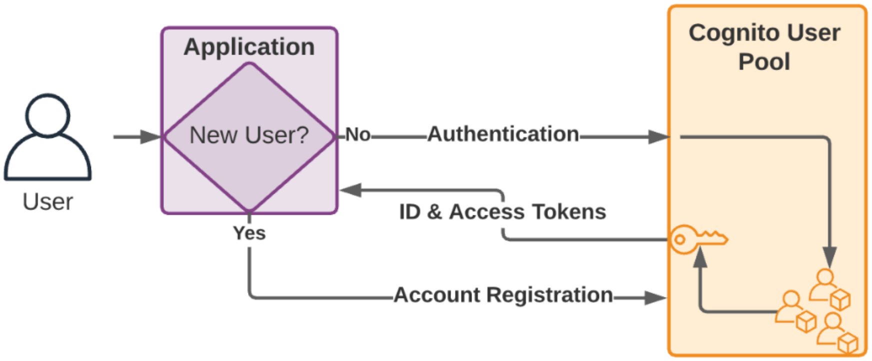
Add Sign-up and Sign-in

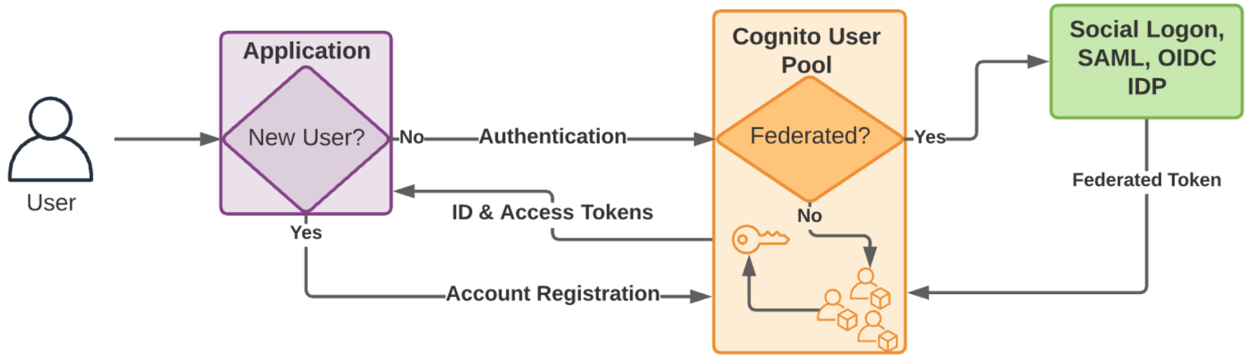
With Cognito User Pools, you can easily and securely add sign-up and sign-in functionality to your mobile and web apps with a fully-managed service that scales to support hundreds of millions of users.

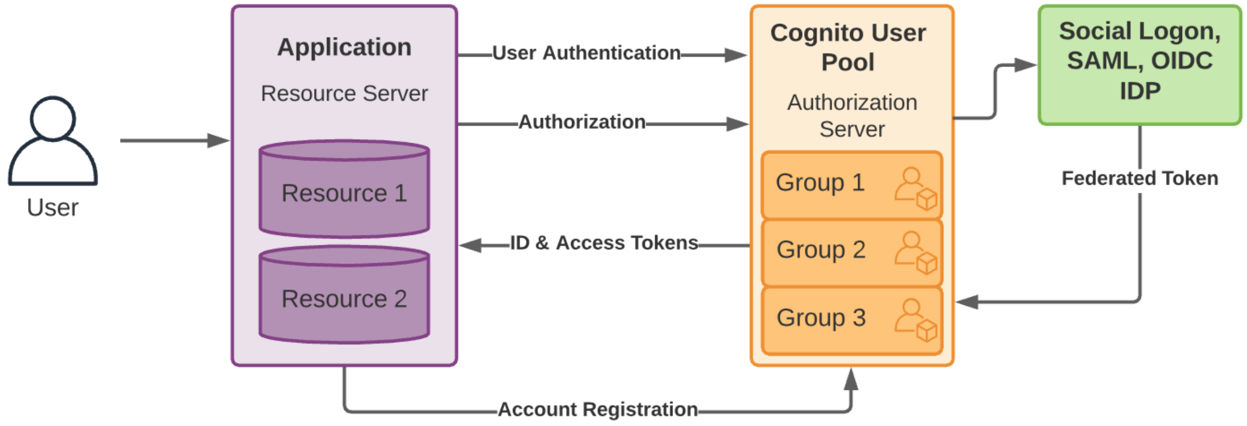
Grant your users access to AWS services

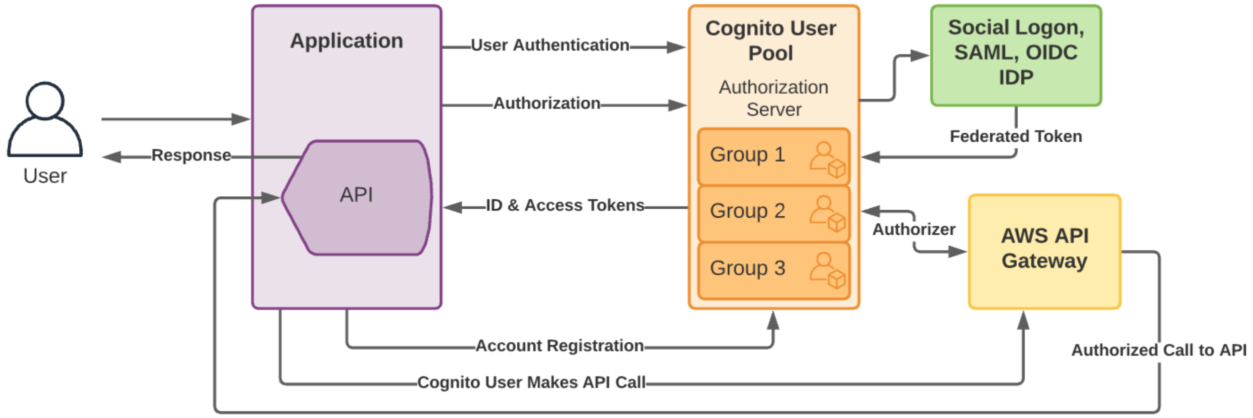
With Cognito Identity Pools, your app can get temporary credentials to access AWS services for anonymous guest users or for users who have signed in.

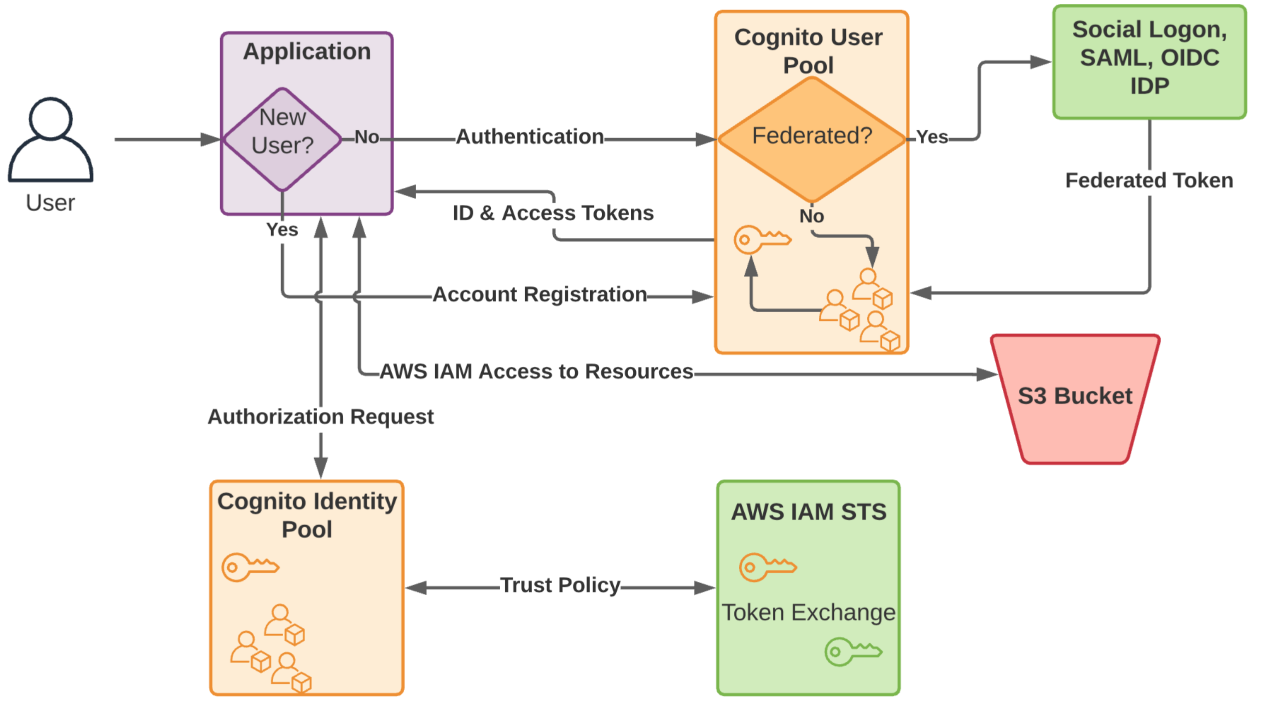

User
Application
Cognito User Pool
1
Clicks Sign In
2
Auth Code Request
Redirect to Login
3
4
Authenticate & Consent
Authorization Code
5
6
Auth Code + ClientID/Secret
Verify Auth Code/ClientID/Secret
7
ID/Access/Refresh Tokens
8

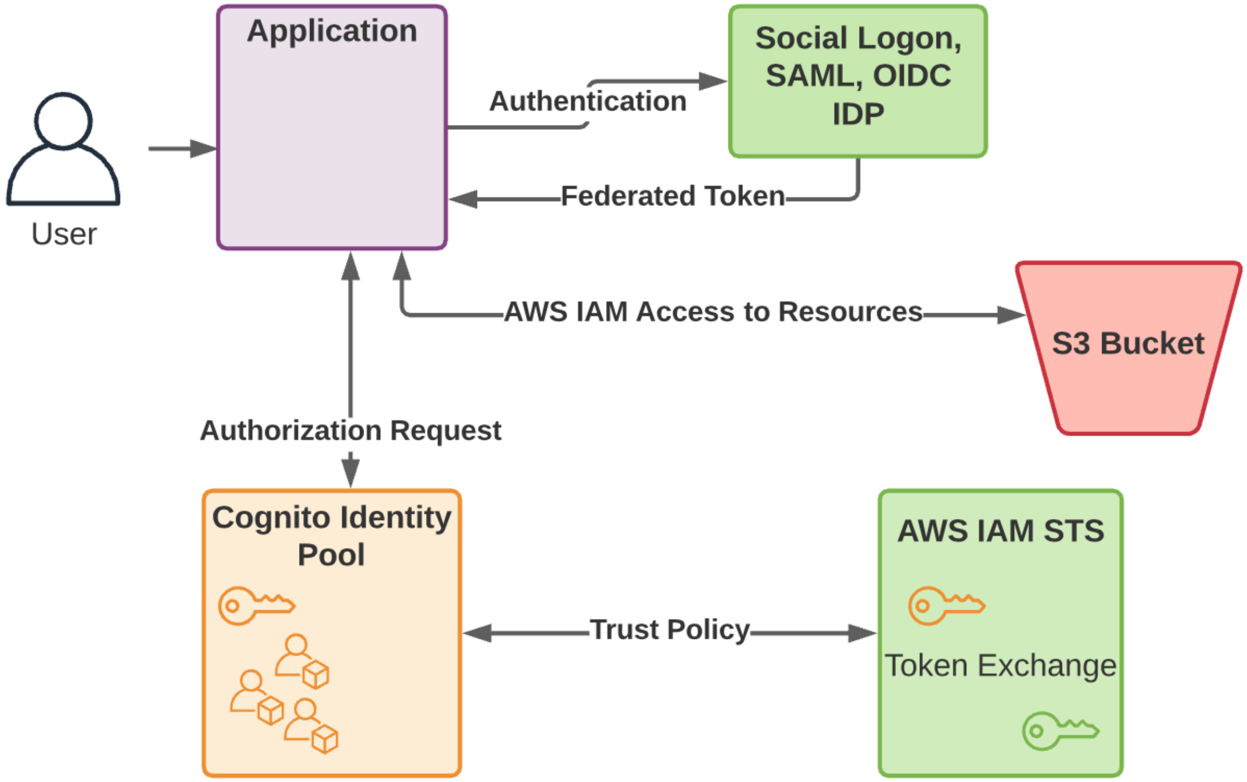

User
Application
New User?
No
Authentication
ID & Access Tokens
Yes
Account Registration
Cognito User Pool

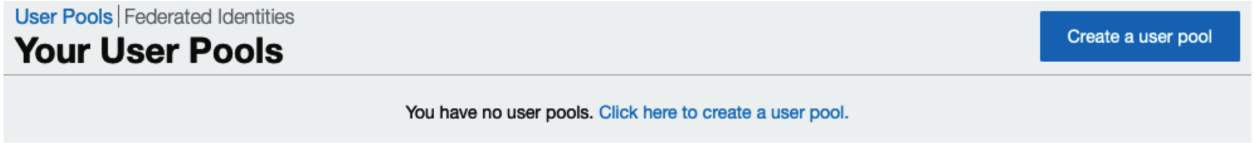

User
Application
New User?
No
Yes
Authentication
ID & Access Tokens
Account Registration
Cognito User Pool
Federated?
Yes
No
Social Logon, SAML, OIDC IDP
Federated Token


User
Application
Resource Server
Resource 1
Resource 2
User Authentication
Authorization
ID & Access Tokens
Account Registration
Cognito User Pool
Authorization Server
Group 1
Group 2
Group 3
Social Logon, SAML, OIDC IDP
Federated Token


User
Response
Application
API
User Authentication
Authorization
ID & Access Tokens
Account Registration
Cognito User Makes API Call
Cognito User Pool
Authorization Server
Group 1
Group 2
Group 3
Social Logon, SAML, OIDC IDP
Federated Token
Authorizer
AWS API Gateway
Authorized Call to API

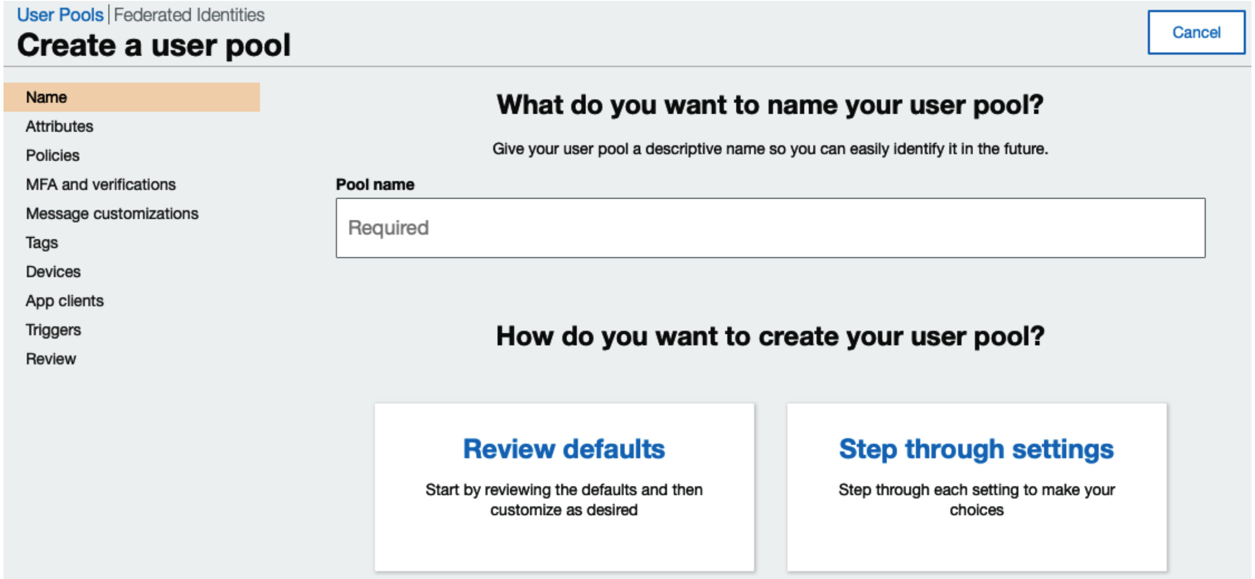

User
Application
New User?
No
Yes
Authentication
ID & Access Tokens
Account Registration
Cognito User Pool
Federated?
Yes
No
Social Logon, SAML, OIDC IDP
Federated Token
AWS IAM Access to Resources
S3 Bucket
Authorization Request
Cognito Identity Pool
Trust Policy
AWS IAM STS
Token Exchange


User
Application
Authentication
Social Logon, SAML, OIDC IDP
Federated Token
AWS IAM Access to Resources
S3 Bucket
Authorization Request
Cognito Identity Pool
Trust Policy
AWS IAM STS
Token Exchange



Your User Pools

You have no user pools. Click here to create a user pool.



Create a user pool

What do you want to name your user pool?

Give your user pool a descriptive name so you can easily identify it in the future.

Pool name

Required

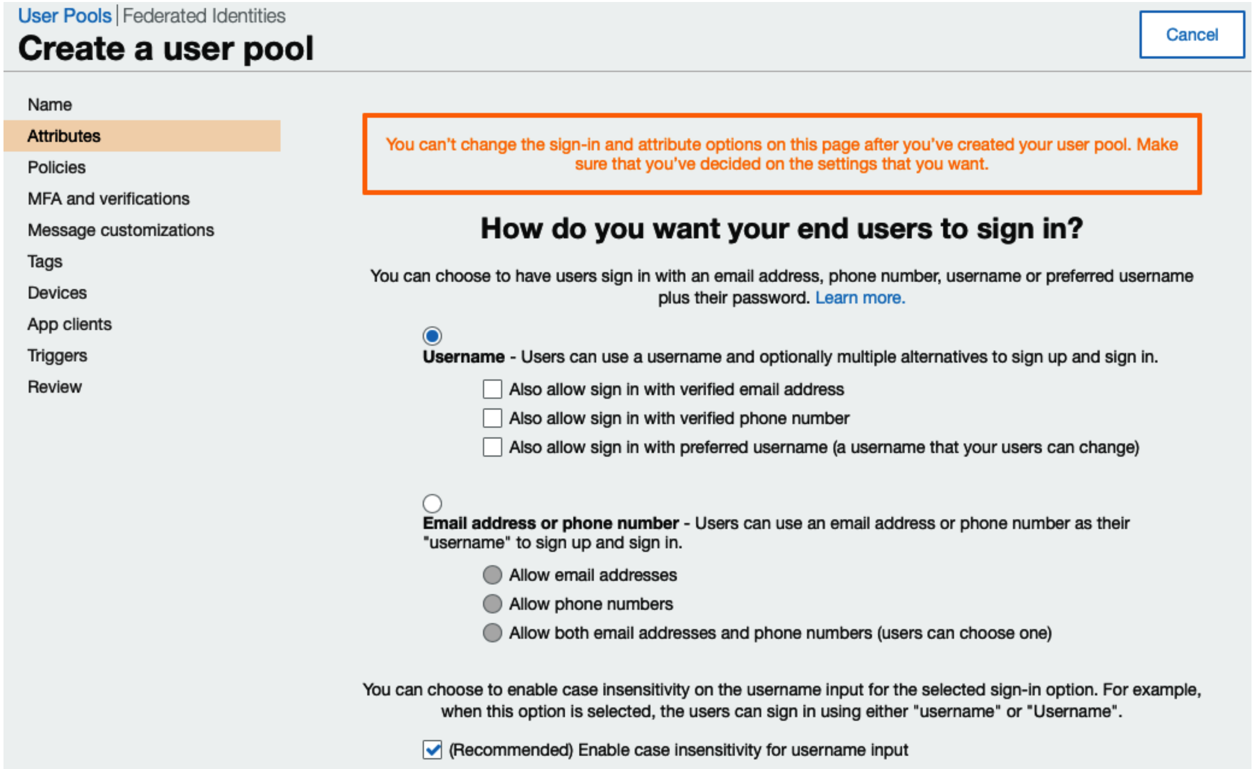
How do you want to create your user pool?

Review defaults

Start by reviewing the defaults and then customize as desired

Step through settings

Step through each setting to make your choices



Create a user pool

You can't change the sign-in and attribute options on this page after you've created your user pool. Make sure that you've decided on the settings that you want.

How do you want your end users to sign in?

You can choose to have users sign in with an email address, phone number, username or preferred username plus their password. Learn more.

● **Username** - Users can use a username and optionally multiple alternatives to sign up and sign in.

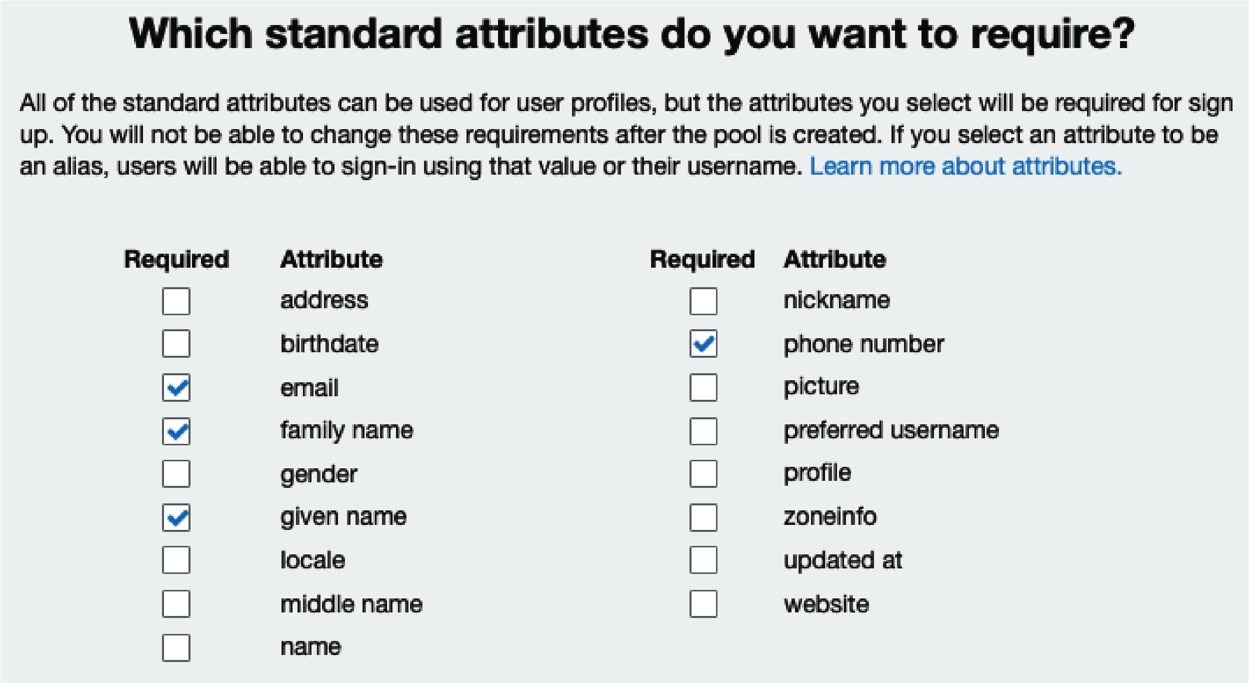
- □ Also allow sign in with verified email address
- □ Also allow sign in with verified phone number
- □ Also allow sign in with preferred username (a username that your users can change)

○ **Email address or phone number** - Users can use an email address or phone number as their "username" to sign up and sign in.

- ○ Allow email addresses
- ○ Allow phone numbers
- ○ Allow both email addresses and phone numbers (users can choose one)

You can choose to enable case insensitivity on the username input for the selected sign-in option. For example, when this option is selected, the users can sign in using either "username" or "Username".

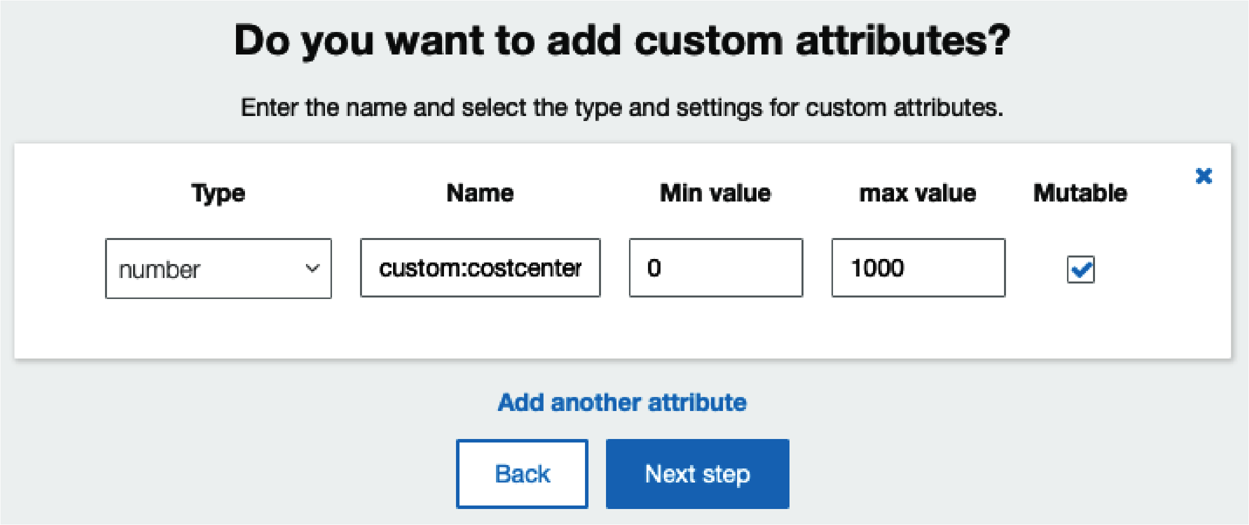
☑ (Recommended) Enable case insensitivity for username input



Which standard attributes do you want to require?

All of the standard attributes can be used for user profiles, but the attributes you select will be required for sign up. You will not be able to change these requirements after the pool is created. If you select an attribute to be an alias, users will be able to sign-in using that value or their username. Learn more about attributes.

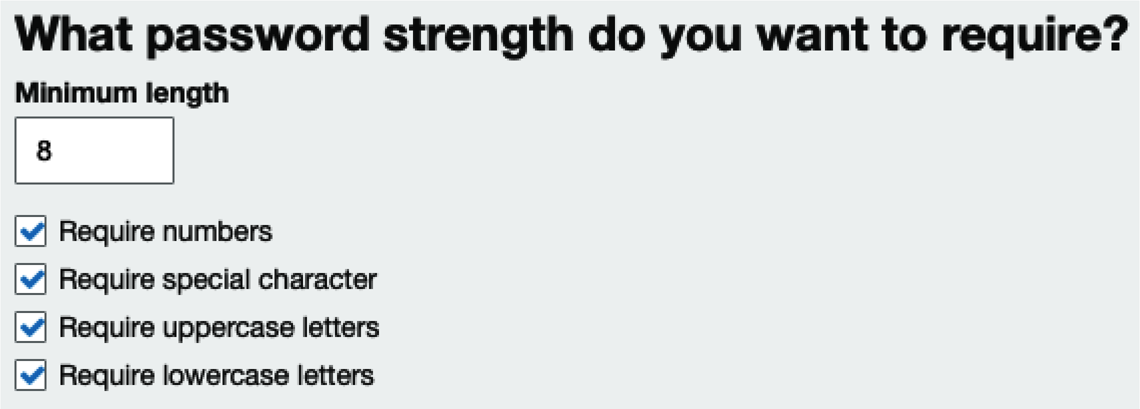
Required	Attribute	Required	Attribute
□	address	□	nickname
□	birthdate	☑	phone number
☑	email	□	picture
☑	family name	□	preferred username
□	gender	□	profile
☑	given name	□	zoneinfo
□	locale	□	updated at
□	middle name	□	website
□	name		



Do you want to add custom attributes?

Enter the name and select the type and settings for custom attributes.

Type	Name	Min value	max value	Mutable
number	custom:costcenter	0	1000	☑



What password strength do you want to require?

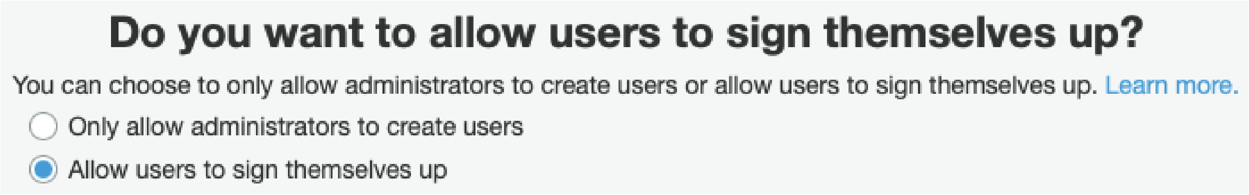
Minimum length: 8

☑ Require numbers

☑ Require special character

☑ Require uppercase letters

☑ Require lowercase letters

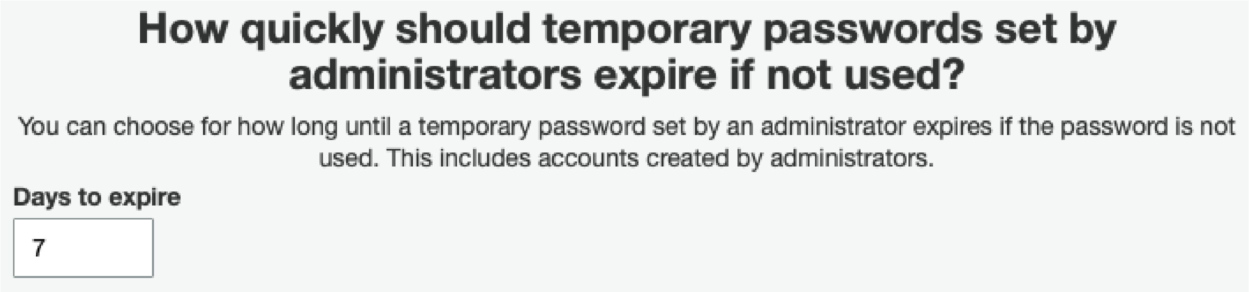


Do you want to allow users to sign themselves up?

You can choose to only allow administrators to create users or allow users to sign themselves up. Learn more.

○ Only allow administrators to create users

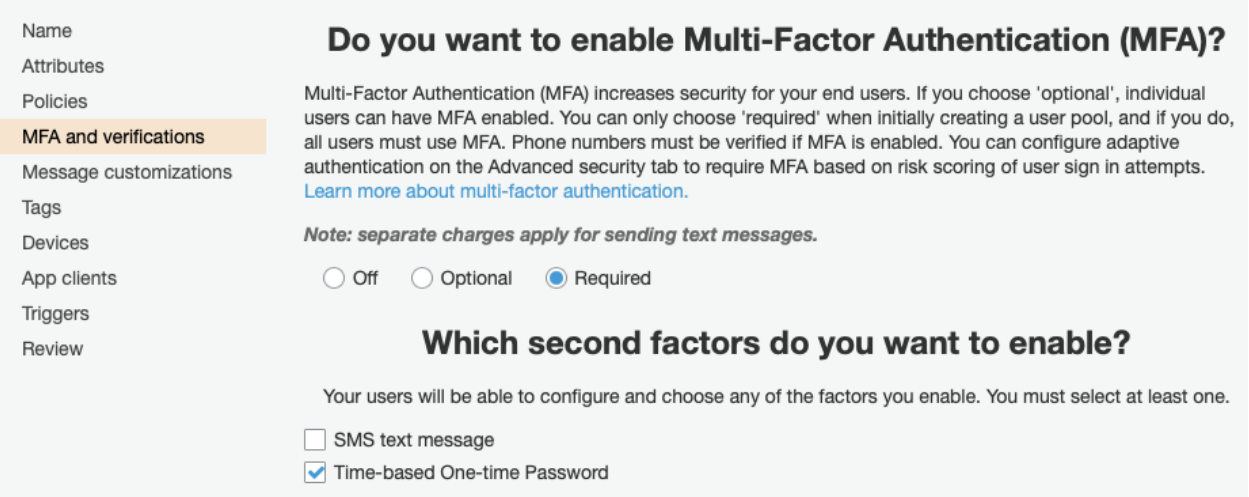
● Allow users to sign themselves up



How quickly should temporary passwords set by administrators expire if not used?

You can choose for how long until a temporary password set by an administrator expires if the password is not used. This includes accounts created by administrators.

Days to expire: 7



Do you want to enable Multi-Factor Authentication (MFA)?

Multi-Factor Authentication (MFA) increases security for your end users. If you choose 'optional', individual users can have MFA enabled. You can only choose 'required' when initially creating a user pool, and if you do, all users must use MFA. Phone numbers must be verified if MFA is enabled. You can configure adaptive authentication on the Advanced security tab to require MFA based on risk scoring of user sign in attempts. Learn more about multi-factor authentication.

Note: separate charges apply for sending text messages.

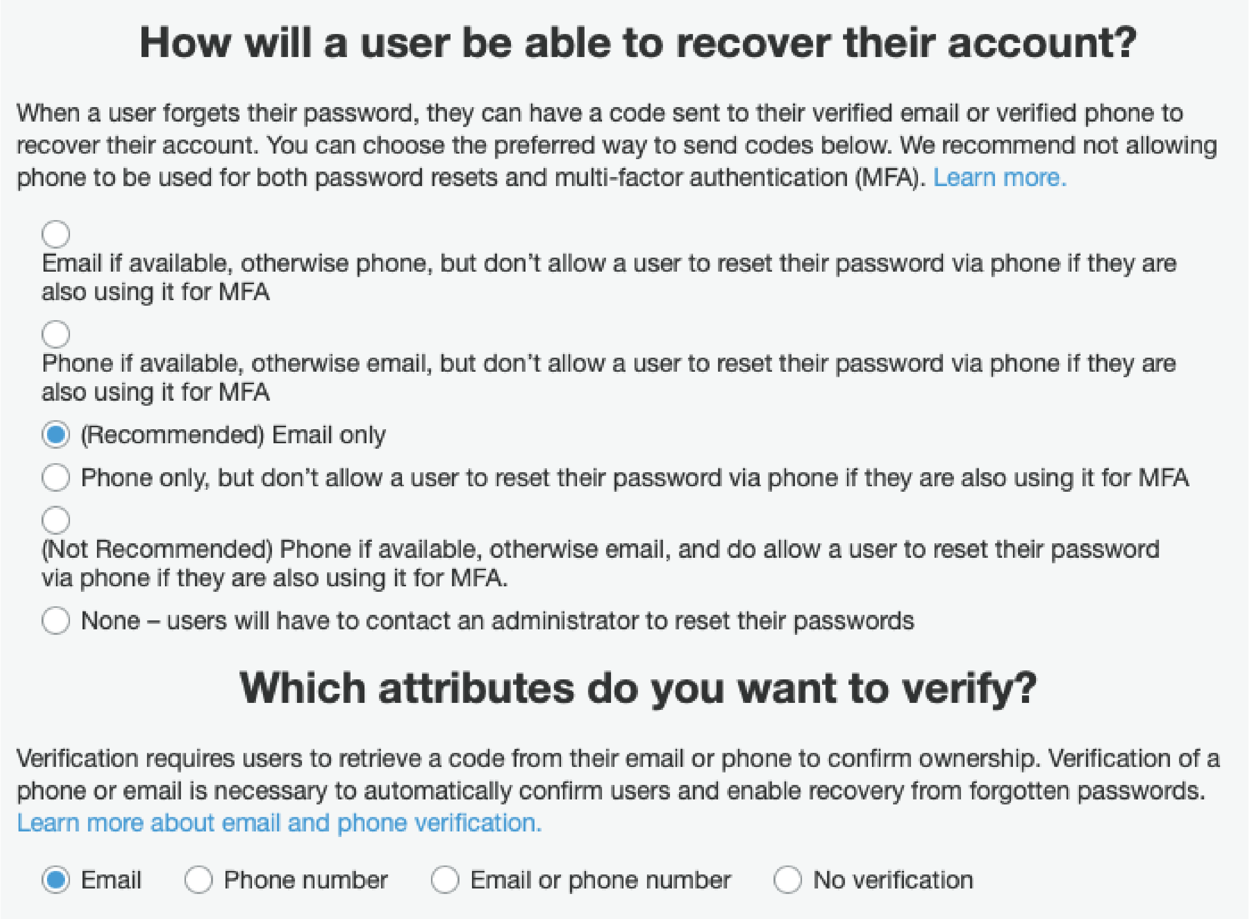
○ Off ○ Optional ● Required

Which second factors do you want to enable?

Your users will be able to configure and choose any of the factors you enable. You must select at least one.

□ SMS text message

☑ Time-based One-time Password



How will a user be able to recover their account?

When a user forgets their password, they can have a code sent to their verified email or verified phone to recover their account. You can choose the preferred way to send codes below. We recommend not allowing phone to be used for both password resets and multi-factor authentication (MFA). Learn more.

○ Email if available, otherwise phone, but don’t allow a user to reset their password via phone if they are also using it for MFA

○ Phone if available, otherwise email, but don’t allow a user to reset their password via phone if they are also using it for MFA

● (Recommended) Email only

○ Phone only, but don’t allow a user to reset their password via phone if they are also using it for MFA

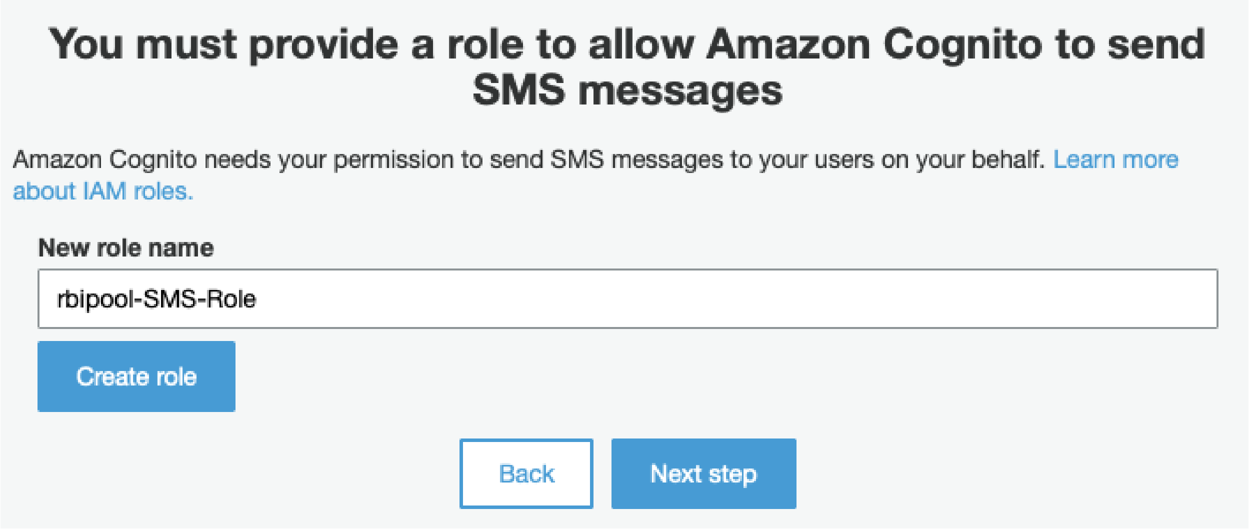
○ (Not Recommended) Phone if available, otherwise email, and do allow a user to reset their password via phone if they are also using it for MFA.

○ None – users will have to contact an administrator to reset their passwords

Which attributes do you want to verify?

Verification requires users to retrieve a code from their email or phone to confirm ownership. Verification of a phone or email is necessary to automatically confirm users and enable recovery from forgotten passwords. Learn more about email and phone verification.

● Email ○ Phone number ○ Email or phone number ○ No verification

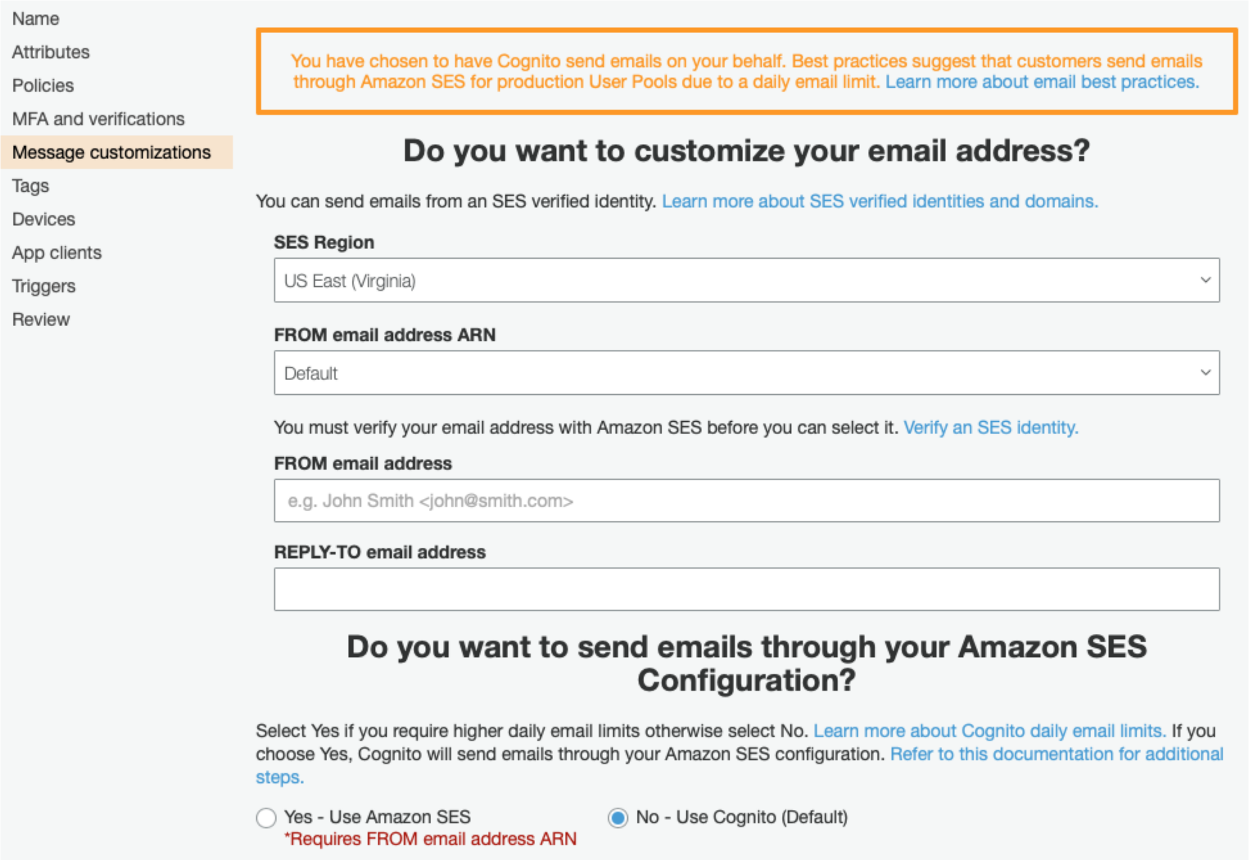


You must provide a role to allow Amazon Cognito to send SMS messages

Amazon Cognito needs your permission to send SMS messages to your users on your behalf. Learn more about IAM roles.

New role name

rbipool-SMS-Role



You have chosen to have Cognito send emails on your behalf. Best practices suggest that customers send emails through Amazon SES for production User Pools due to a daily email limit. Learn more about email best practices.

Do you want to customize your email address?

You can send emails from an SES verified identity. Learn more about SES verified identities and domains.

SES Region

US East (Virginia)

FROM email address ARN

Default

You must verify your email address with Amazon SES before you can select it. Verify an SES identity.

FROM email address

e.g. John Smith <john@smith.com>

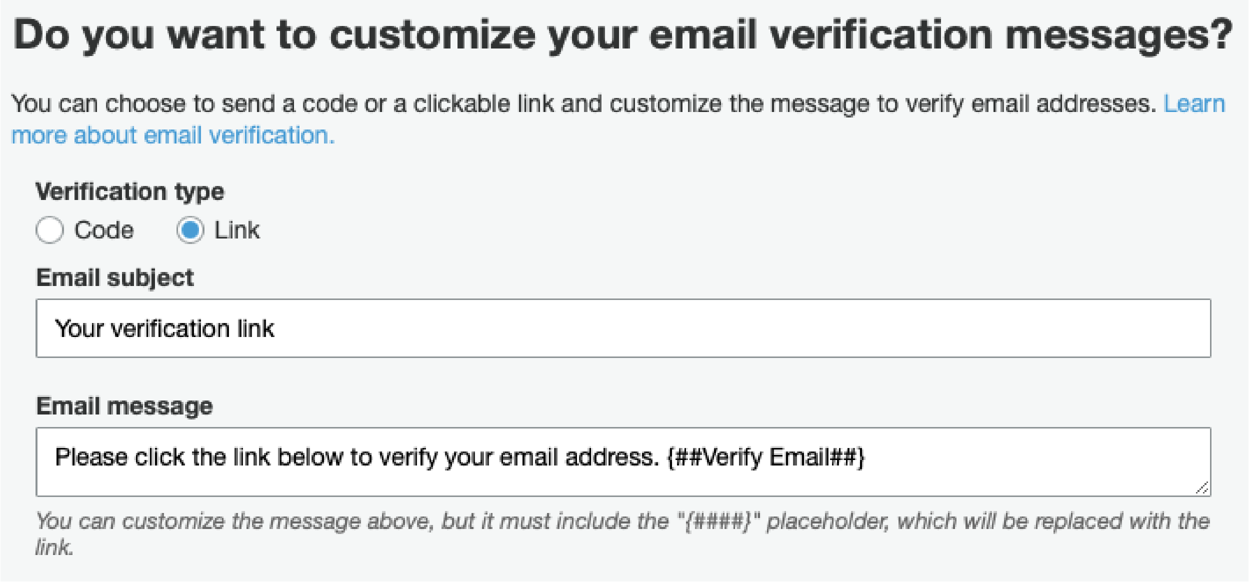
REPLY-TO email address

Do you want to send emails through your Amazon SES Configuration?

Select Yes if you require higher daily email limits otherwise select No. Learn more about Cognito daily email limits. If you choose Yes, Cognito will send emails through your Amazon SES configuration. Refer to this documentation for additional steps.

○ Yes - Use Amazon SES
*Requires FROM email address ARN

● No - Use Cognito (Default)



Do you want to customize your email verification messages?

You can choose to send a code or a clickable link and customize the message to verify email addresses. Learn more about email verification.

Verification type

○ Code ● Link

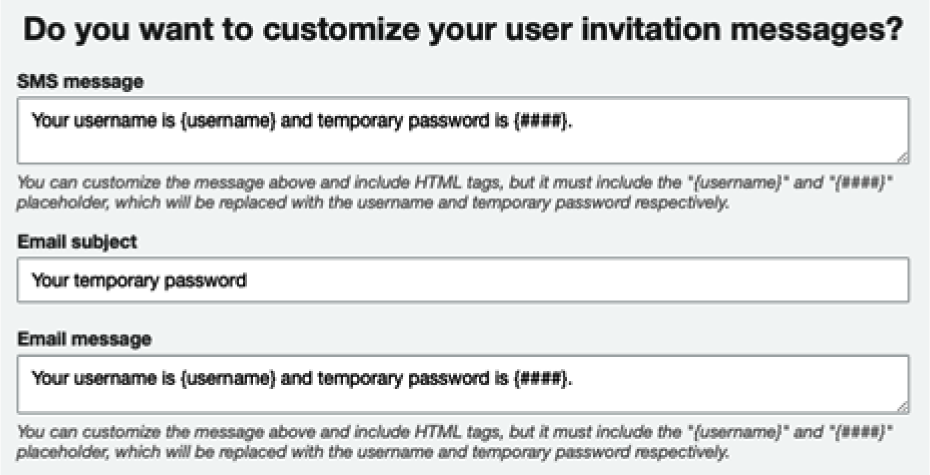
Email subject

Your verification link

Email message

Please click the link below to verify your email address. {##Verify Email##}

You can customize the message above, but it must include the "{####}" placeholder, which will be replaced with the link.



Do you want to customize your user invitation messages?

SMS message

Your username is {username} and temporary password is {####}.

You can customize the message above and include HTML tags, but it must include the "{username}" and "{####}" placeholder, which will be replaced with the username and temporary password respectively.

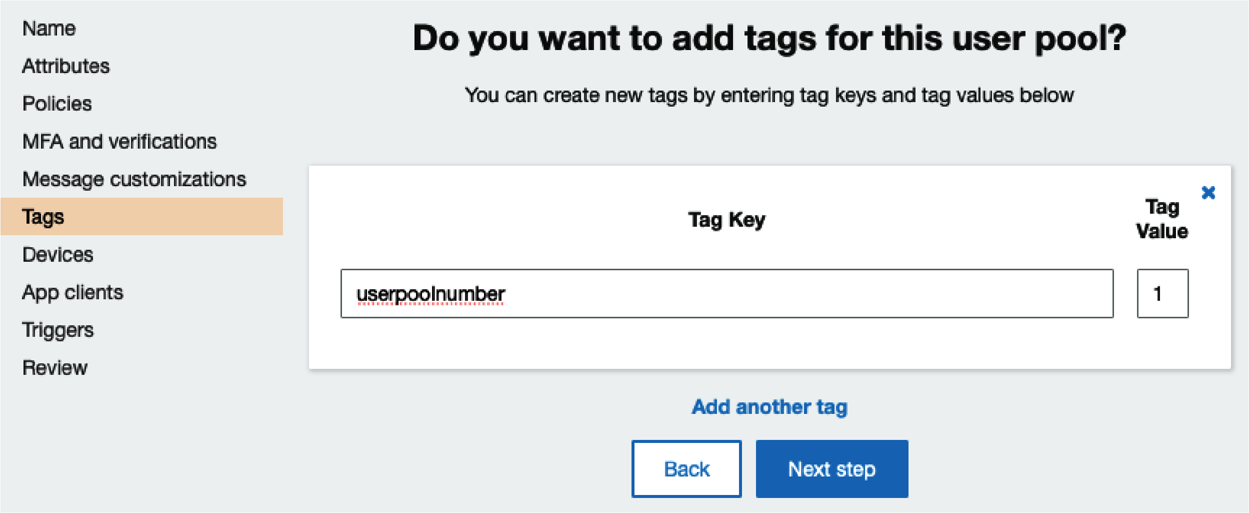
Email subject

Your temporary password

Email message

Your username is {username} and temporary password is {####}.

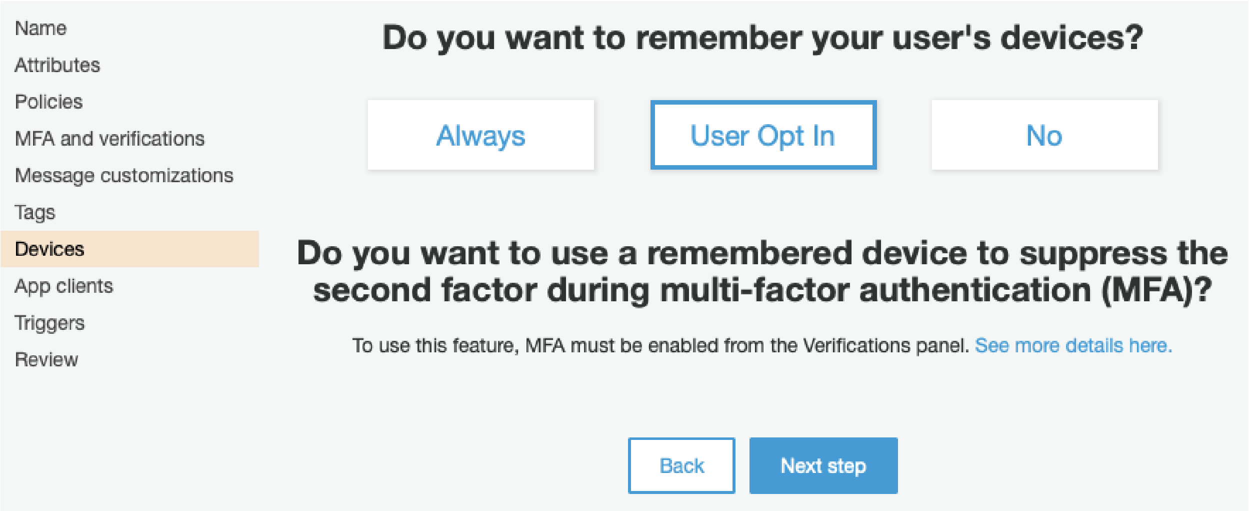
You can customize the message above and include HTML tags, but it must include the "{username}" and "{####}" placeholder, which will be replaced with the username and temporary password respectively.



Do you want to add tags for this user pool?

You can create new tags by entering tag keys and tag values below

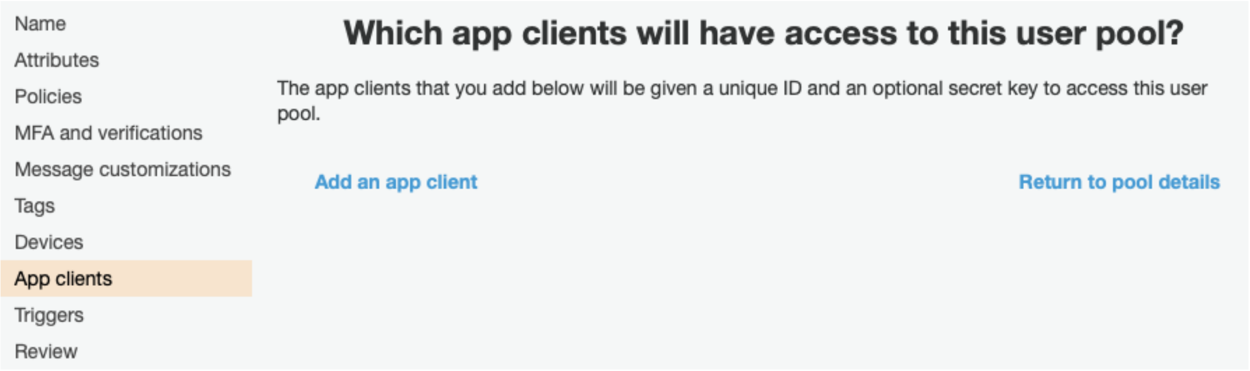
Tag Key	Tag Value
userpoolnumber	1



Do you want to remember your user's devices?

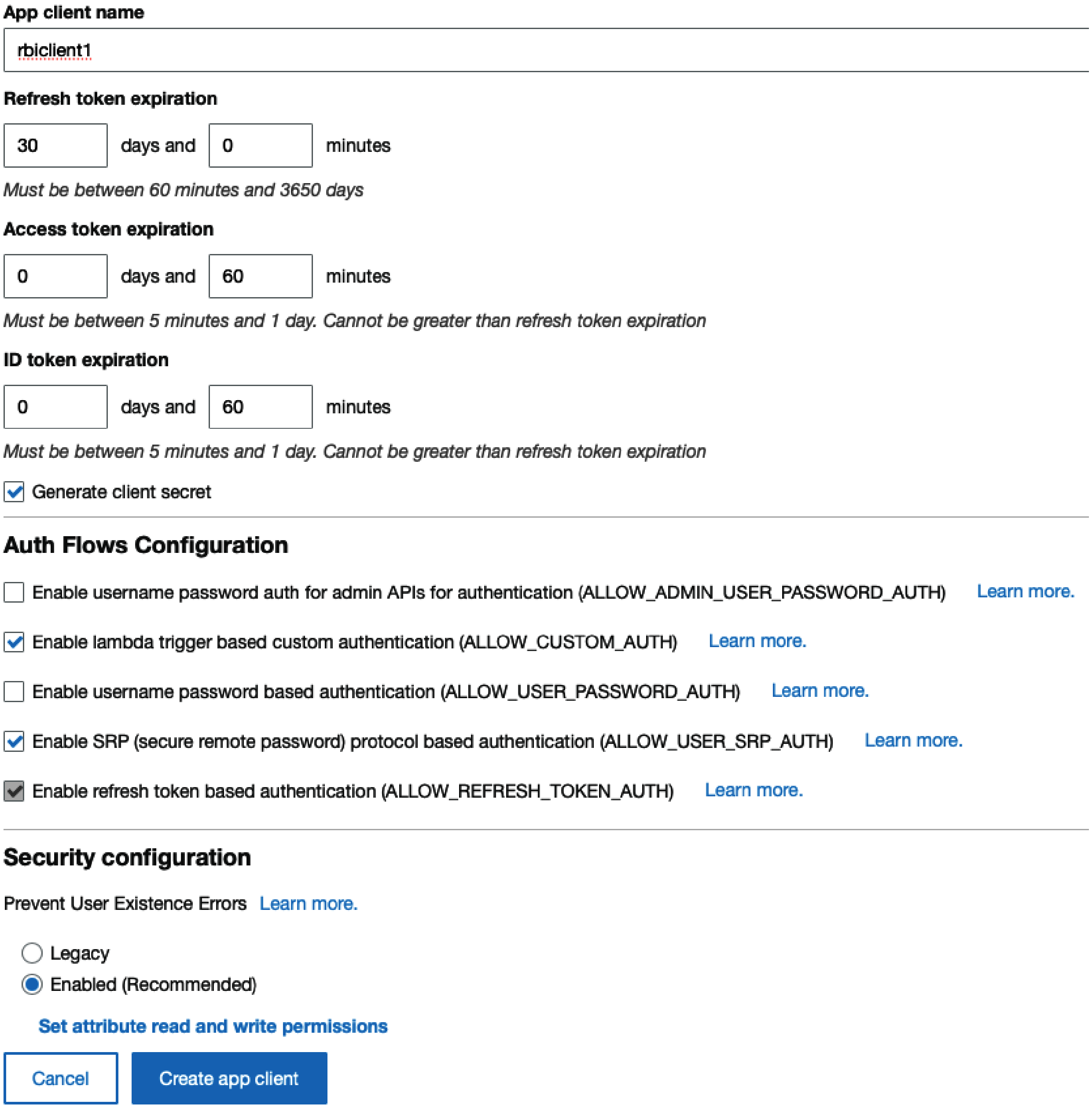
Do you want to use a remembered device to suppress the second factor during multi-factor authentication (MFA)?

To use this feature, MFA must be enabled from the Verifications panel. See more details here.



Which app clients will have access to this user pool?

The app clients that you add below will be given a unique ID and an optional secret key to access this user pool.



App client name

rbiclient1

Refresh token expiration

30 days and 0 minutes

Must be between 60 minutes and 3650 days

Access token expiration

0 days and 60 minutes

Must be between 5 minutes and 1 day. Cannot be greater than refresh token expiration

ID token expiration

0 days and 60 minutes

Must be between 5 minutes and 1 day. Cannot be greater than refresh token expiration

☑ Generate client secret

Auth Flows Configuration

□ Enable username password auth for admin APIs for authentication (ALLOW_ADMIN_USER_PASSWORD_AUTH) Learn more.

☑ Enable lambda trigger based custom authentication (ALLOW_CUSTOM_AUTH) Learn more.

□ Enable username password based authentication (ALLOW_USER_PASSWORD_AUTH) Learn more.

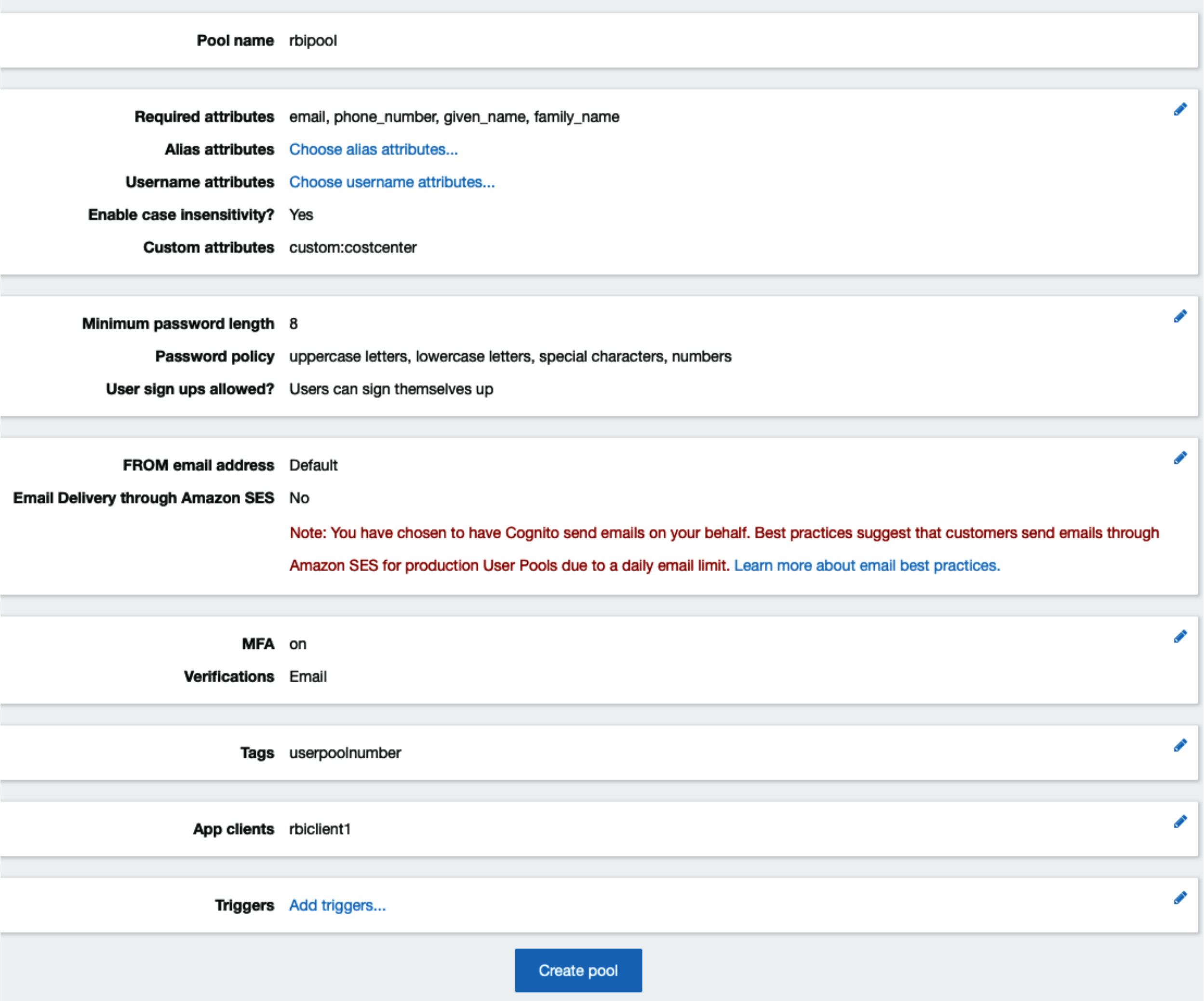
☑ Enable SRP (secure remote password) protocol based authentication (ALLOW_USER_SRP_AUTH) Learn more.

☑ Enable refresh token based authentication (ALLOW_REFRESH_TOKEN_AUTH) Learn more.

Security configuration

Prevent User Existence Errors Learn more.

○ Legacy
● Enabled (Recommended)



Pool name rbipool

Required attributes email, phone_number, given_name, family_name

Alias attributes Choose alias attributes...

Username attributes Choose username attributes...

Enable case insensitivity? Yes

Custom attributes custom:costcenter

Minimum password length 8

Password policy uppercase letters, lowercase letters, special characters, numbers

User sign ups allowed? Users can sign themselves up

FROM email address Default

Email Delivery through Amazon SES No

Note: You have chosen to have Cognito send emails on your behalf. Best practices suggest that customers send emails through Amazon SES for production User Pools due to a daily email limit. Learn more about email best practices.

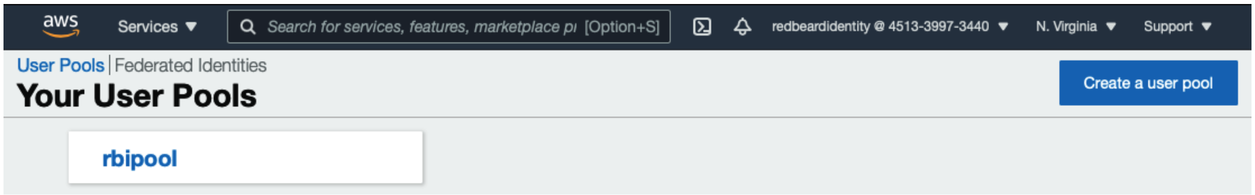
MFA on

Verifications Email

Tags userpoolnumber

App clients rbiclient1

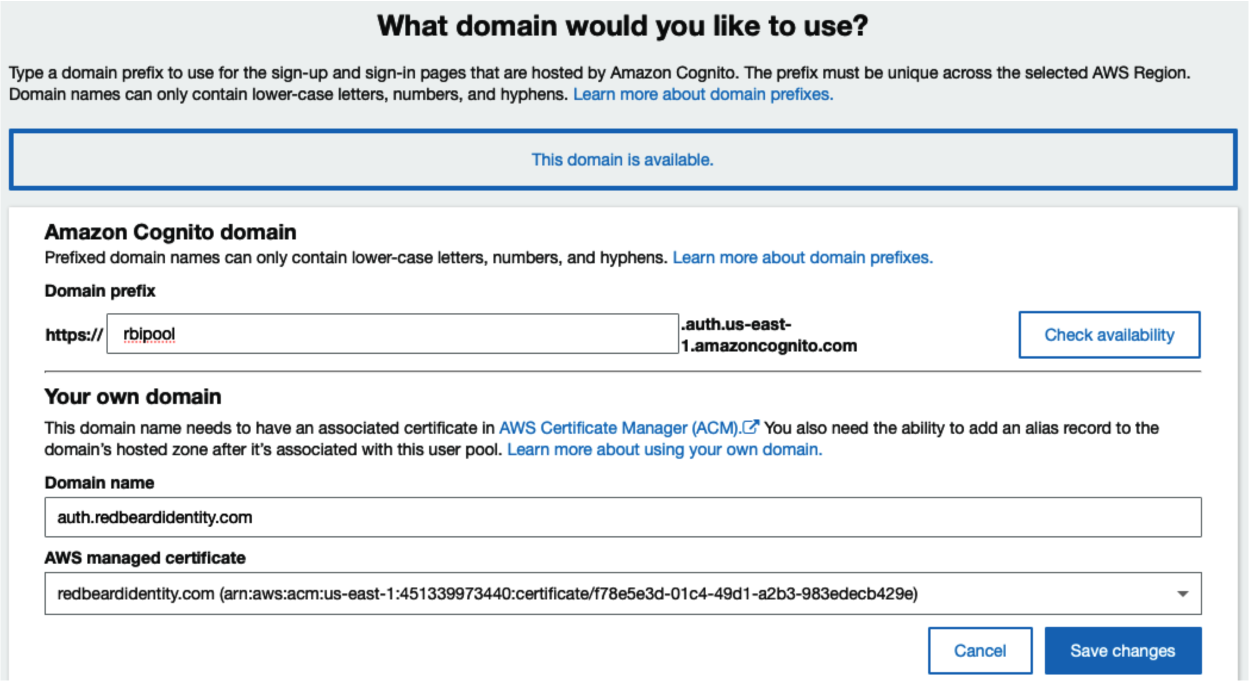
Triggers Add triggers...



aws
Services ▼
Search for services, features, marketplace pı [Option+S]
redbeardidentity @ 4513-3997-3440 ▼
N. Virginia ▼
Support ▼
User Pools | Federated Identities
Create a user pool

Your User Pools

rbipool



What domain would you like to use?

Type a domain prefix to use for the sign-up and sign-in pages that are hosted by Amazon Cognito. The prefix must be unique across the selected AWS Region. Domain names can only contain lower-case letters, numbers, and hyphens. Learn more about domain prefixes.

This domain is available.

Amazon Cognito domain

Prefixed domain names can only contain lower-case letters, numbers, and hyphens. Learn more about domain prefixes.

Domain prefix

https:// rbipool .auth.us-east-1.amazoncognito.com

Your own domain

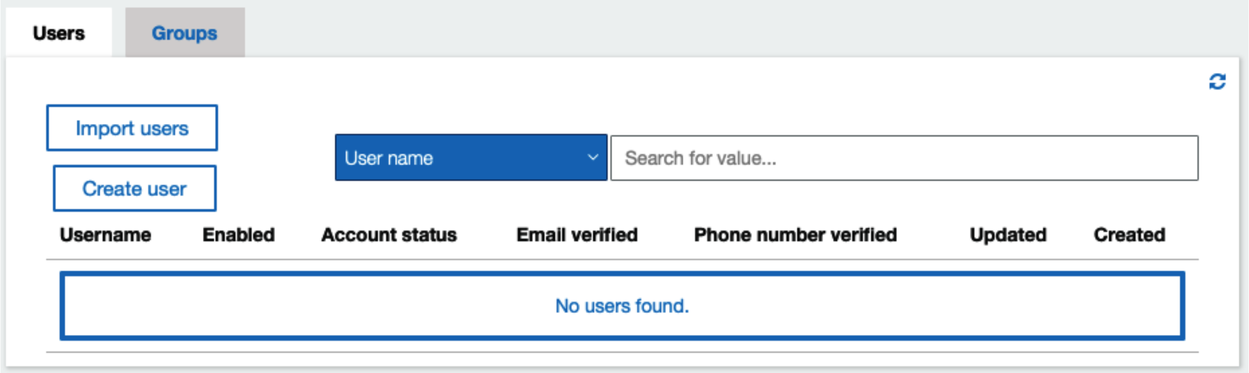
This domain name needs to have an associated certificate in AWS Certificate Manager (ACM). You also need the ability to add an alias record to the domain's hosted zone after it's associated with this user pool. Learn more about using your own domain.

Domain name

auth.redbeardidentity.com

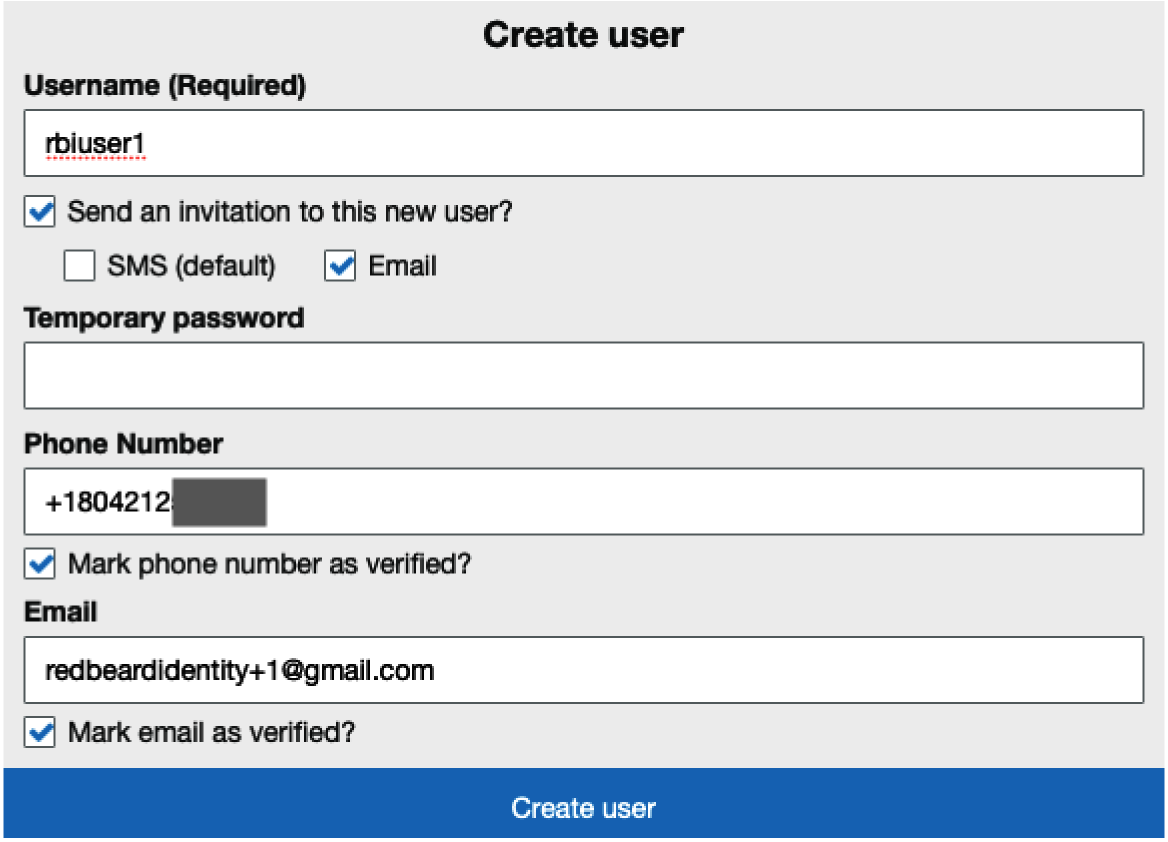
AWS managed certificate

redbeardidentity.com (arn:aws:acm:us-east-1:451339973440:certificate/f78e5e3d-01c4-49d1-a2b3-983edecb429e)



Username	Enabled	Account status	Email verified	Phone number verified	Updated	Created

No users found.



Create user

Username (Required)

rbiuser1

☑ Send an invitation to this new user?

□ SMS (default) ☑ Email

Temporary password

Phone Number

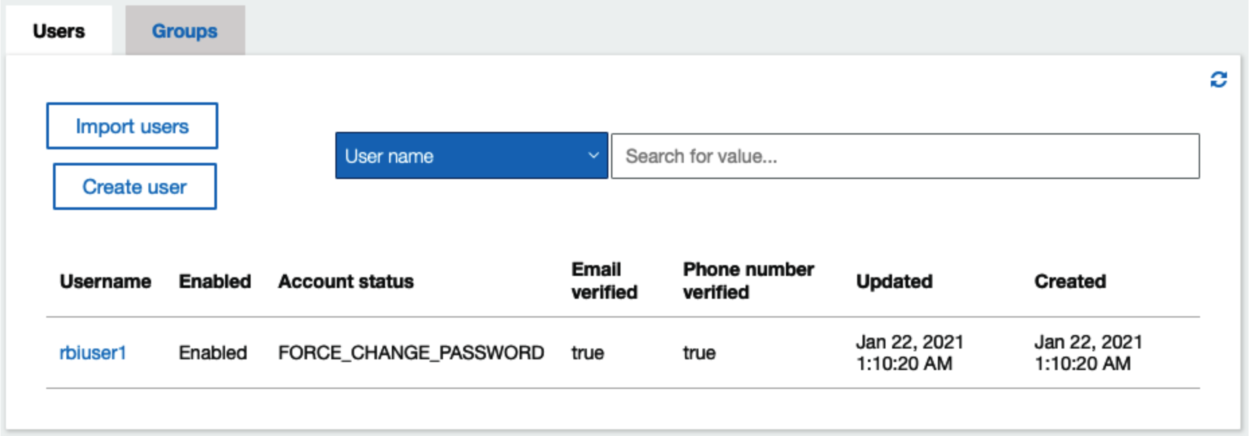
+1804212[redacted]

☑ Mark phone number as verified?

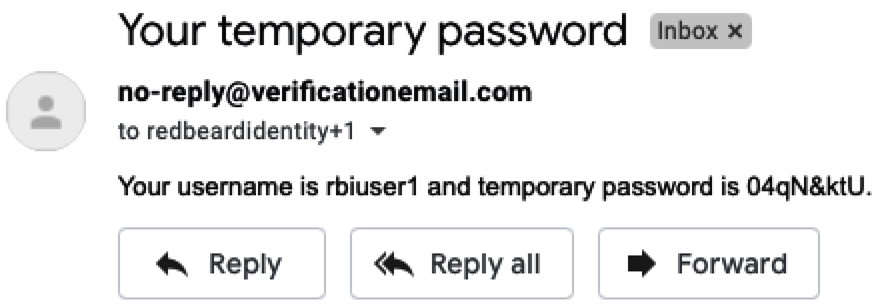
Email

redbeardidentity+1@gmail.com

☑ Mark email as verified?



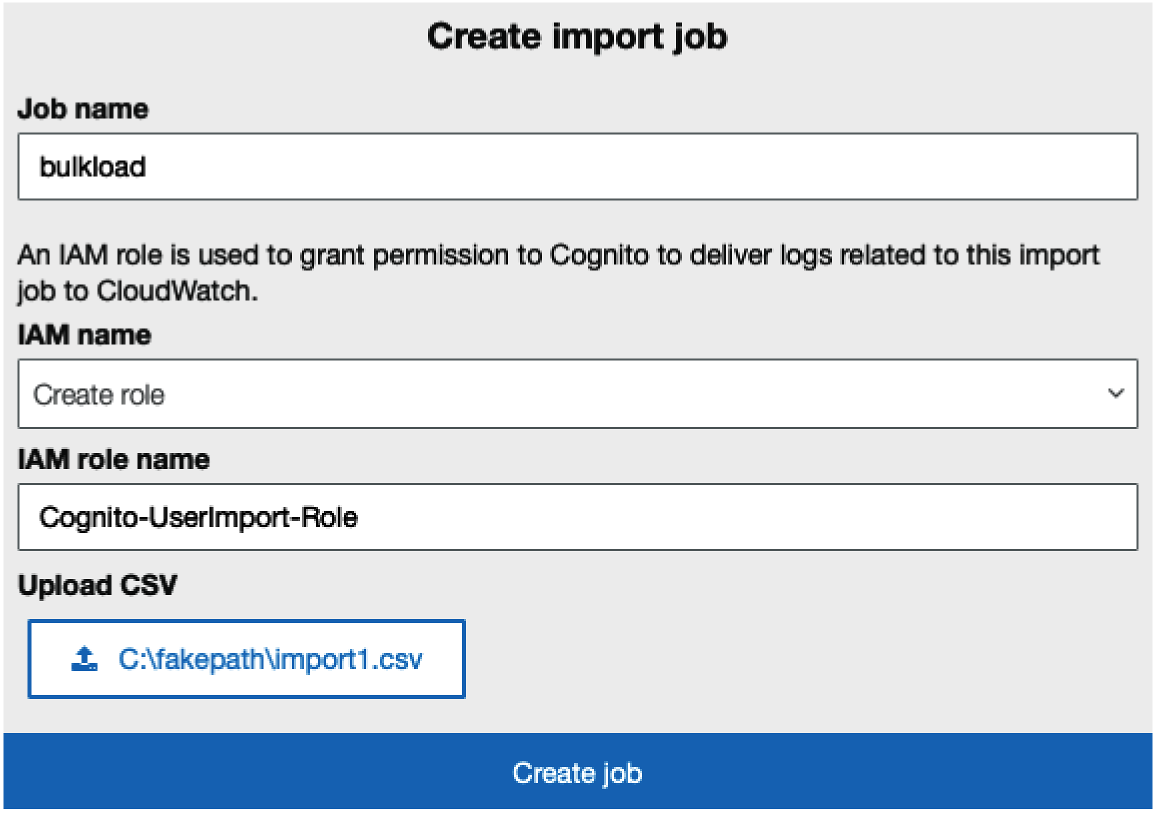
Username	Enabled	Account status	Email verified	Phone number verified	Updated	Created
rbiuser1	Enabled	FORCE_CHANGE_PASSWORD	true	true	Jan 22, 2021 1:10:20 AM	Jan 22, 2021 1:10:20 AM


Your temporary password

no-reply@verificationemail.com

to redbeardidentity+1

Your username is rbiuser1 and temporary password is 04qN&ktU.


Create import job

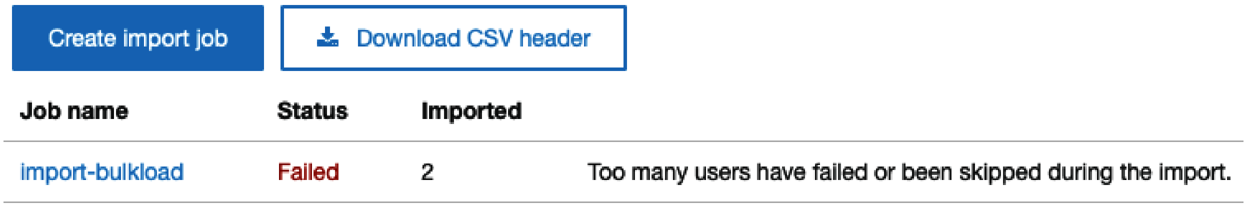
Job name: bulkload

An IAM role is used to grant permission to Cognito to deliver logs related to this import job to CloudWatch.

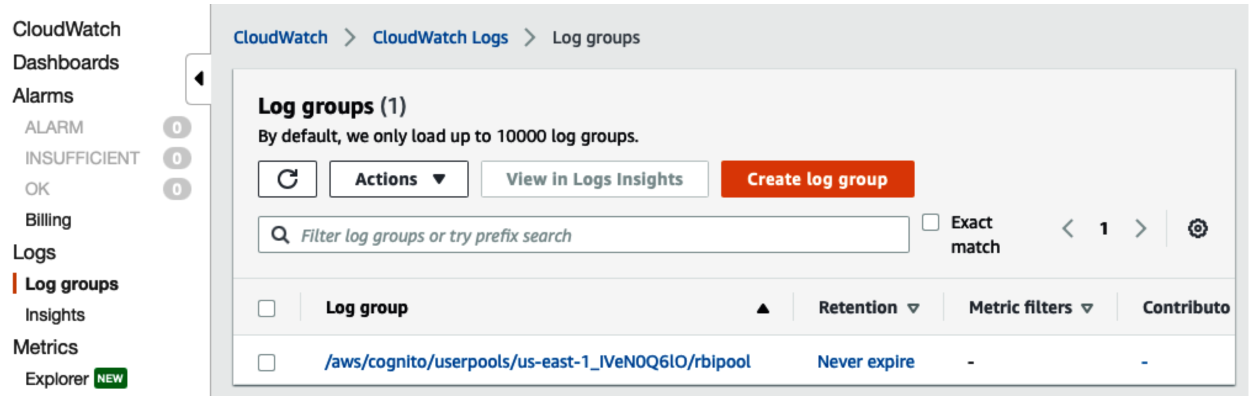
IAM name: Create role

IAM role name: Cognito-UserImport-Role

Upload CSV: C:\fakepath\import1.csv



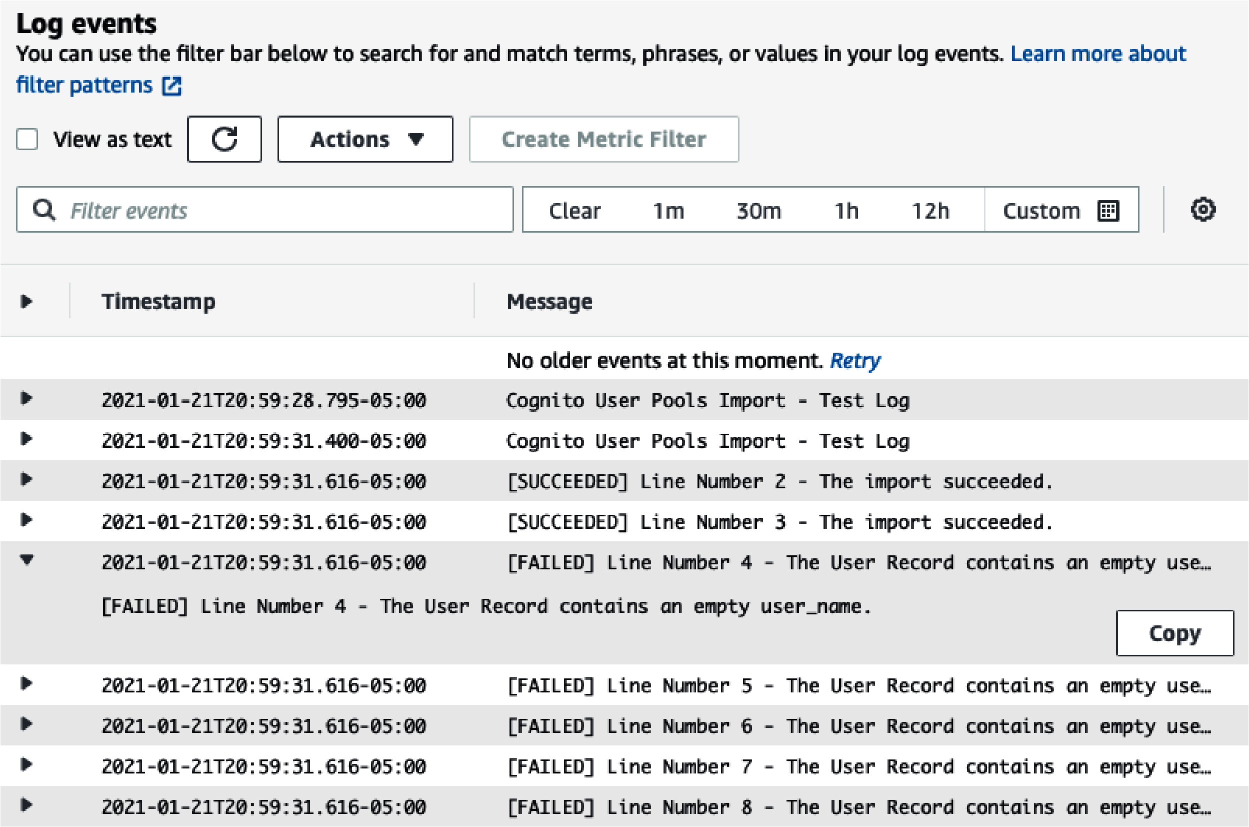
Job name	Status	Imported	
import-bulkload	Failed	2	Too many users have failed or been skipped during the import.



Log groups (1)

By default, we only load up to 10000 log groups.

□	Log group ▲	Retention ▽	Metric filters ▽	Contributo
□	/aws/cognito/userpools/us-east-1_IVeN0Q6lO/rbipool	Never expire	-	-

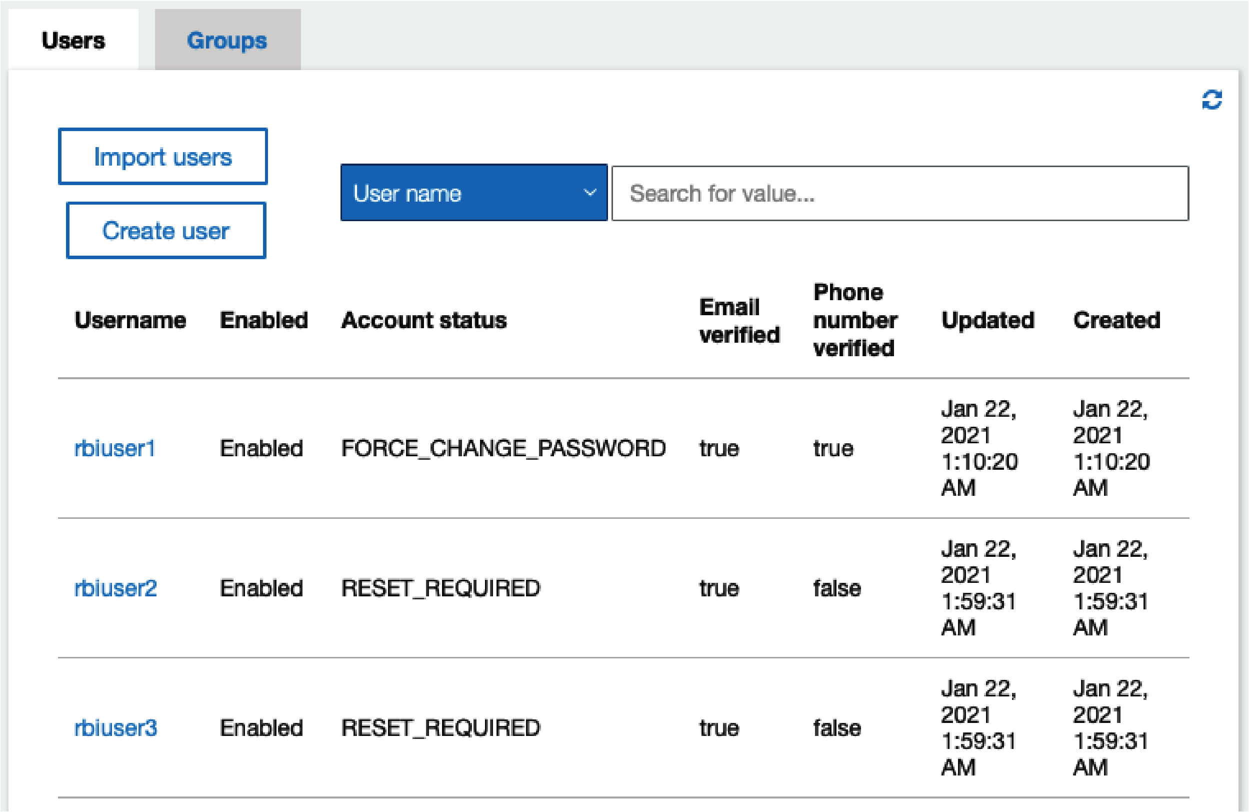


Log events

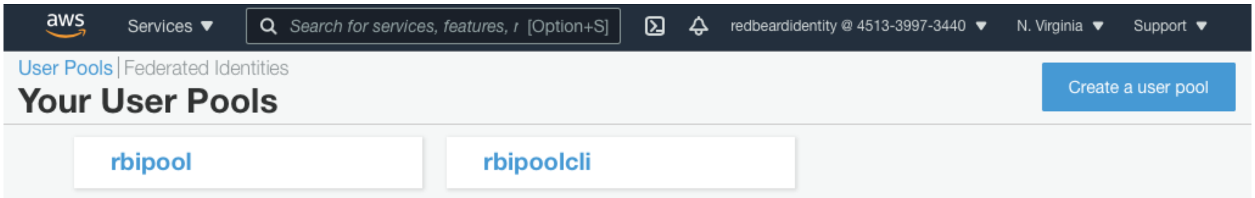
You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns

Timestamp	Message
	No older events at this moment. *Retry*
2021-01-21T20:59:28.795-05:00	Cognito User Pools Import - Test Log
2021-01-21T20:59:31.400-05:00	Cognito User Pools Import - Test Log
2021-01-21T20:59:31.616-05:00	[SUCCEEDED] Line Number 2 - The import succeeded.
2021-01-21T20:59:31.616-05:00	[SUCCEEDED] Line Number 3 - The import succeeded.
2021-01-21T20:59:31.616-05:00	[FAILED] Line Number 4 - The User Record contains an empty use…
2021-01-21T20:59:31.616-05:00	[FAILED] Line Number 5 - The User Record contains an empty use…
2021-01-21T20:59:31.616-05:00	[FAILED] Line Number 6 - The User Record contains an empty use…
2021-01-21T20:59:31.616-05:00	[FAILED] Line Number 7 - The User Record contains an empty use…
2021-01-21T20:59:31.616-05:00	[FAILED] Line Number 8 - The User Record contains an empty use…

```
[FAILED] Line Number 4 - The User Record contains an empty user_name.
```



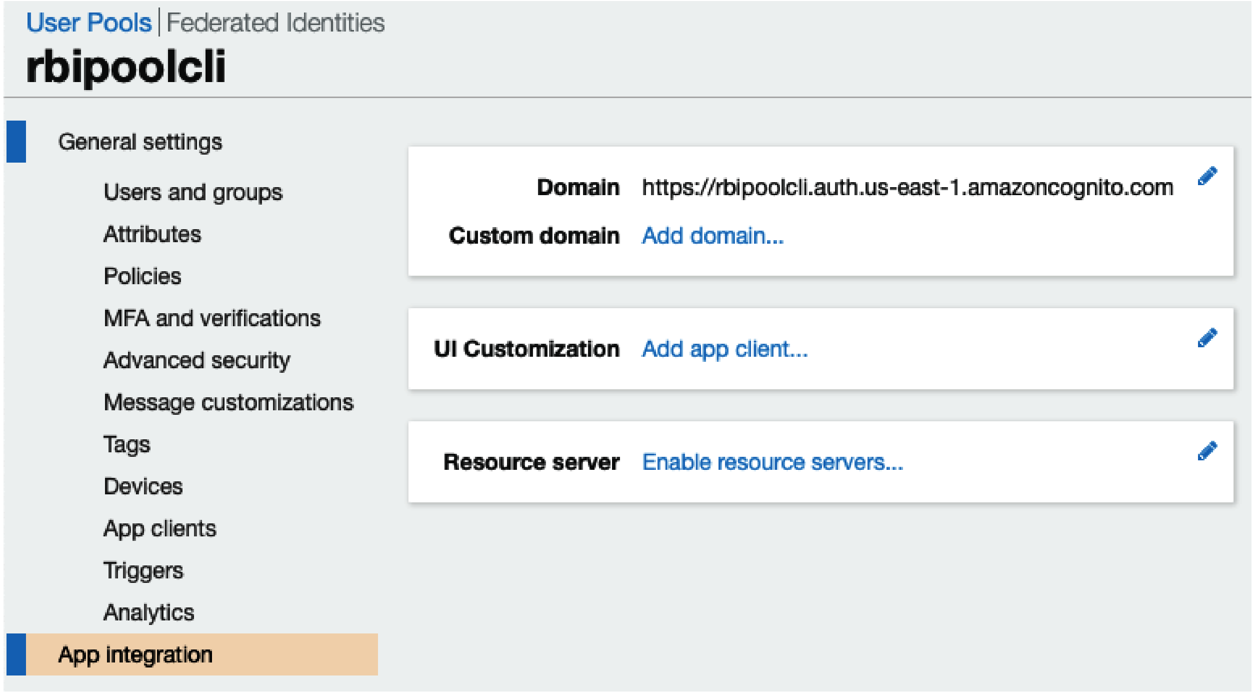
Username	Enabled	Account status	Email verified	Phone number verified	Updated	Created
rbiuser1	Enabled	FORCE_CHANGE_PASSWORD	true	true	Jan 22, 2021 1:10:20 AM	Jan 22, 2021 1:10:20 AM
rbiuser2	Enabled	RESET_REQUIRED	true	false	Jan 22, 2021 1:59:31 AM	Jan 22, 2021 1:59:31 AM
rbiuser3	Enabled	RESET_REQUIRED	true	false	Jan 22, 2021 1:59:31 AM	Jan 22, 2021 1:59:31 AM


aws
Services ▼
Search for services, features, r [Option+S]
redbeardidentity @ 4513-3997-3440 ▼
N. Virginia ▼
Support ▼
User Pools | Federated Identities
Create a user pool

Your User Pools

rbipool

rbipoolcli

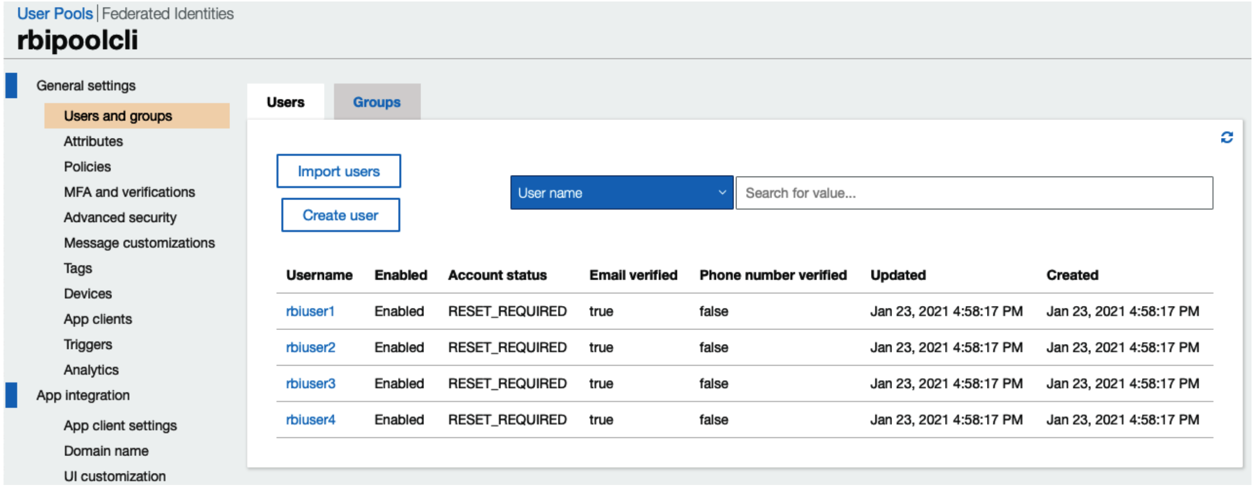


Domain https://rbipoolcli.auth.us-east-1.amazoncognito.com

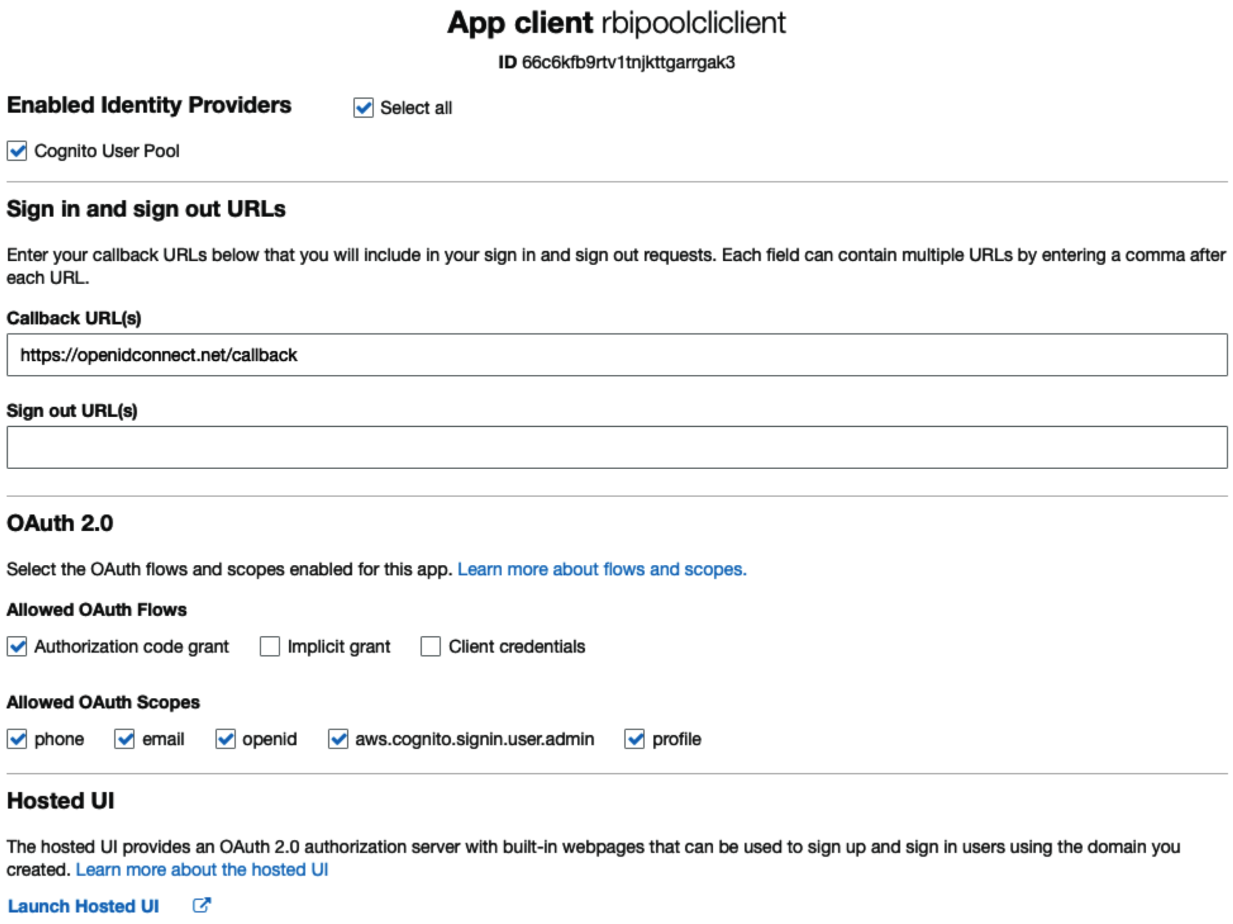
Custom domain Add domain...

UI Customization Add app client...

Resource server Enable resource servers...



Username	Enabled	Account status	Email verified	Phone number verified	Updated	Created
rbiuser1	Enabled	RESET_REQUIRED	true	false	Jan 23, 2021 4:58:17 PM	Jan 23, 2021 4:58:17 PM
rbiuser2	Enabled	RESET_REQUIRED	true	false	Jan 23, 2021 4:58:17 PM	Jan 23, 2021 4:58:17 PM
rbiuser3	Enabled	RESET_REQUIRED	true	false	Jan 23, 2021 4:58:17 PM	Jan 23, 2021 4:58:17 PM
rbiuser4	Enabled	RESET_REQUIRED	true	false	Jan 23, 2021 4:58:17 PM	Jan 23, 2021 4:58:17 PM



App client rbipoolcliclient

ID 66c6kfb9rtv1tnjkttgarrgak3

Enabled Identity Providers ☑ Select all

☑ Cognito User Pool

Sign in and sign out URLs

Enter your callback URLs below that you will include in your sign in and sign out requests. Each field can contain multiple URLs by entering a comma after each URL.

Callback URL(s)

https://openidconnect.net/callback

Sign out URL(s)

OAuth 2.0

Select the OAuth flows and scopes enabled for this app. Learn more about flows and scopes.

Allowed OAuth Flows

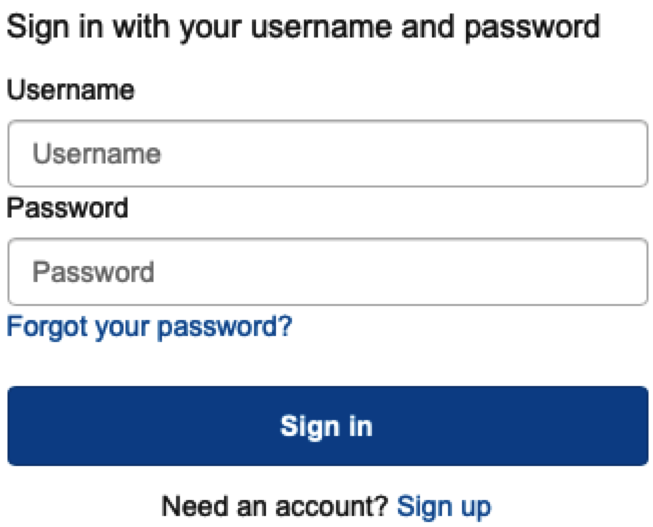
☑ Authorization code grant □ Implicit grant □ Client credentials

Allowed OAuth Scopes

☑ phone ☑ email ☑ openid ☑ aws.cognito.signin.user.admin ☑ profile

Hosted UI

The hosted UI provides an OAuth 2.0 authorization server with built-in webpages that can be used to sign up and sign in users using the domain you created. Learn more about the hosted UI



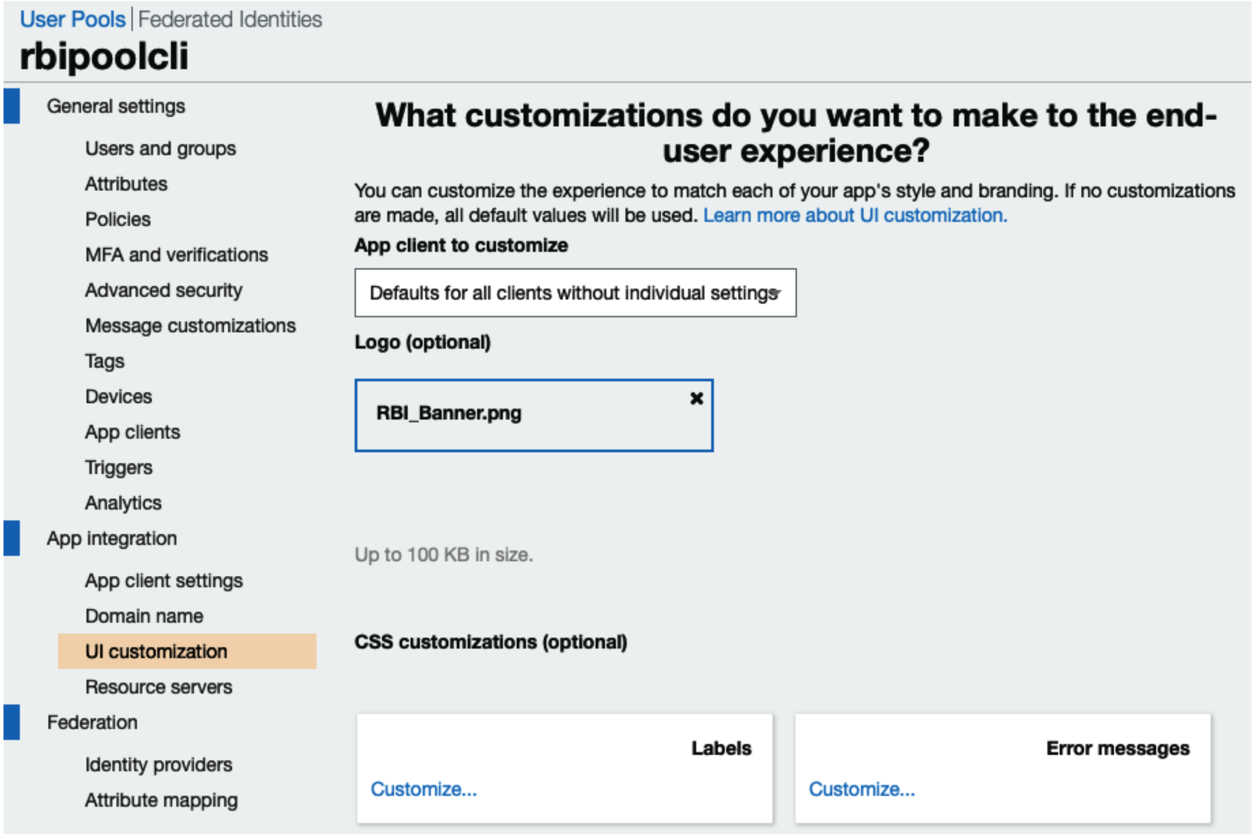
Sign in with your username and password

Username

Username

Password

Password



User Pools | Federated Identities

rbipoolcli

What customizations do you want to make to the end-user experience?

You can customize the experience to match each of your app's style and branding. If no customizations are made, all default values will be used. Learn more about UI customization.

App client to customize

Defaults for all clients without individual settings

Logo (optional)

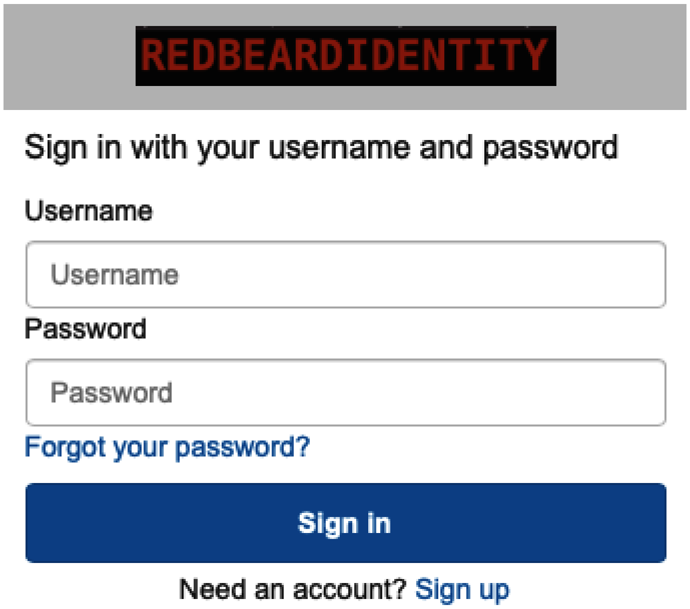
RBI_Banner.png ✖

Up to 100 KB in size.

CSS customizations (optional)

Labels Customize...

Error messages Customize...



Sign in with your username and password

Username

Username

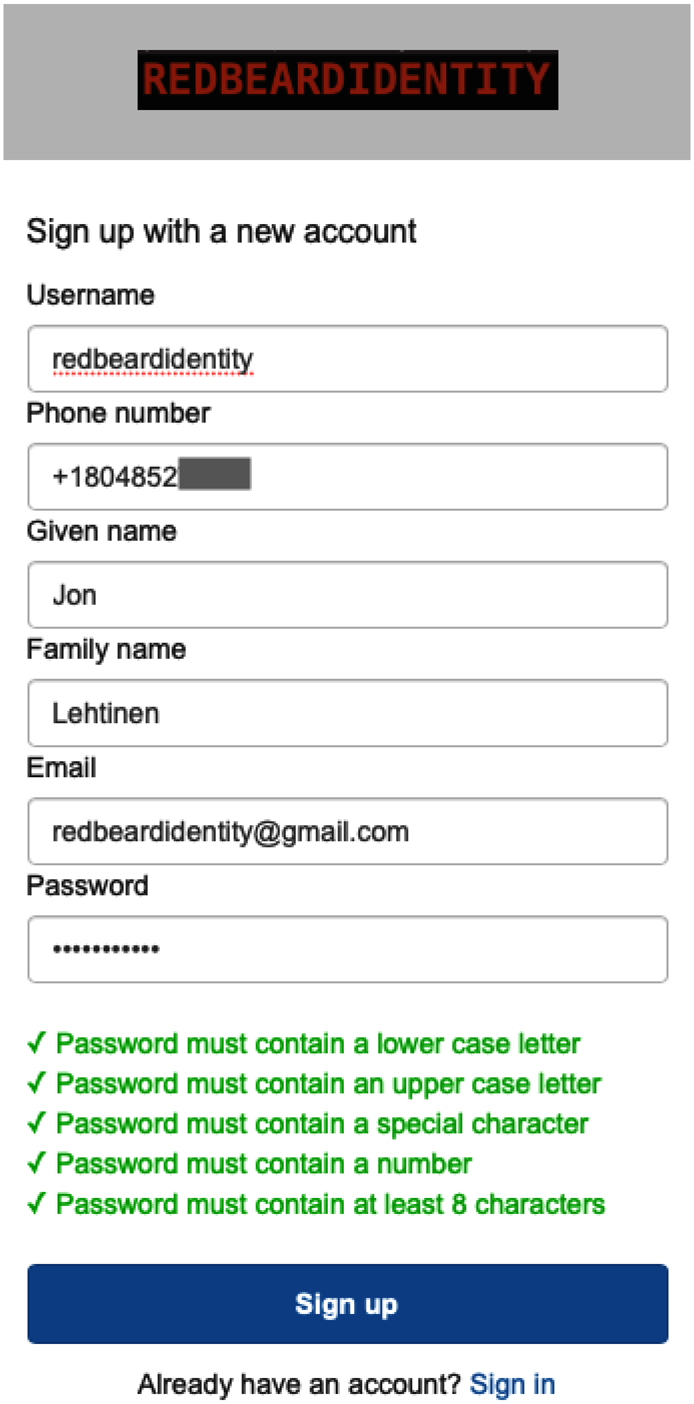
Password

Password

Forgot your password?

Sign in

Need an account? Sign up



REDBEARDIDENTITY

Sign up with a new account

Username

redbeardidentity

Phone number

+1804852[redacted]

Given name

Jon

Family name

Lehtinen

Email

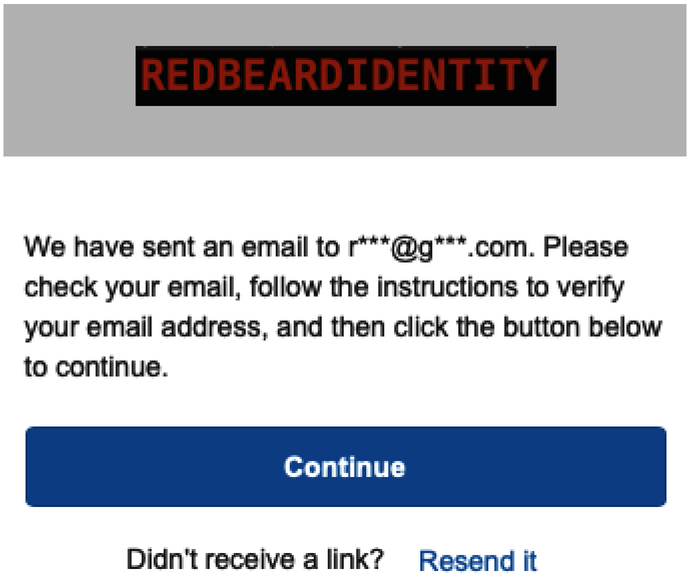
redbeardidentity@gmail.com

Password

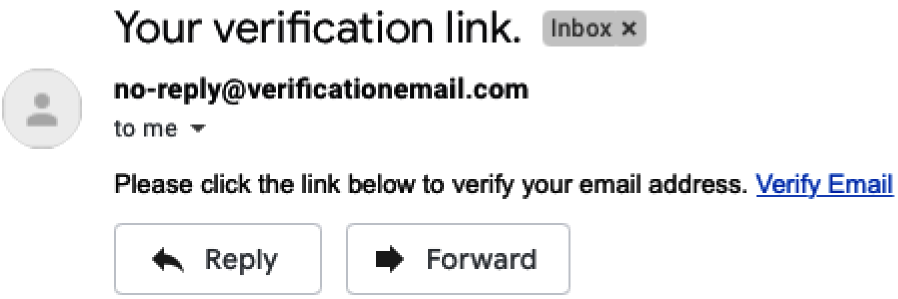
••••••••••••

✓ Password must contain a lower case letter
✓ Password must contain an upper case letter
✓ Password must contain a special character
✓ Password must contain a number
✓ Password must contain at least 8 characters

Already have an account? Sign in



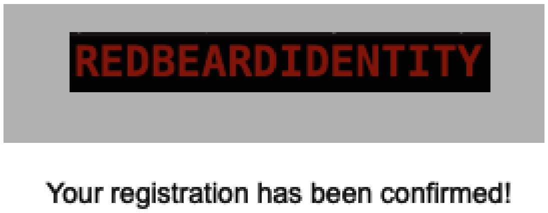
We have sent an email to r***@g***.com. Please check your email, follow the instructions to verify your email address, and then click the button below to continue.


Your verification link.

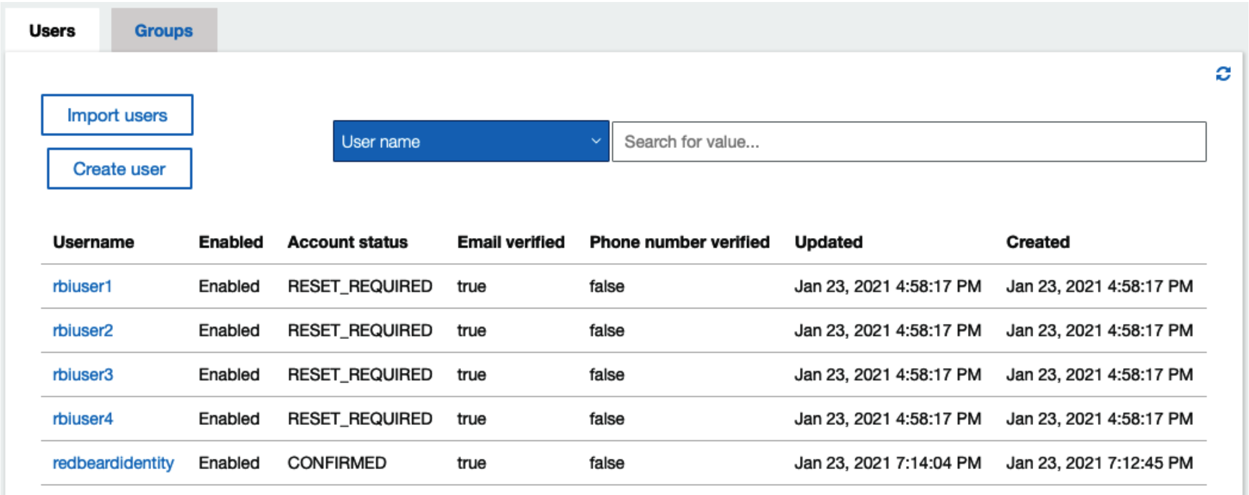
no-reply@verificationemail.com

to me

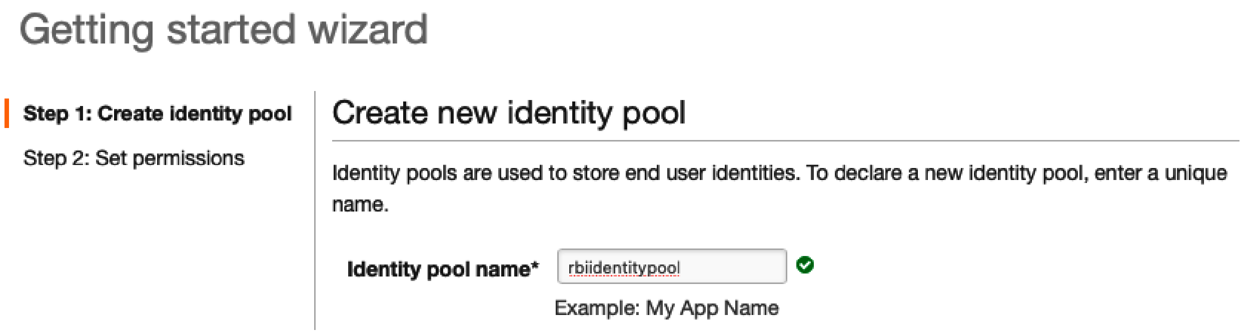
Please click the link below to verify your email address. Verify Email



Your registration has been confirmed!



Username	Enabled	Account status	Email verified	Phone number verified	Updated	Created
rbiuser1	Enabled	RESET_REQUIRED	true	false	Jan 23, 2021 4:58:17 PM	Jan 23, 2021 4:58:17 PM
rbiuser2	Enabled	RESET_REQUIRED	true	false	Jan 23, 2021 4:58:17 PM	Jan 23, 2021 4:58:17 PM
rbiuser3	Enabled	RESET_REQUIRED	true	false	Jan 23, 2021 4:58:17 PM	Jan 23, 2021 4:58:17 PM
rbiuser4	Enabled	RESET_REQUIRED	true	false	Jan 23, 2021 4:58:17 PM	Jan 23, 2021 4:58:17 PM
redbeardidentity	Enabled	CONFIRMED	true	false	Jan 23, 2021 7:14:04 PM	Jan 23, 2021 7:12:45 PM


Getting started wizard

Step 1: Create identity pool

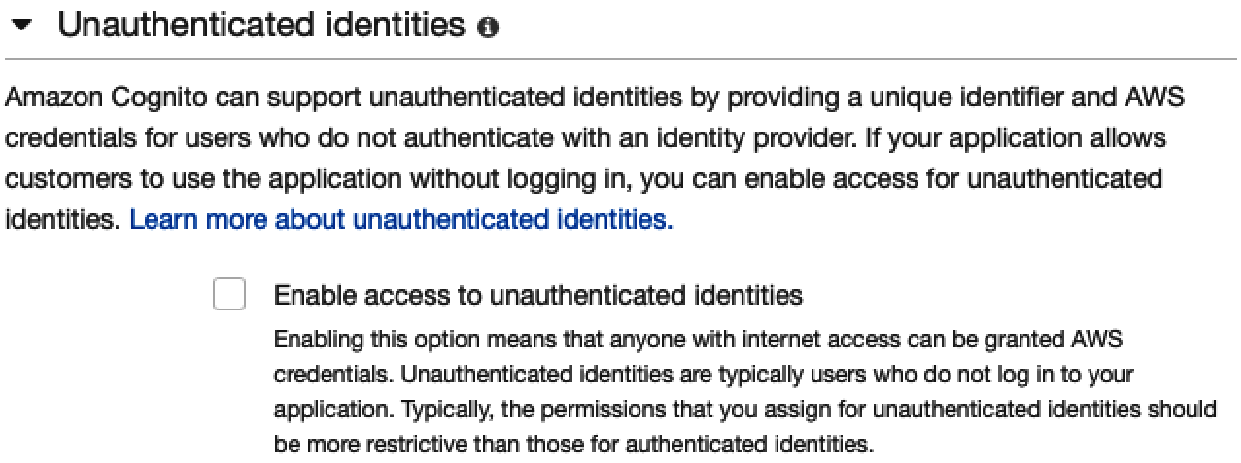
Step 2: Set permissions

Create new identity pool

Identity pools are used to store end user identities. To declare a new identity pool, enter a unique name.

Identity pool name* rbiidentitypool ✓

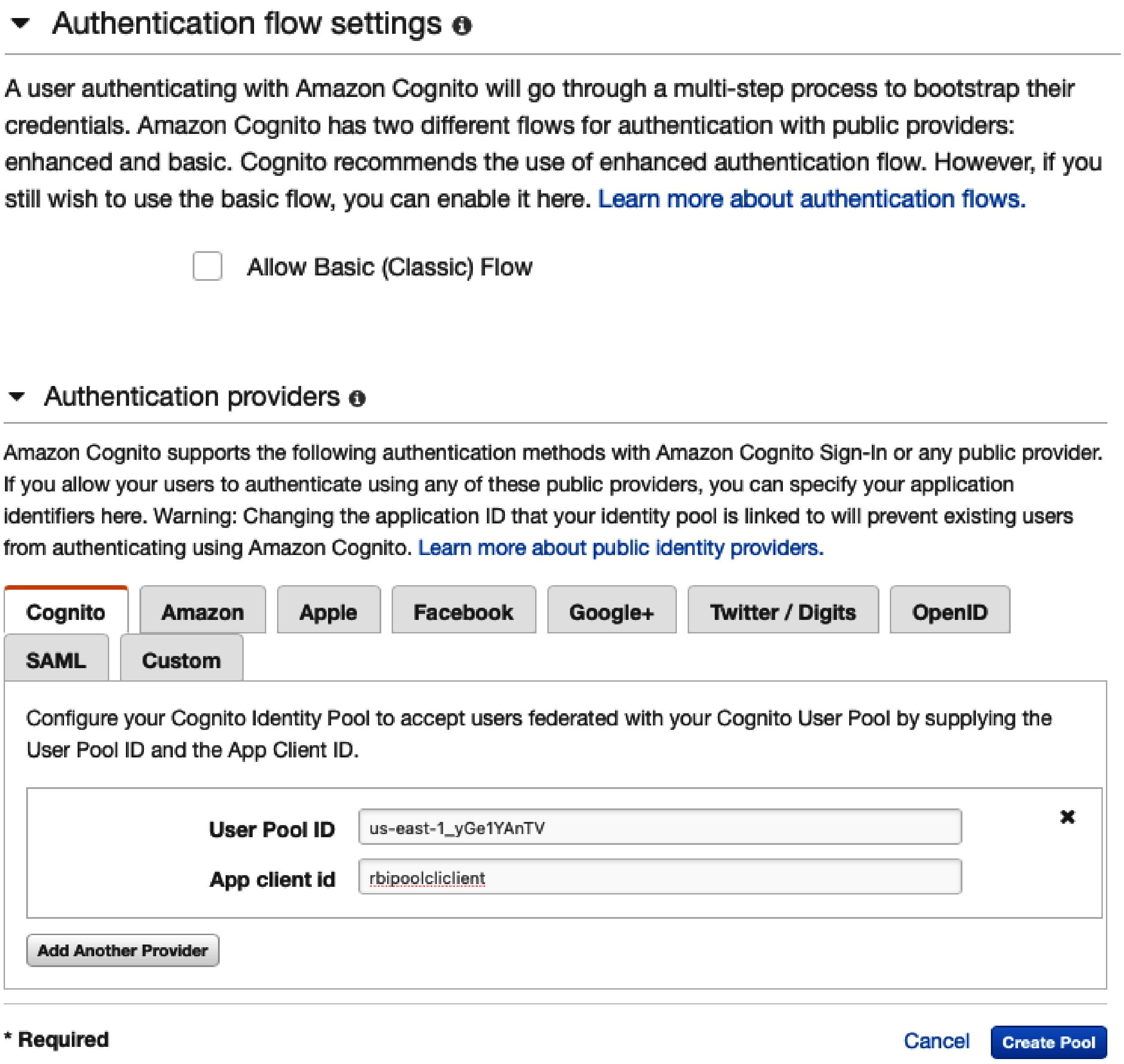
Example: My App Name


Unauthenticated identities

Amazon Cognito can support unauthenticated identities by providing a unique identifier and AWS credentials for users who do not authenticate with an identity provider. If your application allows customers to use the application without logging in, you can enable access for unauthenticated identities. Learn more about unauthenticated identities.

□ Enable access to unauthenticated identities

Enabling this option means that anyone with internet access can be granted AWS credentials. Unauthenticated identities are typically users who do not log in to your application. Typically, the permissions that you assign for unauthenticated identities should be more restrictive than those for authenticated identities.



Authentication flow settings

A user authenticating with Amazon Cognito will go through a multi-step process to bootstrap their credentials. Amazon Cognito has two different flows for authentication with public providers: enhanced and basic. Cognito recommends the use of enhanced authentication flow. However, if you still wish to use the basic flow, you can enable it here. Learn more about authentication flows.

□ Allow Basic (Classic) Flow

Authentication providers

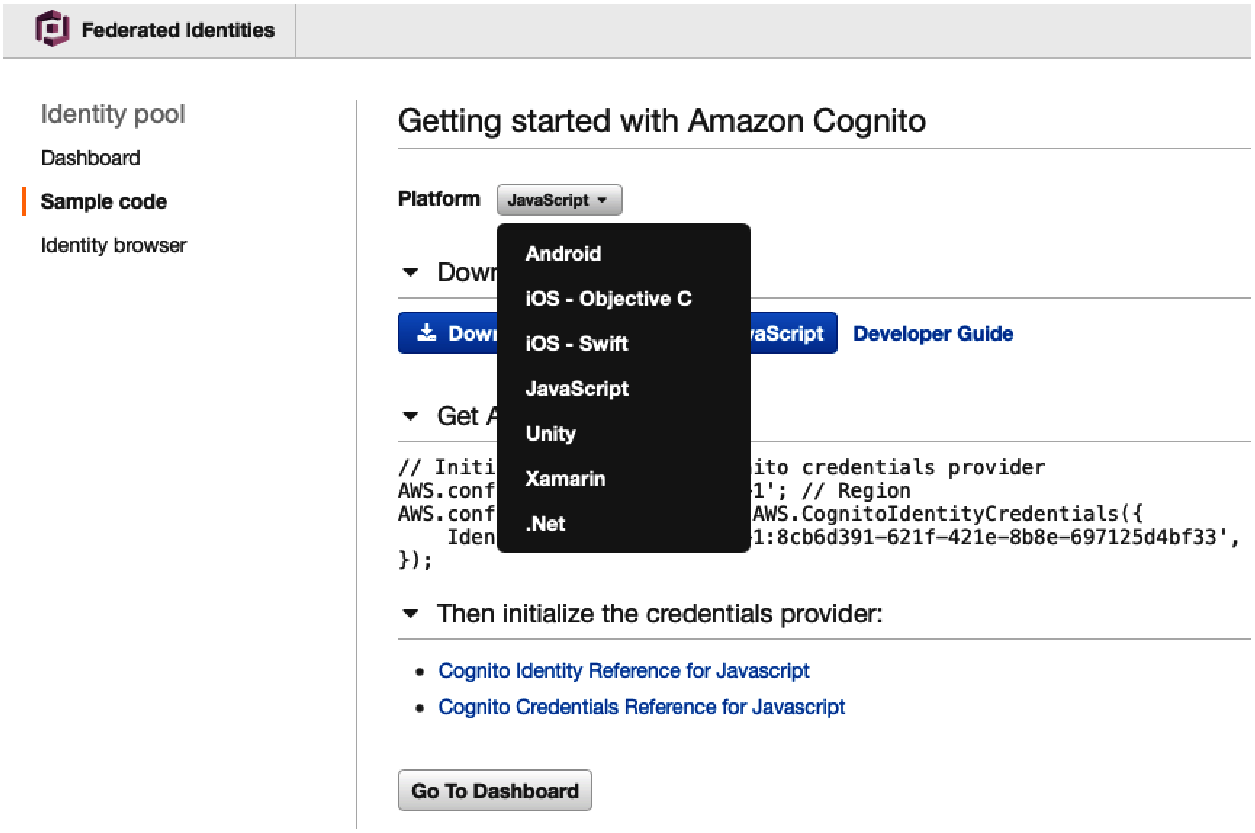
Amazon Cognito supports the following authentication methods with Amazon Cognito Sign-In or any public provider. If you allow your users to authenticate using any of these public providers, you can specify your application identifiers here. Warning: Changing the application ID that your identity pool is linked to will prevent existing users from authenticating using Amazon Cognito. Learn more about public identity providers.

Configure your Cognito Identity Pool to accept users federated with your Cognito User Pool by supplying the User Pool ID and the App Client ID.

User Pool ID us-east-1_yGe1YAnTV

App client id rbipoolcliclient

*** Required**



Getting started with Amazon Cognito

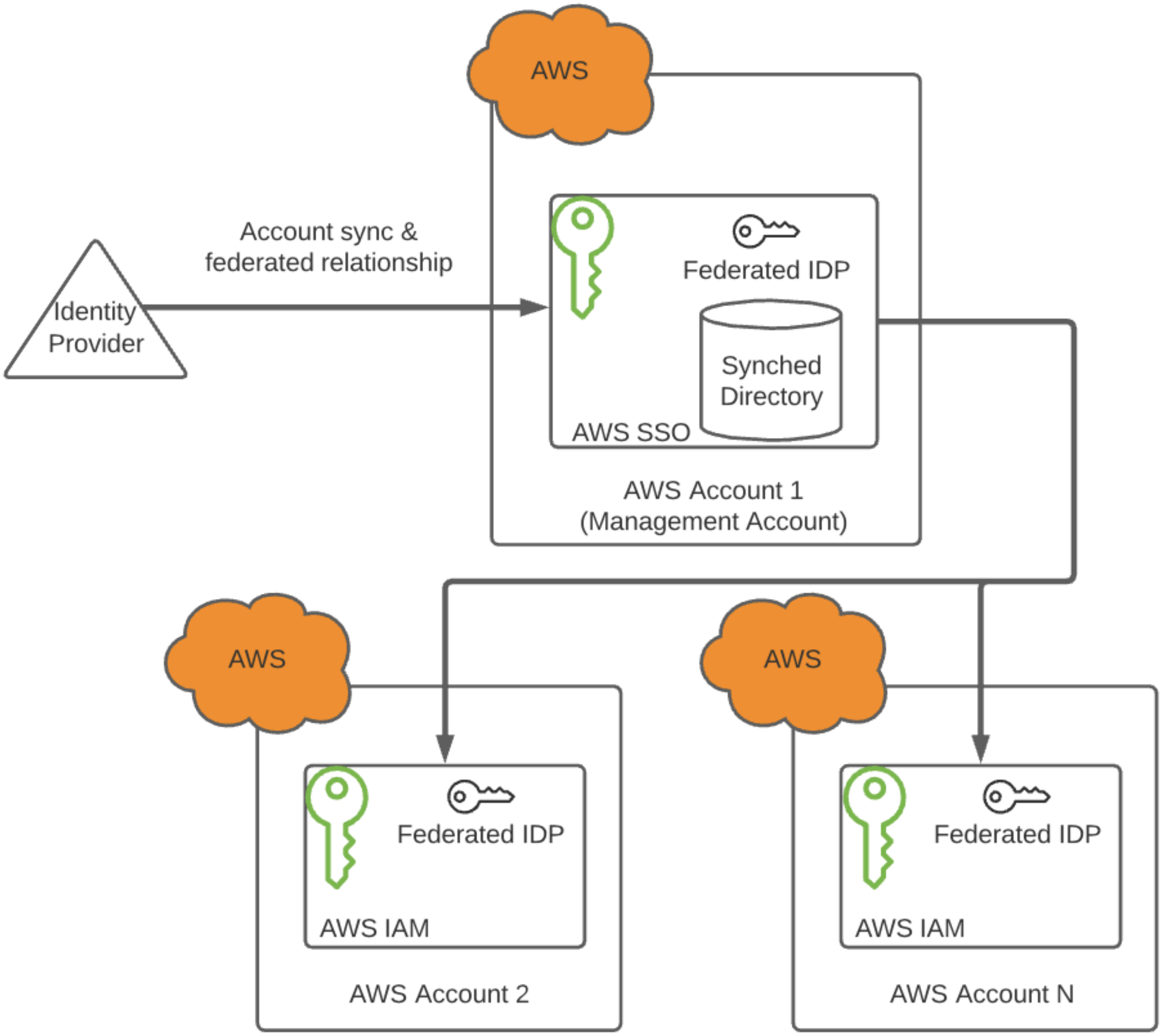
Platform JavaScript

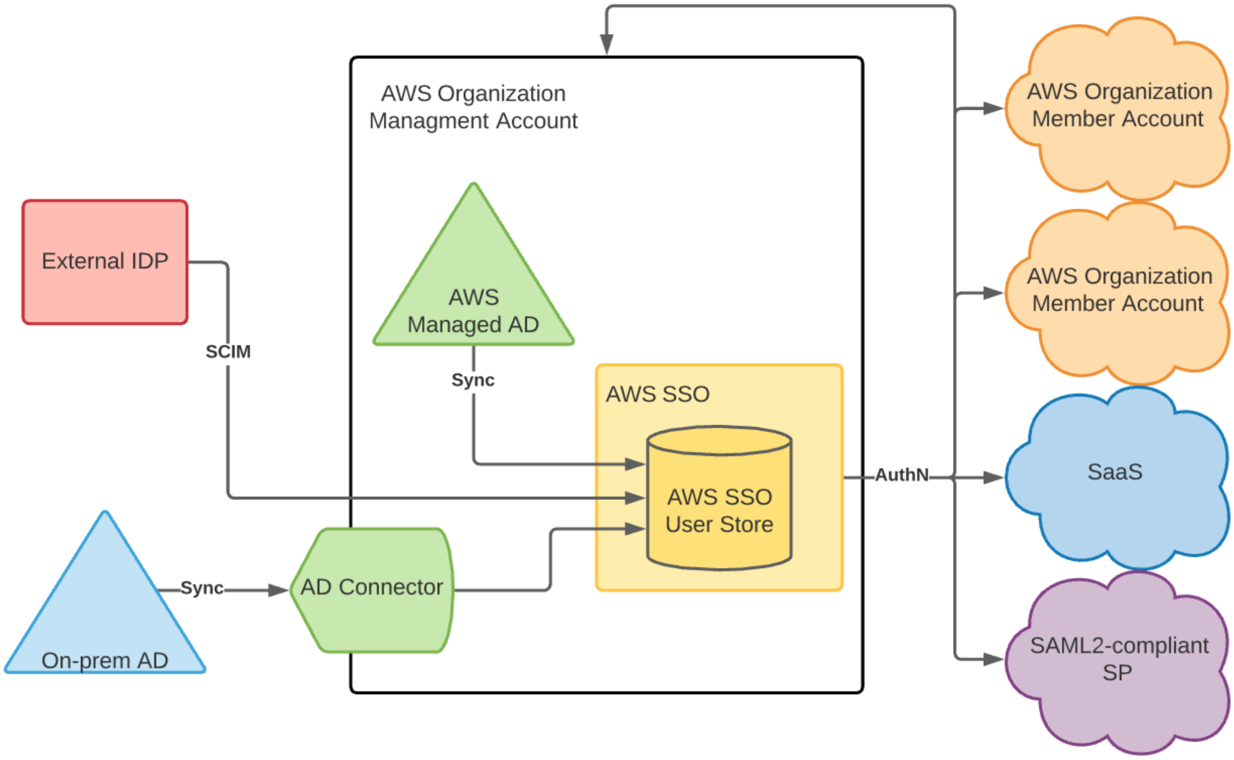
```
// Initi                   ito credentials provider
AWS.conf                   1'; // Region
AWS.conf                   AWS.CognitoIdentityCredentials({
    Iden                   1:8cb6d391-621f-421e-8b8e-697125d4bf33',
});
```

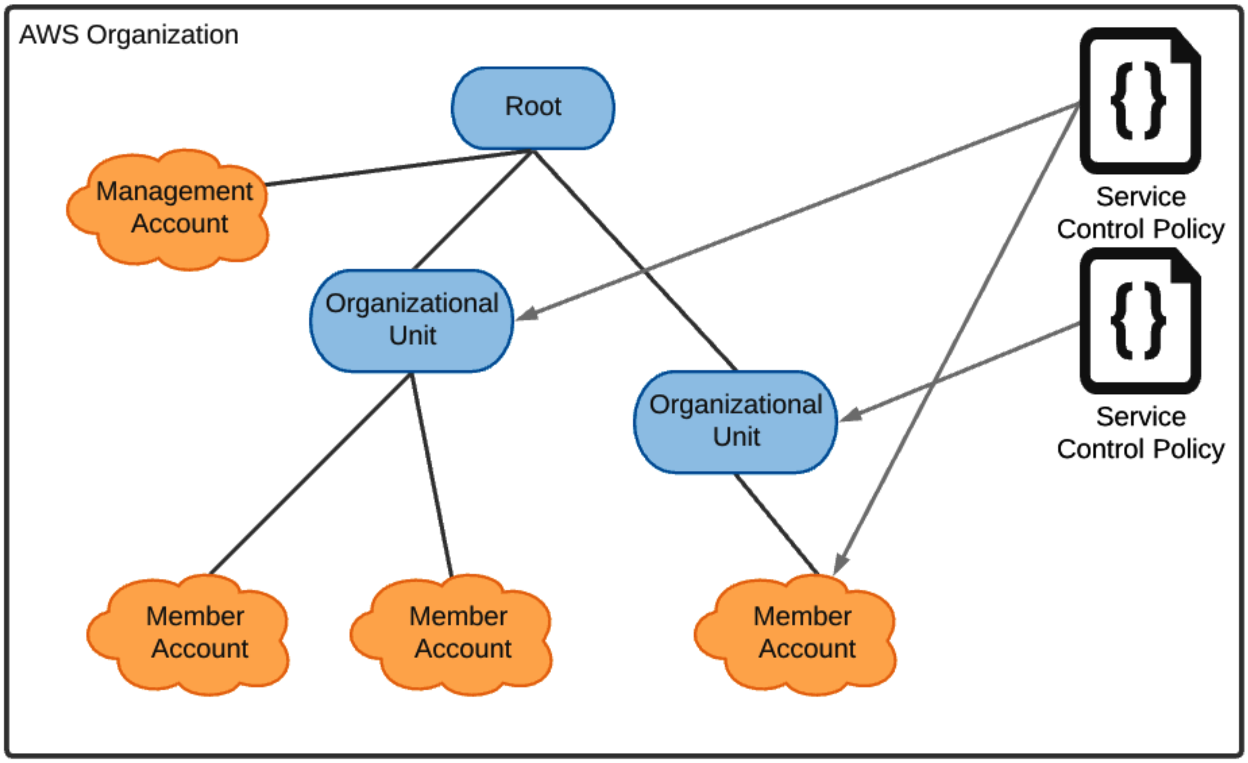
Then initialize the credentials provider:

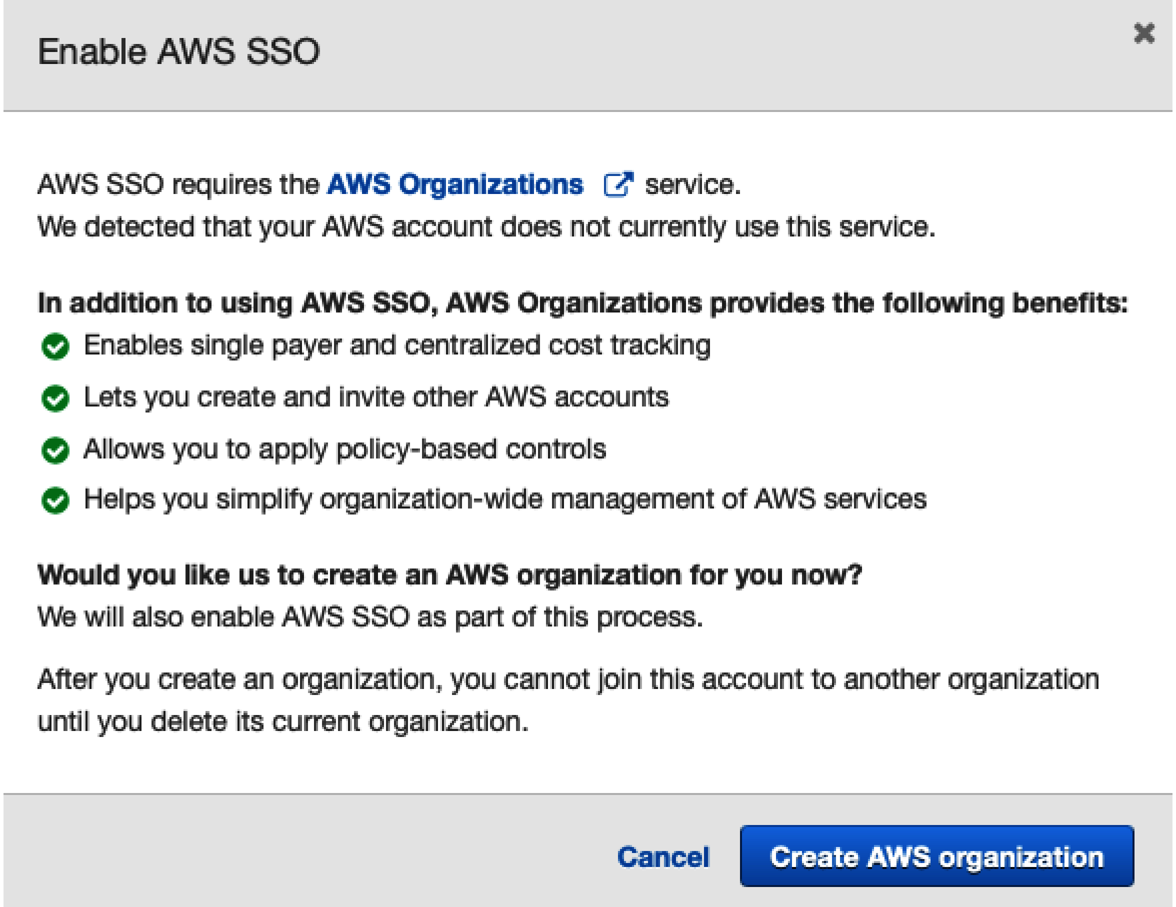
- Cognito Identity Reference for Javascript
- Cognito Credentials Reference for Javascript

Chapter 6: Introduction to AWS Organizations and AWS Single Sign-On




AWS Organization
Managment Account
External IDP
SCIM
AWS
Managed AD
Sync
AWS SSO
AWS SSO
User Store
AuthN
On-prem AD
Sync
AD Connector
AWS Organization
Member Account
AWS Organization
Member Account
SaaS
SAML2-compliant
SP


AWS Organization
Root
Management
Account
Organizational
Unit
Organizational
Unit
Member
Account
Member
Account
Member
Account
Service
Control Policy
Service
Control Policy



Enable AWS SSO

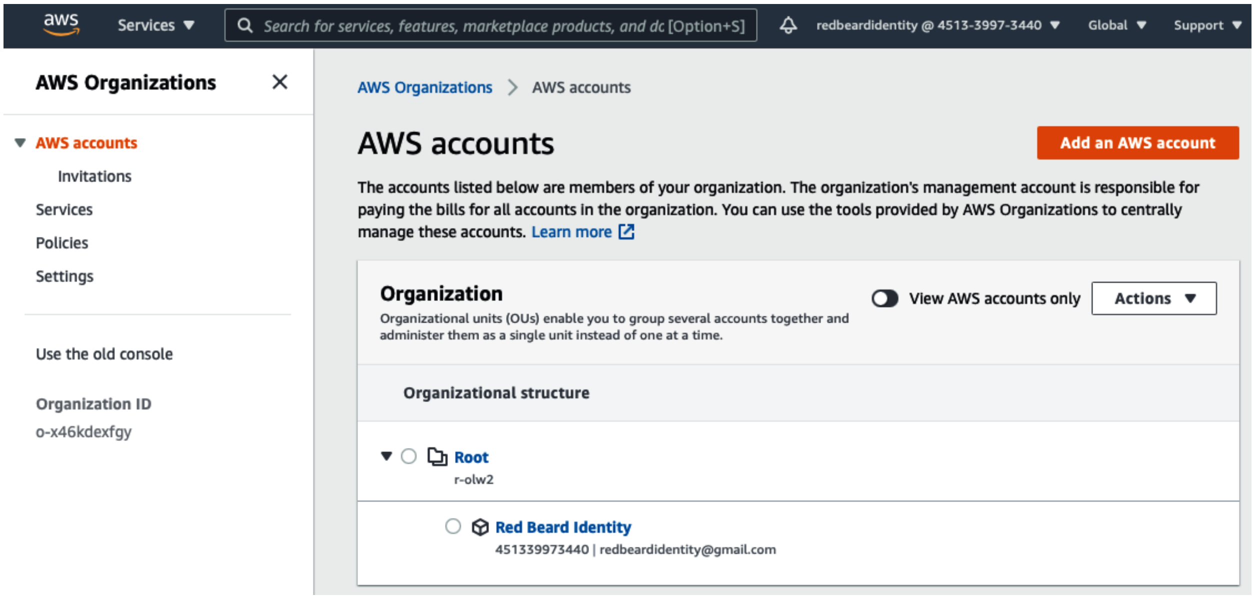
AWS SSO requires the **AWS Organizations** service.
We detected that your AWS account does not currently use this service.

In addition to using AWS SSO, AWS Organizations provides the following benefits:

- ✓ Enables single payer and centralized cost tracking
- ✓ Lets you create and invite other AWS accounts
- ✓ Allows you to apply policy-based controls
- ✓ Helps you simplify organization-wide management of AWS services

Would you like us to create an AWS organization for you now?
We will also enable AWS SSO as part of this process.

After you create an organization, you cannot join this account to another organization until you delete its current organization.



Organization ID
o-x46kdexfgy

AWS accounts

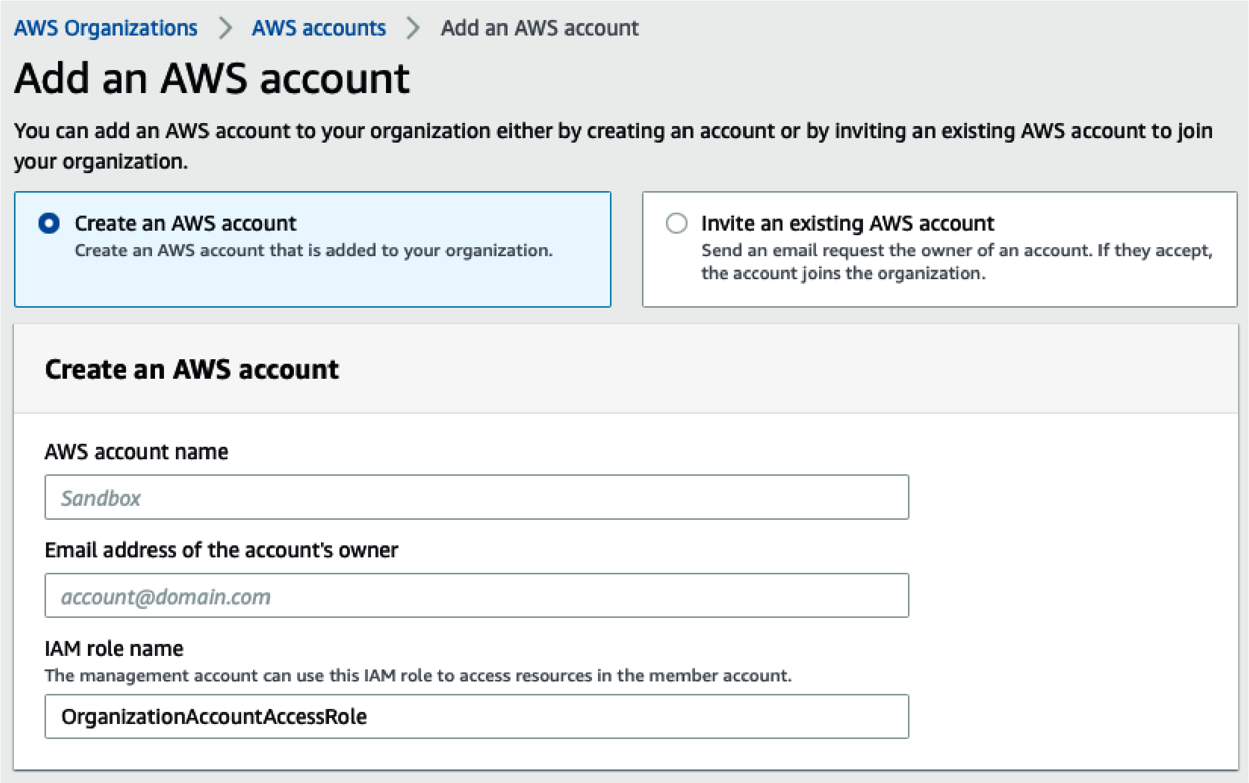
The accounts listed below are members of your organization. The organization's management account is responsible for paying the bills for all accounts in the organization. You can use the tools provided by AWS Organizations to centrally manage these accounts. Learn more

Organization
Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

Organizational structure

Root
r-olw2

Red Beard Identity
451339973440 | redbeardidentity@gmail.com



AWS Organizations > AWS accounts > Add an AWS account

Add an AWS account

You can add an AWS account to your organization either by creating an account or by inviting an existing AWS account to join your organization.

● Create an AWS account
Create an AWS account that is added to your organization.

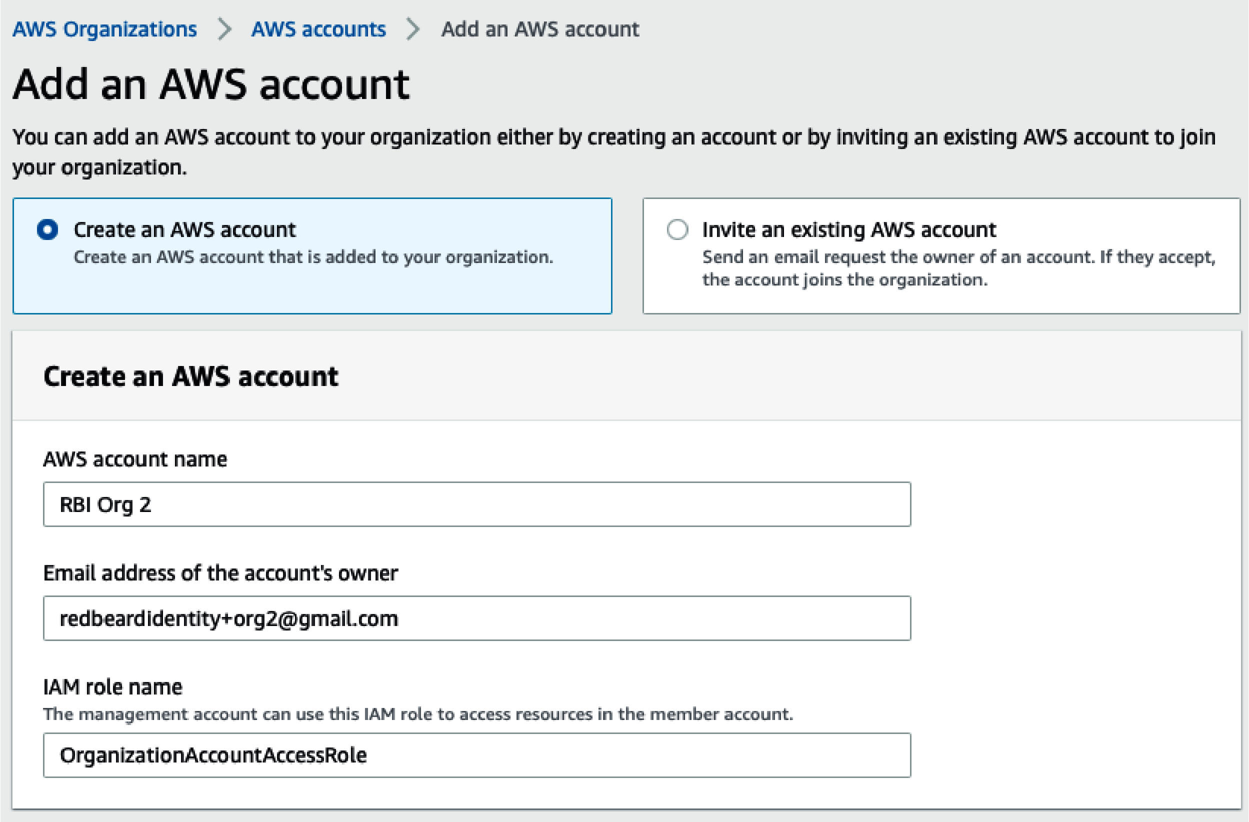
○ Invite an existing AWS account
Send an email request the owner of an account. If they accept, the account joins the organization.

Create an AWS account

AWS account name
Sandbox

Email address of the account's owner
account@domain.com

IAM role name
The management account can use this IAM role to access resources in the member account.
OrganizationAccountAccessRole



AWS Organizations > AWS accounts > Add an AWS account

Add an AWS account

You can add an AWS account to your organization either by creating an account or by inviting an existing AWS account to join your organization.

● Create an AWS account
Create an AWS account that is added to your organization.

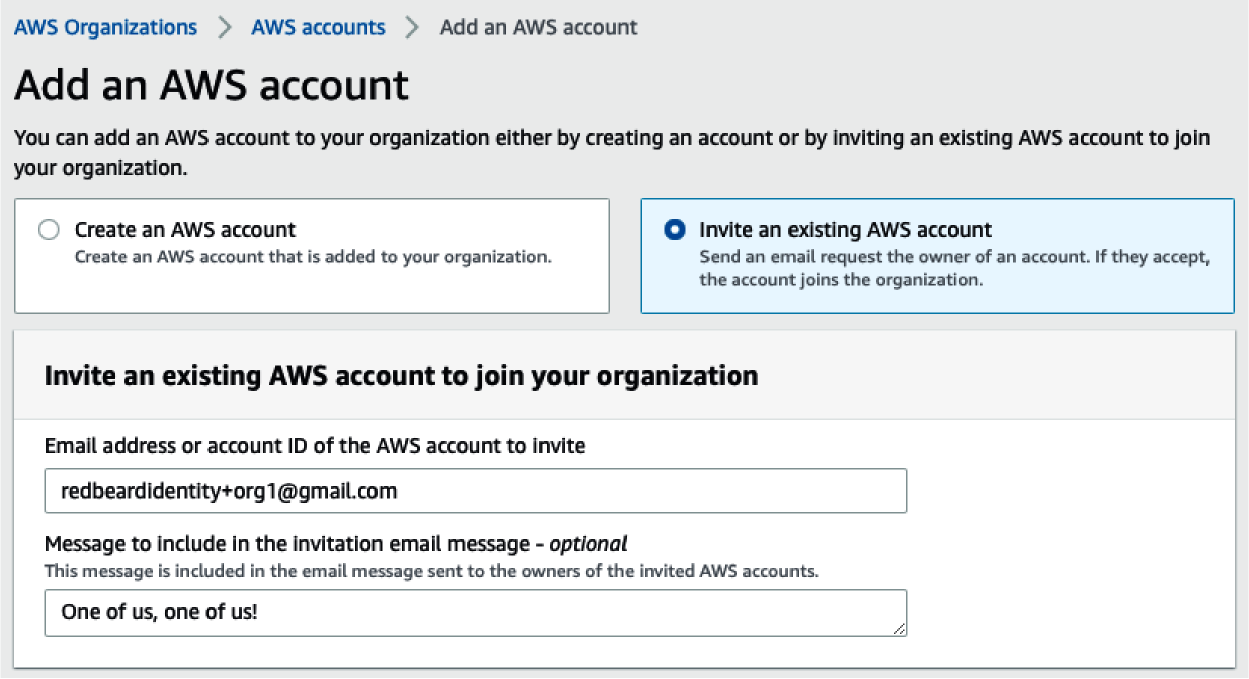
○ Invite an existing AWS account
Send an email request the owner of an account. If they accept, the account joins the organization.

Create an AWS account

AWS account name
RBI Org 2

Email address of the account's owner
redbeardidentity+org2@gmail.com

IAM role name
The management account can use this IAM role to access resources in the member account.
OrganizationAccountAccessRole



Add an AWS account

You can add an AWS account to your organization either by creating an account or by inviting an existing AWS account to join your organization.

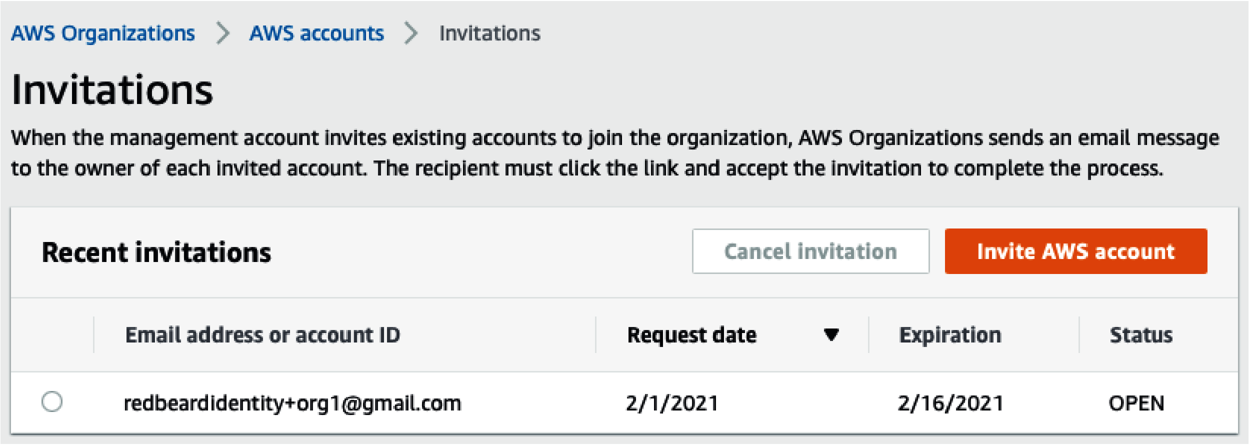
○ Create an AWS account
Create an AWS account that is added to your organization.

● Invite an existing AWS account
Send an email request the owner of an account. If they accept, the account joins the organization.

Invite an existing AWS account to join your organization

Email address or account ID of the AWS account to invite: redbeardidentity+org1@gmail.com

Message to include in the invitation email message - *optional*
This message is included in the email message sent to the owners of the invited AWS accounts.
One of us, one of us!



Invitations

When the management account invites existing accounts to join the organization, AWS Organizations sends an email message to the owner of each invited account. The recipient must click the link and accept the invitation to complete the process.

Recent invitations

	Email address or account ID	Request date ▼	Expiration	Status
○	redbeardidentity+org1@gmail.com	2/1/2021	2/16/2021	OPEN

Hello,

Red Beard Identity (owned by redbeardidentity@gmail.com) would like to add your AWS account (redbeardidentity+org1@gmail.com) to their AWS organization as a member account.

The following notes were provided with this invitation: One of us, one of us!

Organizations allows customers to easily manage multiple AWS accounts. If you accept the invitation, all activity in your AWS account will be billed to the AWS account of Red Beard Identity, and Red Beard Identity will be able to view the AWS usage and charges for your account.

An AWS organization can have one of the following feature sets: all features or consolidated billing only. Most organizations are set up with access to all features, which includes administrative and access controls within the organization. In some cases, an organization may choose to only enable consolidated billing features and later decide to enable all features. Management accounts for consolidated billing organizations may direct AWS to enable all features in the organization with at least 14 days' notice to you that may be sent by email. You can view which feature set the organization has enabled through the console link below. For more information about Organizations features, see the Organizations documentation.

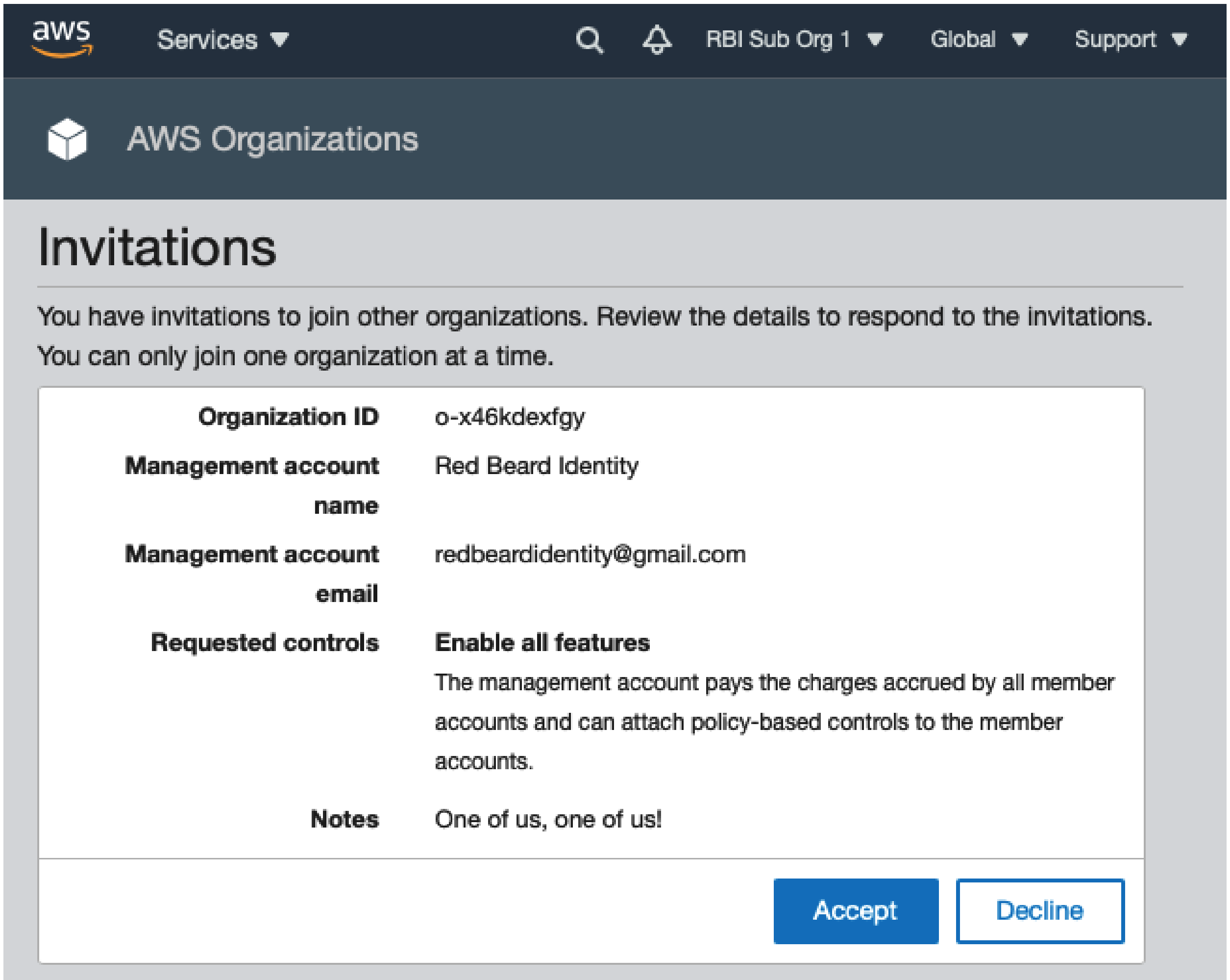
To view the invitation, including what features have been enabled, click this link:

https://console.aws.amazon.com/organizations/home#/invites

To learn more about AWS Organizations, see What is AWS Organizations?

Thank you for using Amazon Web Services.

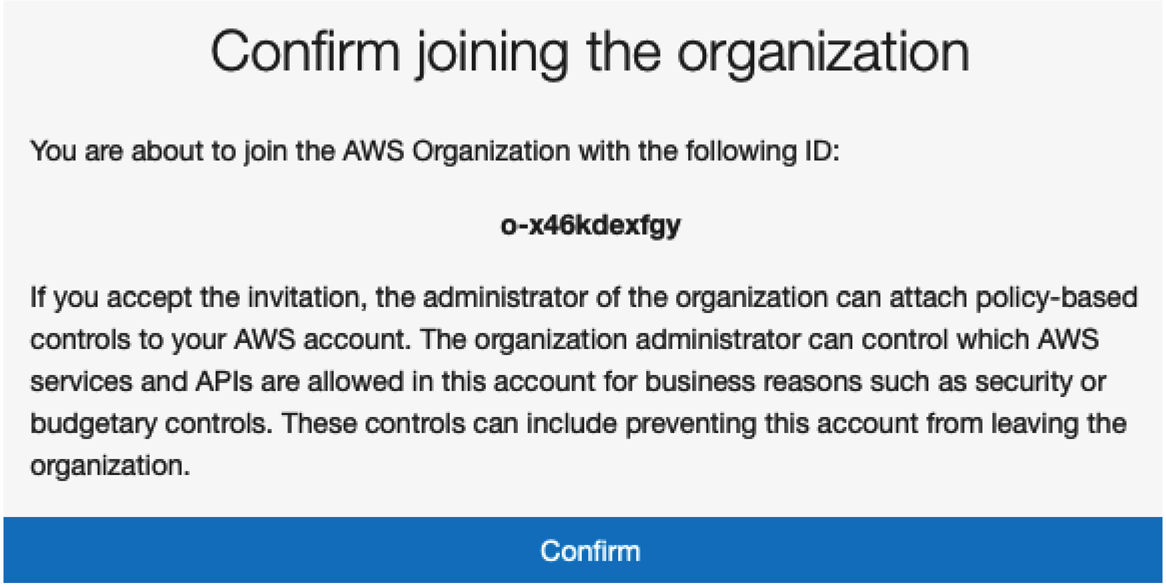
Sincerely,
Amazon Web Services



Invitations

You have invitations to join other organizations. Review the details to respond to the invitations. You can only join one organization at a time.

Organization ID	o-x46kdexfgy
Management account name	Red Beard Identity
Management account email	redbeardidentity@gmail.com
Requested controls	**Enable all features** The management account pays the charges accrued by all member accounts and can attach policy-based controls to the member accounts.
Notes	One of us, one of us!

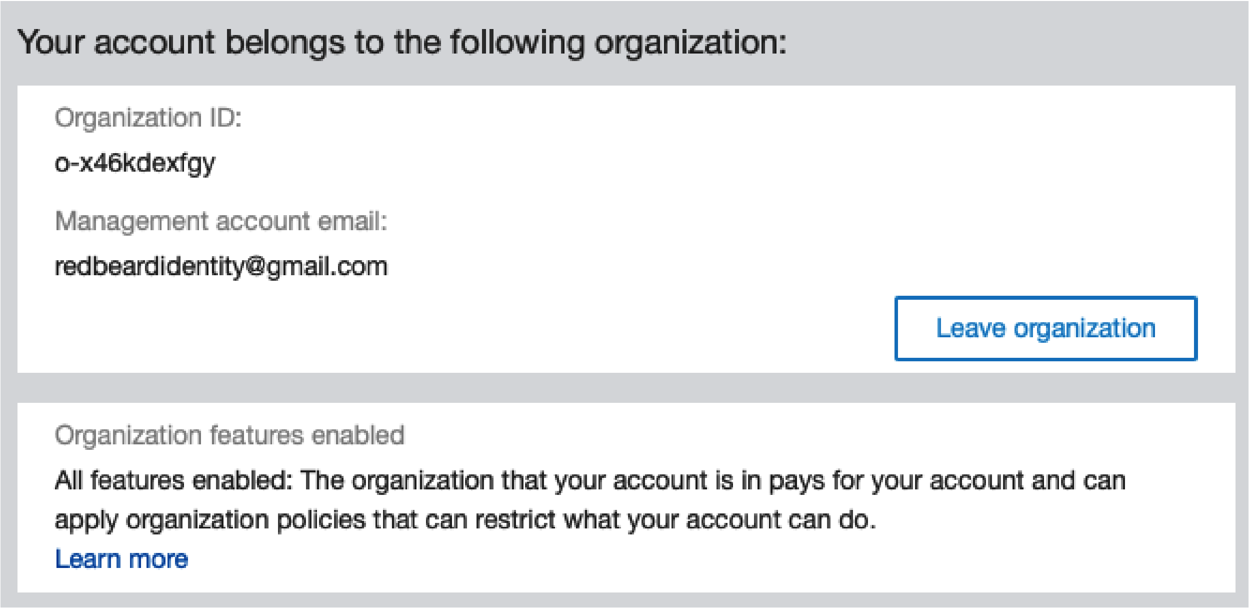


Confirm joining the organization

You are about to join the AWS Organization with the following ID:

o-x46kdexfgy

If you accept the invitation, the administrator of the organization can attach policy-based controls to your AWS account. The organization administrator can control which AWS services and APIs are allowed in this account for business reasons such as security or budgetary controls. These controls can include preventing this account from leaving the organization.



Your account belongs to the following organization:

Organization ID:

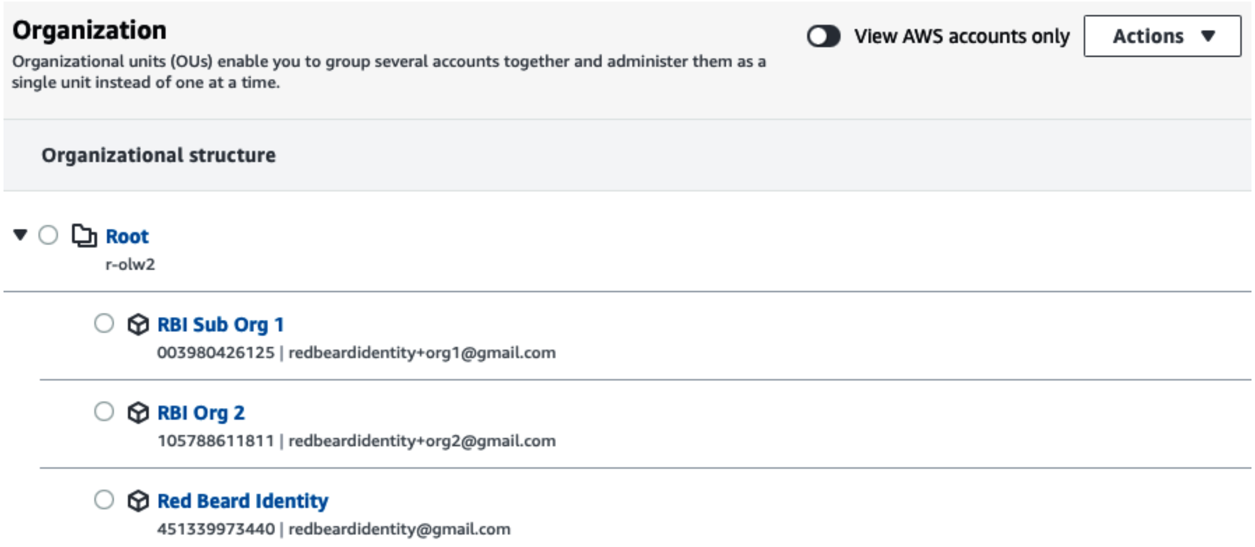
o-x46kdexfgy

Management account email:

redbeardidentity@gmail.com

Organization features enabled

All features enabled: The organization that your account is in pays for your account and can apply organization policies that can restrict what your account can do.



Organization

Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

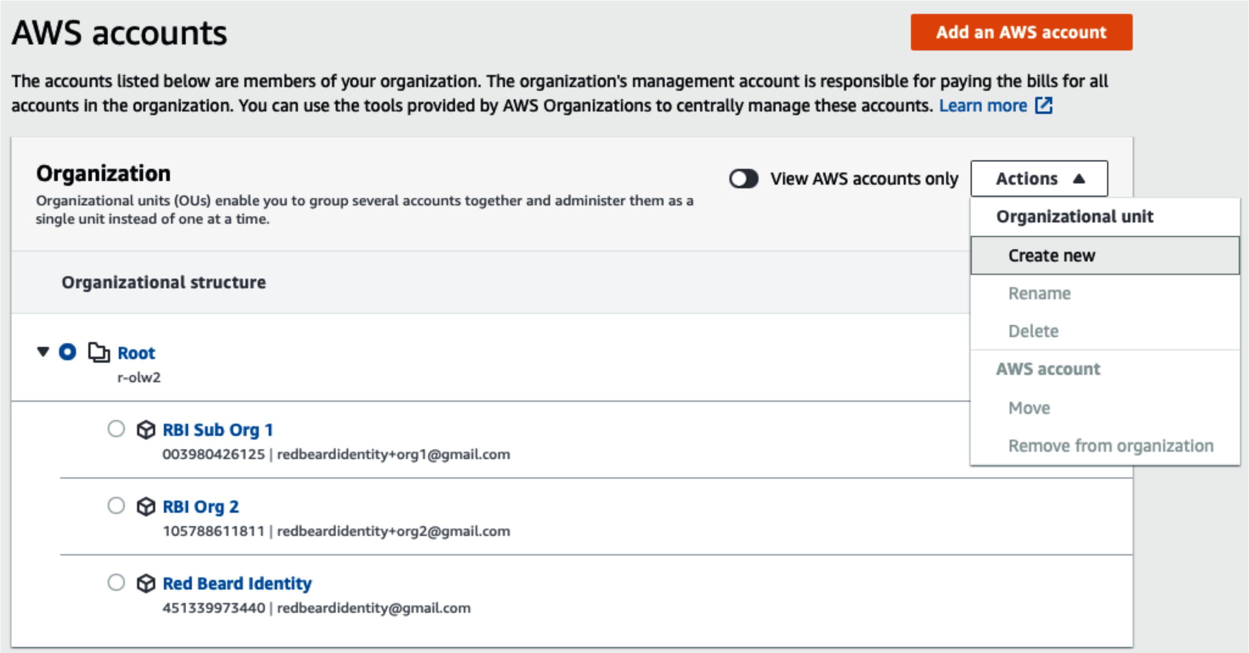
Organizational structure

▼ ○ Root
r-olw2

○ RBI Sub Org 1
003980426125 | redbeardidentity+org1@gmail.com

○ RBI Org 2
105788611811 | redbeardidentity+org2@gmail.com

○ Red Beard Identity
451339973440 | redbeardidentity@gmail.com



AWS accounts

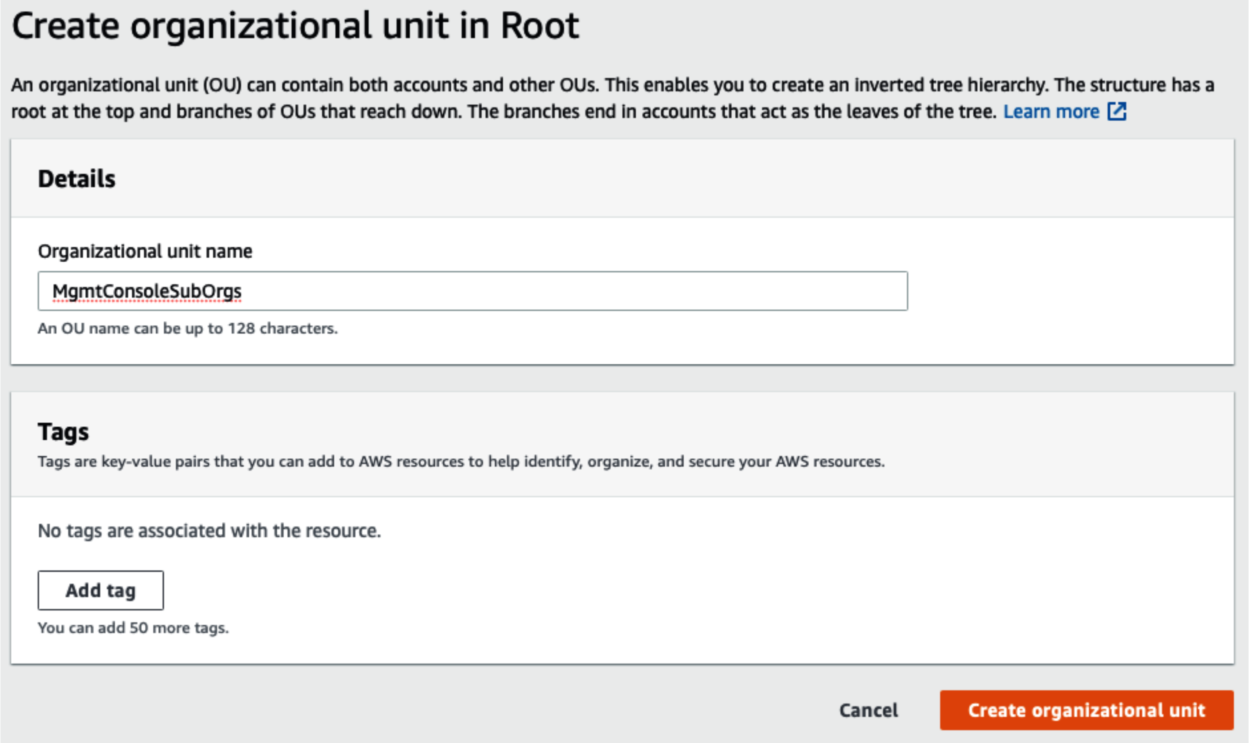
The accounts listed below are members of your organization. The organization's management account is responsible for paying the bills for all accounts in the organization. You can use the tools provided by AWS Organizations to centrally manage these accounts. Learn more

Organization

Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

Organizational structure

- ● Root
  r-olw2
  - ○ RBI Sub Org 1
    003980426125 | redbeardidentity+org1@gmail.com
  - ○ RBI Org 2
    105788611811 | redbeardidentity+org2@gmail.com
  - ○ Red Beard Identity
    451339973440 | redbeardidentity@gmail.com



Create organizational unit in Root

An organizational unit (OU) can contain both accounts and other OUs. This enables you to create an inverted tree hierarchy. The structure has a root at the top and branches of OUs that reach down. The branches end in accounts that act as the leaves of the tree. Learn more

Details

Organizational unit name: MgmtConsoleSubOrgs

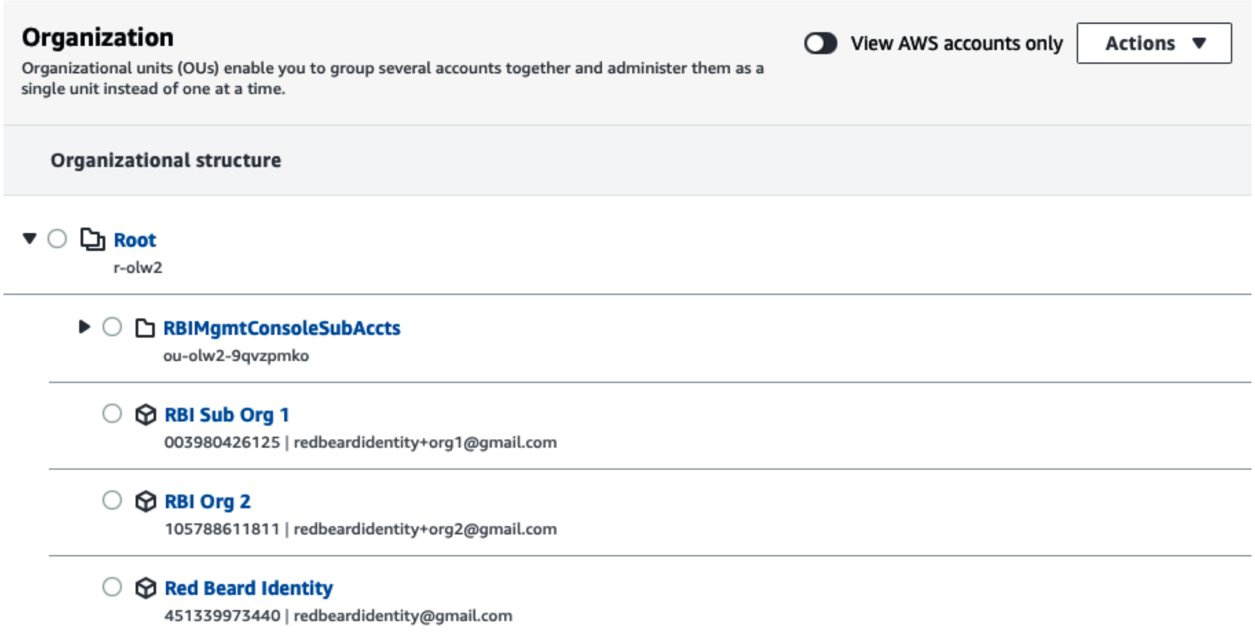
An OU name can be up to 128 characters.

Tags

Tags are key-value pairs that you can add to AWS resources to help identify, organize, and secure your AWS resources.

No tags are associated with the resource.

You can add 50 more tags.

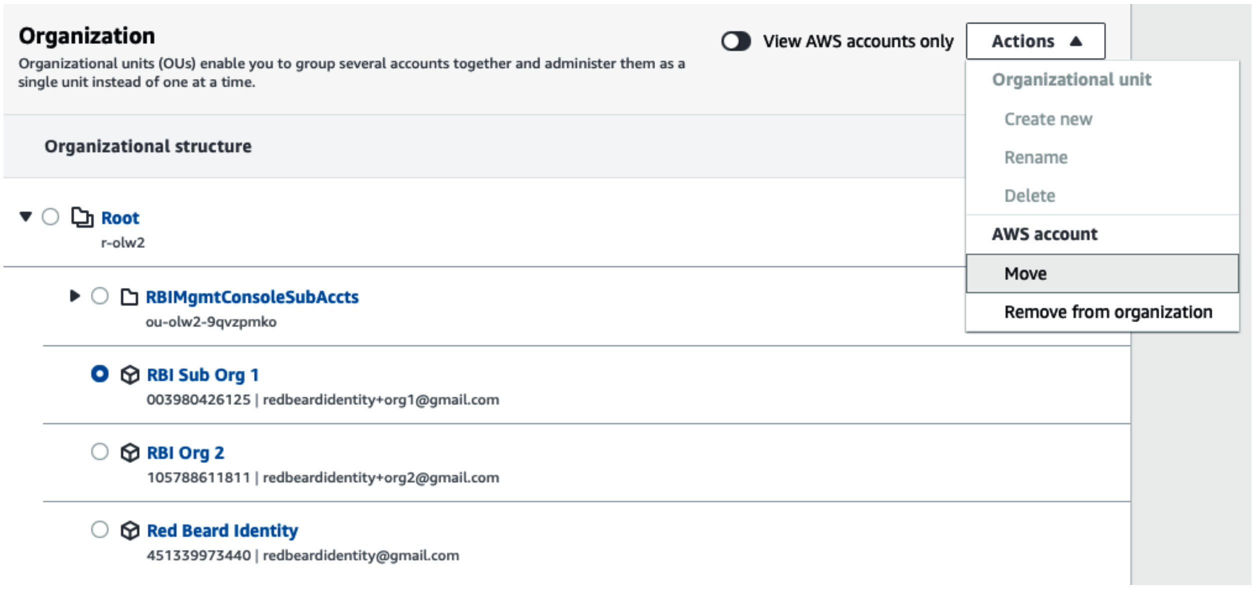


Organization

Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

Organizational structure

- ▼ ○ Root
  r-olw2
  - ▶ ○ RBIMgmtConsoleSubAccts
    ou-olw2-9qvzpmko
  - ○ RBI Sub Org 1
    003980426125 | redbeardidentity+org1@gmail.com
  - ○ RBI Org 2
    105788611811 | redbeardidentity+org2@gmail.com
  - ○ Red Beard Identity
    451339973440 | redbeardidentity@gmail.com

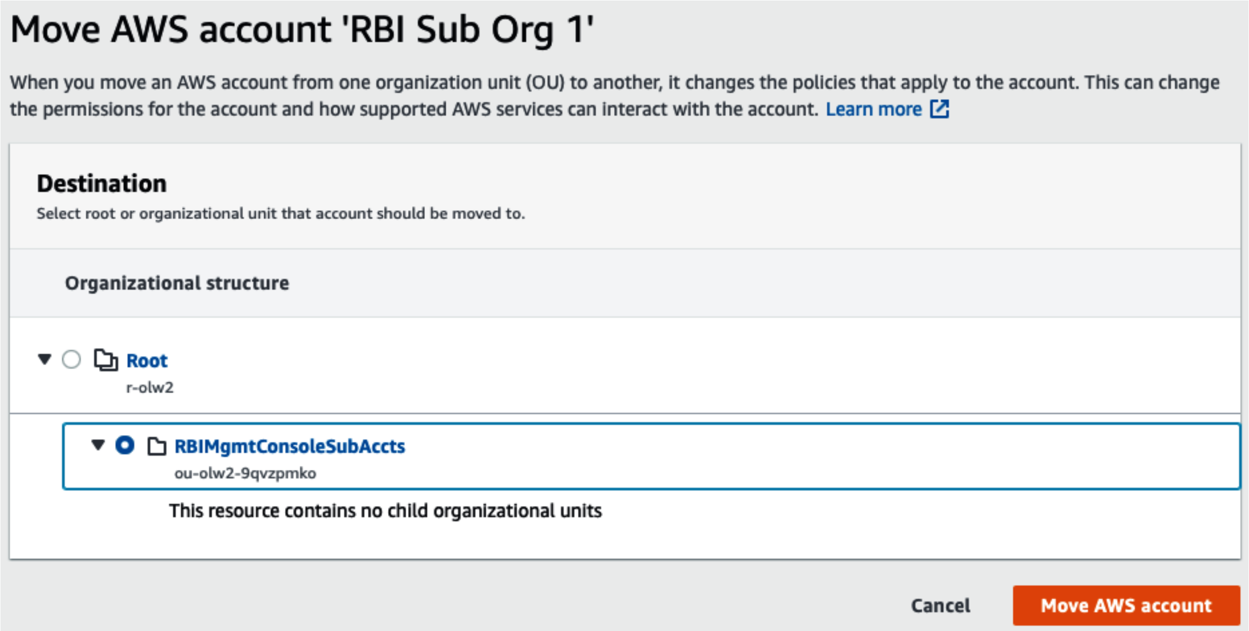


Organization

Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

Organizational structure

- ▼ ○ Root
  r-olw2
  - ▶ ○ RBIMgmtConsoleSubAccts
    ou-olw2-9qvzpmko
  - ● RBI Sub Org 1
    003980426125 | redbeardidentity+org1@gmail.com
  - ○ RBI Org 2
    105788611811 | redbeardidentity+org2@gmail.com
  - ○ Red Beard Identity
    451339973440 | redbeardidentity@gmail.com



Move AWS account 'RBI Sub Org 1'

When you move an AWS account from one organization unit (OU) to another, it changes the policies that apply to the account. This can change the permissions for the account and how supported AWS services can interact with the account. Learn more

Destination

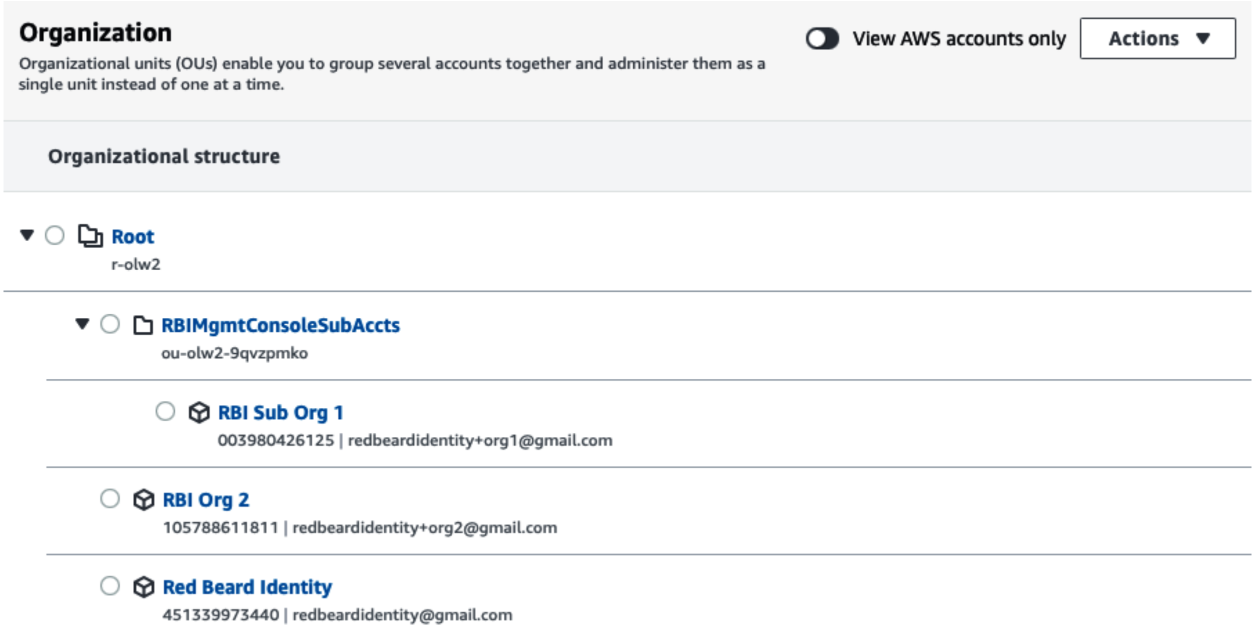
Select root or organizational unit that account should be moved to.

Organizational structure

▼ ○ Root
r-olw2

▼ ● RBIMgmtConsoleSubAccts
ou-olw2-9qvzpmko

This resource contains no child organizational units



Organization

Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

Organizational structure

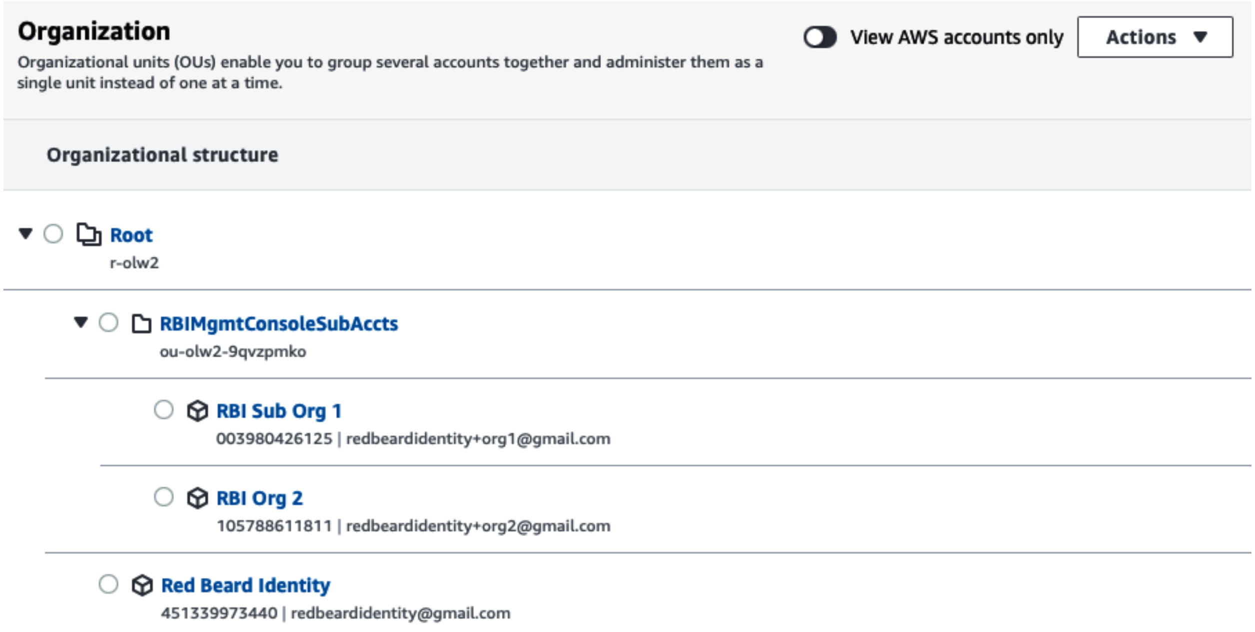
▼ ○ Root
r-olw2

▼ ○ RBIMgmtConsoleSubAccts
ou-olw2-9qvzpmko

○ RBI Sub Org 1
003980426125 | redbeardidentity+org1@gmail.com

○ RBI Org 2
105788611811 | redbeardidentity+org2@gmail.com

○ Red Beard Identity
451339973440 | redbeardidentity@gmail.com



Organization

Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

Organizational structure

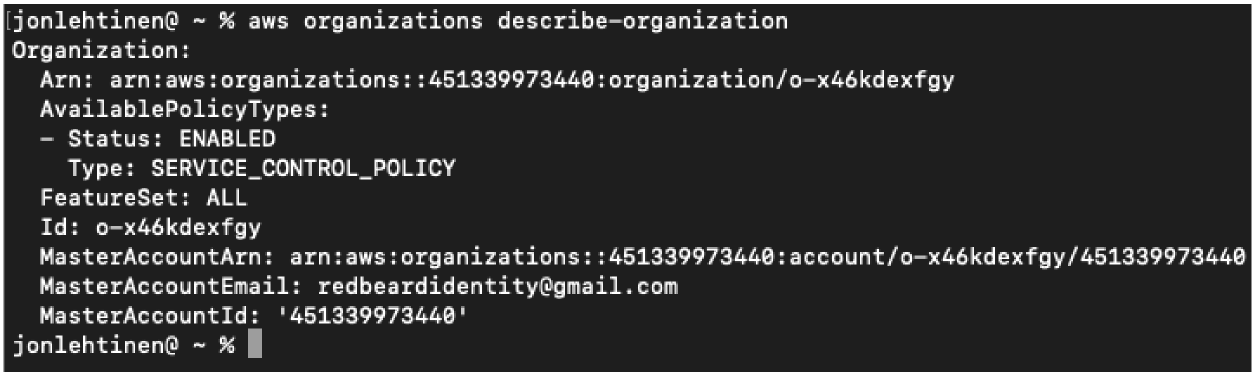
▼ ○ **Root**
r-olw2

▼ ○ **RBIMgmtConsoleSubAccts**
ou-olw2-9qvzpmko

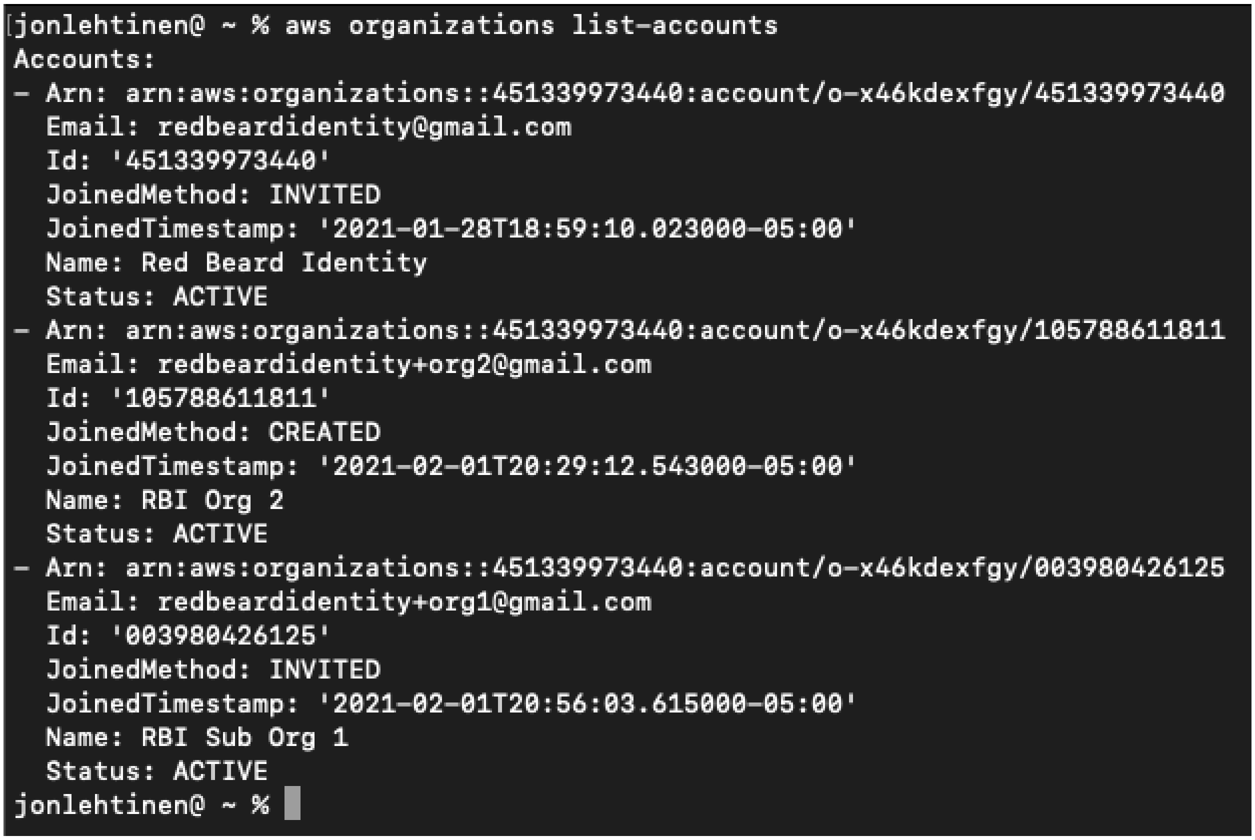
○ **RBI Sub Org 1**
003980426125 | redbeardidentity+org1@gmail.com

○ **RBI Org 2**
105788611811 | redbeardidentity+org2@gmail.com

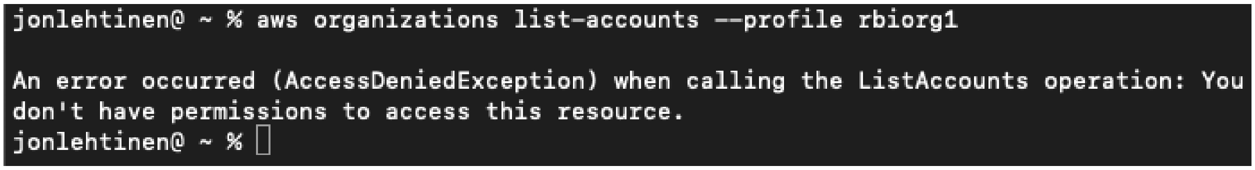
○ **Red Beard Identity**
451339973440 | redbeardidentity@gmail.com



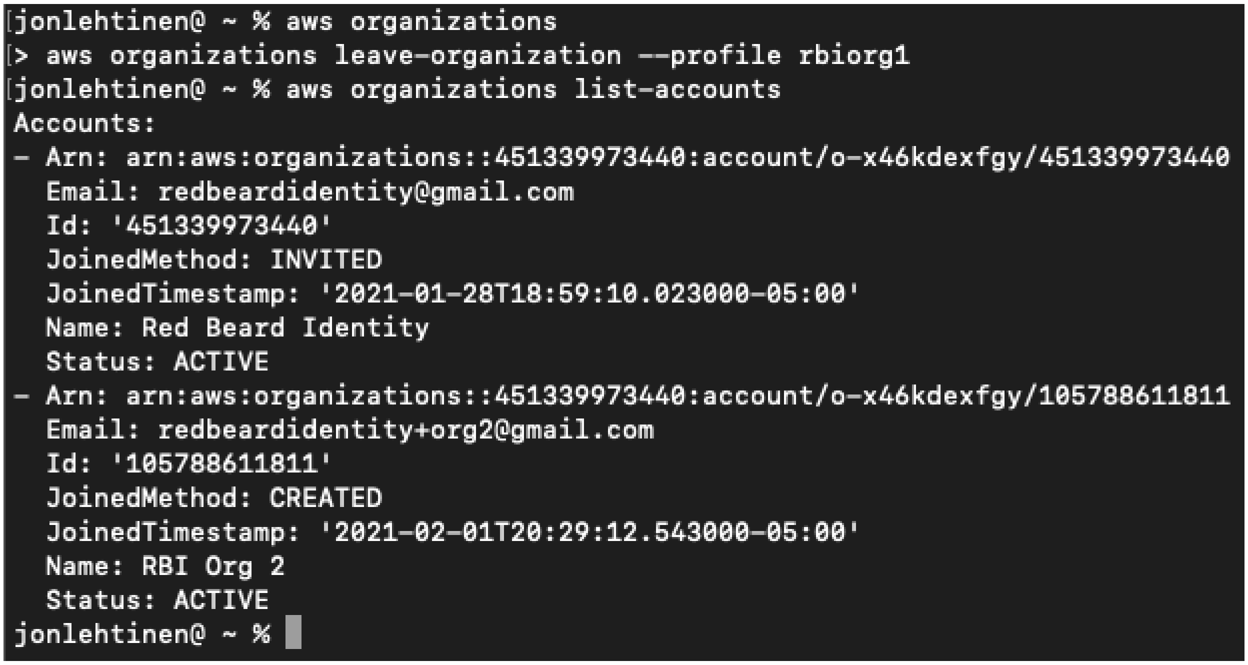
```
[jonlehtinen@ ~ % aws organizations describe-organization
Organization:
  Arn: arn:aws:organizations::451339973440:organization/o-x46kdexfgy
  AvailablePolicyTypes:
  - Status: ENABLED
    Type: SERVICE_CONTROL_POLICY
  FeatureSet: ALL
  Id: o-x46kdexfgy
  MasterAccountArn: arn:aws:organizations::451339973440:account/o-x46kdexfgy/451339973440
  MasterAccountEmail: redbeardidentity@gmail.com
  MasterAccountId: '451339973440'
jonlehtinen@ ~ %
```



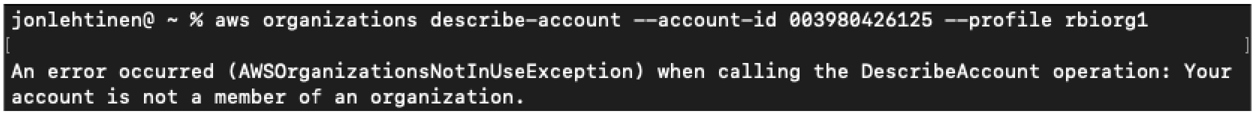
```
jonlehtinen@ ~ % aws organizations list-accounts
Accounts:
- Arn: arn:aws:organizations::451339973440:account/o-x46kdexfgy/451339973440
  Email: redbeardidentity@gmail.com
  Id: '451339973440'
  JoinedMethod: INVITED
  JoinedTimestamp: '2021-01-28T18:59:10.023000-05:00'
  Name: Red Beard Identity
  Status: ACTIVE
- Arn: arn:aws:organizations::451339973440:account/o-x46kdexfgy/105788611811
  Email: redbeardidentity+org2@gmail.com
  Id: '105788611811'
  JoinedMethod: CREATED
  JoinedTimestamp: '2021-02-01T20:29:12.543000-05:00'
  Name: RBI Org 2
  Status: ACTIVE
- Arn: arn:aws:organizations::451339973440:account/o-x46kdexfgy/003980426125
  Email: redbeardidentity+org1@gmail.com
  Id: '003980426125'
  JoinedMethod: INVITED
  JoinedTimestamp: '2021-02-01T20:56:03.615000-05:00'
  Name: RBI Sub Org 1
  Status: ACTIVE
jonlehtinen@ ~ %
```



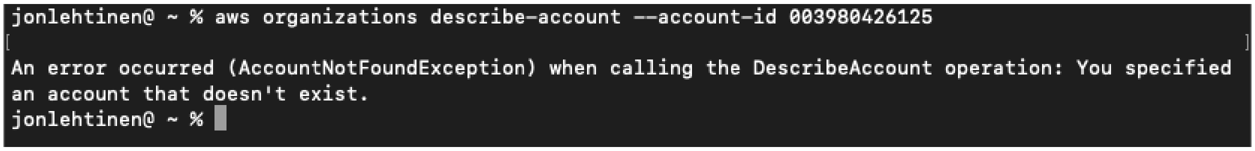
```
jonlehtinen@ ~ % aws organizations list-accounts --profile rbiorg1

An error occurred (AccessDeniedException) when calling the ListAccounts operation: You
don't have permissions to access this resource.
jonlehtinen@ ~ %
```



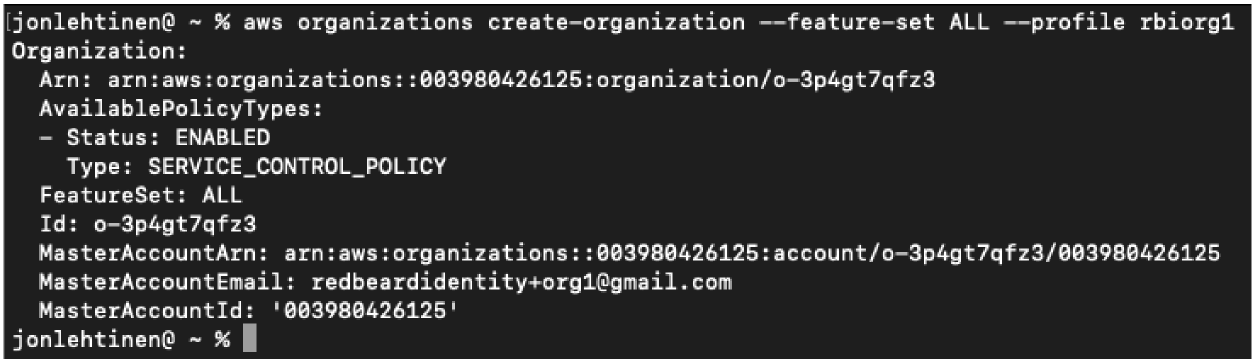
```
[jonlehtinen@ ~ % aws organizations
[> aws organizations leave-organization --profile rbiorg1
[jonlehtinen@ ~ % aws organizations list-accounts
Accounts:
- Arn: arn:aws:organizations::451339973440:account/o-x46kdexfgy/451339973440
  Email: redbeardidentity@gmail.com
  Id: '451339973440'
  JoinedMethod: INVITED
  JoinedTimestamp: '2021-01-28T18:59:10.023000-05:00'
  Name: Red Beard Identity
  Status: ACTIVE
- Arn: arn:aws:organizations::451339973440:account/o-x46kdexfgy/105788611811
  Email: redbeardidentity+org2@gmail.com
  Id: '105788611811'
  JoinedMethod: CREATED
  JoinedTimestamp: '2021-02-01T20:29:12.543000-05:00'
  Name: RBI Org 2
  Status: ACTIVE
jonlehtinen@ ~ %
```



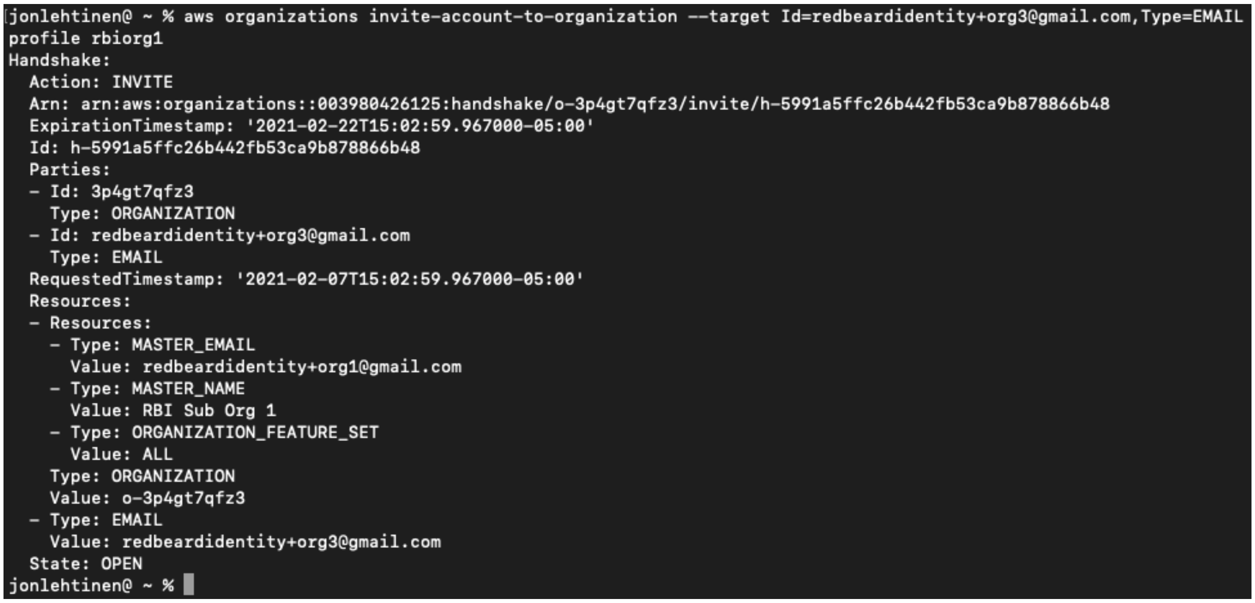
```
jonlehtinen@ ~ % aws organizations describe-account --account-id 003980426125 --profile rbiorg1
[                                                                                                  ]
An error occurred (AWSOrganizationsNotInUseException) when calling the DescribeAccount operation: Your
account is not a member of an organization.
```



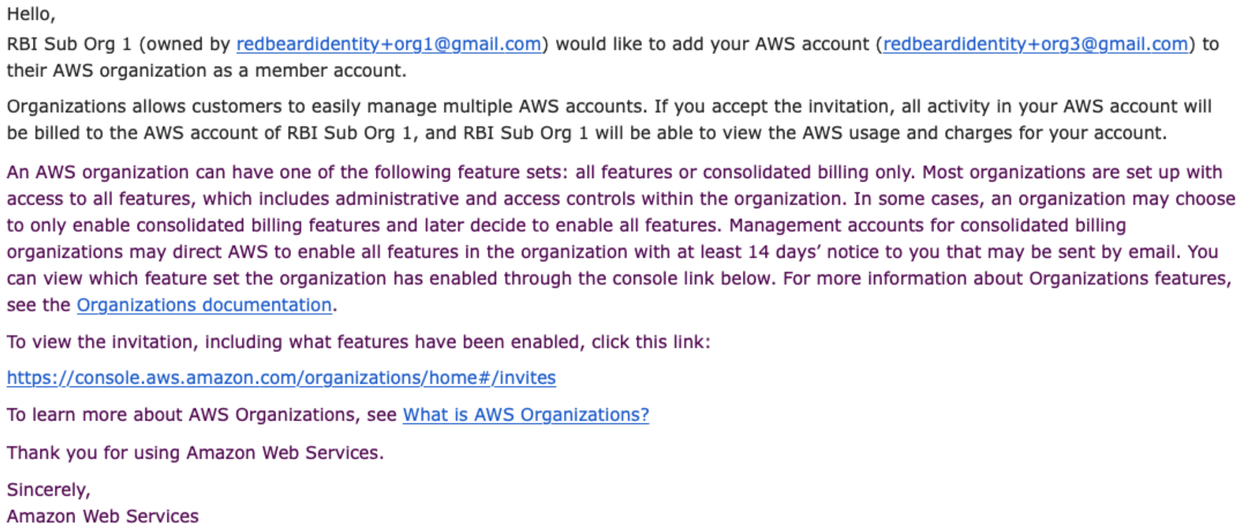
```
jonlehtinen@ ~ % aws organizations describe-account --account-id 003980426125
[                                                                                                  ]
An error occurred (AccountNotFoundException) when calling the DescribeAccount operation: You specified
an account that doesn't exist.
jonlehtinen@ ~ %
```



```
[jonlehtinen@ ~ % aws organizations create-organization --feature-set ALL --profile rbiorg1
Organization:
  Arn: arn:aws:organizations::003980426125:organization/o-3p4gt7qfz3
  AvailablePolicyTypes:
  - Status: ENABLED
    Type: SERVICE_CONTROL_POLICY
  FeatureSet: ALL
  Id: o-3p4gt7qfz3
  MasterAccountArn: arn:aws:organizations::003980426125:account/o-3p4gt7qfz3/003980426125
  MasterAccountEmail: redbeardidentity+org1@gmail.com
  MasterAccountId: '003980426125'
jonlehtinen@ ~ %
```



```
jonlehtinen@ ~ % aws organizations invite-account-to-organization --target Id=redbeardidentity+org3@gmail.com,Type=EMAIL
profile rbiorg1
Handshake:
  Action: INVITE
  Arn: arn:aws:organizations::003980426125:handshake/o-3p4gt7qfz3/invite/h-5991a5ffc26b442fb53ca9b878866b48
  ExpirationTimestamp: '2021-02-22T15:02:59.967000-05:00'
  Id: h-5991a5ffc26b442fb53ca9b878866b48
  Parties:
  - Id: 3p4gt7qfz3
    Type: ORGANIZATION
  - Id: redbeardidentity+org3@gmail.com
    Type: EMAIL
  RequestedTimestamp: '2021-02-07T15:02:59.967000-05:00'
  Resources:
  - Resources:
    - Type: MASTER_EMAIL
      Value: redbeardidentity+org1@gmail.com
    - Type: MASTER_NAME
      Value: RBI Sub Org 1
    - Type: ORGANIZATION_FEATURE_SET
      Value: ALL
    Type: ORGANIZATION
    Value: o-3p4gt7qfz3
  - Type: EMAIL
    Value: redbeardidentity+org3@gmail.com
  State: OPEN
jonlehtinen@ ~ %
```



Hello,

RBI Sub Org 1 (owned by redbeardidentity+org1@gmail.com) would like to add your AWS account (redbeardidentity+org3@gmail.com) to their AWS organization as a member account.

Organizations allows customers to easily manage multiple AWS accounts. If you accept the invitation, all activity in your AWS account will be billed to the AWS account of RBI Sub Org 1, and RBI Sub Org 1 will be able to view the AWS usage and charges for your account.

An AWS organization can have one of the following feature sets: all features or consolidated billing only. Most organizations are set up with access to all features, which includes administrative and access controls within the organization. In some cases, an organization may choose to only enable consolidated billing features and later decide to enable all features. Management accounts for consolidated billing organizations may direct AWS to enable all features in the organization with at least 14 days' notice to you that may be sent by email. You can view which feature set the organization has enabled through the console link below. For more information about Organizations features, see the Organizations documentation.

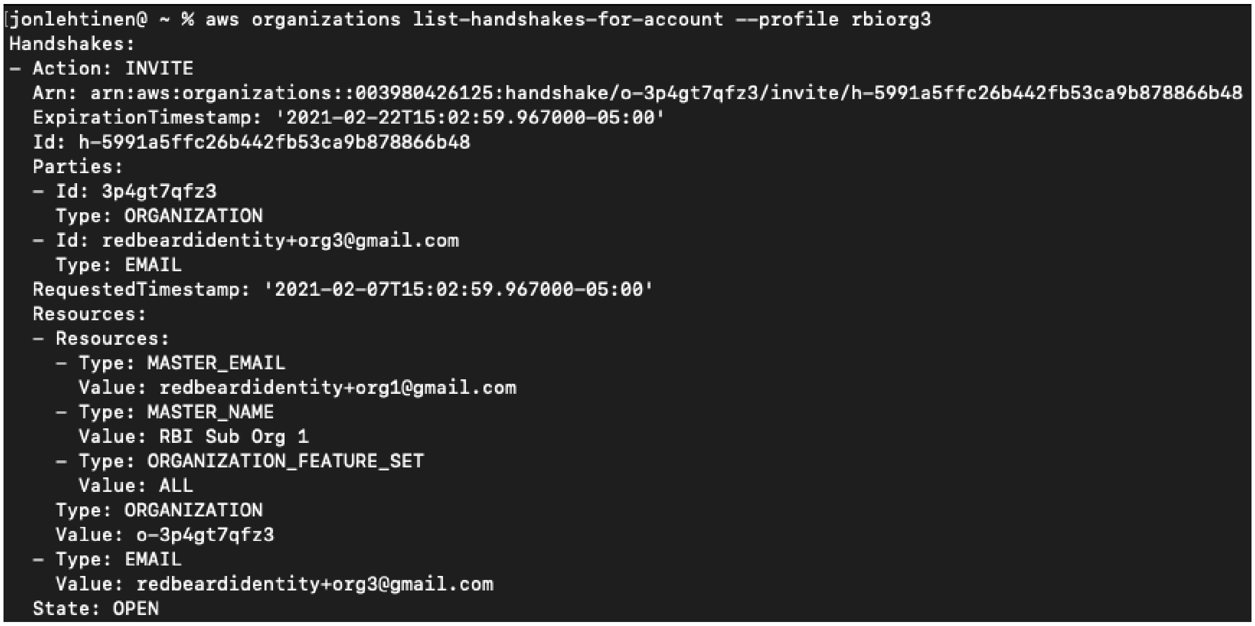
To view the invitation, including what features have been enabled, click this link:

https://console.aws.amazon.com/organizations/home#/invites

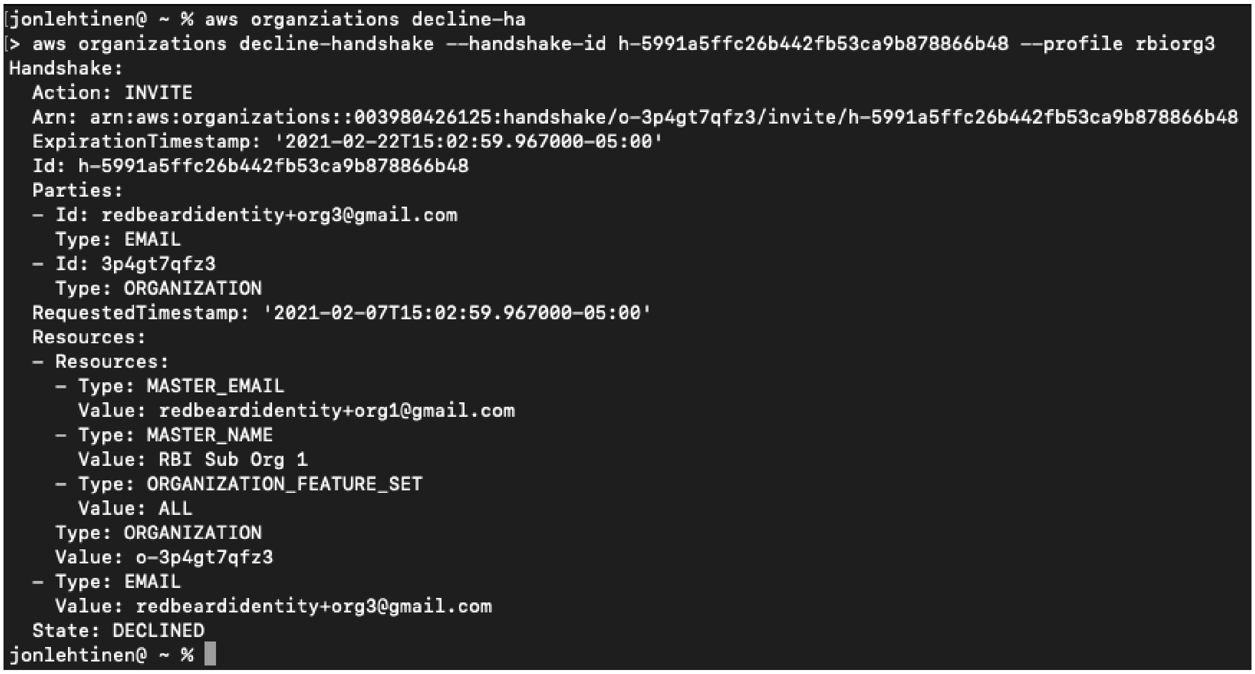
To learn more about AWS Organizations, see What is AWS Organizations?

Thank you for using Amazon Web Services.

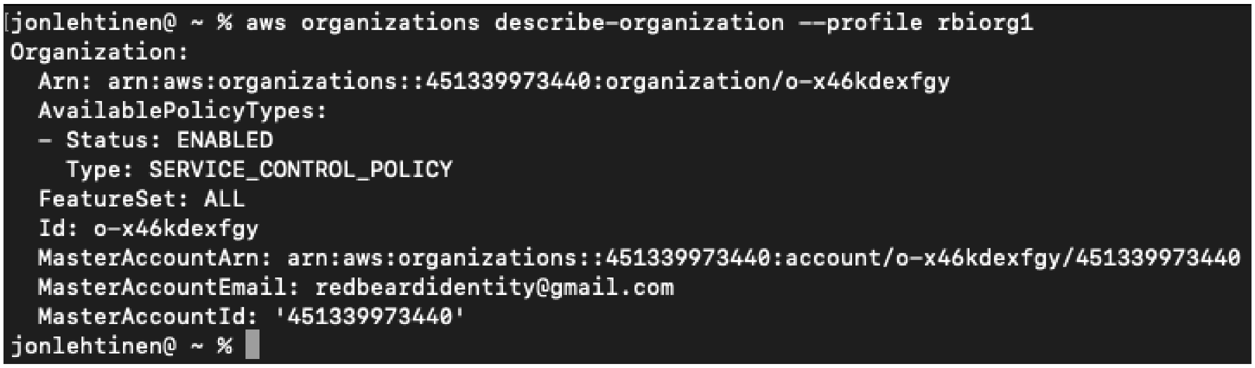
Sincerely,
Amazon Web Services



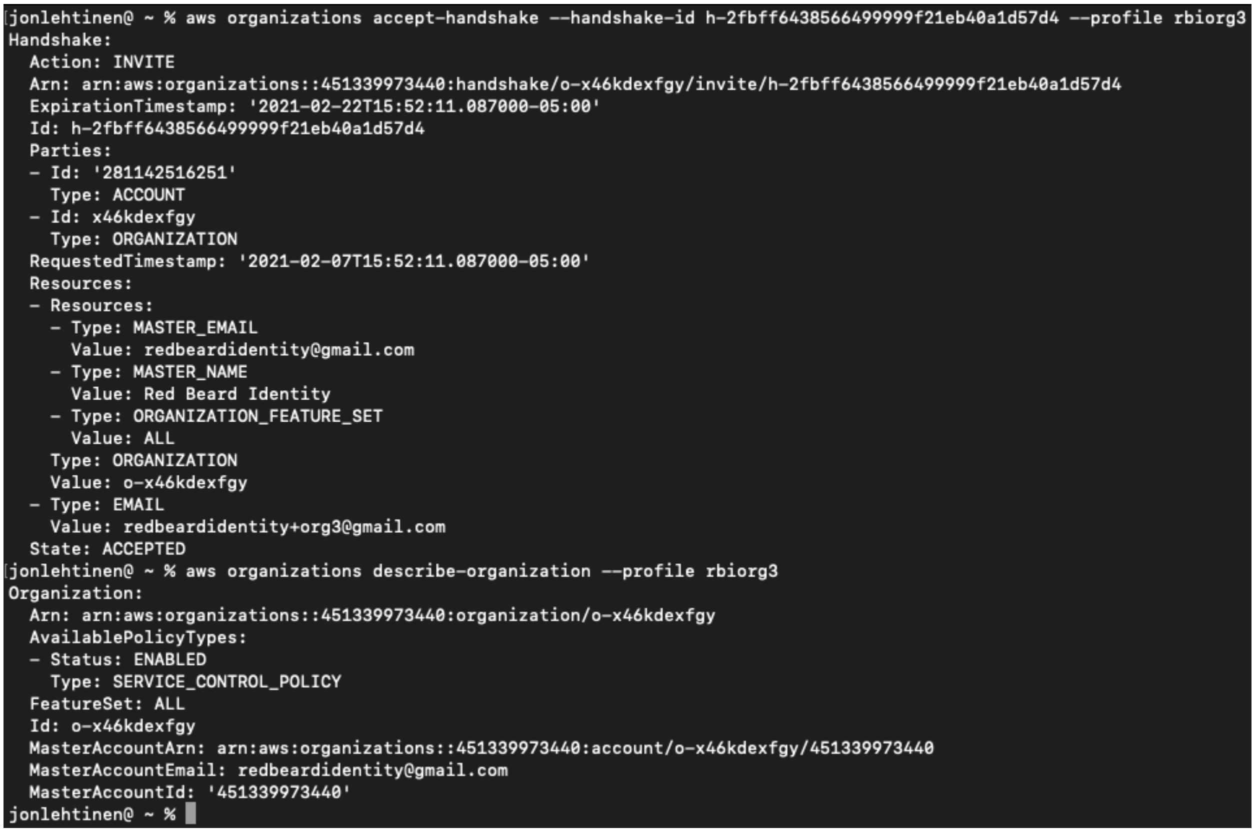
```
[jonlehtinen@ ~ % aws organizations list-handshakes-for-account --profile rbiorg3
Handshakes:
- Action: INVITE
  Arn: arn:aws:organizations::003980426125:handshake/o-3p4gt7qfz3/invite/h-5991a5ffc26b442fb53ca9b878866b48
  ExpirationTimestamp: '2021-02-22T15:02:59.967000-05:00'
  Id: h-5991a5ffc26b442fb53ca9b878866b48
  Parties:
  - Id: 3p4gt7qfz3
    Type: ORGANIZATION
  - Id: redbeardidentity+org3@gmail.com
    Type: EMAIL
  RequestedTimestamp: '2021-02-07T15:02:59.967000-05:00'
  Resources:
  - Resources:
    - Type: MASTER_EMAIL
      Value: redbeardidentity+org1@gmail.com
    - Type: MASTER_NAME
      Value: RBI Sub Org 1
    - Type: ORGANIZATION_FEATURE_SET
      Value: ALL
    Type: ORGANIZATION
    Value: o-3p4gt7qfz3
  - Type: EMAIL
    Value: redbeardidentity+org3@gmail.com
  State: OPEN
```



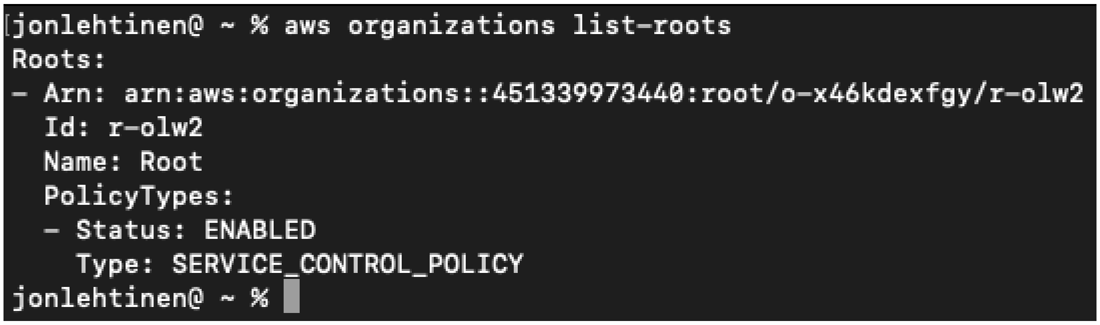
```
[jonlehtinen@ ~ % aws organziations decline-ha
[> aws organizations decline-handshake --handshake-id h-5991a5ffc26b442fb53ca9b878866b48 --profile rbiorg3
Handshake:
  Action: INVITE
  Arn: arn:aws:organizations::003980426125:handshake/o-3p4gt7qfz3/invite/h-5991a5ffc26b442fb53ca9b878866b48
  ExpirationTimestamp: '2021-02-22T15:02:59.967000-05:00'
  Id: h-5991a5ffc26b442fb53ca9b878866b48
  Parties:
  - Id: redbeardidentity+org3@gmail.com
    Type: EMAIL
  - Id: 3p4gt7qfz3
    Type: ORGANIZATION
  RequestedTimestamp: '2021-02-07T15:02:59.967000-05:00'
  Resources:
  - Resources:
    - Type: MASTER_EMAIL
      Value: redbeardidentity+org1@gmail.com
    - Type: MASTER_NAME
      Value: RBI Sub Org 1
    - Type: ORGANIZATION_FEATURE_SET
      Value: ALL
    Type: ORGANIZATION
    Value: o-3p4gt7qfz3
  - Type: EMAIL
    Value: redbeardidentity+org3@gmail.com
  State: DECLINED
jonlehtinen@ ~ %
```



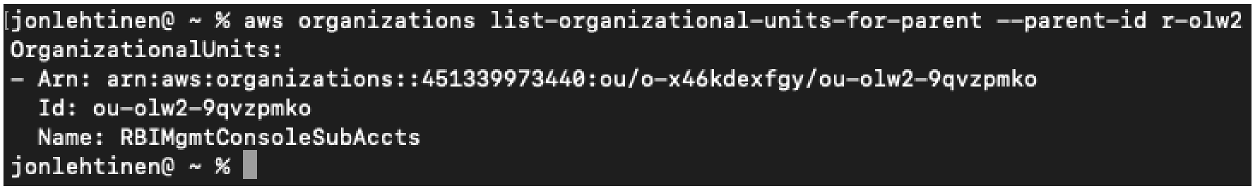
```
[jonlehtinen@ ~ % aws organizations describe-organization --profile rbiorg1
Organization:
  Arn: arn:aws:organizations::451339973440:organization/o-x46kdexfgy
  AvailablePolicyTypes:
  - Status: ENABLED
    Type: SERVICE_CONTROL_POLICY
  FeatureSet: ALL
  Id: o-x46kdexfgy
  MasterAccountArn: arn:aws:organizations::451339973440:account/o-x46kdexfgy/451339973440
  MasterAccountEmail: redbeardidentity@gmail.com
  MasterAccountId: '451339973440'
jonlehtinen@ ~ %
```



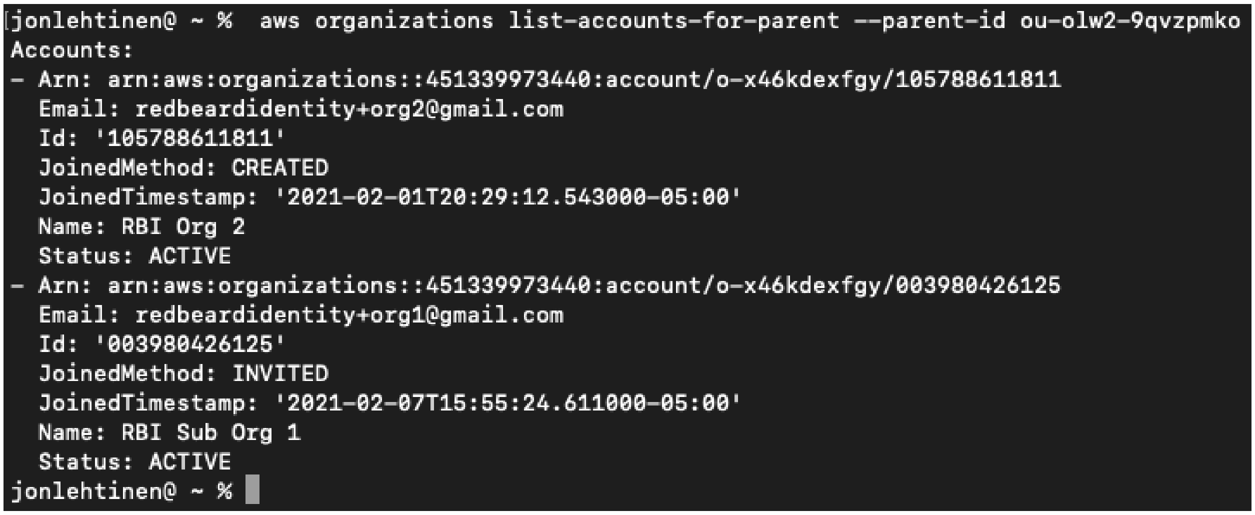
```
[jonlehtinen@ ~ % aws organizations accept-handshake --handshake-id h-2fbff6438566499999f21eb40a1d57d4 --profile rbiorg3
Handshake:
  Action: INVITE
  Arn: arn:aws:organizations::451339973440:handshake/o-x46kdexfgy/invite/h-2fbff6438566499999f21eb40a1d57d4
  ExpirationTimestamp: '2021-02-22T15:52:11.087000-05:00'
  Id: h-2fbff6438566499999f21eb40a1d57d4
  Parties:
  - Id: '281142516251'
    Type: ACCOUNT
  - Id: x46kdexfgy
    Type: ORGANIZATION
  RequestedTimestamp: '2021-02-07T15:52:11.087000-05:00'
  Resources:
  - Resources:
    - Type: MASTER_EMAIL
      Value: redbeardidentity@gmail.com
    - Type: MASTER_NAME
      Value: Red Beard Identity
    - Type: ORGANIZATION_FEATURE_SET
      Value: ALL
    Type: ORGANIZATION
    Value: o-x46kdexfgy
  - Type: EMAIL
    Value: redbeardidentity+org3@gmail.com
  State: ACCEPTED
[jonlehtinen@ ~ % aws organizations describe-organization --profile rbiorg3
Organization:
  Arn: arn:aws:organizations::451339973440:organization/o-x46kdexfgy
  AvailablePolicyTypes:
  - Status: ENABLED
    Type: SERVICE_CONTROL_POLICY
  FeatureSet: ALL
  Id: o-x46kdexfgy
  MasterAccountArn: arn:aws:organizations::451339973440:account/o-x46kdexfgy/451339973440
  MasterAccountEmail: redbeardidentity@gmail.com
  MasterAccountId: '451339973440'
jonlehtinen@ ~ %
```



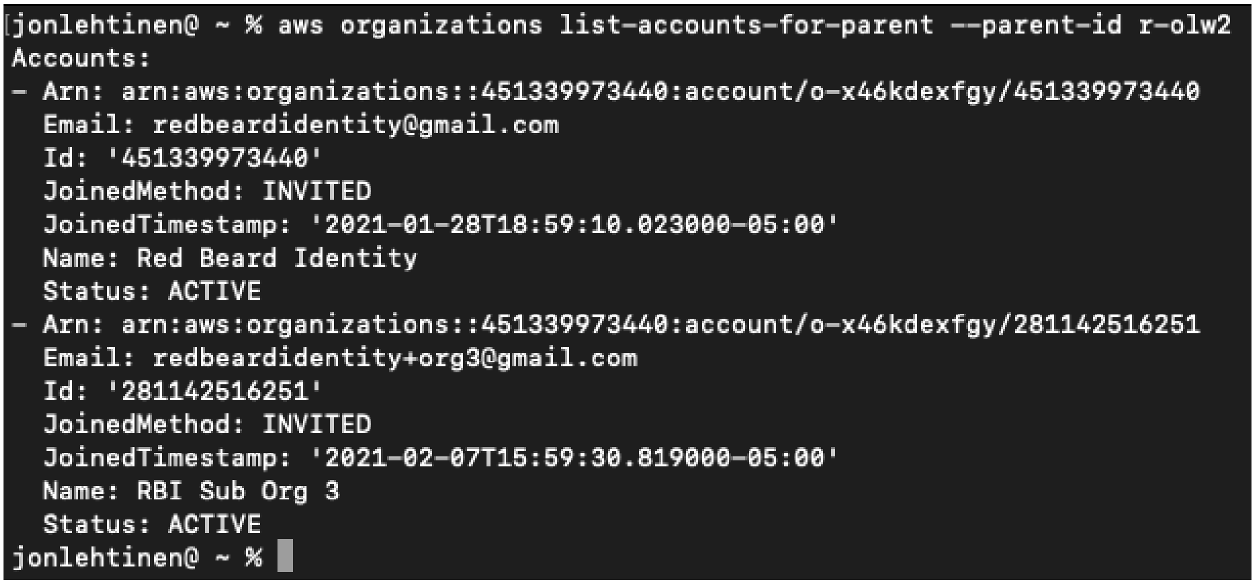
```
[jonlehtinen@ ~ % aws organizations list-roots
Roots:
- Arn: arn:aws:organizations::451339973440:root/o-x46kdexfgy/r-olw2
  Id: r-olw2
  Name: Root
  PolicyTypes:
  - Status: ENABLED
    Type: SERVICE_CONTROL_POLICY
jonlehtinen@ ~ %
```



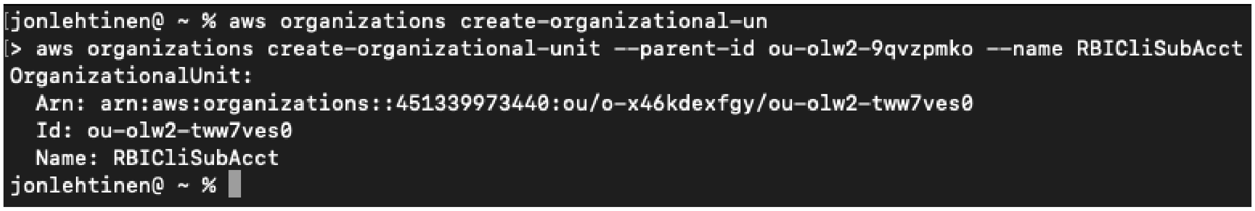
```
[jonlehtinen@ ~ % aws organizations list-organizational-units-for-parent --parent-id r-olw2
OrganizationalUnits:
- Arn: arn:aws:organizations::451339973440:ou/o-x46kdexfgy/ou-olw2-9qvzpmko
  Id: ou-olw2-9qvzpmko
  Name: RBIMgmtConsoleSubAccts
jonlehtinen@ ~ %
```



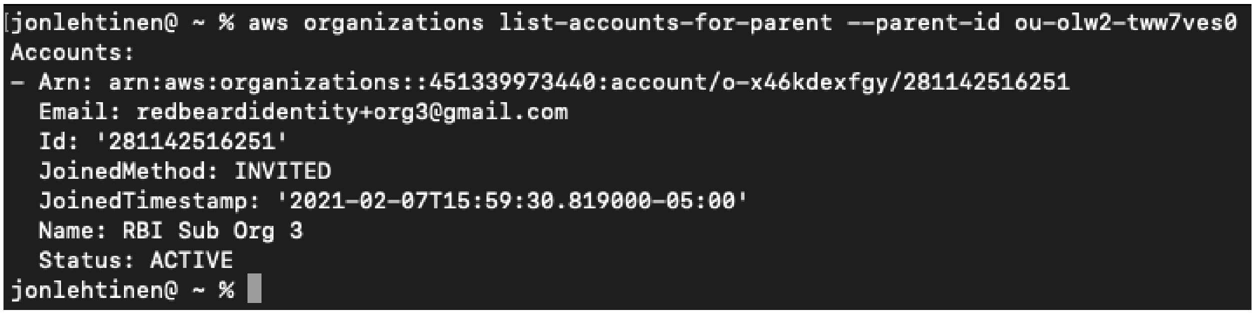
```
[jonlehtinen@ ~ %  aws organizations list-accounts-for-parent --parent-id ou-olw2-9qvzpmko
Accounts:
- Arn: arn:aws:organizations::451339973440:account/o-x46kdexfgy/105788611811
  Email: redbeardidentity+org2@gmail.com
  Id: '105788611811'
  JoinedMethod: CREATED
  JoinedTimestamp: '2021-02-01T20:29:12.543000-05:00'
  Name: RBI Org 2
  Status: ACTIVE
- Arn: arn:aws:organizations::451339973440:account/o-x46kdexfgy/003980426125
  Email: redbeardidentity+org1@gmail.com
  Id: '003980426125'
  JoinedMethod: INVITED
  JoinedTimestamp: '2021-02-07T15:55:24.611000-05:00'
  Name: RBI Sub Org 1
  Status: ACTIVE
jonlehtinen@ ~ %
```



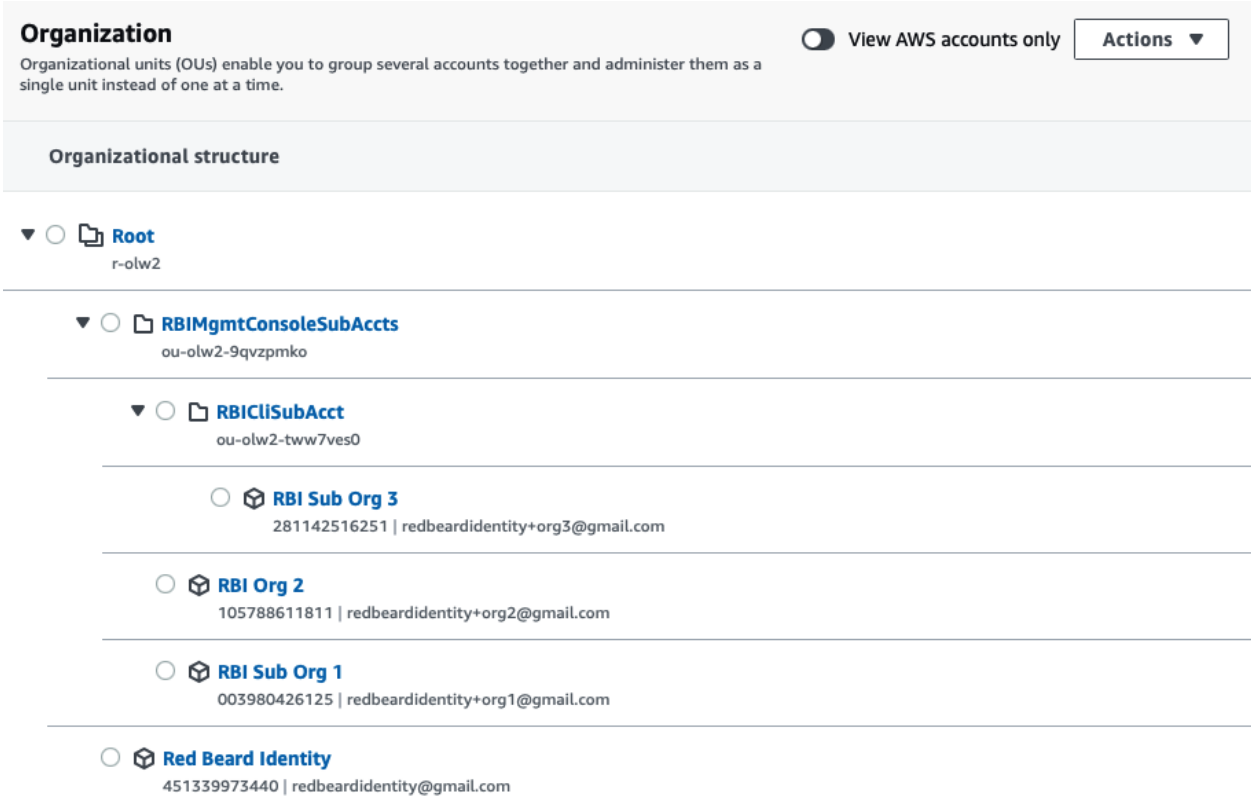
```
[jonlehtinen@ ~ % aws organizations list-accounts-for-parent --parent-id r-olw2
Accounts:
- Arn: arn:aws:organizations::451339973440:account/o-x46kdexfgy/451339973440
  Email: redbeardidentity@gmail.com
  Id: '451339973440'
  JoinedMethod: INVITED
  JoinedTimestamp: '2021-01-28T18:59:10.023000-05:00'
  Name: Red Beard Identity
  Status: ACTIVE
- Arn: arn:aws:organizations::451339973440:account/o-x46kdexfgy/281142516251
  Email: redbeardidentity+org3@gmail.com
  Id: '281142516251'
  JoinedMethod: INVITED
  JoinedTimestamp: '2021-02-07T15:59:30.819000-05:00'
  Name: RBI Sub Org 3
  Status: ACTIVE
jonlehtinen@ ~ %
```



```
[jonlehtinen@ ~ % aws organizations create-organizational-un
[> aws organizations create-organizational-unit --parent-id ou-olw2-9qvzpmko --name RBICliSubAcct
OrganizationalUnit:
  Arn: arn:aws:organizations::451339973440:ou/o-x46kdexfgy/ou-olw2-tww7ves0
  Id: ou-olw2-tww7ves0
  Name: RBICliSubAcct
jonlehtinen@ ~ %
```



```
[jonlehtinen@ ~ % aws organizations list-accounts-for-parent --parent-id ou-olw2-tww7ves0
Accounts:
- Arn: arn:aws:organizations::451339973440:account/o-x46kdexfgy/281142516251
  Email: redbeardidentity+org3@gmail.com
  Id: '281142516251'
  JoinedMethod: INVITED
  JoinedTimestamp: '2021-02-07T15:59:30.819000-05:00'
  Name: RBI Sub Org 3
  Status: ACTIVE
jonlehtinen@ ~ %
```

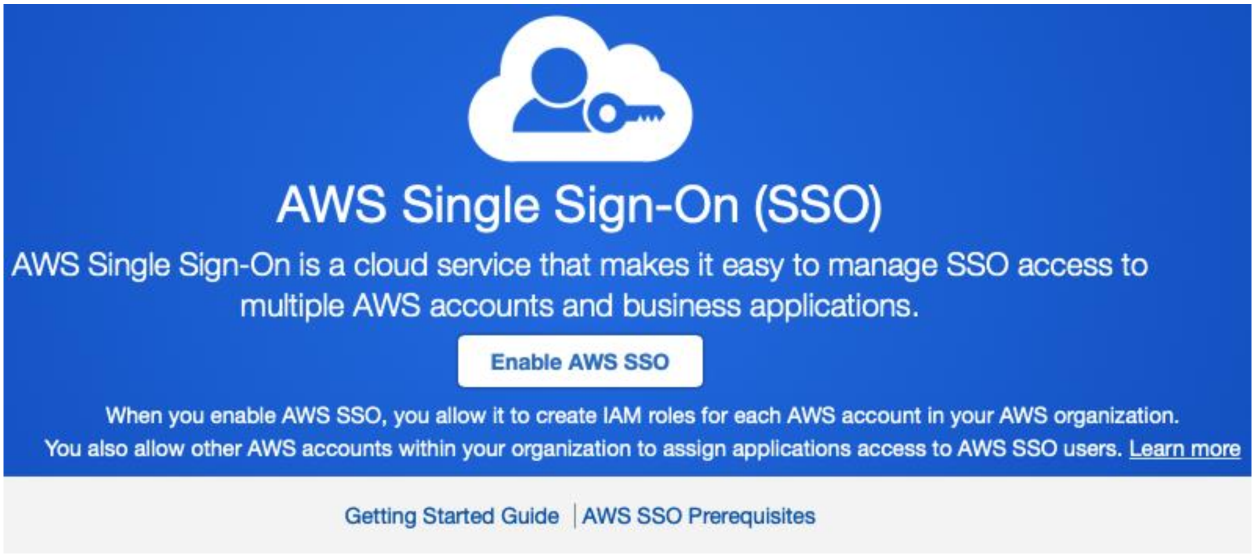


Organization

Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

Organizational structure

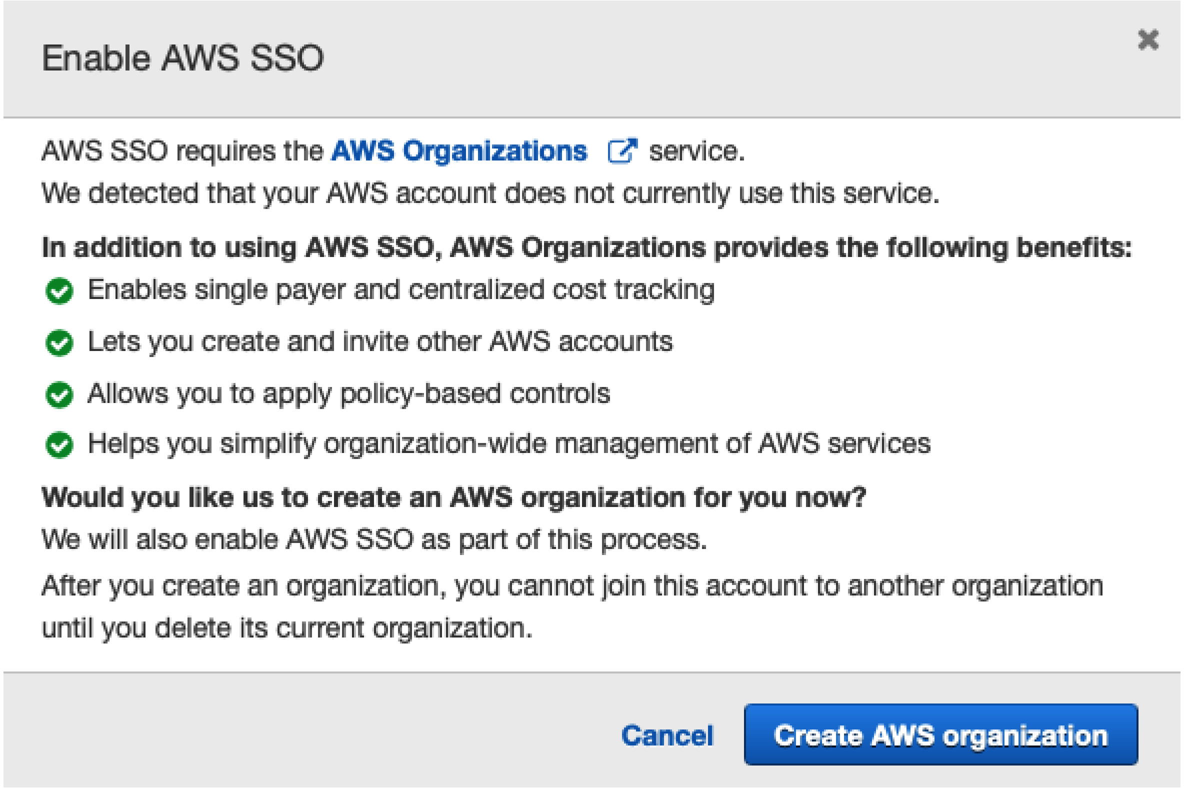
- ○ **Root**
  r-olw2
  - ○ **RBIMgmtConsoleSubAccts**
    ou-olw2-9qvzpmko
    - ○ **RBICliSubAcct**
      ou-olw2-tww7ves0
      - ○ **RBI Sub Org 3**
        281142516251 | redbeardidentity+org3@gmail.com
    - ○ **RBI Org 2**
      105788611811 | redbeardidentity+org2@gmail.com
    - ○ **RBI Sub Org 1**
      003980426125 | redbeardidentity+org1@gmail.com
  - ○ **Red Beard Identity**
    451339973440 | redbeardidentity@gmail.com



AWS Single Sign-On (SSO)

AWS Single Sign-On is a cloud service that makes it easy to manage SSO access to multiple AWS accounts and business applications.

When you enable AWS SSO, you allow it to create IAM roles for each AWS account in your AWS organization. You also allow other AWS accounts within your organization to assign applications access to AWS SSO users. Learn more



Enable AWS SSO

AWS SSO requires the **AWS Organizations** service.
We detected that your AWS account does not currently use this service.

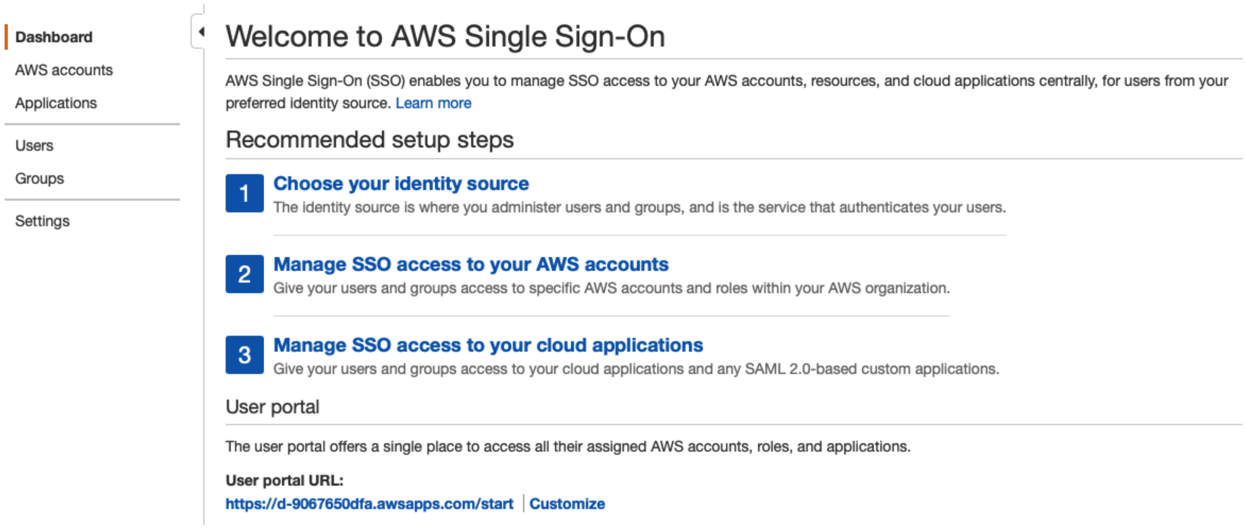
In addition to using AWS SSO, AWS Organizations provides the following benefits:

- ✓ Enables single payer and centralized cost tracking
- ✓ Lets you create and invite other AWS accounts
- ✓ Allows you to apply policy-based controls
- ✓ Helps you simplify organization-wide management of AWS services

Would you like us to create an AWS organization for you now?

We will also enable AWS SSO as part of this process.

After you create an organization, you cannot join this account to another organization until you delete its current organization.



Welcome to AWS Single Sign-On

AWS Single Sign-On (SSO) enables you to manage SSO access to your AWS accounts, resources, and cloud applications centrally, for users from your preferred identity source. Learn more

Recommended setup steps

1 **Choose your identity source**
The identity source is where you administer users and groups, and is the service that authenticates your users.

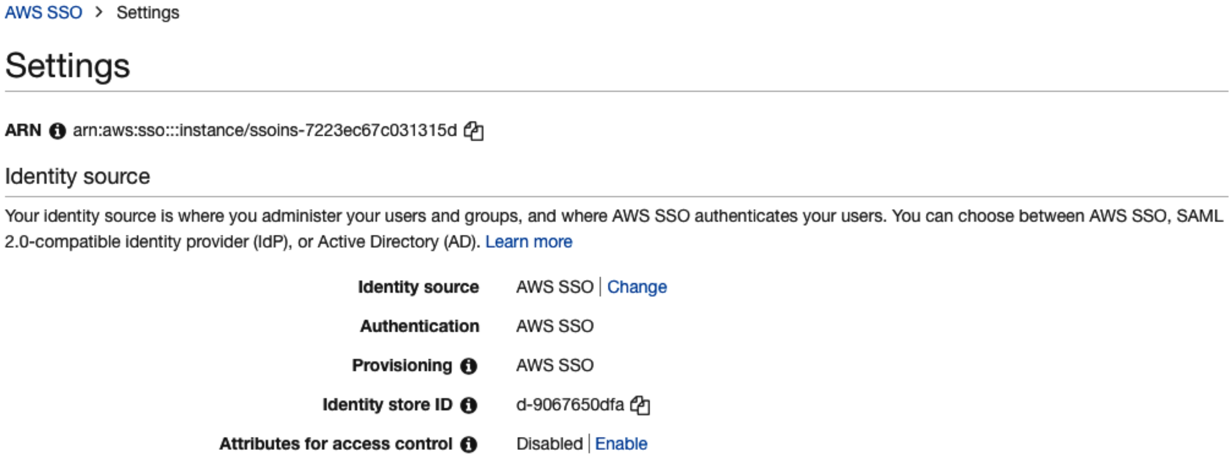
2 **Manage SSO access to your AWS accounts**
Give your users and groups access to specific AWS accounts and roles within your AWS organization.

3 **Manage SSO access to your cloud applications**
Give your users and groups access to your cloud applications and any SAML 2.0-based custom applications.

User portal

The user portal offers a single place to access all their assigned AWS accounts, roles, and applications.

User portal URL:
https://d-9067650dfa.awsapps.com/start | Customize



AWS SSO > Settings

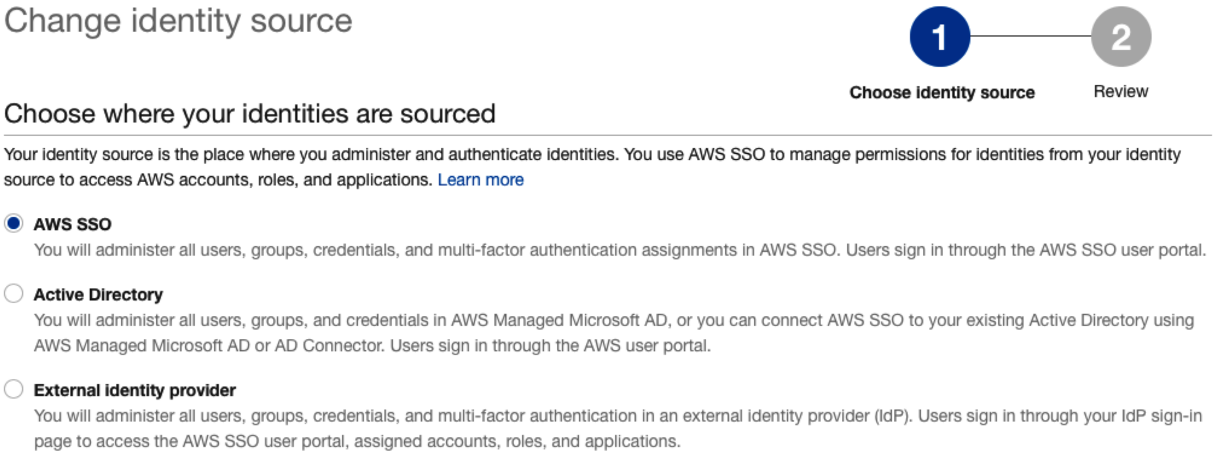
Settings

ARN arn:aws:sso:::instance/ssoins-7223ec67c031315d

Identity source

Your identity source is where you administer your users and groups, and where AWS SSO authenticates your users. You can choose between AWS SSO, SAML 2.0-compatible identity provider (IdP), or Active Directory (AD). Learn more

Identity source	AWS SSO | Change
Authentication	AWS SSO
Provisioning	AWS SSO
Identity store ID	d-9067650dfa
Attributes for access control	Disabled | Enable



Change identity source

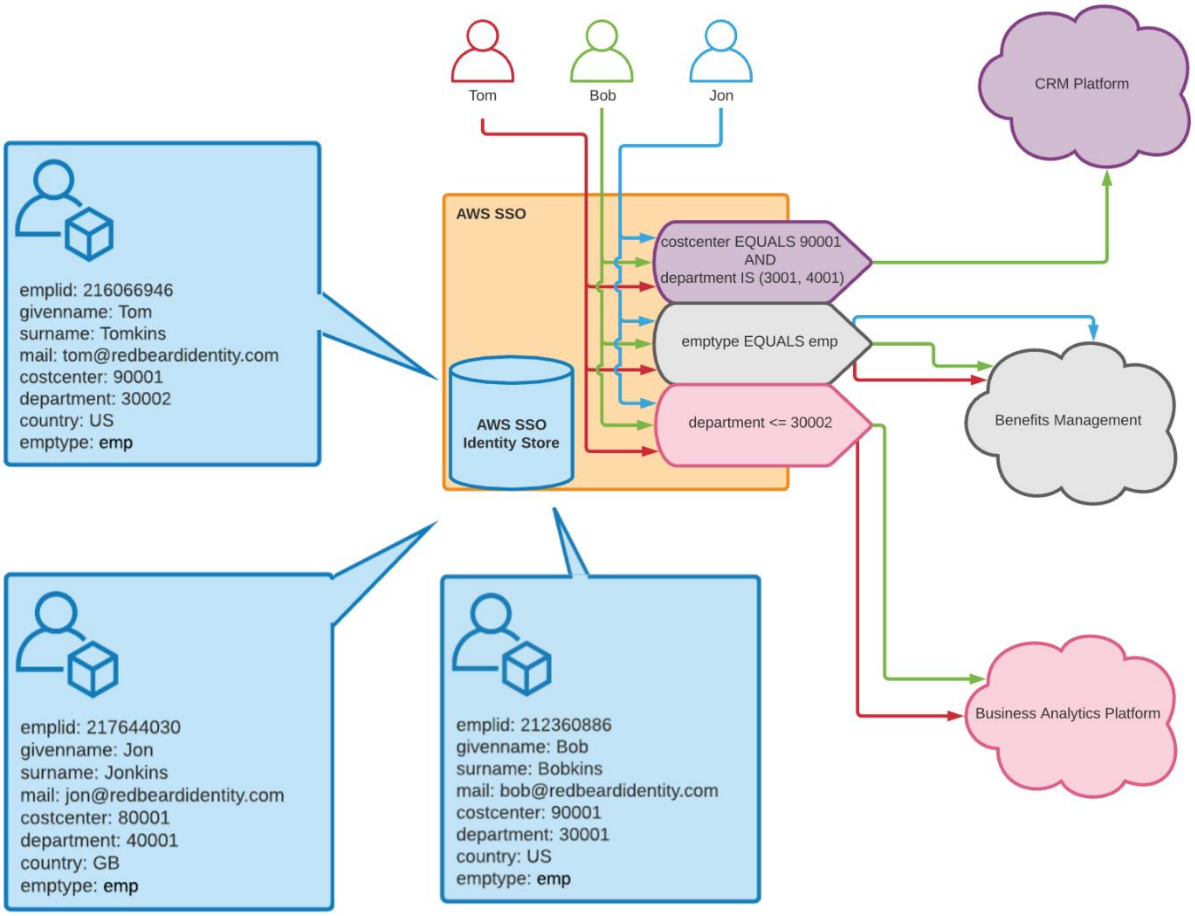
Choose where your identities are sourced

Your identity source is the place where you administer and authenticate identities. You use AWS SSO to manage permissions for identities from your identity source to access AWS accounts, roles, and applications. Learn more

● **AWS SSO**
You will administer all users, groups, credentials, and multi-factor authentication assignments in AWS SSO. Users sign in through the AWS SSO user portal.

○ **Active Directory**
You will administer all users, groups, and credentials in AWS Managed Microsoft AD, or you can connect AWS SSO to your existing Active Directory using AWS Managed Microsoft AD or AD Connector. Users sign in through the AWS user portal.

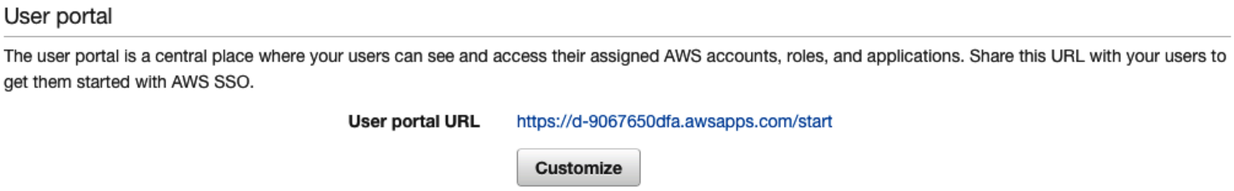
○ **External identity provider**
You will administer all users, groups, credentials, and multi-factor authentication in an external identity provider (IdP). Users sign in through your IdP sign-in page to access the AWS SSO user portal, assigned accounts, roles, and applications.



emplid: 216066946
givenname: Tom
surname: Tomkins
mail: tom@redbeardidentity.com
costcenter: 90001
department: 30002
country: US
emptype: **emp**

emplid: 217644030
givenname: Jon
surname: Jonkins
mail: jon@redbeardidentity.com
costcenter: 80001
department: 40001
country: GB
emptype: **emp**

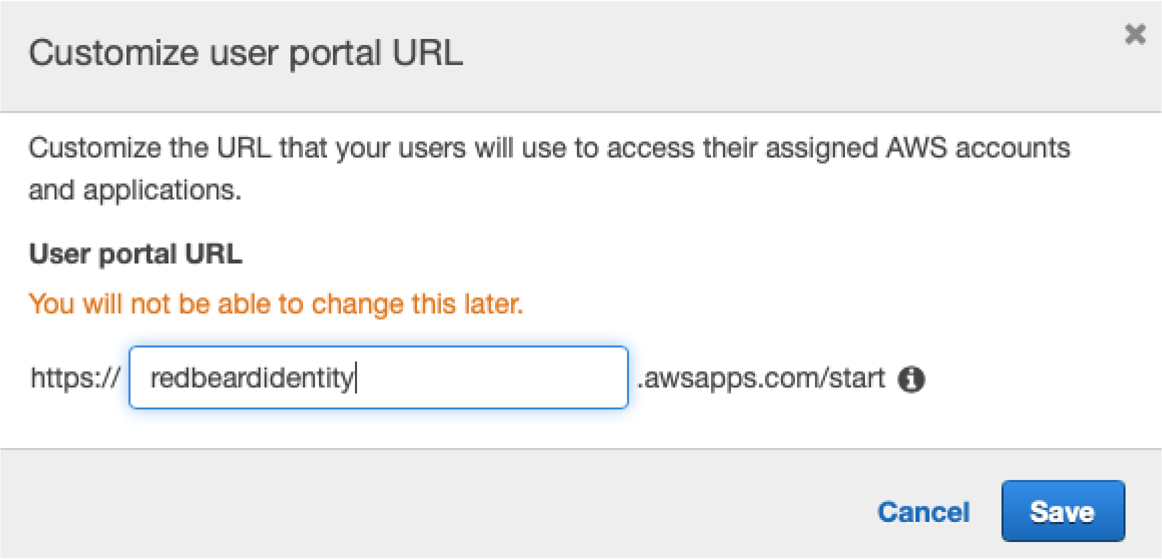
emplid: 212360886
givenname: Bob
surname: Bobkins
mail: bob@redbeardidentity.com
costcenter: 90001
department: 30001
country: US
emptype: **emp**



User portal

The user portal is a central place where your users can see and access their assigned AWS accounts, roles, and applications. Share this URL with your users to get them started with AWS SSO.

User portal URL https://d-9067650dfa.awsapps.com/start



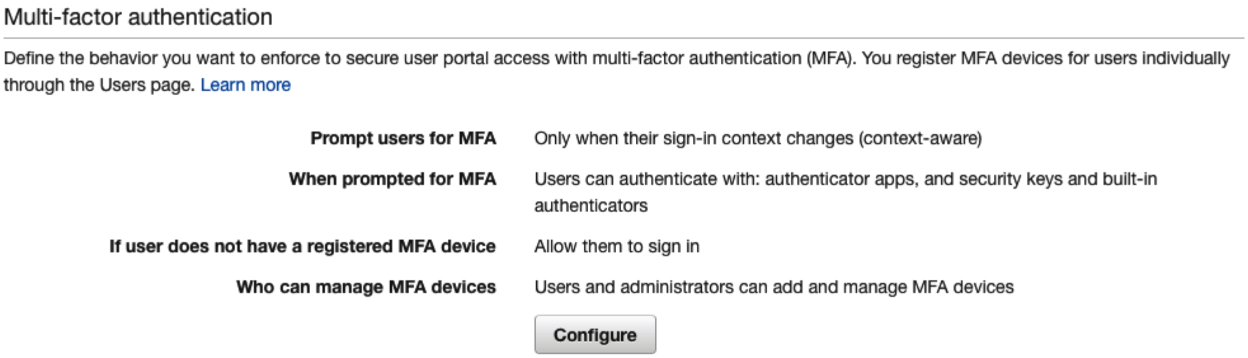
Customize user portal URL

Customize the URL that your users will use to access their assigned AWS accounts and applications.

User portal URL

You will not be able to change this later.

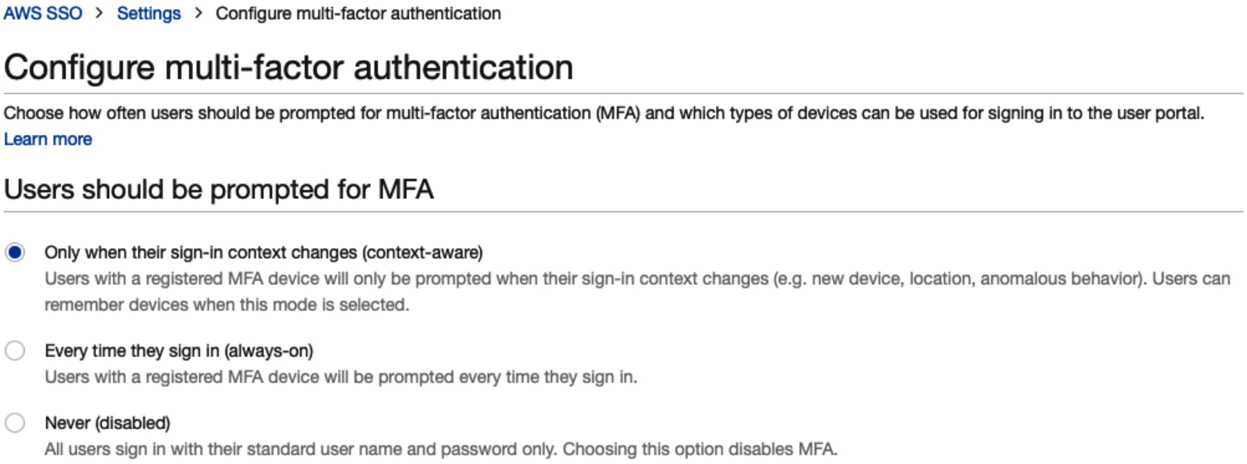
https:// redbeardidentity .awsapps.com/start



Multi-factor authentication

Define the behavior you want to enforce to secure user portal access with multi-factor authentication (MFA). You register MFA devices for users individually through the Users page. Learn more

Prompt users for MFA	Only when their sign-in context changes (context-aware)
When prompted for MFA	Users can authenticate with: authenticator apps, and security keys and built-in authenticators
If user does not have a registered MFA device	Allow them to sign in
Who can manage MFA devices	Users and administrators can add and manage MFA devices



AWS SSO > Settings > Configure multi-factor authentication

Configure multi-factor authentication

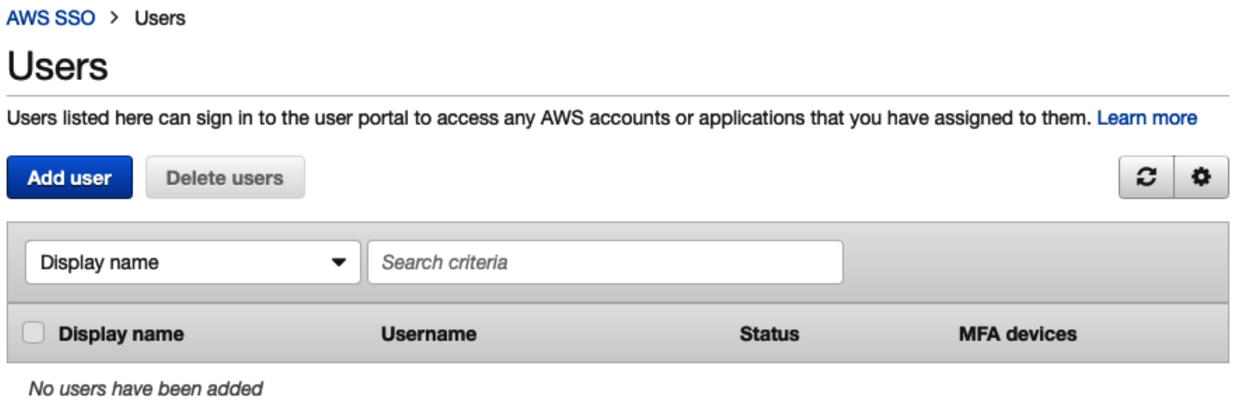
Choose how often users should be prompted for multi-factor authentication (MFA) and which types of devices can be used for signing in to the user portal. Learn more

Users should be prompted for MFA

● Only when their sign-in context changes (context-aware)
Users with a registered MFA device will only be prompted when their sign-in context changes (e.g. new device, location, anomalous behavior). Users can remember devices when this mode is selected.

○ Every time they sign in (always-on)
Users with a registered MFA device will be prompted every time they sign in.

○ Never (disabled)
All users sign in with their standard user name and password only. Choosing this option disables MFA.

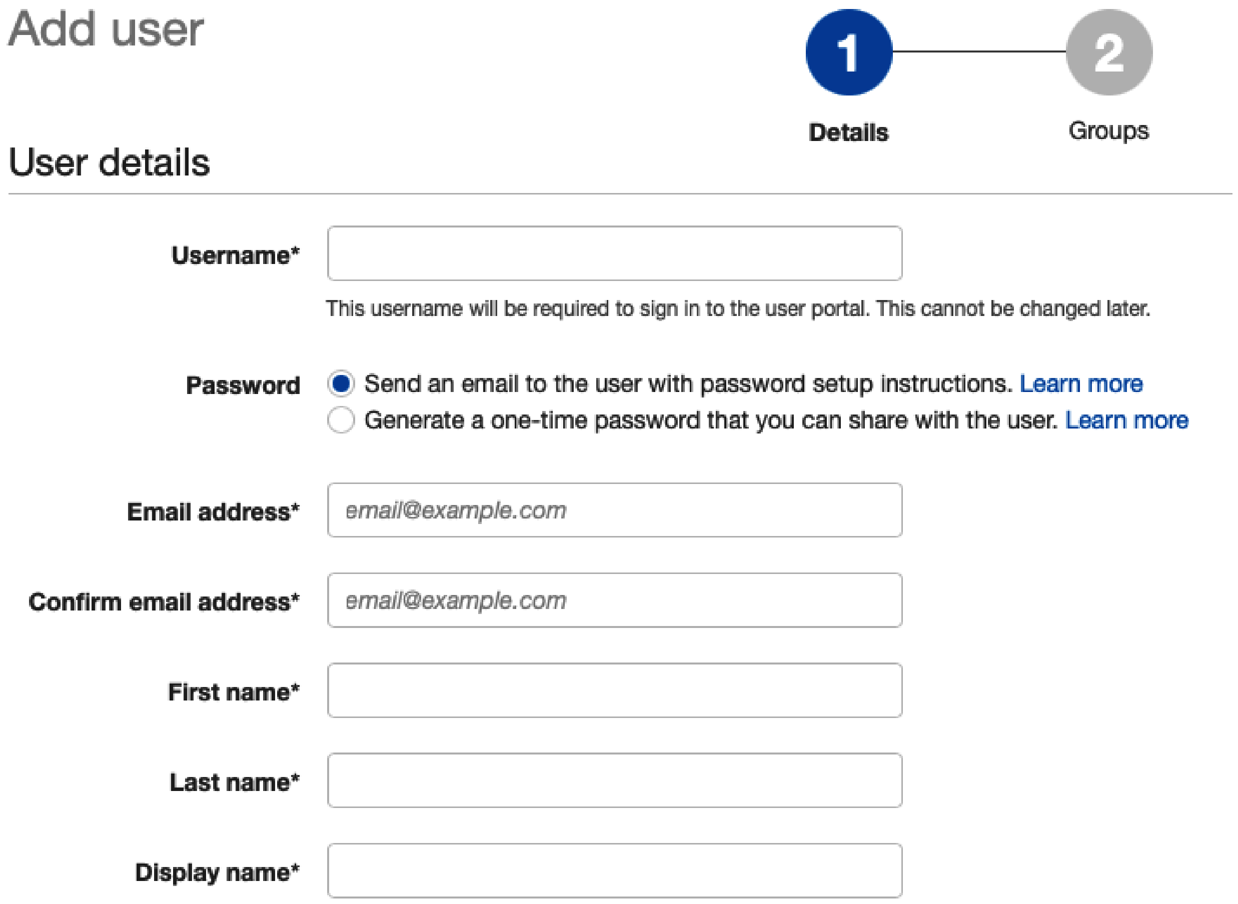


Users

Users listed here can sign in to the user portal to access any AWS accounts or applications that you have assigned to them. Learn more

□ Display name	Username	Status	MFA devices

No users have been added



Add user

User details

Username*

This username will be required to sign in to the user portal. This cannot be changed later.

Password
● Send an email to the user with password setup instructions. Learn more
○ Generate a one-time password that you can share with the user. Learn more

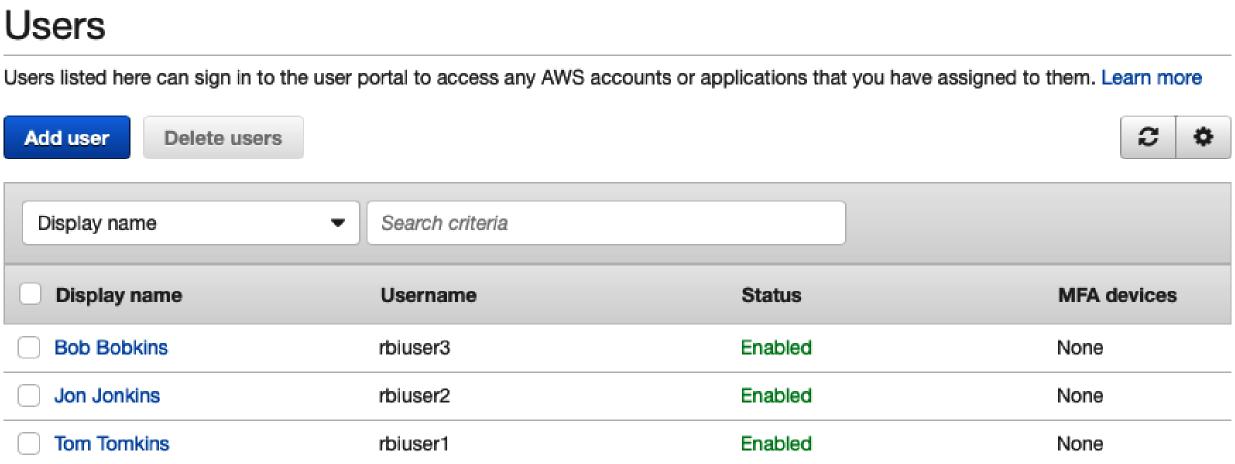
Email address* email@example.com

Confirm email address* email@example.com

First name*

Last name*

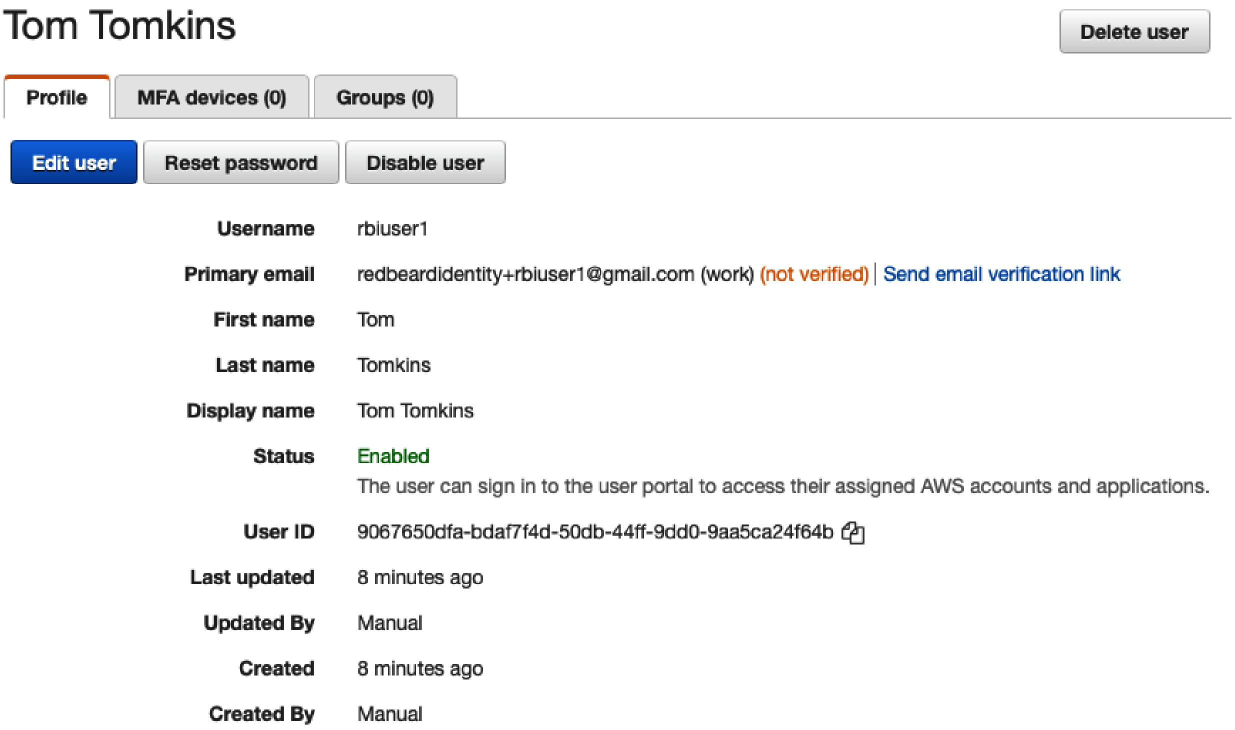
Display name*



Users

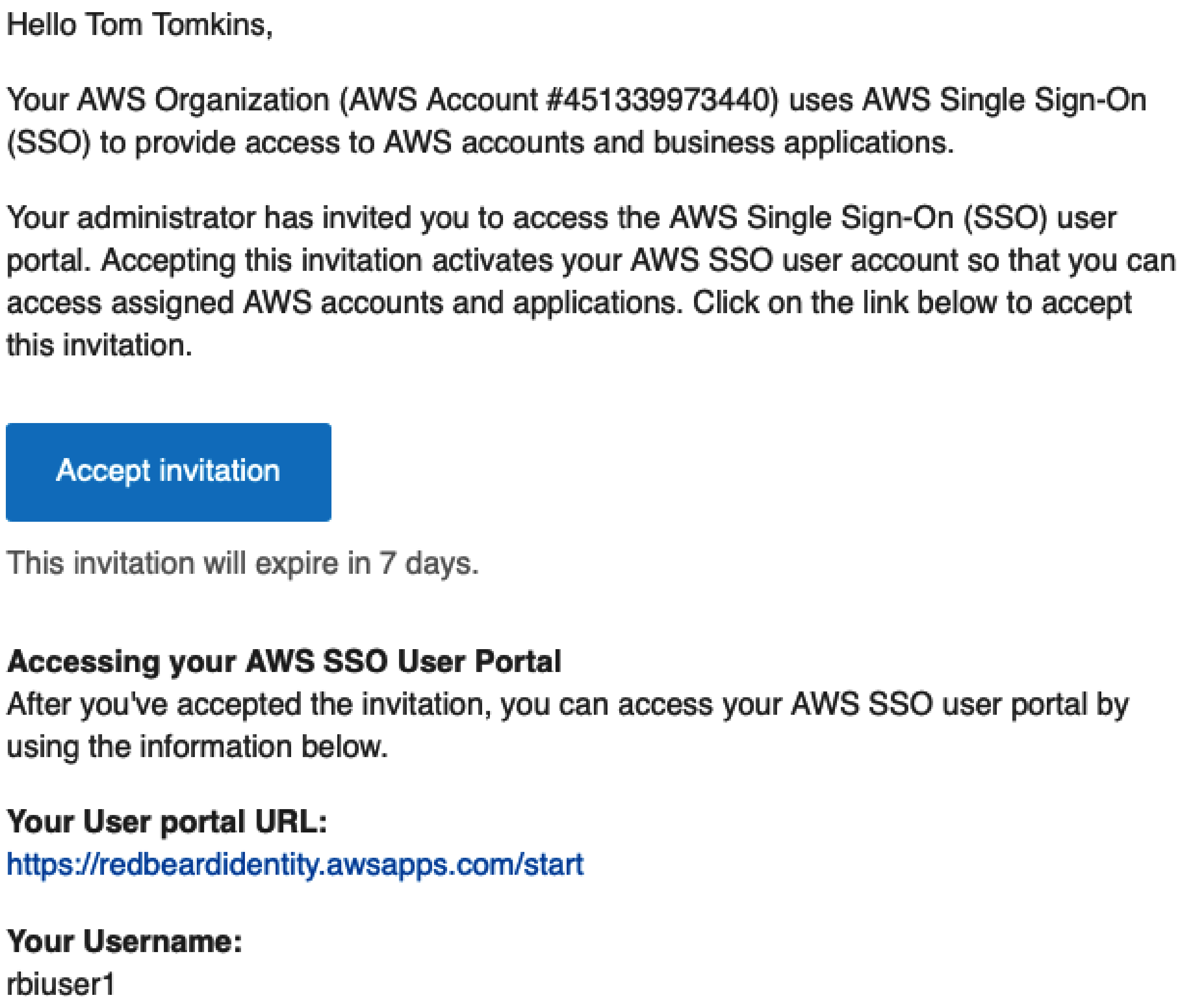
Users listed here can sign in to the user portal to access any AWS accounts or applications that you have assigned to them. Learn more

□ Display name	Username	Status	MFA devices
□ Bob Bobkins	rbiuser3	Enabled	None
□ Jon Jonkins	rbiuser2	Enabled	None
□ Tom Tomkins	rbiuser1	Enabled	None



Tom Tomkins

Username	rbiuser1
Primary email	redbeardidentity+rbiuser1@gmail.com (work) (not verified) | Send email verification link
First name	Tom
Last name	Tomkins
Display name	Tom Tomkins
Status	Enabled The user can sign in to the user portal to access their assigned AWS accounts and applications.
User ID	9067650dfa-bdaf7f4d-50db-44ff-9dd0-9aa5ca24f64b
Last updated	8 minutes ago
Updated By	Manual
Created	8 minutes ago
Created By	Manual



Hello Tom Tomkins,

Your AWS Organization (AWS Account #451339973440) uses AWS Single Sign-On (SSO) to provide access to AWS accounts and business applications.

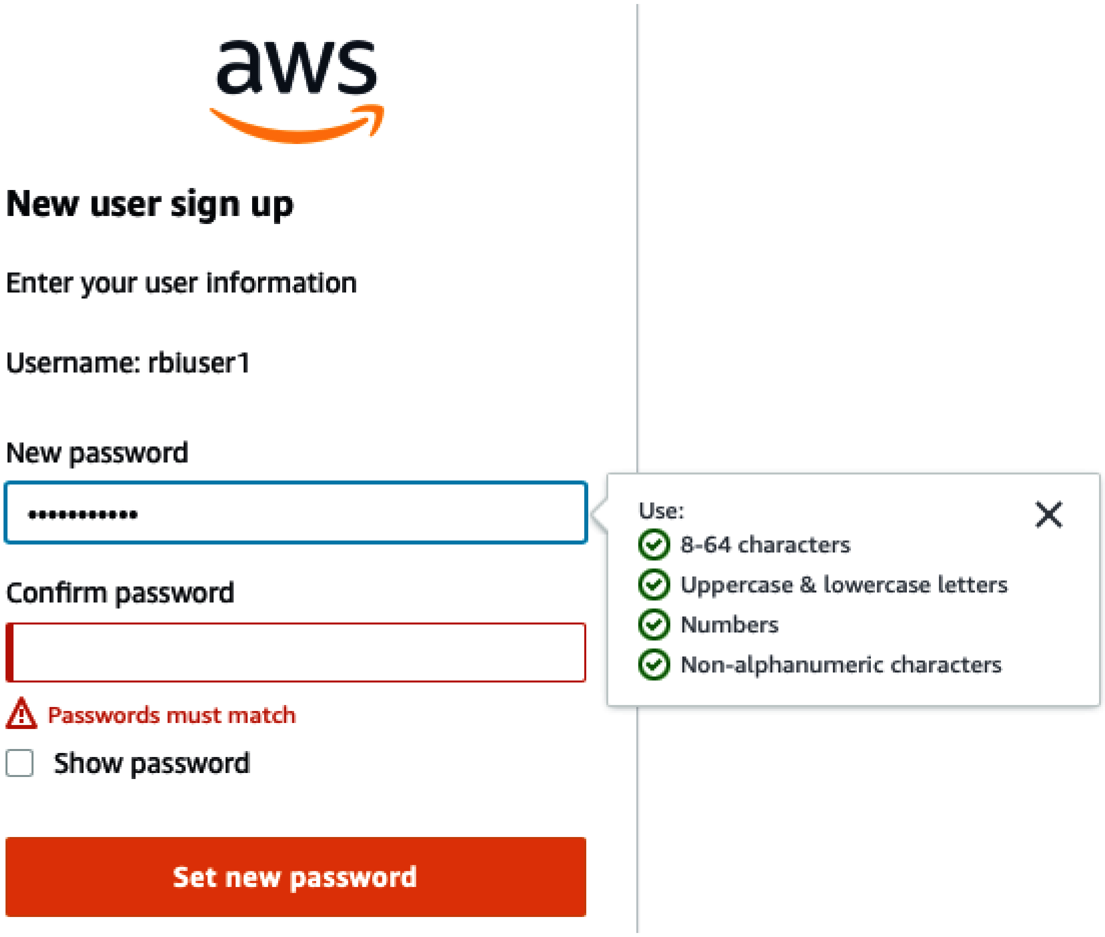
Your administrator has invited you to access the AWS Single Sign-On (SSO) user portal. Accepting this invitation activates your AWS SSO user account so that you can access assigned AWS accounts and applications. Click on the link below to accept this invitation.

This invitation will expire in 7 days.

Accessing your AWS SSO User Portal
After you've accepted the invitation, you can access your AWS SSO user portal by using the information below.

Your User portal URL:
https://redbeardidentity.awsapps.com/start

Your Username:
rbiuser1



New user sign up

Enter your user information

Username: rbiuser1

New password

••••••••••••

Confirm password

⚠ Passwords must match

□ Show password

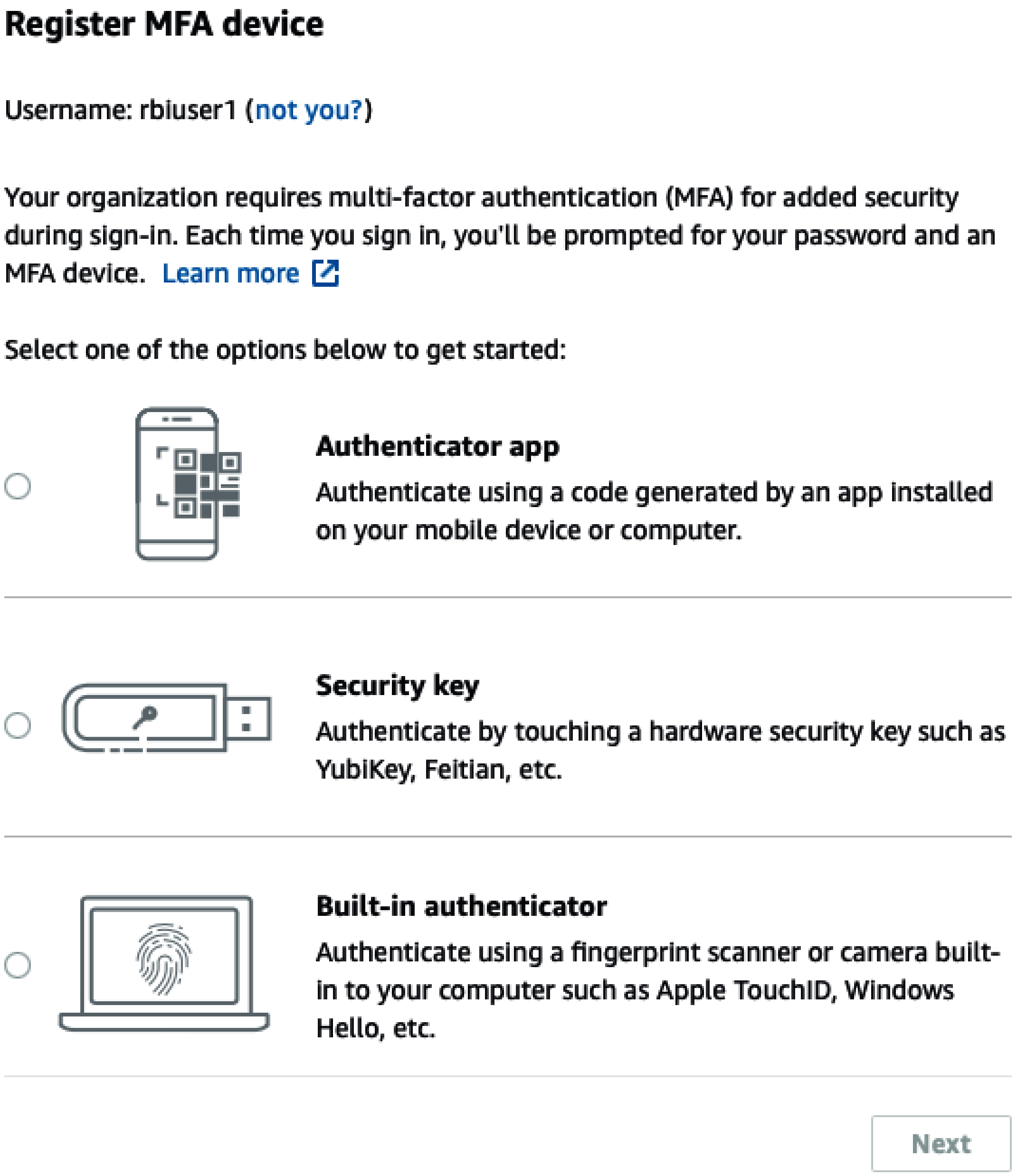
Use:

✓ 8-64 characters

✓ Uppercase & lowercase letters

✓ Numbers

✓ Non-alphanumeric characters



Register MFA device

Username: rbiuser1 (not you?)

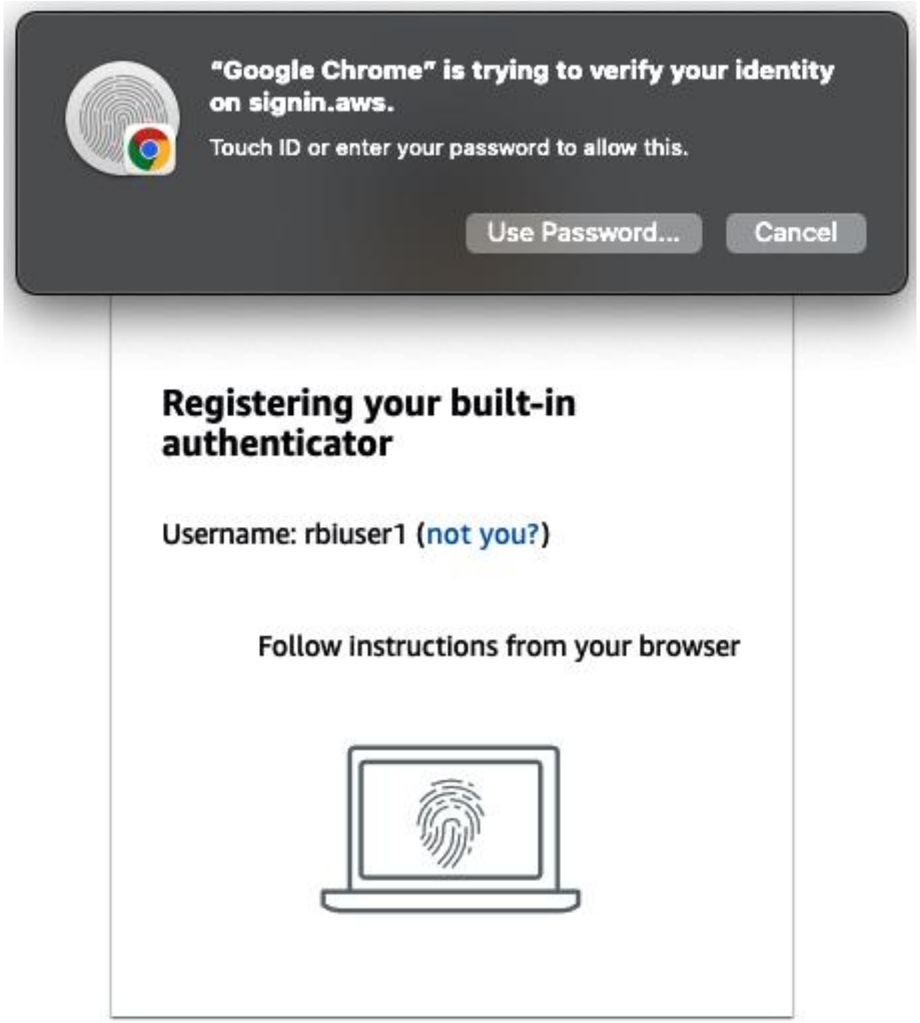
Your organization requires multi-factor authentication (MFA) for added security during sign-in. Each time you sign in, you'll be prompted for your password and an MFA device. Learn more

Select one of the options below to get started:

○ **Authenticator app**
Authenticate using a code generated by an app installed on your mobile device or computer.

○ **Security key**
Authenticate by touching a hardware security key such as YubiKey, Feitian, etc.

○ **Built-in authenticator**
Authenticate using a fingerprint scanner or camera built-in to your computer such as Apple TouchID, Windows Hello, etc.



"Google Chrome" is trying to verify your identity on signin.aws.

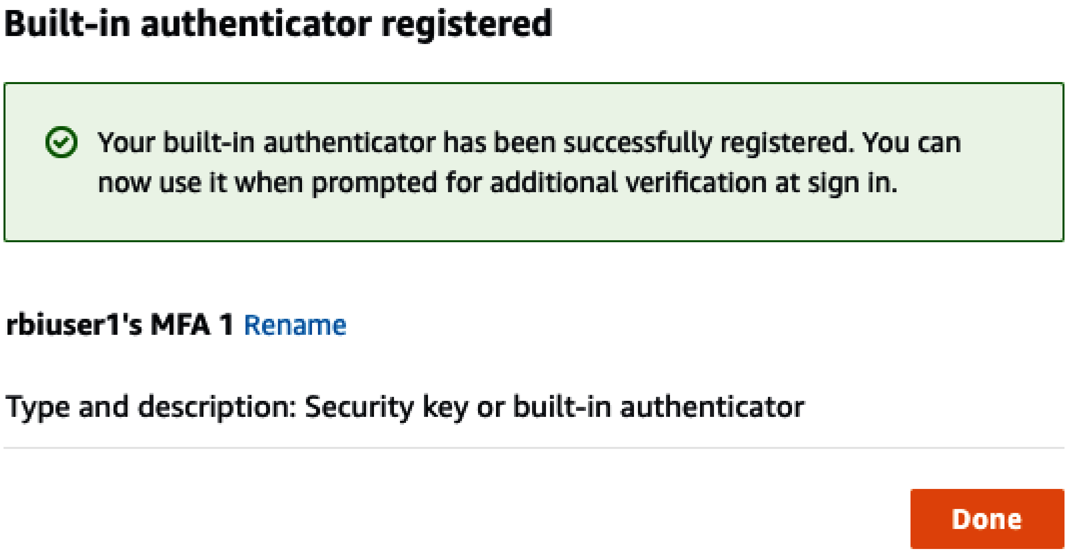
Touch ID or enter your password to allow this.

Use Password... Cancel

Registering your built-in authenticator

Username: rbiuser1 (not you?)

Follow instructions from your browser



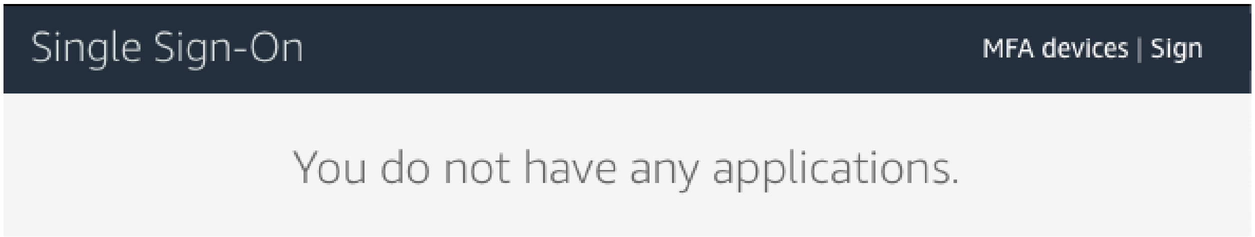
Built-in authenticator registered

Your built-in authenticator has been successfully registered. You can now use it when prompted for additional verification at sign in.

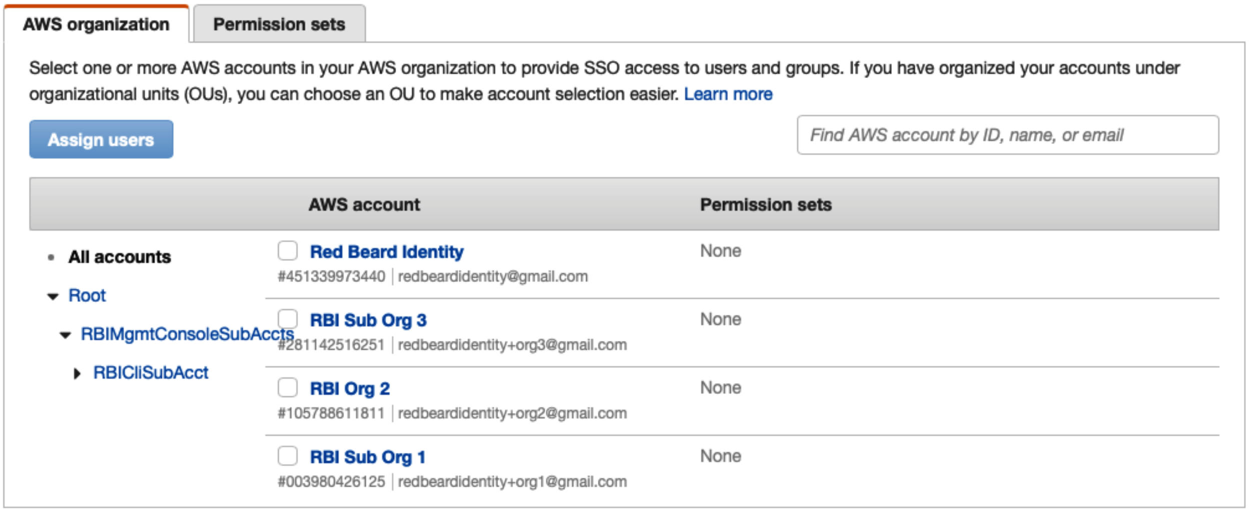
rbiuser1's MFA 1 Rename

Type and description: Security key or built-in authenticator

Done



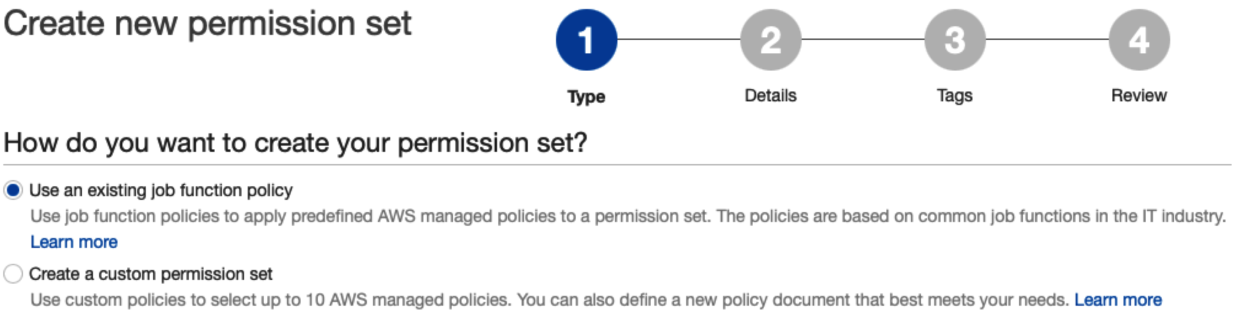
You do not have any applications.



Select one or more AWS accounts in your AWS organization to provide SSO access to users and groups. If you have organized your accounts under organizational units (OUs), you can choose an OU to make account selection easier. Learn more

- **All accounts**
- Root
  - RBIMgmtConsoleSubAccts
    - RBICliSubAcct

AWS account	Permission sets
□ **Red Beard Identity** #451339973440 | redbeardidentity@gmail.com	None
□ **RBI Sub Org 3** #281142516251 | redbeardidentity+org3@gmail.com	None
□ **RBI Org 2** #105788611811 | redbeardidentity+org2@gmail.com	None
□ **RBI Sub Org 1** #003980426125 | redbeardidentity+org1@gmail.com	None

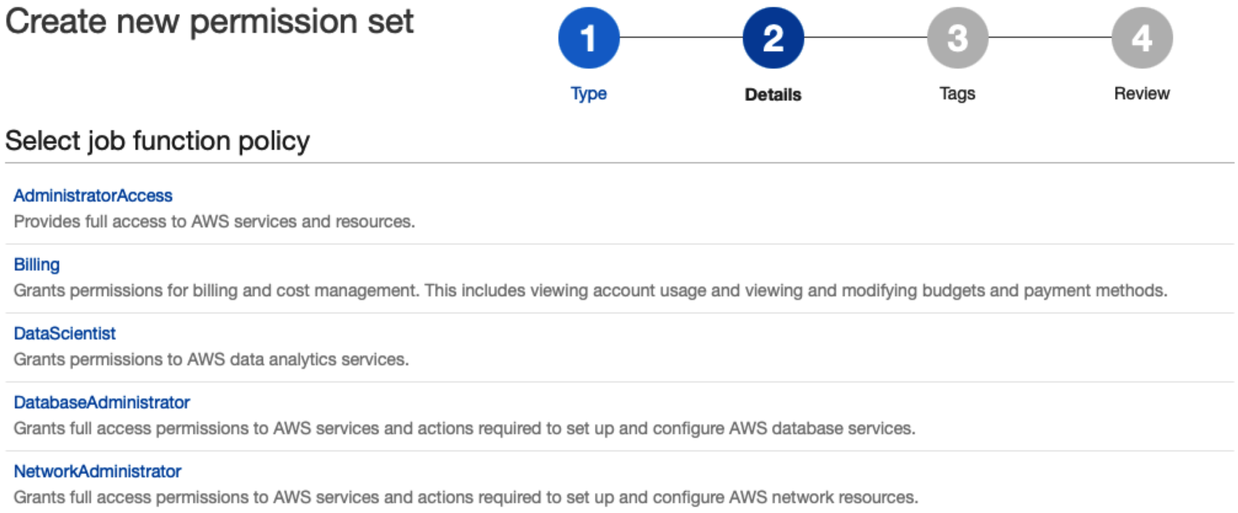


Create new permission set

How do you want to create your permission set?

● Use an existing job function policy
Use job function policies to apply predefined AWS managed policies to a permission set. The policies are based on common job functions in the IT industry. Learn more

○ Create a custom permission set
Use custom policies to select up to 10 AWS managed policies. You can also define a new policy document that best meets your needs. Learn more



Create new permission set

Select job function policy

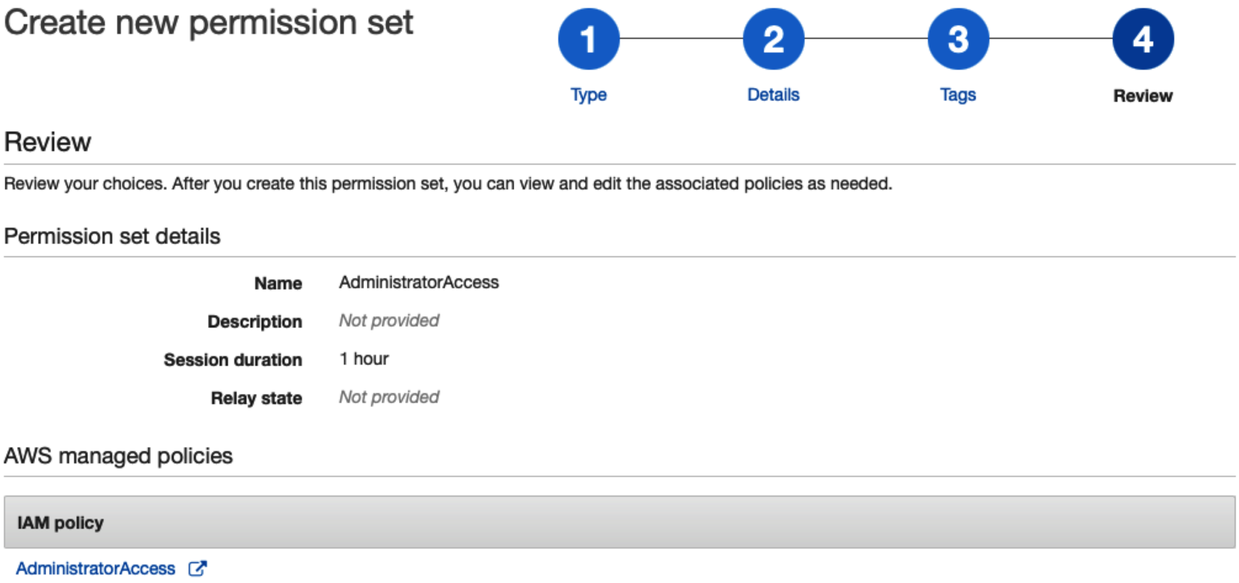
AdministratorAccess
Provides full access to AWS services and resources.

Billing
Grants permissions for billing and cost management. This includes viewing account usage and viewing and modifying budgets and payment methods.

DataScientist
Grants permissions to AWS data analytics services.

DatabaseAdministrator
Grants full access permissions to AWS services and actions required to set up and configure AWS database services.

NetworkAdministrator
Grants full access permissions to AWS services and actions required to set up and configure AWS network resources.



Create new permission set

Review

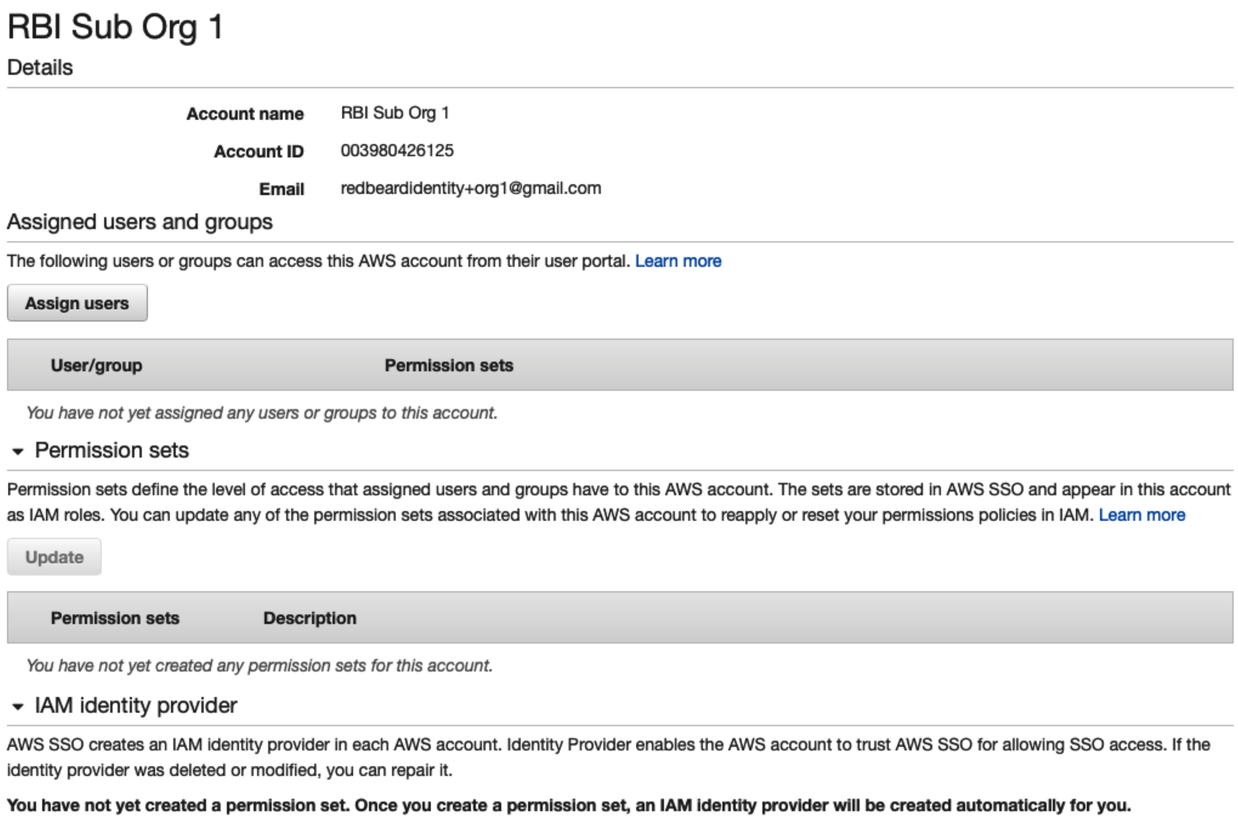
Review your choices. After you create this permission set, you can view and edit the associated policies as needed.

Permission set details

Name	AdministratorAccess
Description	*Not provided*
Session duration	1 hour
Relay state	*Not provided*

AWS managed policies

IAM policy
AdministratorAccess



RBI Sub Org 1

Details

Account name	RBI Sub Org 1
Account ID	003980426125
Email	redbeardidentity+org1@gmail.com

Assigned users and groups

The following users or groups can access this AWS account from their user portal. Learn more

User/group	Permission sets

You have not yet assigned any users or groups to this account.

▾ Permission sets

Permission sets define the level of access that assigned users and groups have to this AWS account. The sets are stored in AWS SSO and appear in this account as IAM roles. You can update any of the permission sets associated with this AWS account to reapply or reset your permissions policies in IAM. Learn more

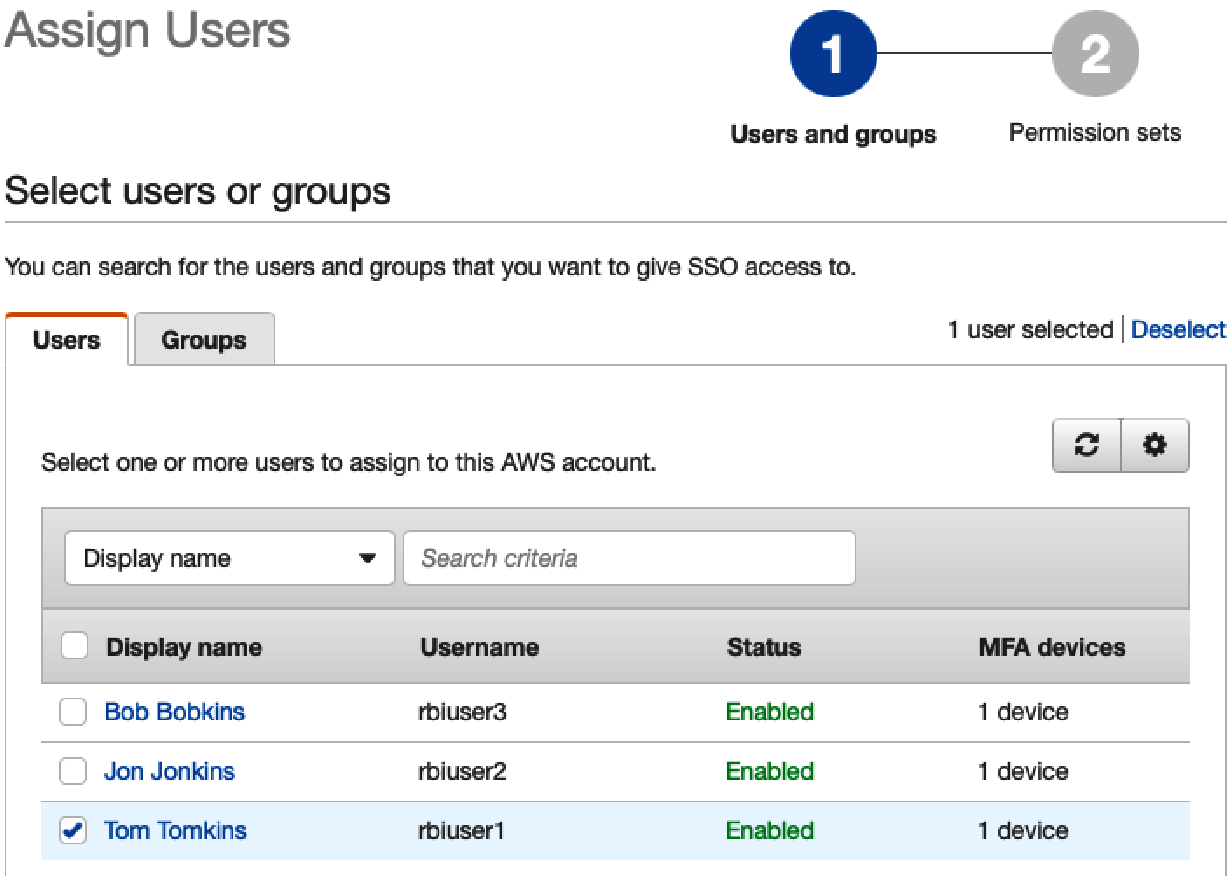
Permission sets	Description

You have not yet created any permission sets for this account.

▾ IAM identity provider

AWS SSO creates an IAM identity provider in each AWS account. Identity Provider enables the AWS account to trust AWS SSO for allowing SSO access. If the identity provider was deleted or modified, you can repair it.

You have not yet created a permission set. Once you create a permission set, an IAM identity provider will be created automatically for you.



Assign Users

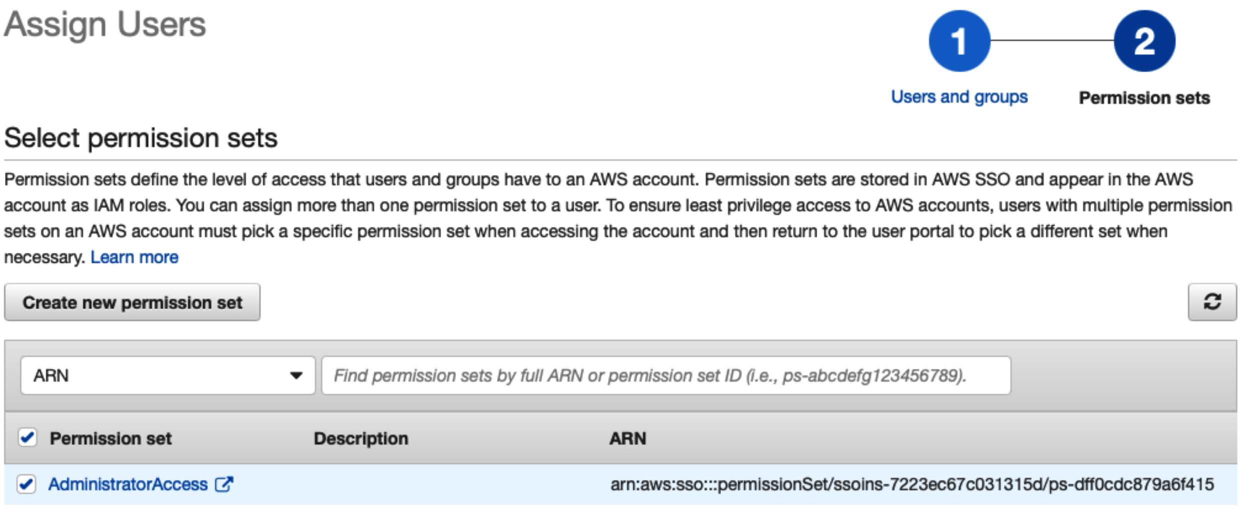
Select users or groups

You can search for the users and groups that you want to give SSO access to.

1 user selected | Deselect

Select one or more users to assign to this AWS account.

□	Display name	Username	Status	MFA devices
□	Bob Bobkins	rbiuser3	Enabled	1 device
□	Jon Jonkins	rbiuser2	Enabled	1 device
☑	Tom Tomkins	rbiuser1	Enabled	1 device



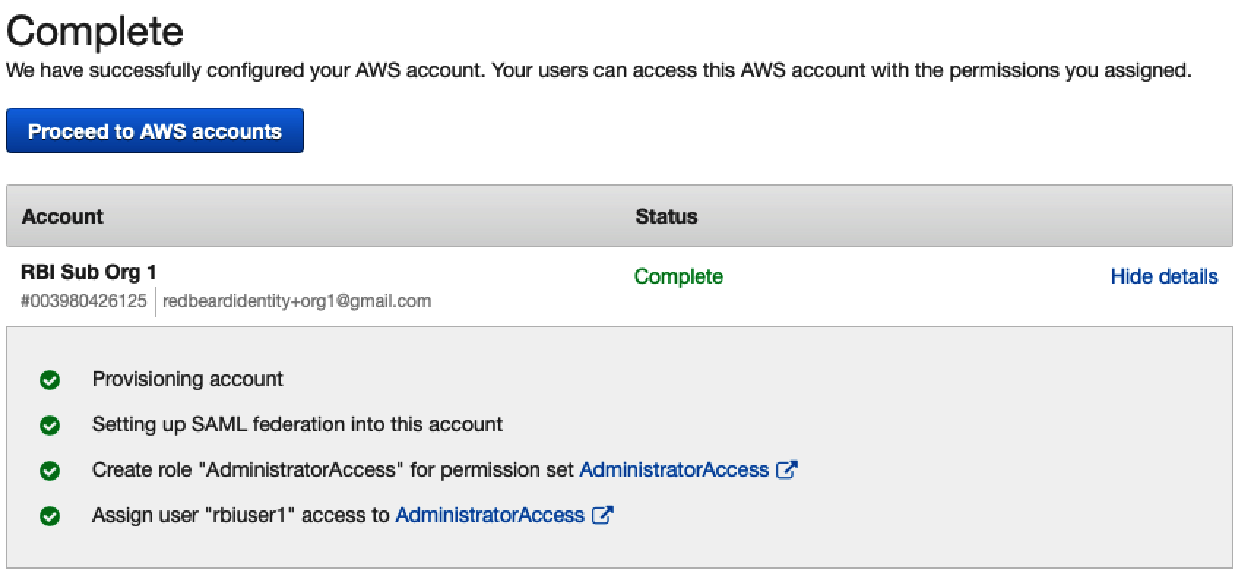
Assign Users

Select permission sets

Permission sets define the level of access that users and groups have to an AWS account. Permission sets are stored in AWS SSO and appear in the AWS account as IAM roles. You can assign more than one permission set to a user. To ensure least privilege access to AWS accounts, users with multiple permission sets on an AWS account must pick a specific permission set when accessing the account and then return to the user portal to pick a different set when necessary. Learn more

Create new permission set
ARN ▾
Find permission sets by full ARN or permission set ID (i.e., ps-abcdefg123456789).

☑	Permission set	Description	ARN
☑	AdministratorAccess		arn:aws:sso:::permissionSet/ssoins-7223ec67c031315d/ps-dff0cdc879a6f415

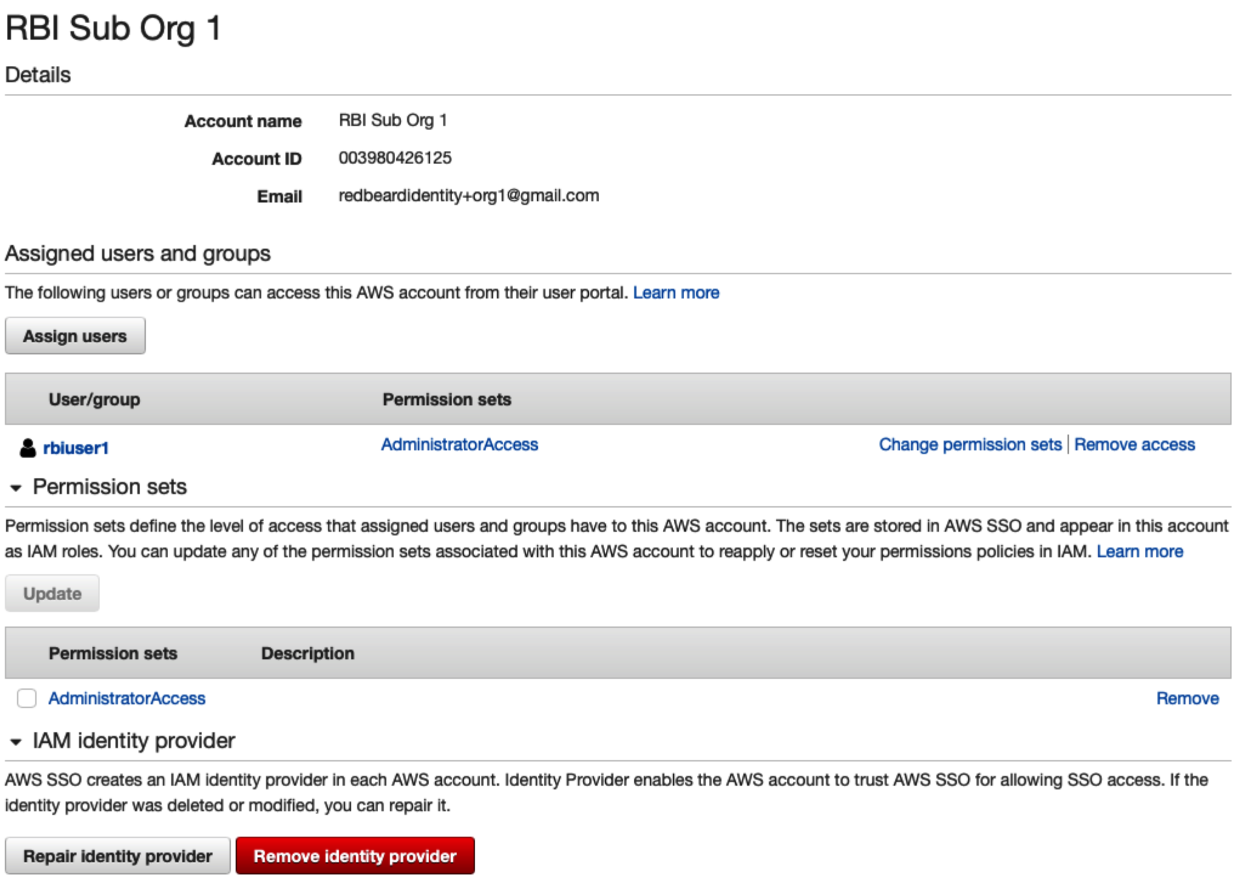


Complete

We have successfully configured your AWS account. Your users can access this AWS account with the permissions you assigned.

Account	Status	
RBI Sub Org 1 #003980426125 | redbeardidentity+org1@gmail.com	Complete	Hide details

- ✓ Provisioning account
- ✓ Setting up SAML federation into this account
- ✓ Create role "AdministratorAccess" for permission set AdministratorAccess
- ✓ Assign user "rbiuser1" access to AdministratorAccess



RBI Sub Org 1

Details

Account name	RBI Sub Org 1
Account ID	003980426125
Email	redbeardidentity+org1@gmail.com

Assigned users and groups

The following users or groups can access this AWS account from their user portal. Learn more

User/group	Permission sets	
rbiuser1	AdministratorAccess	Change permission sets | Remove access

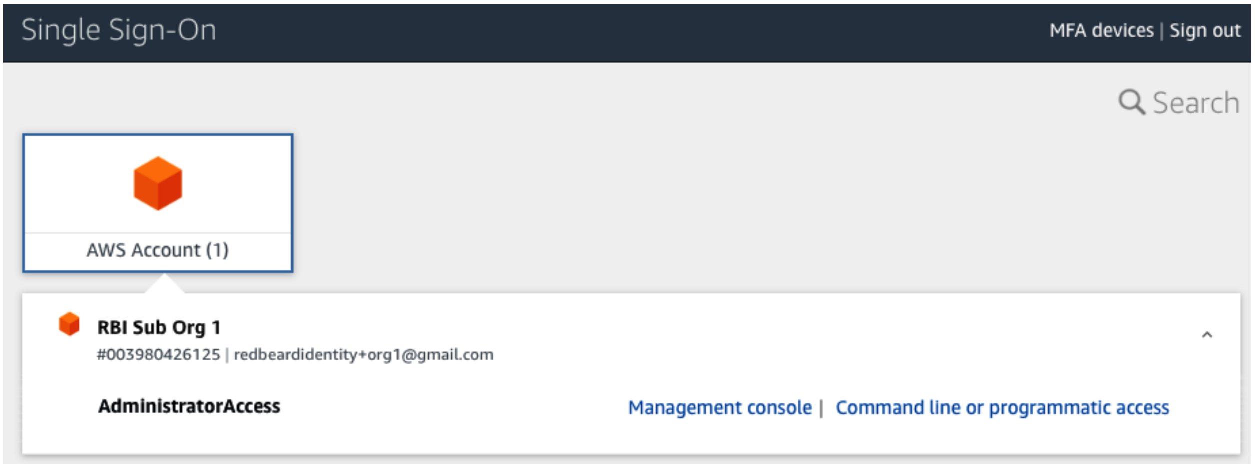
▾ Permission sets

Permission sets define the level of access that assigned users and groups have to this AWS account. The sets are stored in AWS SSO and appear in this account as IAM roles. You can update any of the permission sets associated with this AWS account to reapply or reset your permissions policies in IAM. Learn more

Permission sets	Description	
□ AdministratorAccess		Remove

▾ IAM identity provider

AWS SSO creates an IAM identity provider in each AWS account. Identity Provider enables the AWS account to trust AWS SSO for allowing SSO access. If the identity provider was deleted or modified, you can repair it.



Single Sign-On

MFA devices | Sign out

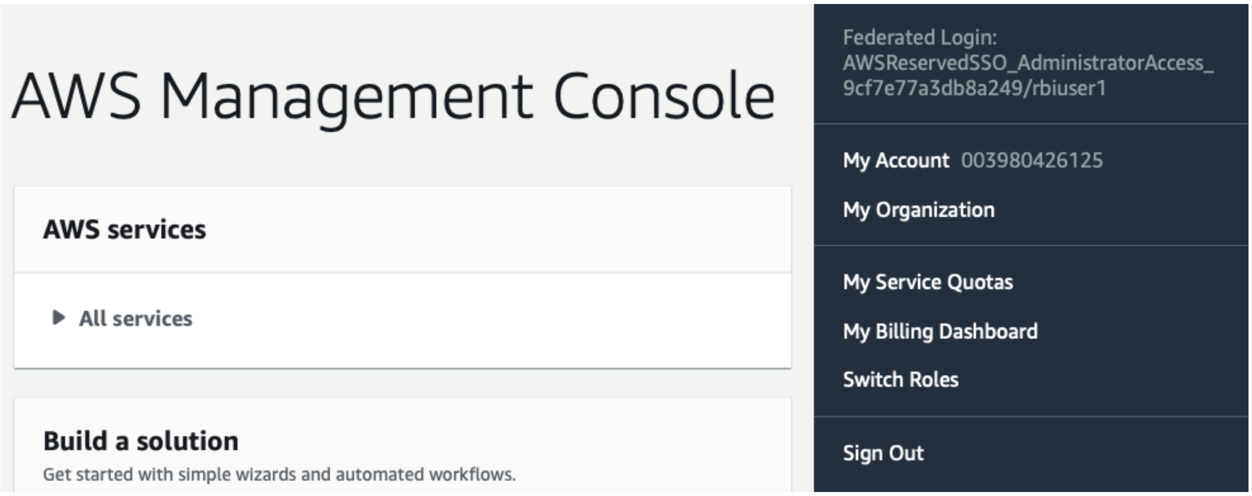
Search

AWS Account (1)

RBI Sub Org 1
#003980426125 | redbeardidentity+org1@gmail.com

AdministratorAccess

Management console | Command line or programmatic access



AWS Management Console

AWS services

▶ All services

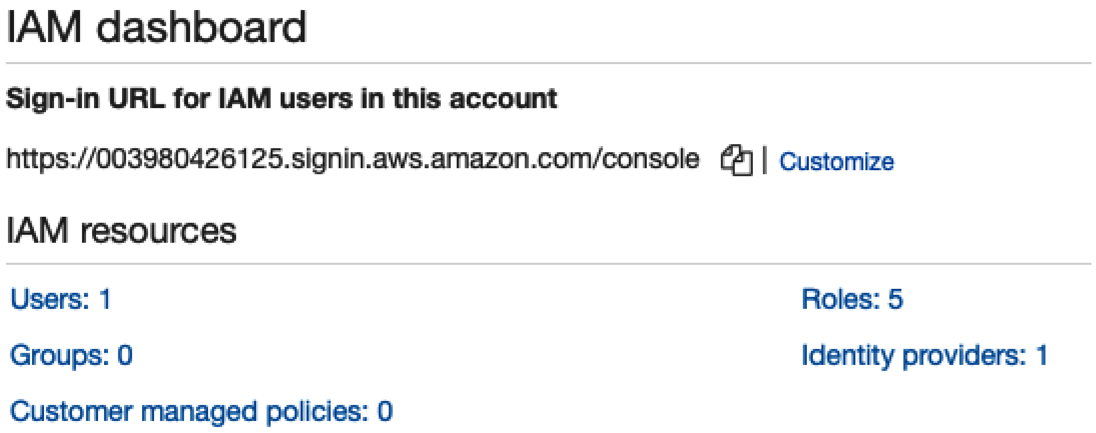
Build a solution
Get started with simple wizards and automated workflows.

Federated Login:
AWSReservedSSO_AdministratorAccess_
9cf7e77a3db8a249/rbiuser1

My Account 003980426125
My Organization

My Service Quotas
My Billing Dashboard
Switch Roles

Sign Out



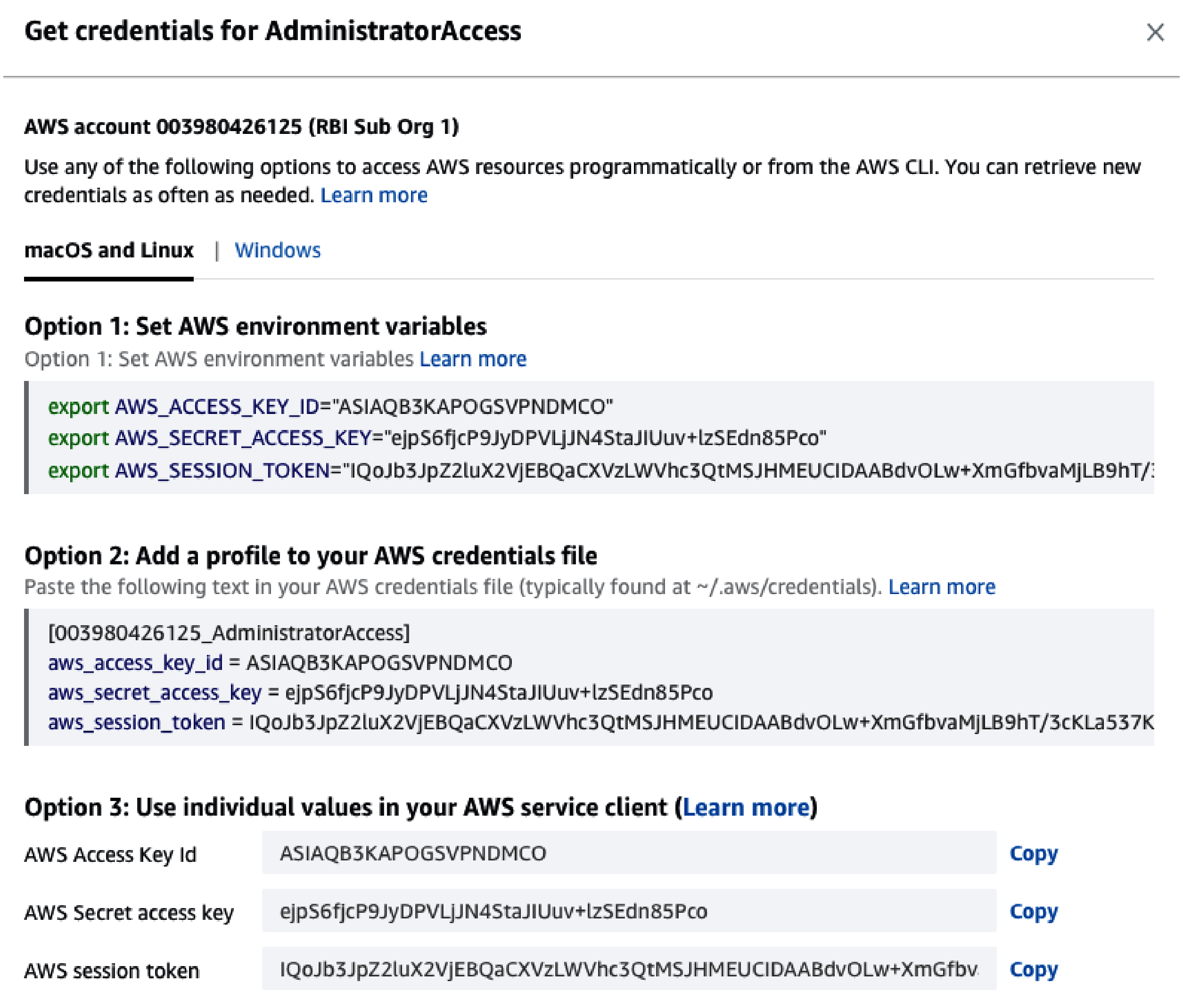
IAM dashboard

Sign-in URL for IAM users in this account

https://003980426125.signin.aws.amazon.com/console | Customize

IAM resources

Users: 1	Roles: 5
Groups: 0	Identity providers: 1
Customer managed policies: 0	



Get credentials for AdministratorAccess

AWS account 003980426125 (RBI Sub Org 1)

Use any of the following options to access AWS resources programmatically or from the AWS CLI. You can retrieve new credentials as often as needed. Learn more

Option 1: Set AWS environment variables

Option 1: Set AWS environment variables Learn more

```
export AWS_ACCESS_KEY_ID="ASIAQB3KAPOGSVPNDMCO"
export AWS_SECRET_ACCESS_KEY="ejpS6fjcP9JyDPVLjJN4StaJIUuv+lzSEdn85Pco"
export AWS_SESSION_TOKEN="IQoJb3JpZ2luX2VjEBQaCXVzLWVhc3QtMSJHMEUCIDAABdvOLw+XmGfbvaMjLB9hT/3
```

Option 2: Add a profile to your AWS credentials file

Paste the following text in your AWS credentials file (typically found at ~/.aws/credentials). Learn more

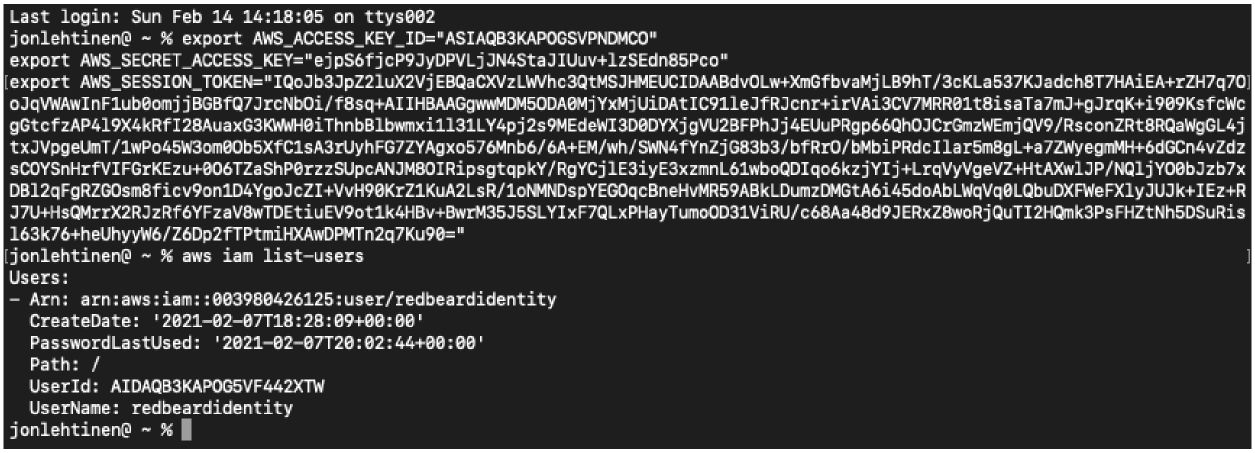
```
[003980426125_AdministratorAccess]
aws_access_key_id = ASIAQB3KAPOGSVPNDMCO
aws_secret_access_key = ejpS6fjcP9JyDPVLjJN4StaJIUuv+lzSEdn85Pco
aws_session_token = IQoJb3JpZ2luX2VjEBQaCXVzLWVhc3QtMSJHMEUCIDAABdvOLw+XmGfbvaMjLB9hT/3cKLa537K
```

Option 3: Use individual values in your AWS service client (Learn more)

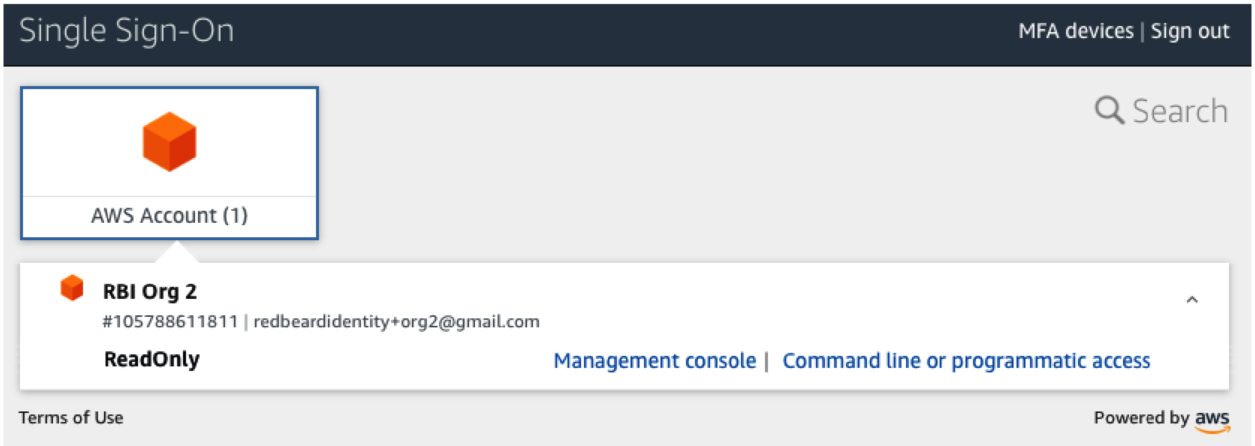
AWS Access Key Id: ASIAQB3KAPOGSVPNDMCO

AWS Secret access key: ejpS6fjcP9JyDPVLjJN4StaJIUuv+lzSEdn85Pco

AWS session token: IQoJb3JpZ2luX2VjEBQaCXVzLWVhc3QtMSJHMEUCIDAABdvOLw+XmGfbv



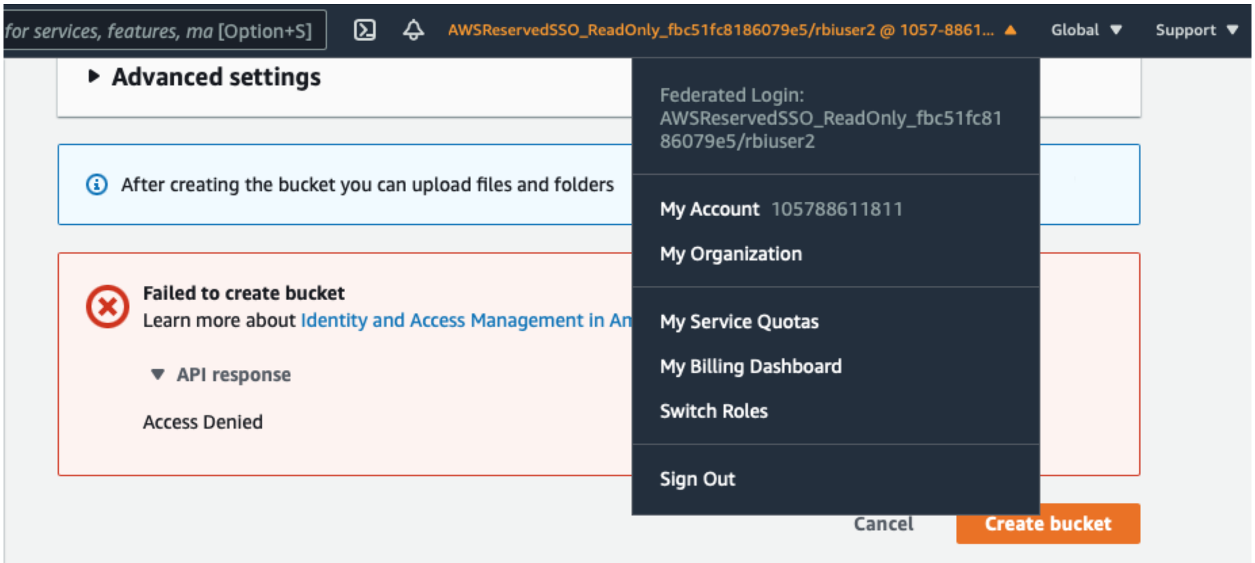
```
Last login: Sun Feb 14 14:18:05 on ttys002
jonlehtinen@ ~ % export AWS_ACCESS_KEY_ID="ASIAQB3KAPOGSVPNDMCO"
export AWS_SECRET_ACCESS_KEY="ejpS6fjcP9JyDPVLjJN4StaJIUuv+lzSEdn85Pco"
[export AWS_SESSION_TOKEN="IQoJb3JpZ2luX2VjEBQaCXVzLWVhc3QtMSJHMEUCIDAABdvOLw+XmGfbvaMjLB9hT/3cKLa537KJadch8T7HAiEA+rZH7q7O]
oJqVWAwInF1ub0omjjBGBfQ7JrcNbOi/f8sq+AIIHBAAGgwwMDM5ODA0MjYxMjUiDAtIC91leJfRJcnr+irVAi3CV7MRR01t8isaTa7mJ+gJrqK+i909KsfcWc
gGtcfzAP4l9X4kRfI28AuaxG3KWWH0iThnbBlbwmxi1l31LY4pj2s9MEdeWI3D0DYXjgVU2BFPhJj4EUuPRgp66QhOJCrGmzWEmjQV9/RsconZRt8RQaWgGL4j
txJVpgeUmT/1wPo45W3om0Ob5XfC1sA3rUyhFG7ZYAgxo576Mnb6/6A+EM/wh/SWN4fYnZjG83b3/bfRrO/bMbiPRdcIlar5m8gL+a7ZWyegmMH+6dGCn4vZdz
sCOYSnHrfVIFGrKEzu+0O6TZaShP0rzzSUpcANJM8OIRipsgtqpkY/RgYCjlE3iyE3xzmnL61wboQDIqo6kzjYIj+LrqVyVgeVZ+HtAXwlJP/NQljYO0bJzb7x
DBl2qFgRZGOsm8ficv9on1D4YgoJcZI+VvH90KrZ1KuA2LsR/1oNMNDspYEGOqcBneHvMR59ABkLDumzDMGtA6i45doAbLWqVq0LQbuDXFWeFXlyJUJk+IEz+R
J7U+HsQMrrX2RJzRf6YFzaV8wTDEtiuEV9ot1k4HBv+BwrM35J5SLYIxF7QLxPHayTumoOD31ViRU/c68Aa48d9JERxZ8woRjQuTI2HQmk3PsFHZtNh5DSuRis
l63k76+heUhyyW6/Z6Dp2fTPtmiHXAwDPMTn2q7Ku90="
[jonlehtinen@ ~ % aws iam list-users                                                                                        ]
Users:
- Arn: arn:aws:iam::003980426125:user/redbeardidentity
  CreateDate: '2021-02-07T18:28:09+00:00'
  PasswordLastUsed: '2021-02-07T20:02:44+00:00'
  Path: /
  UserId: AIDAQB3KAPOG5VF442XTW
  UserName: redbeardidentity
jonlehtinen@ ~ % 
```



RBI Org 2

#105788611811 | redbeardidentity+org2@gmail.com

ReadOnly


for services, features, ma [Option+S]
AWSReservedSSO_ReadOnly_fbc51fc8186079e5/rbiuser2 @ 1057-8861...
Global
Support
Advanced settings

After creating the bucket you can upload files and folders

Failed to create bucket

Learn more about Identity and Access Management in An

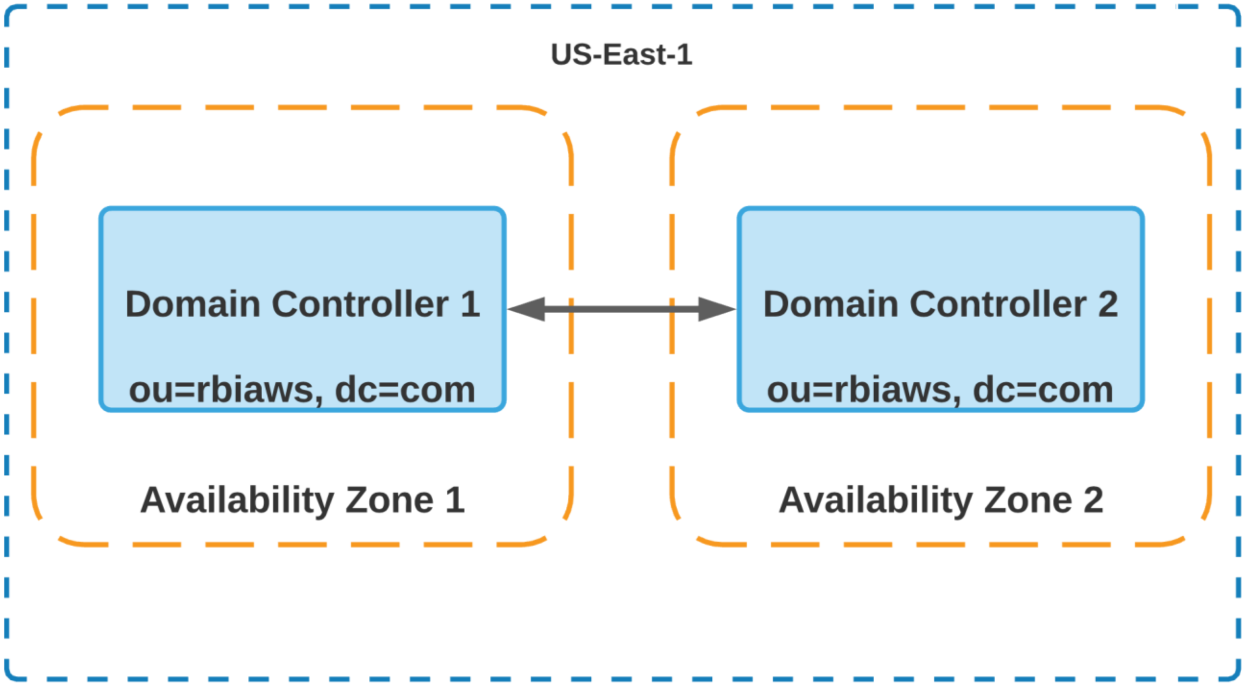
API response

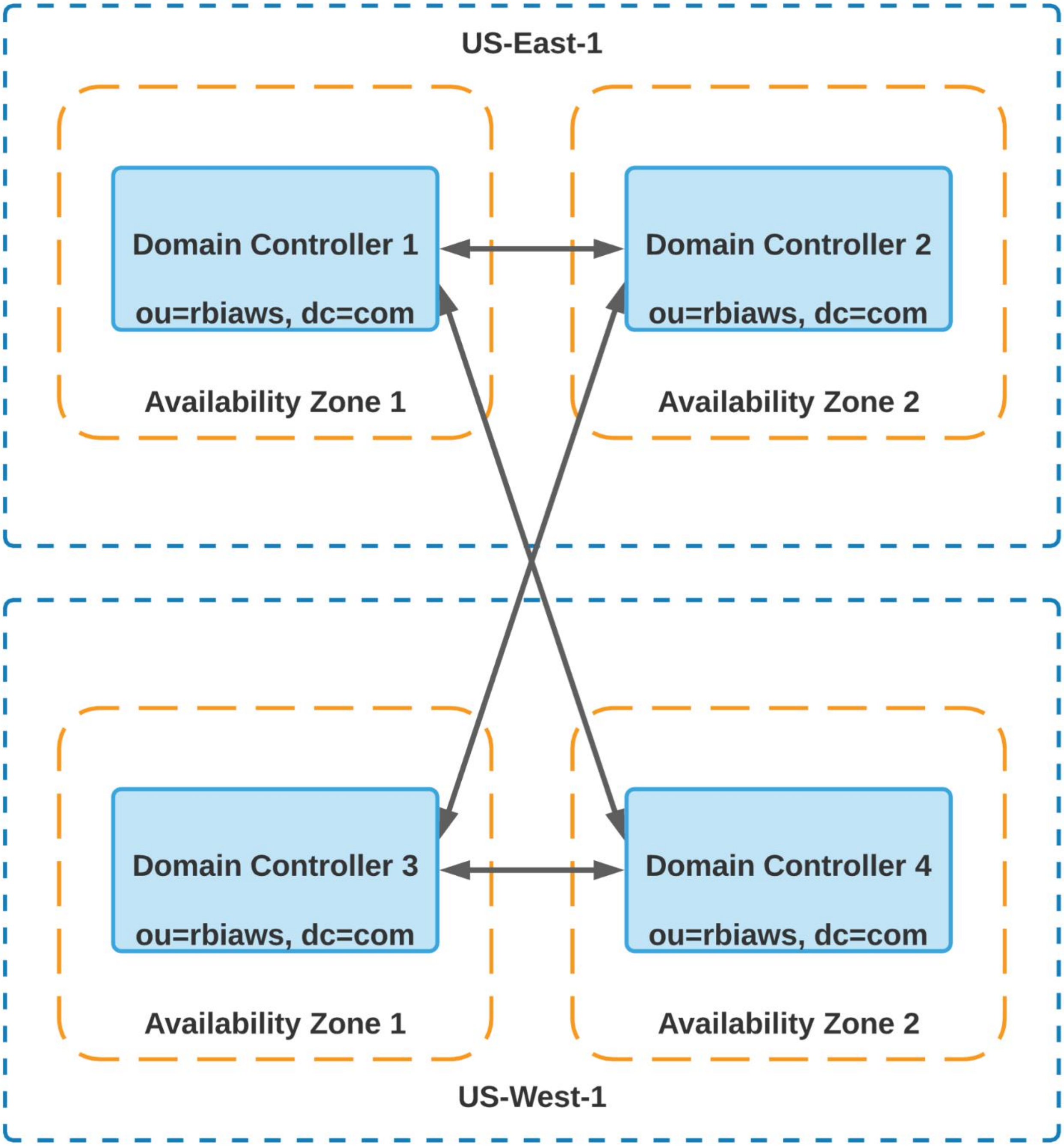
Access Denied

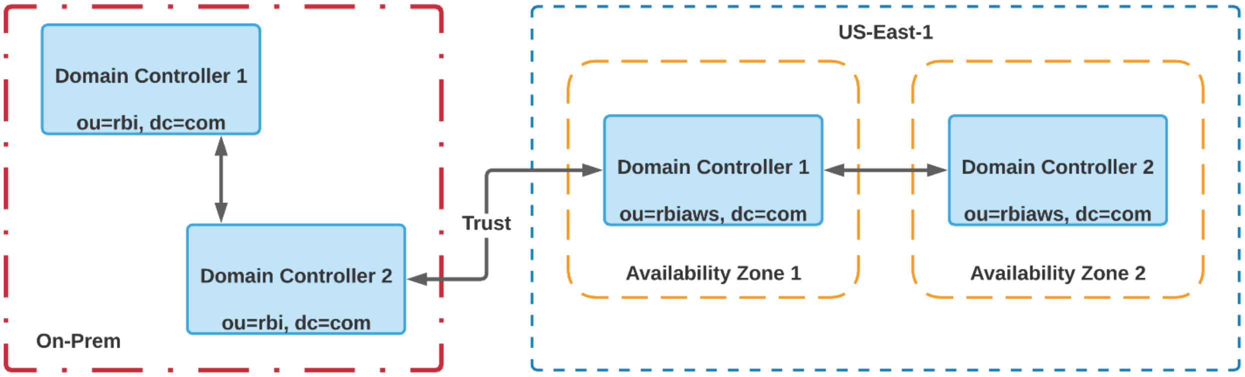
Federated Login: AWSReservedSSO_ReadOnly_fbc51fc8186079e5/rbiuser2

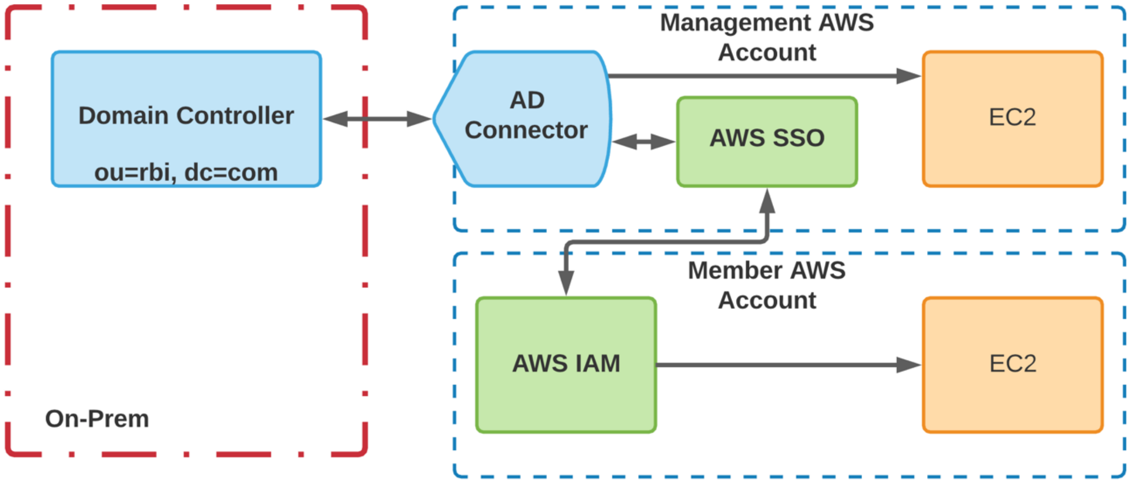
My Account 105788611811

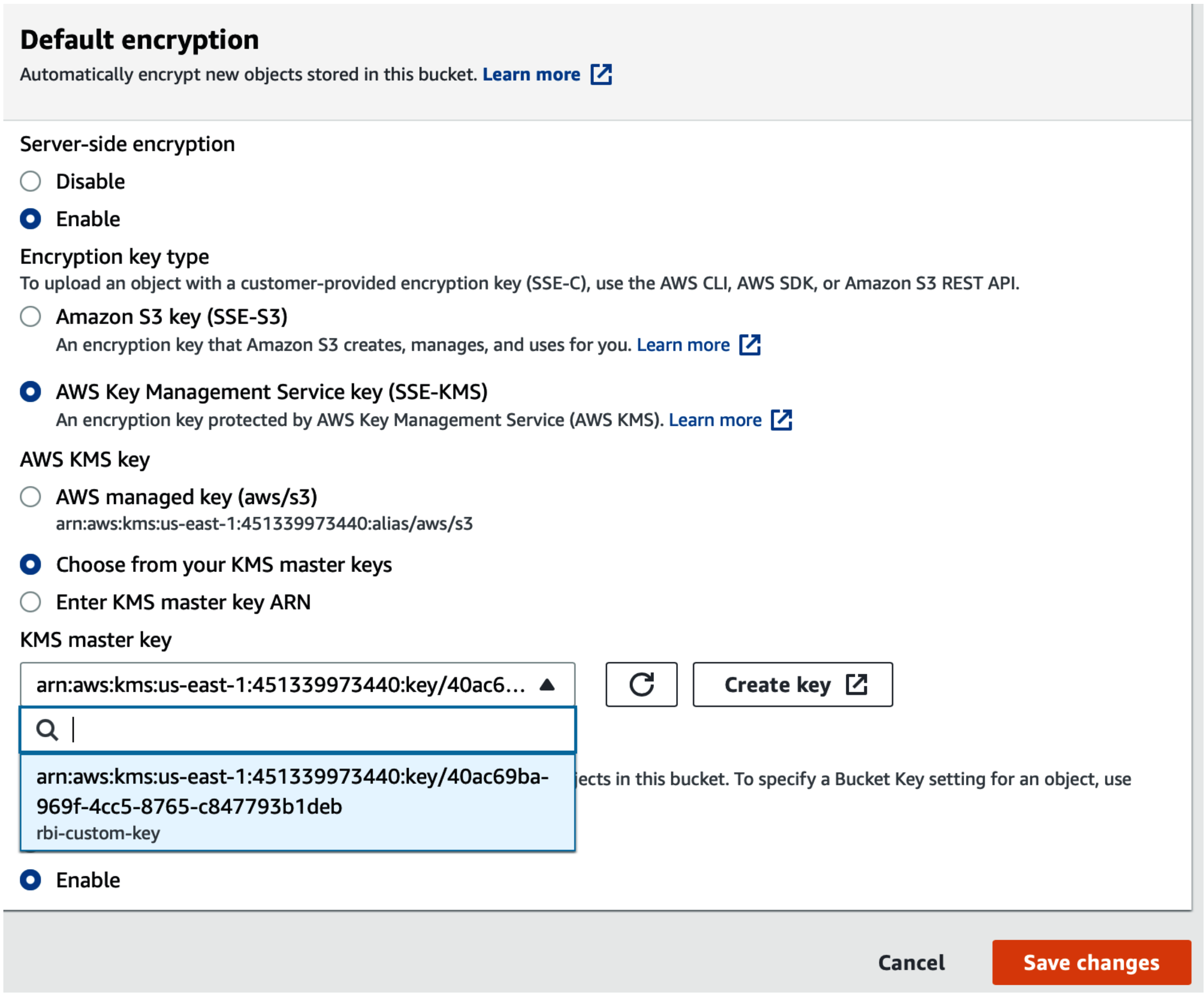
Chapter 7: Other AWS Identity Services




US-East-1
Domain Controller 1
ou=rbiaws, dc=com
Domain Controller 2
ou=rbiaws, dc=com
Availability Zone 1
Availability Zone 2
Domain Controller 3
ou=rbiaws, dc=com
Domain Controller 4
ou=rbiaws, dc=com
Availability Zone 1
Availability Zone 2
US-West-1


Domain Controller 1
ou=rbi, dc=com
Domain Controller 2
ou=rbi, dc=com
On-Prem
Trust
US-East-1
Domain Controller 1
ou=rbiaws, dc=com
Availability Zone 1
Domain Controller 2
ou=rbiaws, dc=com
Availability Zone 2


Domain Controller
ou=rbi, dc=com
On-Prem
Management AWS Account
AD Connector
AWS SSO
EC2
Member AWS Account
AWS IAM
EC2



Default encryption

Automatically encrypt new objects stored in this bucket. Learn more

Server-side encryption

○ Disable

● Enable

Encryption key type

To upload an object with a customer-provided encryption key (SSE-C), use the AWS CLI, AWS SDK, or Amazon S3 REST API.

○ Amazon S3 key (SSE-S3)

An encryption key that Amazon S3 creates, manages, and uses for you. Learn more

● AWS Key Management Service key (SSE-KMS)

An encryption key protected by AWS Key Management Service (AWS KMS). Learn more

AWS KMS key

○ AWS managed key (aws/s3)

arn:aws:kms:us-east-1:451339973440:alias/aws/s3

● Choose from your KMS master keys

○ Enter KMS master key ARN

KMS master key

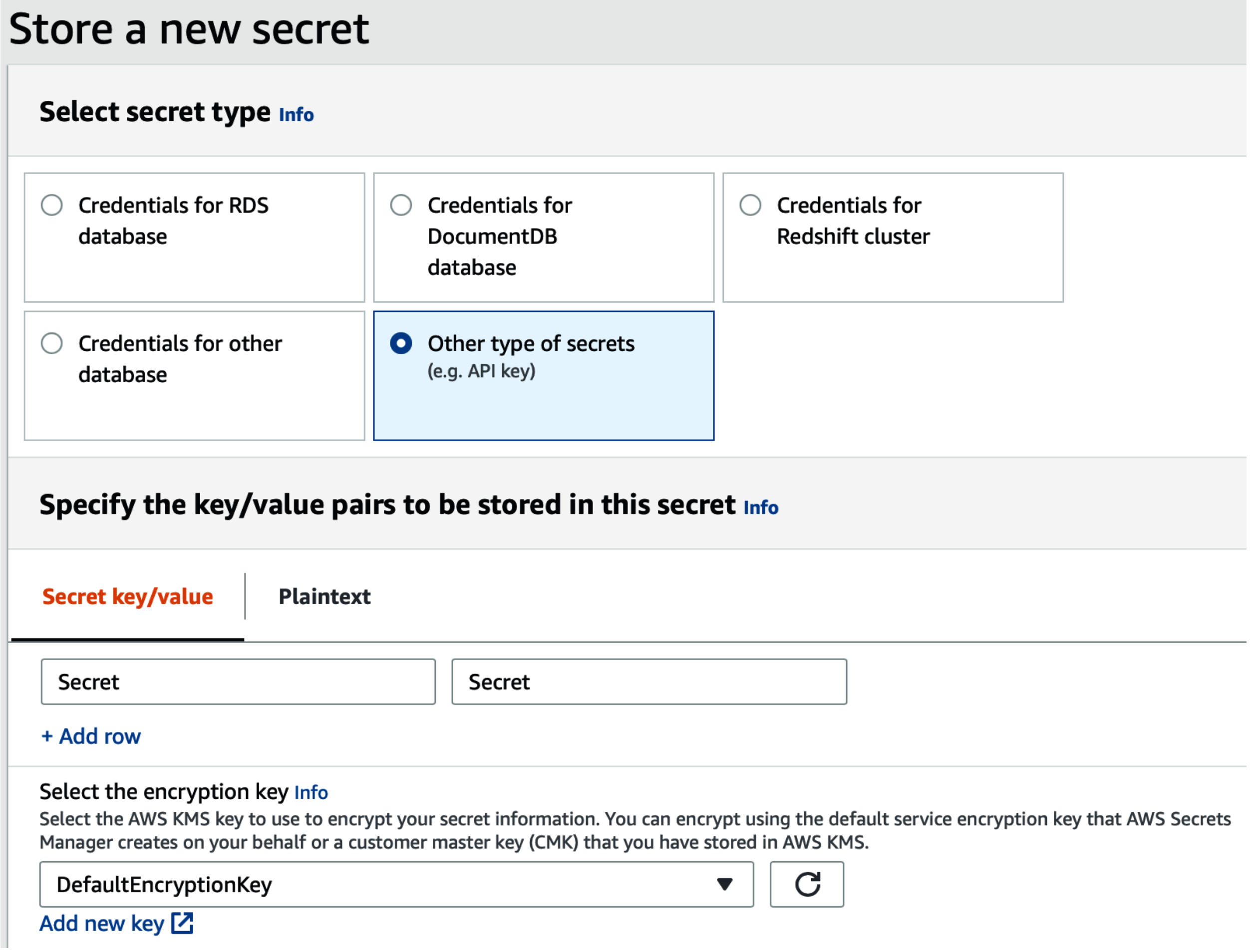
arn:aws:kms:us-east-1:451339973440:key/40ac6…

arn:aws:kms:us-east-1:451339973440:key/40ac69ba-969f-4cc5-8765-c847793b1deb

rbi-custom-key

jects in this bucket. To specify a Bucket Key setting for an object, use

● Enable



Store a new secret

Select secret type Info

○ Credentials for RDS database

○ Credentials for DocumentDB database

○ Credentials for Redshift cluster

○ Credentials for other database

● Other type of secrets (e.g. API key)

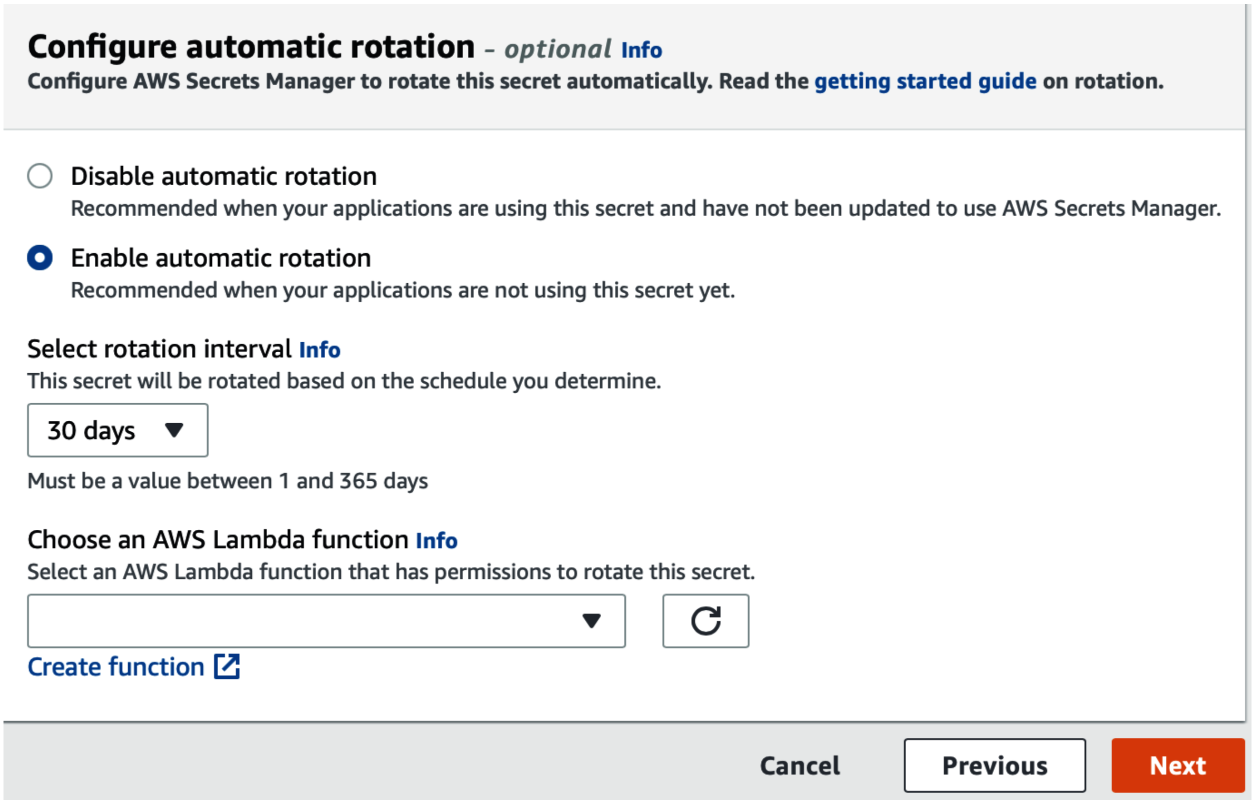
Specify the key/value pairs to be stored in this secret Info

Secret	Secret

Select the encryption key Info

Select the AWS KMS key to use to encrypt your secret information. You can encrypt using the default service encryption key that AWS Secrets Manager creates on your behalf or a customer master key (CMK) that you have stored in AWS KMS.

DefaultEncryptionKey ▼



Configure automatic rotation - *optional* Info

Configure AWS Secrets Manager to rotate this secret automatically. Read the getting started guide on rotation.

○ Disable automatic rotation
Recommended when your applications are using this secret and have not been updated to use AWS Secrets Manager.

● Enable automatic rotation
Recommended when your applications are not using this secret yet.

Select rotation interval Info
This secret will be rotated based on the schedule you determine.

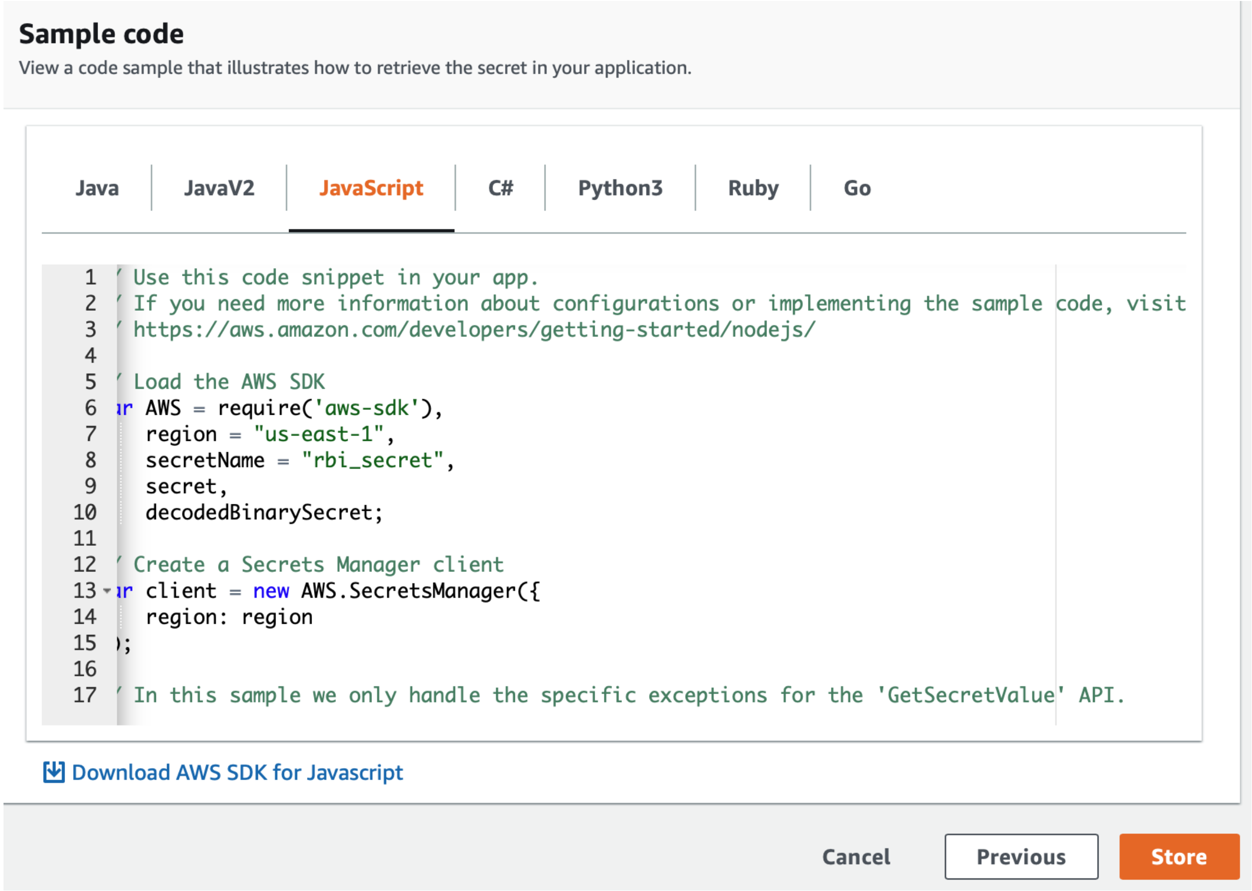
30 days ▼

Must be a value between 1 and 365 days

Choose an AWS Lambda function Info
Select an AWS Lambda function that has permissions to rotate this secret.

▼

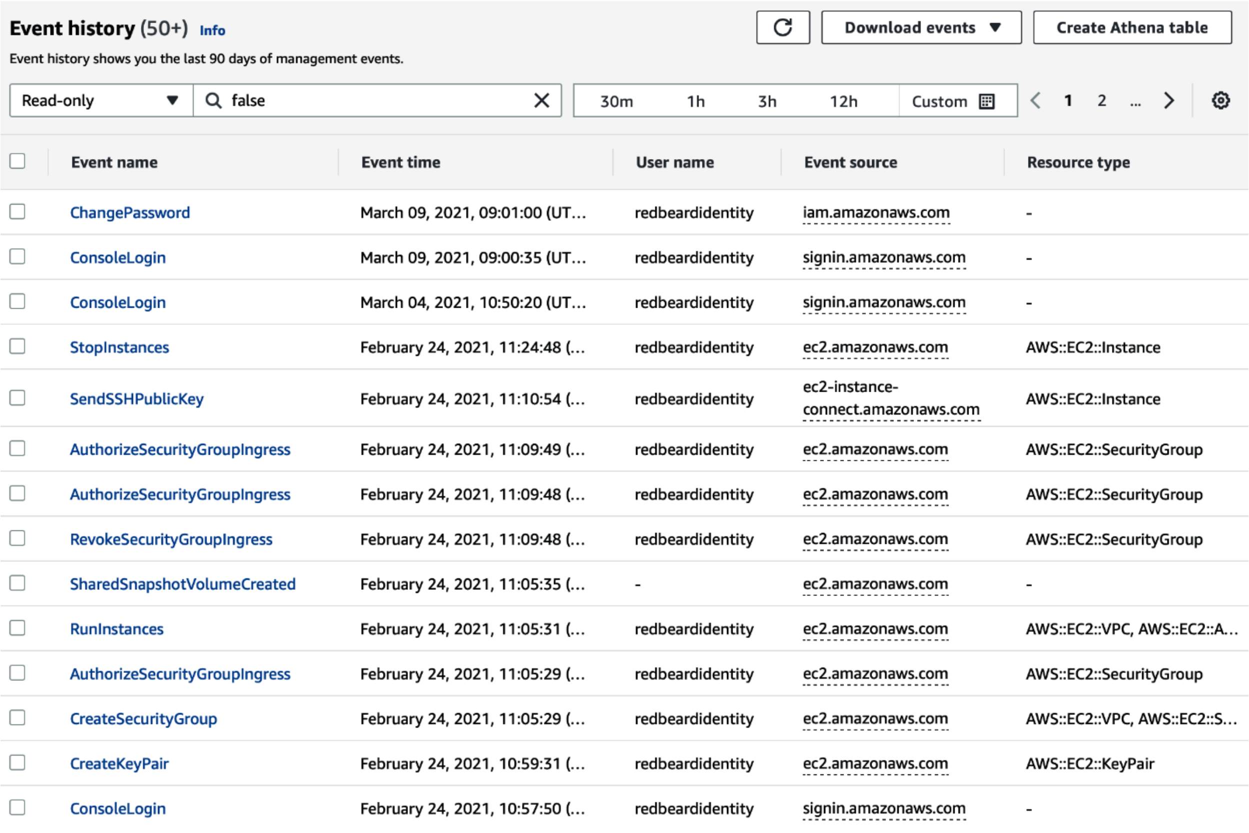
Create function



Sample code

View a code sample that illustrates how to retrieve the secret in your application.

```
' Use this code snippet in your app.
' If you need more information about configurations or implementing the sample code, visit
' https://aws.amazon.com/developers/getting-started/nodejs/

' Load the AWS SDK
ar AWS = require('aws-sdk'),
   region = "us-east-1",
   secretName = "rbi_secret",
   secret,
   decodedBinarySecret;

' Create a Secrets Manager client
ar client = new AWS.SecretsManager({
   region: region
);

' In this sample we only handle the specific exceptions for the 'GetSecretValue' API.
```

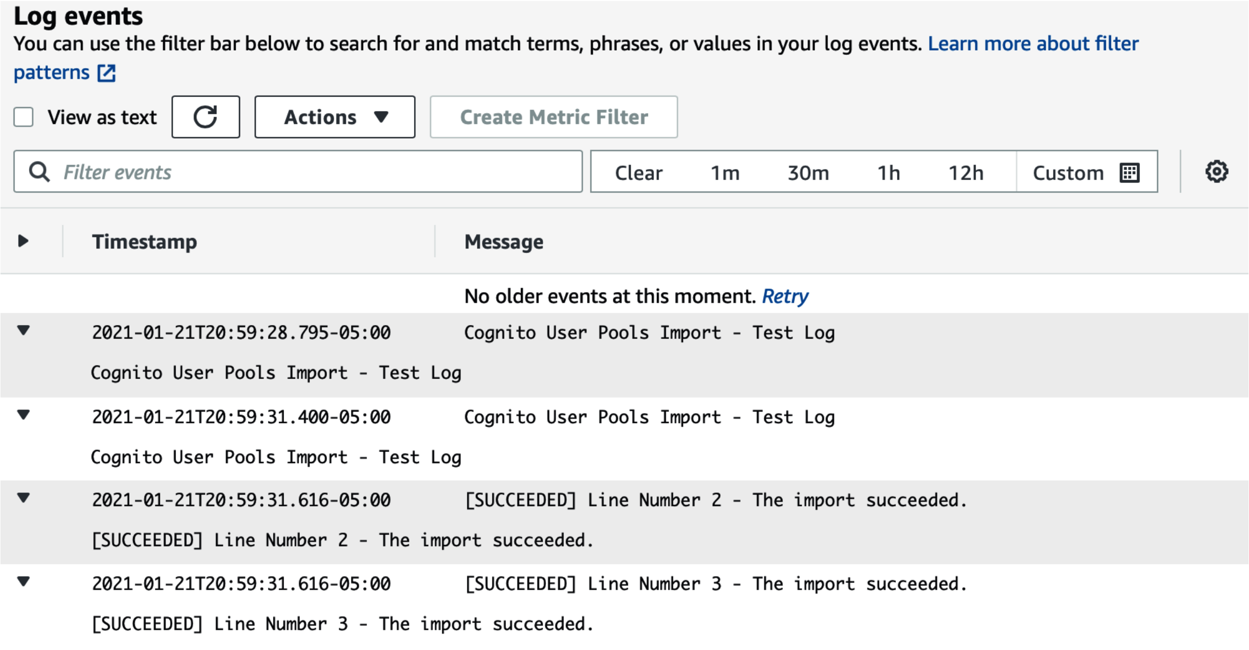


Event history (50+) Info

Event history shows you the last 90 days of management events.

Read-only ▼ false

□	Event name	Event time	User name	Event source	Resource type
□	ChangePassword	March 09, 2021, 09:01:00 (UT...	redbeardidentity	iam.amazonaws.com	-
□	ConsoleLogin	March 09, 2021, 09:00:35 (UT...	redbeardidentity	signin.amazonaws.com	-
□	ConsoleLogin	March 04, 2021, 10:50:20 (UT...	redbeardidentity	signin.amazonaws.com	-
□	StopInstances	February 24, 2021, 11:24:48 (...	redbeardidentity	ec2.amazonaws.com	AWS::EC2::Instance
□	SendSSHPublicKey	February 24, 2021, 11:10:54 (...	redbeardidentity	ec2-instance-connect.amazonaws.com	AWS::EC2::Instance
□	AuthorizeSecurityGroupIngress	February 24, 2021, 11:09:49 (...	redbeardidentity	ec2.amazonaws.com	AWS::EC2::SecurityGroup
□	AuthorizeSecurityGroupIngress	February 24, 2021, 11:09:48 (...	redbeardidentity	ec2.amazonaws.com	AWS::EC2::SecurityGroup
□	RevokeSecurityGroupIngress	February 24, 2021, 11:09:48 (...	redbeardidentity	ec2.amazonaws.com	AWS::EC2::SecurityGroup
□	SharedSnapshotVolumeCreated	February 24, 2021, 11:05:35 (...	-	ec2.amazonaws.com	-
□	RunInstances	February 24, 2021, 11:05:31 (...	redbeardidentity	ec2.amazonaws.com	AWS::EC2::VPC, AWS::EC2::A...
□	AuthorizeSecurityGroupIngress	February 24, 2021, 11:05:29 (...	redbeardidentity	ec2.amazonaws.com	AWS::EC2::SecurityGroup
□	CreateSecurityGroup	February 24, 2021, 11:05:29 (...	redbeardidentity	ec2.amazonaws.com	AWS::EC2::VPC, AWS::EC2::S...
□	CreateKeyPair	February 24, 2021, 10:59:31 (...	redbeardidentity	ec2.amazonaws.com	AWS::EC2::KeyPair
□	ConsoleLogin	February 24, 2021, 10:57:50 (...	redbeardidentity	signin.amazonaws.com	-



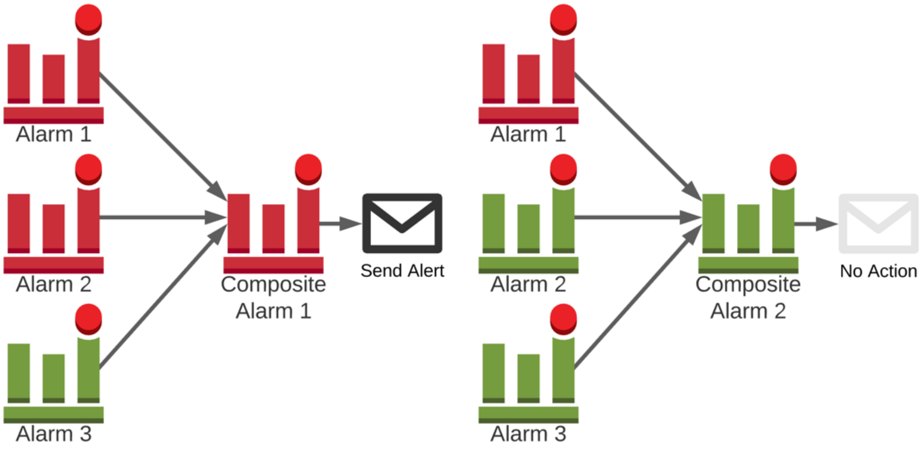
Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns

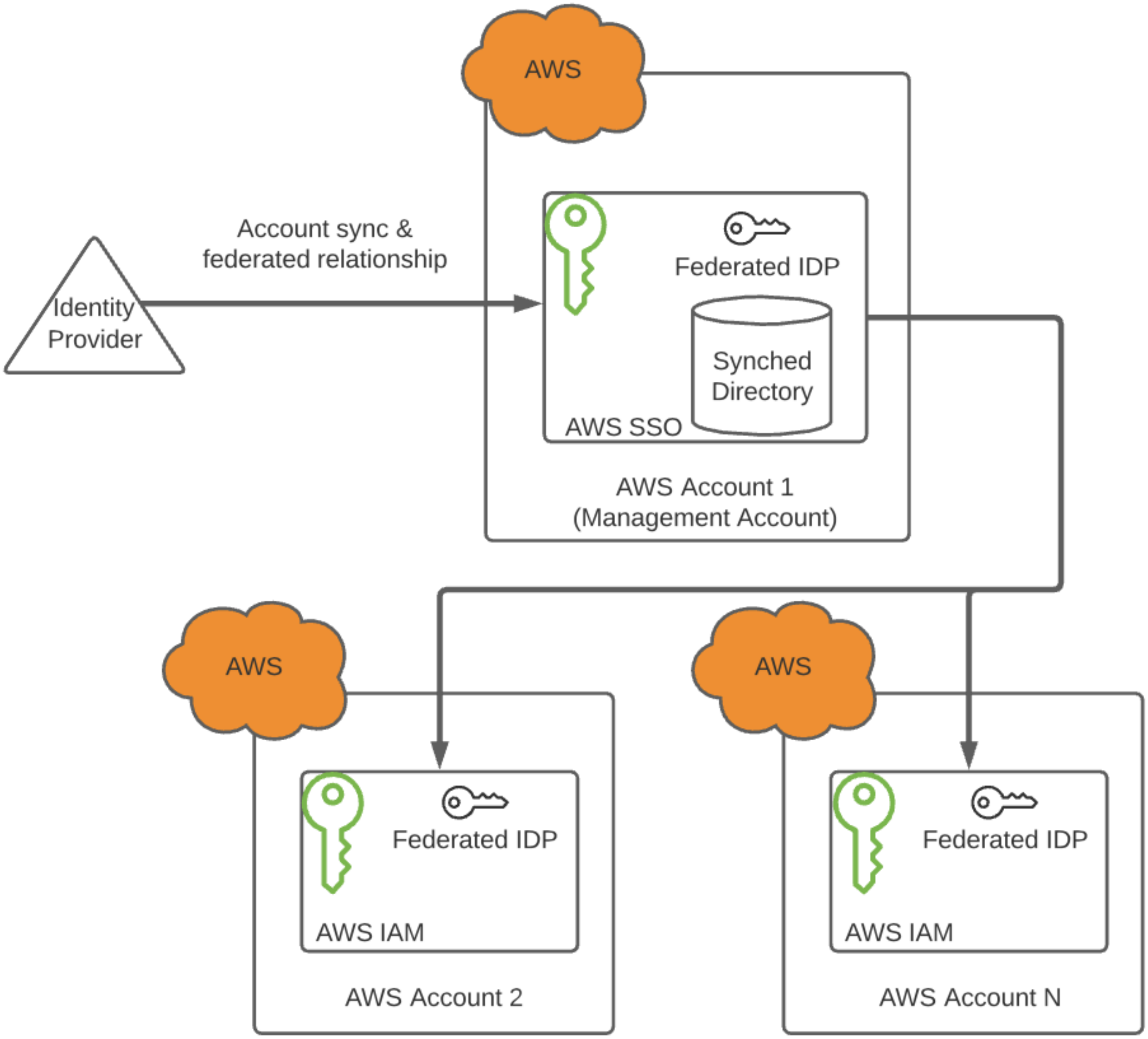
▶	Timestamp	Message

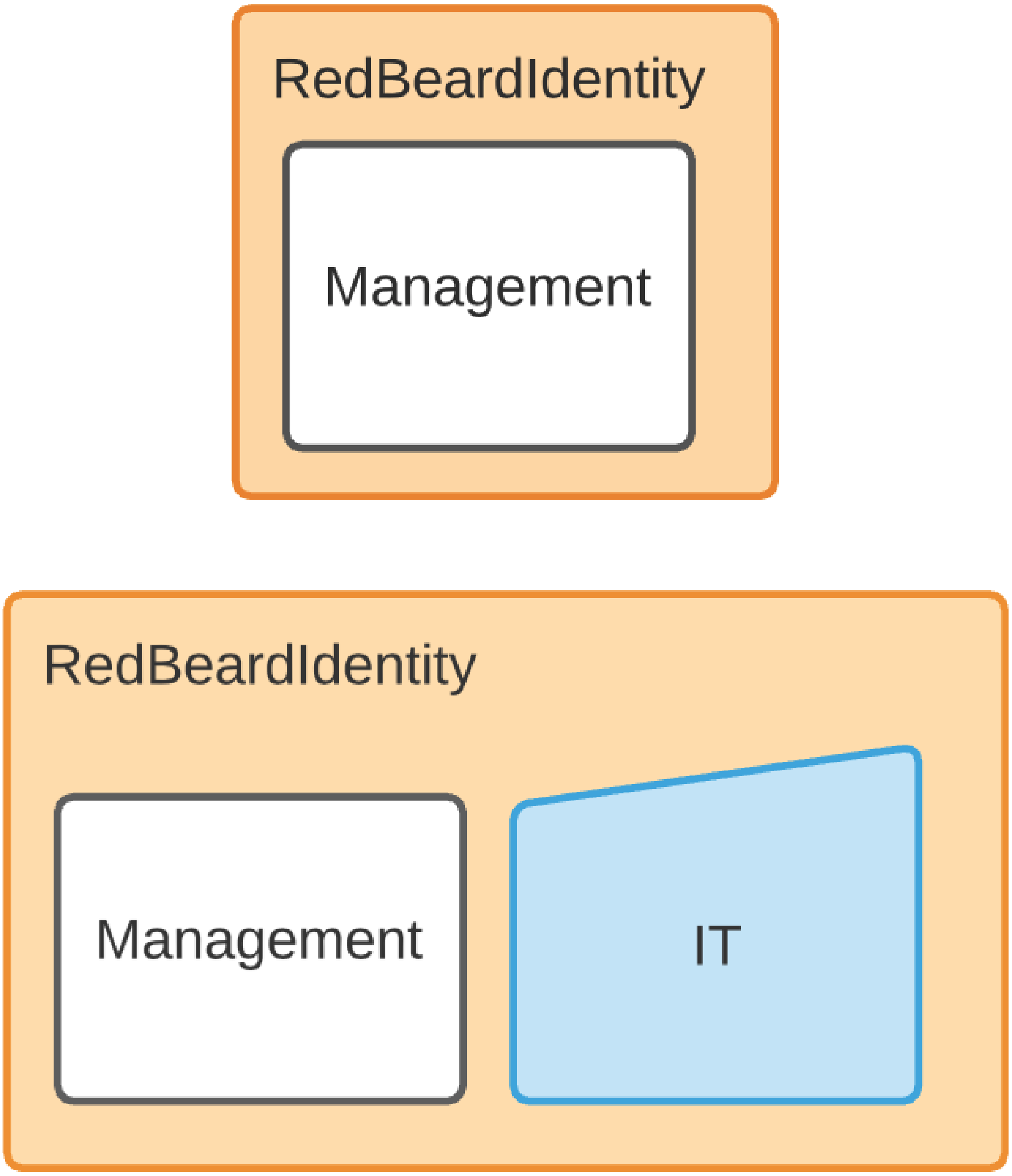
No older events at this moment. *Retry*

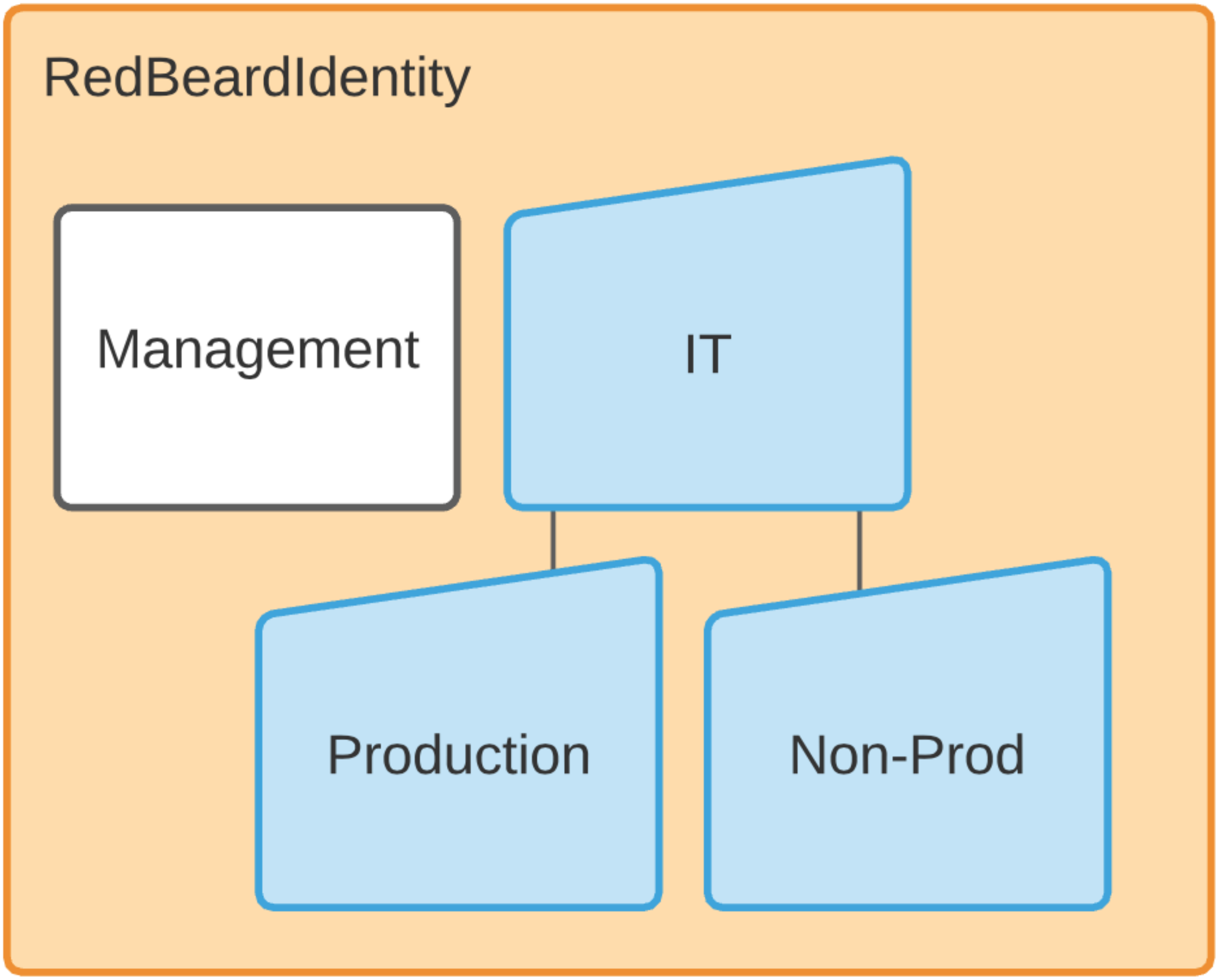
```
▼   2021-01-21T20:59:28.795-05:00      Cognito User Pools Import - Test Log
    Cognito User Pools Import - Test Log
▼   2021-01-21T20:59:31.400-05:00      Cognito User Pools Import - Test Log
    Cognito User Pools Import - Test Log
▼   2021-01-21T20:59:31.616-05:00      [SUCCEEDED] Line Number 2 - The import succeeded.
    [SUCCEEDED] Line Number 2 - The import succeeded.
▼   2021-01-21T20:59:31.616-05:00      [SUCCEEDED] Line Number 3 - The import succeeded.
    [SUCCEEDED] Line Number 3 - The import succeeded.
```

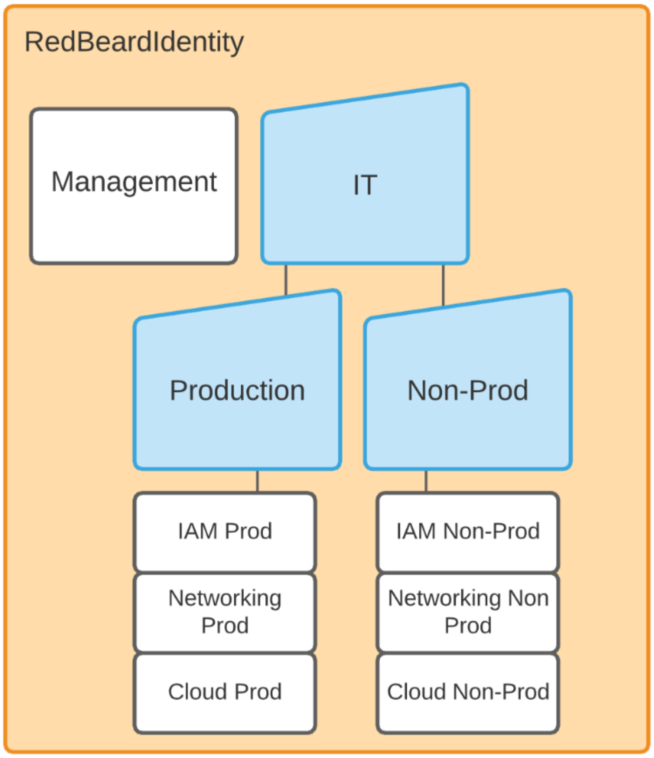

Alarm 1
Alarm 2
Alarm 3
Composite Alarm 1
Send Alert
Alarm 1
Alarm 2
Alarm 3
Composite Alarm 2
No Action

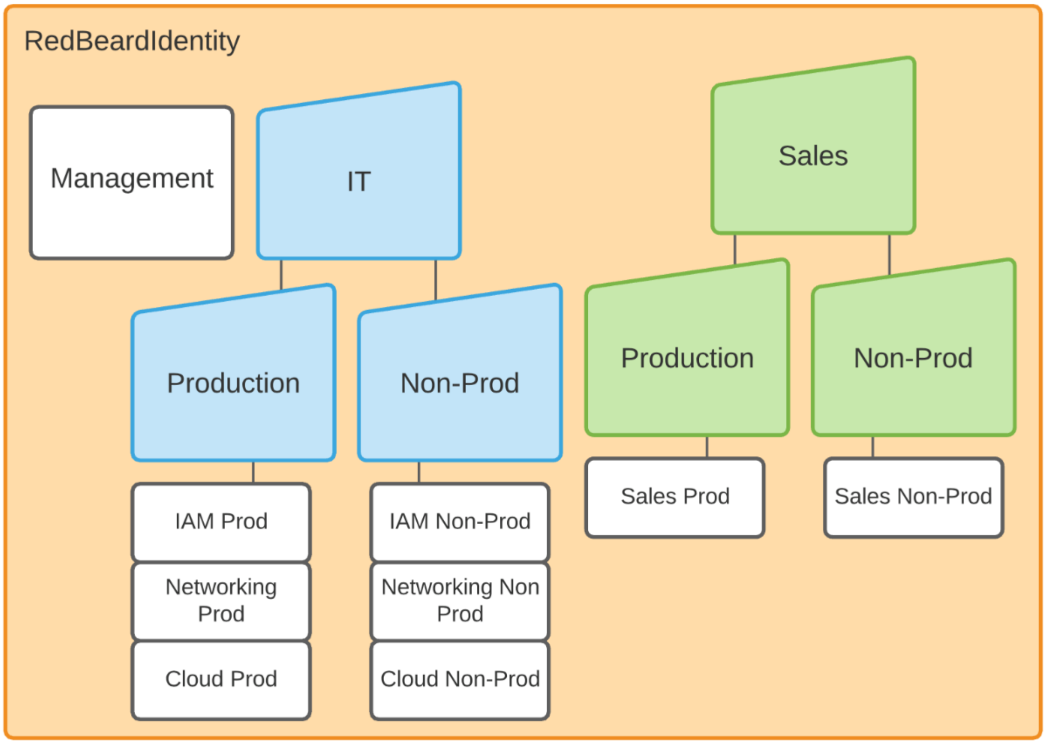
Chapter 8: An Ounce of Prevention – Planning Your Administrative Model

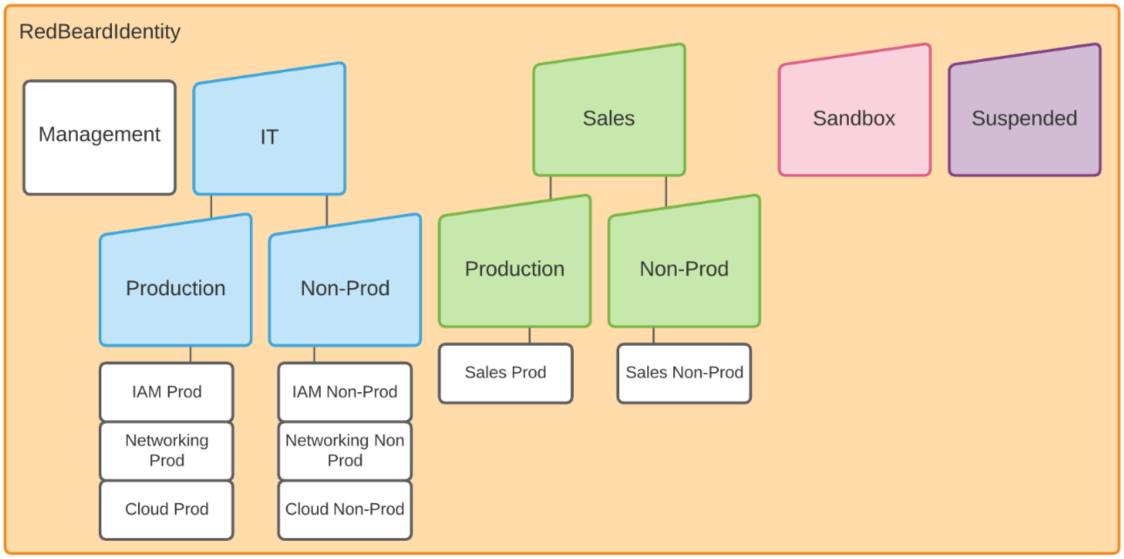


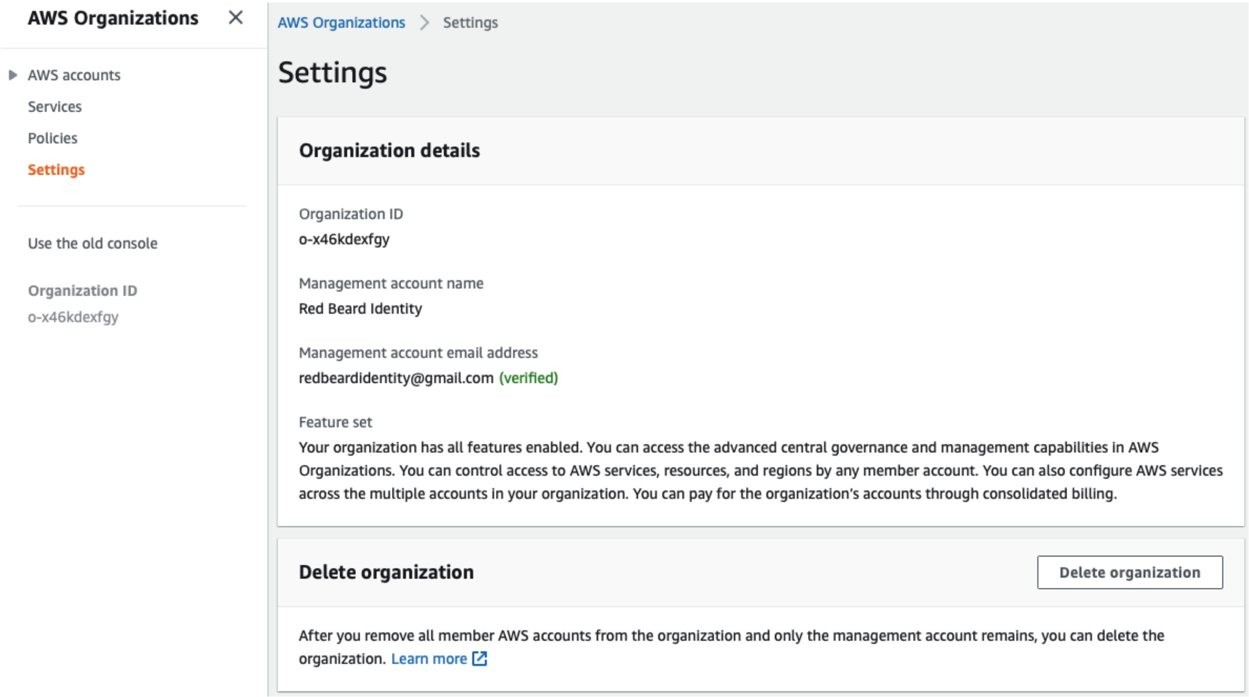

RedBeardIdentity
Management
RedBeardIdentity
Management
IT


RedBeardIdentity
Management
IT
Production
Non-Prod


RedBeardIdentity
Management
IT
Production
Non-Prod
IAM Prod
Networking Prod
Cloud Prod
IAM Non-Prod
Networking Non Prod
Cloud Non-Prod


RedBeardIdentity
Management
IT
Sales
Production
Non-Prod
Production
Non-Prod
Sales Prod
Sales Non-Prod
IAM Prod
Networking Prod
Cloud Prod
IAM Non-Prod
Networking Non Prod
Cloud Non-Prod





Settings

Organization details

Organization ID
o-x46kdexfgy

Management account name
Red Beard Identity

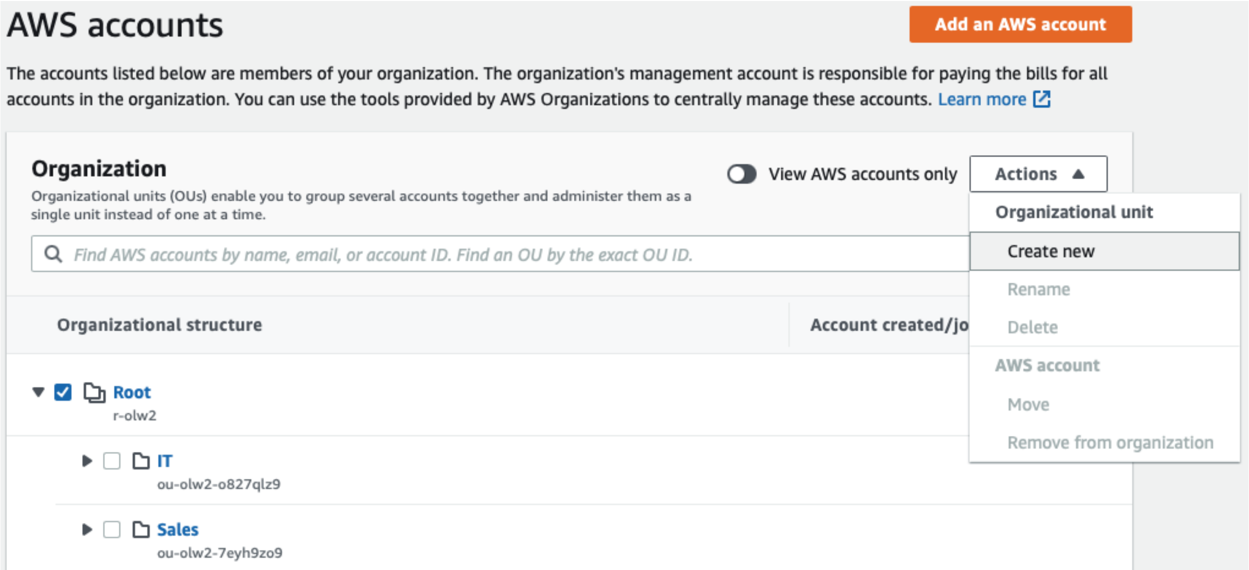
Management account email address
redbeardidentity@gmail.com (verified)

Feature set
Your organization has all features enabled. You can access the advanced central governance and management capabilities in AWS Organizations. You can control access to AWS services, resources, and regions by any member account. You can also configure AWS services across the multiple accounts in your organization. You can pay for the organization's accounts through consolidated billing.

Delete organization

Delete organization

After you remove all member AWS accounts from the organization and only the management account remains, you can delete the organization. Learn more



AWS accounts

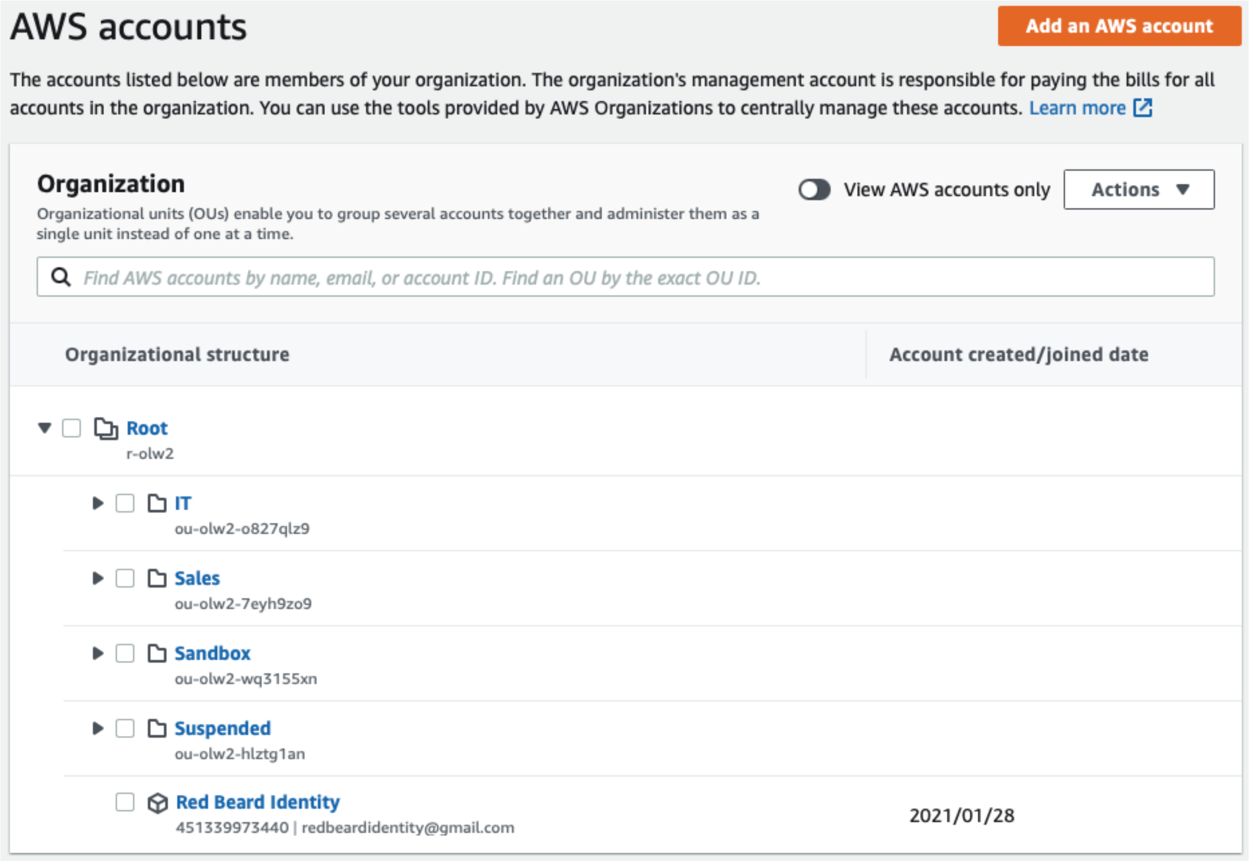
The accounts listed below are members of your organization. The organization's management account is responsible for paying the bills for all accounts in the organization. You can use the tools provided by AWS Organizations to centrally manage these accounts. Learn more

Organization

Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

Find AWS accounts by name, email, or account ID. Find an OU by the exact OU ID.

Organizational structure	Account created/jo
▼ ☑ Root r-olw2	
▶ □ IT ou-olw2-o827qlz9	
▶ □ Sales ou-olw2-7eyh9zo9	



AWS accounts

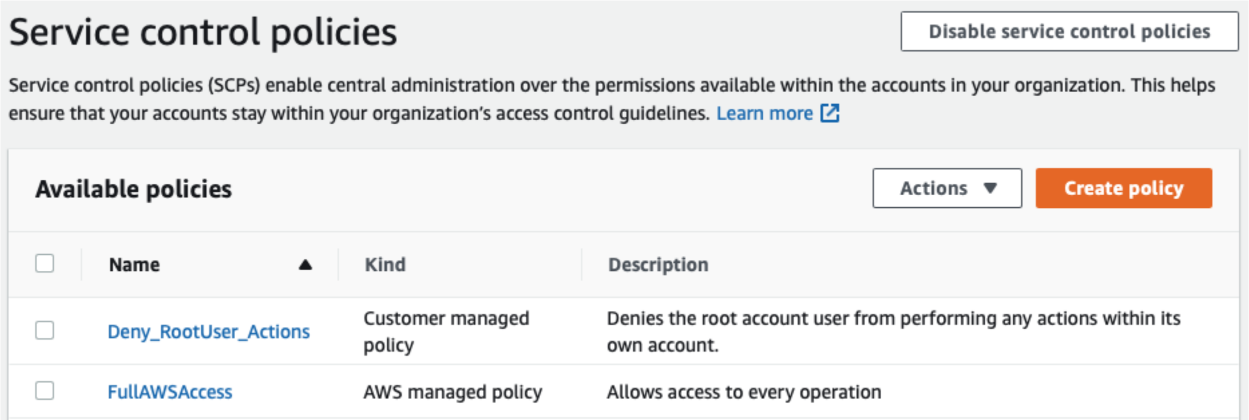
The accounts listed below are members of your organization. The organization's management account is responsible for paying the bills for all accounts in the organization. You can use the tools provided by AWS Organizations to centrally manage these accounts. Learn more

Organization

Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

Find AWS accounts by name, email, or account ID. Find an OU by the exact OU ID.

Organizational structure	Account created/joined date
▼ □ Root r-olw2	
▶ □ IT ou-olw2-o827qlz9	
▶ □ Sales ou-olw2-7eyh9zo9	
▶ □ Sandbox ou-olw2-wq3155xn	
▶ □ Suspended ou-olw2-hlztg1an	
□ Red Beard Identity 451339973440 | redbeardidentity@gmail.com	2021/01/28



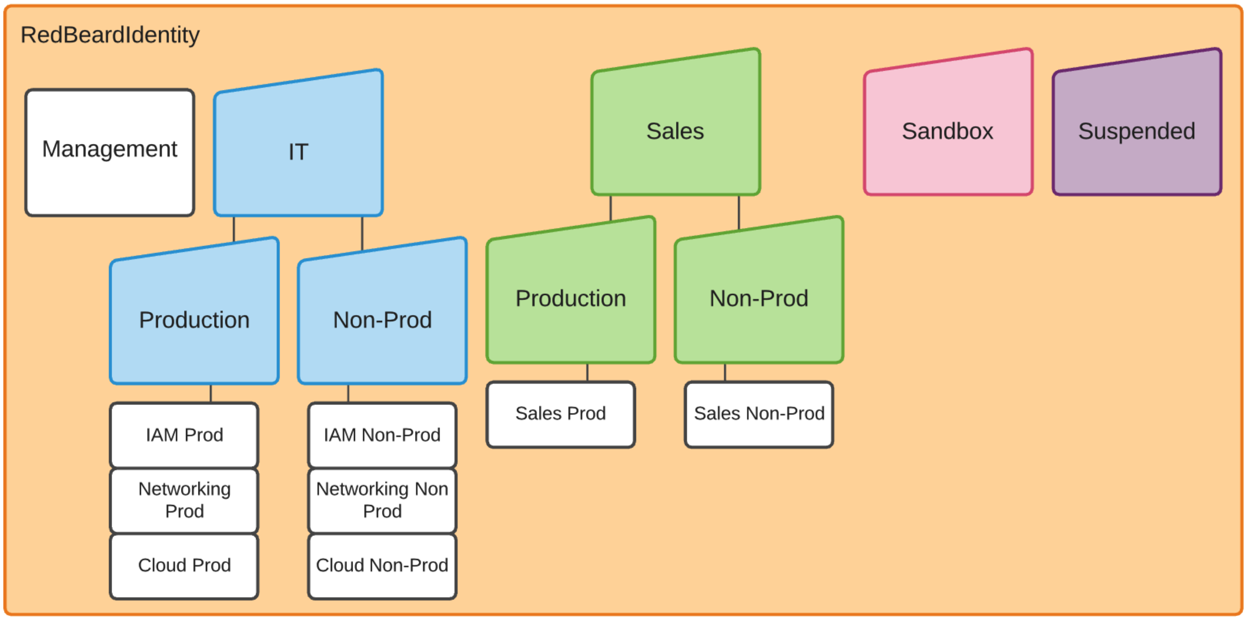
Service control policies

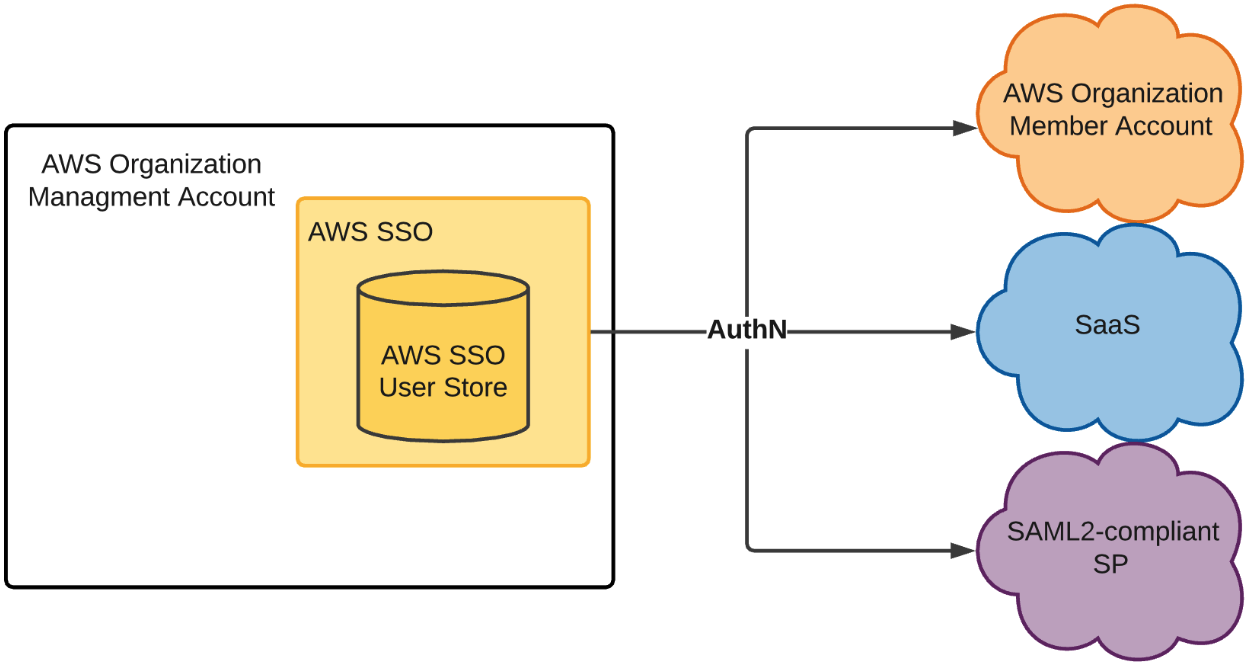
Service control policies (SCPs) enable central administration over the permissions available within the accounts in your organization. This helps ensure that your accounts stay within your organization's access control guidelines. Learn more

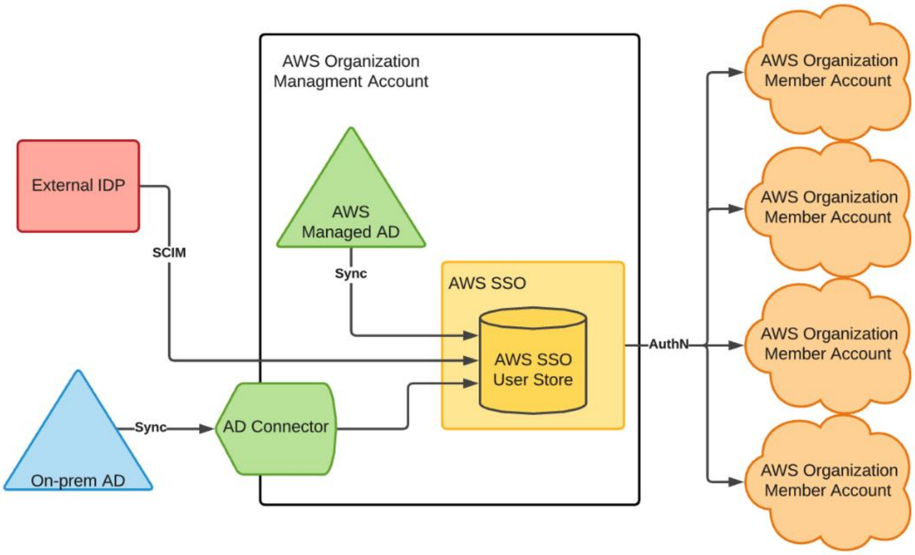
Available policies

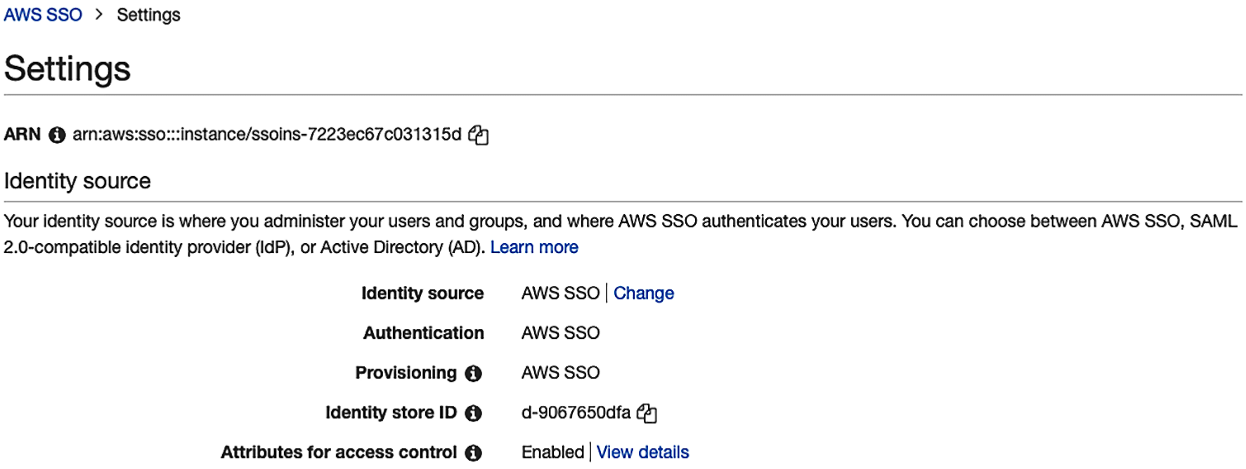
□	Name ▲	Kind	Description
□	Deny_RootUser_Actions	Customer managed policy	Denies the root account user from performing any actions within its own account.
□	FullAWSAccess	AWS managed policy	Allows access to every operation

Chapter 9: Bringing Your Admins into the AWS Administrative Backplane




AWS Organization Managment Account
AWS SSO
AWS SSO User Store
AuthN
AWS Organization Member Account
SaaS
SAML2-compliant SP





AWS SSO > Settings

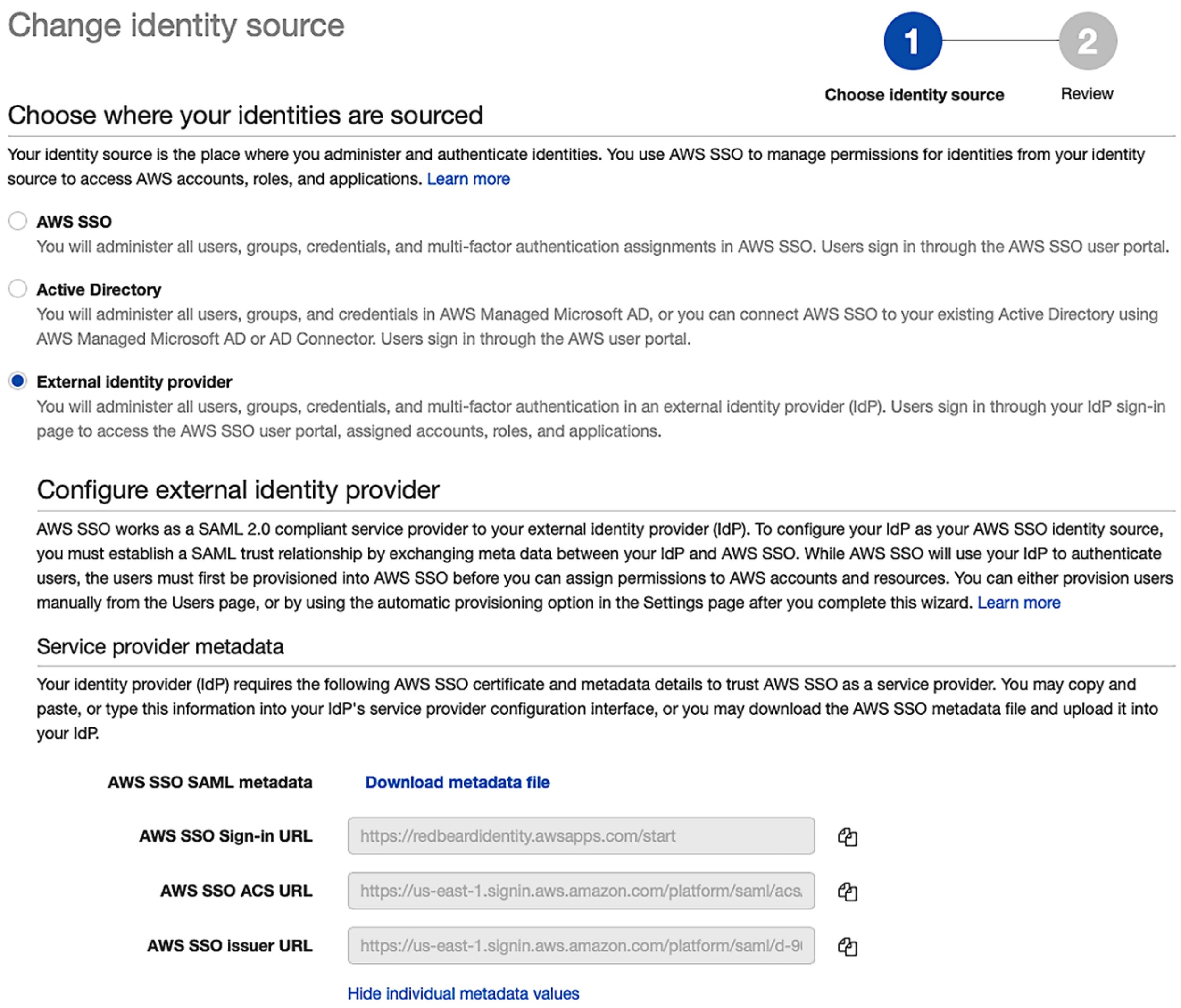
Settings

ARN arn:aws:sso:::instance/ssoins-7223ec67c031315d

Identity source

Your identity source is where you administer your users and groups, and where AWS SSO authenticates your users. You can choose between AWS SSO, SAML 2.0-compatible identity provider (IdP), or Active Directory (AD). Learn more

Identity source	AWS SSO | Change
Authentication	AWS SSO
Provisioning	AWS SSO
Identity store ID	d-9067650dfa
Attributes for access control	Enabled | View details



Change identity source

Choose where your identities are sourced

Your identity source is the place where you administer and authenticate identities. You use AWS SSO to manage permissions for identities from your identity source to access AWS accounts, roles, and applications. Learn more

○ **AWS SSO**
You will administer all users, groups, credentials, and multi-factor authentication assignments in AWS SSO. Users sign in through the AWS SSO user portal.

○ **Active Directory**
You will administer all users, groups, and credentials in AWS Managed Microsoft AD, or you can connect AWS SSO to your existing Active Directory using AWS Managed Microsoft AD or AD Connector. Users sign in through the AWS user portal.

● **External identity provider**
You will administer all users, groups, credentials, and multi-factor authentication in an external identity provider (IdP). Users sign in through your IdP sign-in page to access the AWS SSO user portal, assigned accounts, roles, and applications.

Configure external identity provider

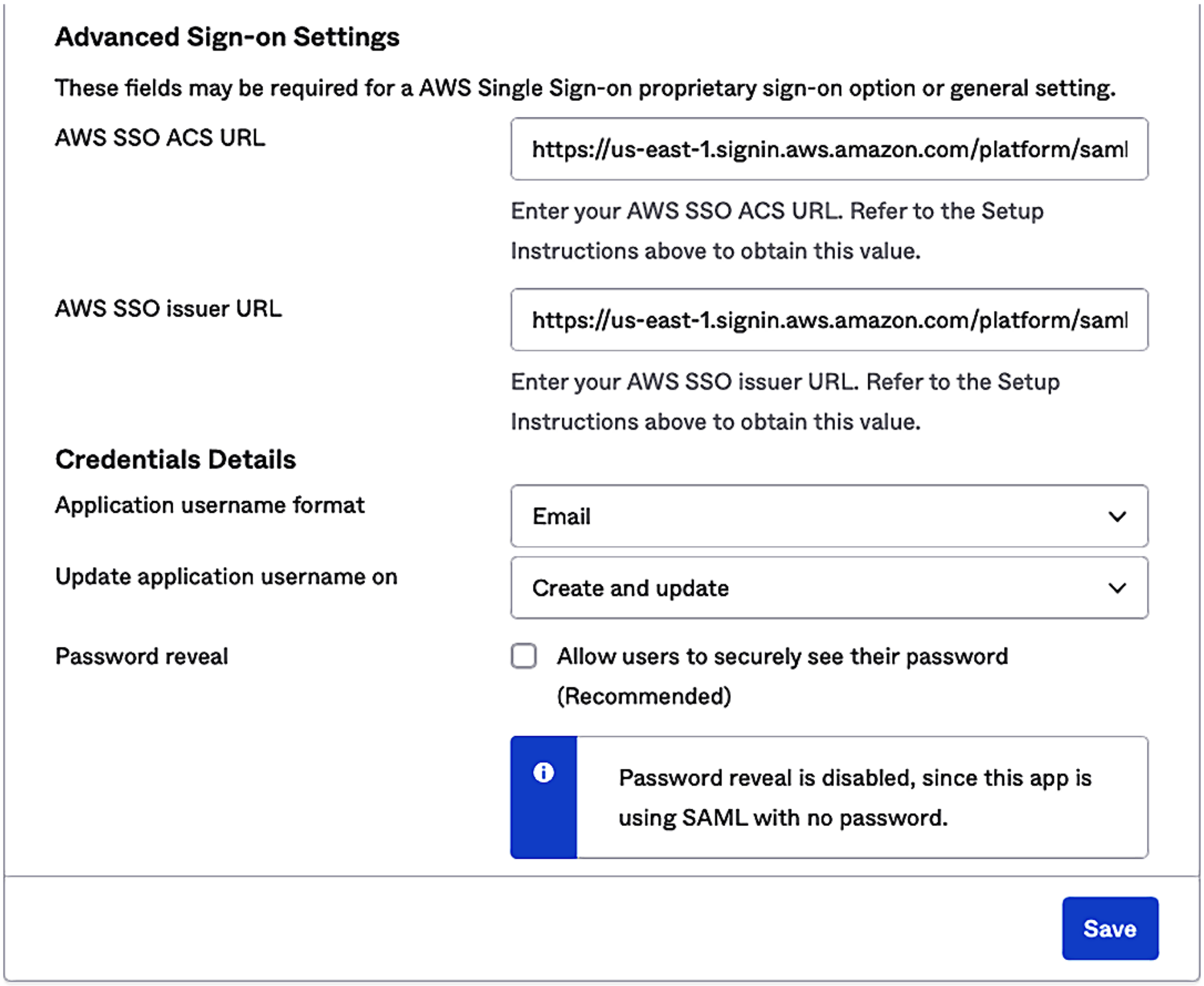
AWS SSO works as a SAML 2.0 compliant service provider to your external identity provider (IdP). To configure your IdP as your AWS SSO identity source, you must establish a SAML trust relationship by exchanging meta data between your IdP and AWS SSO. While AWS SSO will use your IdP to authenticate users, the users must first be provisioned into AWS SSO before you can assign permissions to AWS accounts and resources. You can either provision users manually from the Users page, or by using the automatic provisioning option in the Settings page after you complete this wizard. Learn more

Service provider metadata

Your identity provider (IdP) requires the following AWS SSO certificate and metadata details to trust AWS SSO as a service provider. You may copy and paste, or type this information into your IdP's service provider configuration interface, or you may download the AWS SSO metadata file and upload it into your IdP.

AWS SSO SAML metadata	**Download metadata file**
AWS SSO Sign-in URL	https://redbeardidentity.awsapps.com/start
AWS SSO ACS URL	https://us-east-1.signin.aws.amazon.com/platform/saml/acs,
AWS SSO issuer URL	https://us-east-1.signin.aws.amazon.com/platform/saml/d-9

Hide individual metadata values



Advanced Sign-on Settings

These fields may be required for a AWS Single Sign-on proprietary sign-on option or general setting.

AWS SSO ACS URL: https://us-east-1.signin.aws.amazon.com/platform/saml

Enter your AWS SSO ACS URL. Refer to the Setup Instructions above to obtain this value.

AWS SSO issuer URL: https://us-east-1.signin.aws.amazon.com/platform/saml

Enter your AWS SSO issuer URL. Refer to the Setup Instructions above to obtain this value.

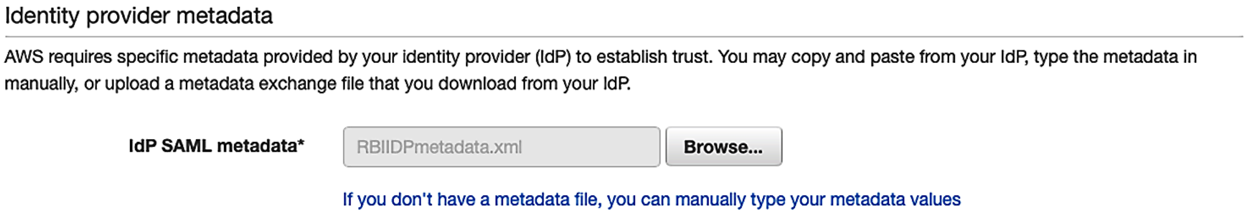
Credentials Details

Application username format: Email

Update application username on: Create and update

Password reveal: □ Allow users to securely see their password (Recommended)

Password reveal is disabled, since this app is using SAML with no password.

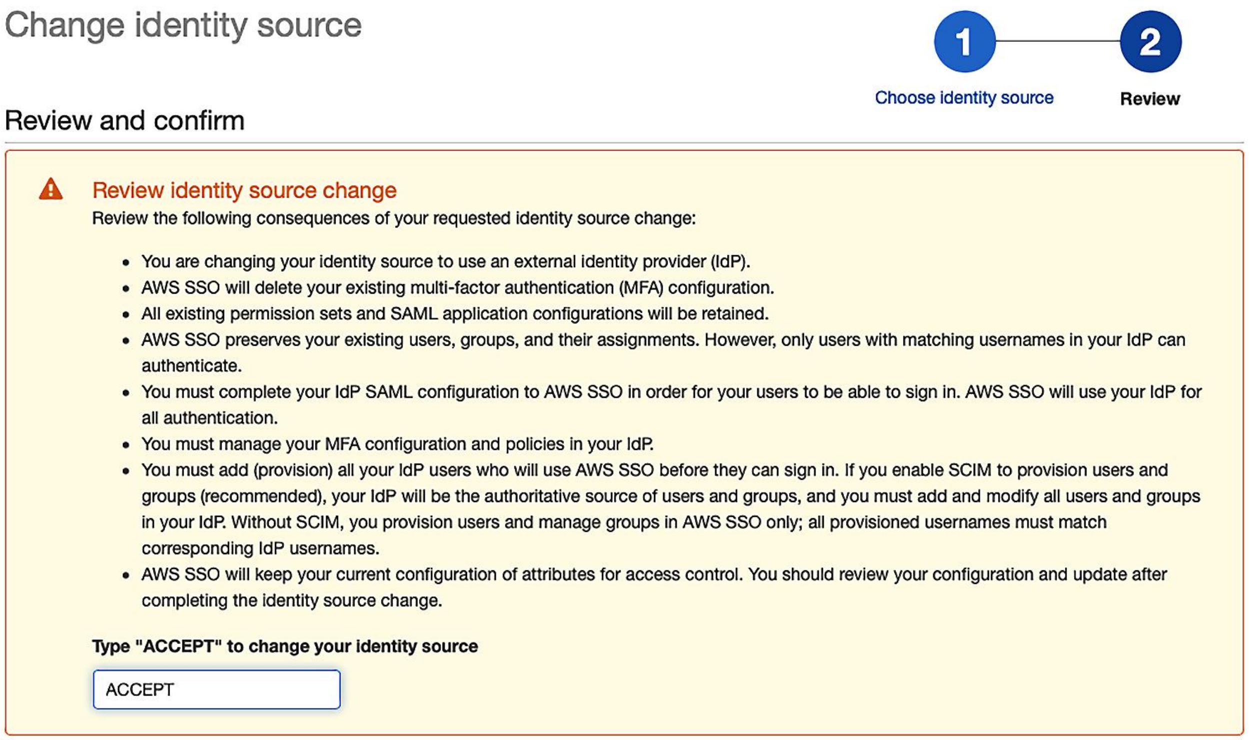


Identity provider metadata

AWS requires specific metadata provided by your identity provider (IdP) to establish trust. You may copy and paste from your IdP, type the metadata in manually, or upload a metadata exchange file that you download from your IdP.

IdP SAML metadata*: RBIIDPmetadata.xml

If you don't have a metadata file, you can manually type your metadata values



Change identity source

Review and confirm

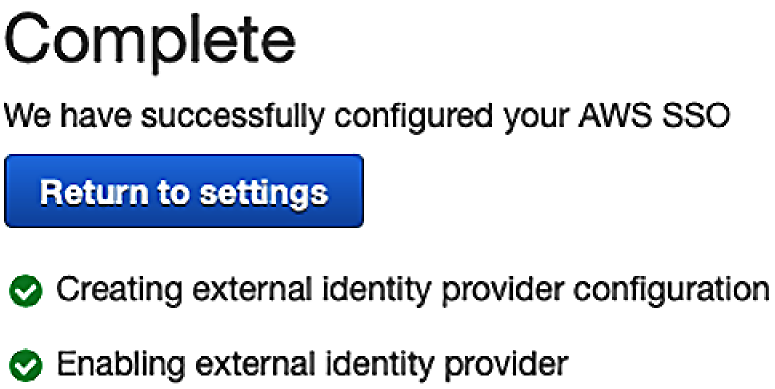
⚠ Review identity source change

Review the following consequences of your requested identity source change:

- You are changing your identity source to use an external identity provider (IdP).
- AWS SSO will delete your existing multi-factor authentication (MFA) configuration.
- All existing permission sets and SAML application configurations will be retained.
- AWS SSO preserves your existing users, groups, and their assignments. However, only users with matching usernames in your IdP can authenticate.
- You must complete your IdP SAML configuration to AWS SSO in order for your users to be able to sign in. AWS SSO will use your IdP for all authentication.
- You must manage your MFA configuration and policies in your IdP.
- You must add (provision) all your IdP users who will use AWS SSO before they can sign in. If you enable SCIM to provision users and groups (recommended), your IdP will be the authoritative source of users and groups, and you must add and modify all users and groups in your IdP. Without SCIM, you provision users and manage groups in AWS SSO only; all provisioned usernames must match corresponding IdP usernames.
- AWS SSO will keep your current configuration of attributes for access control. You should review your configuration and update after completing the identity source change.

Type "ACCEPT" to change your identity source

ACCEPT

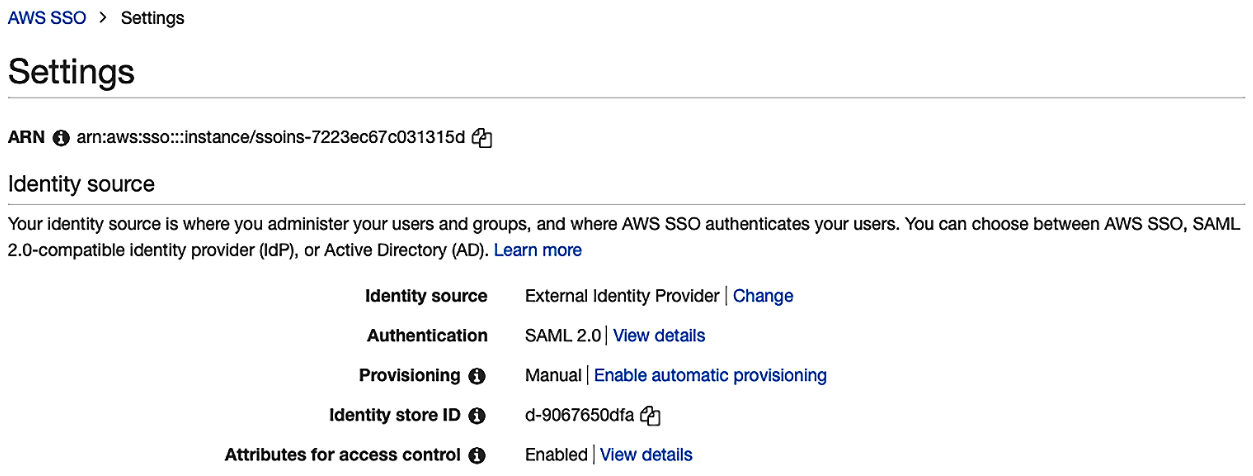


Complete

We have successfully configured your AWS SSO

✓ Creating external identity provider configuration

✓ Enabling external identity provider



AWS SSO > Settings

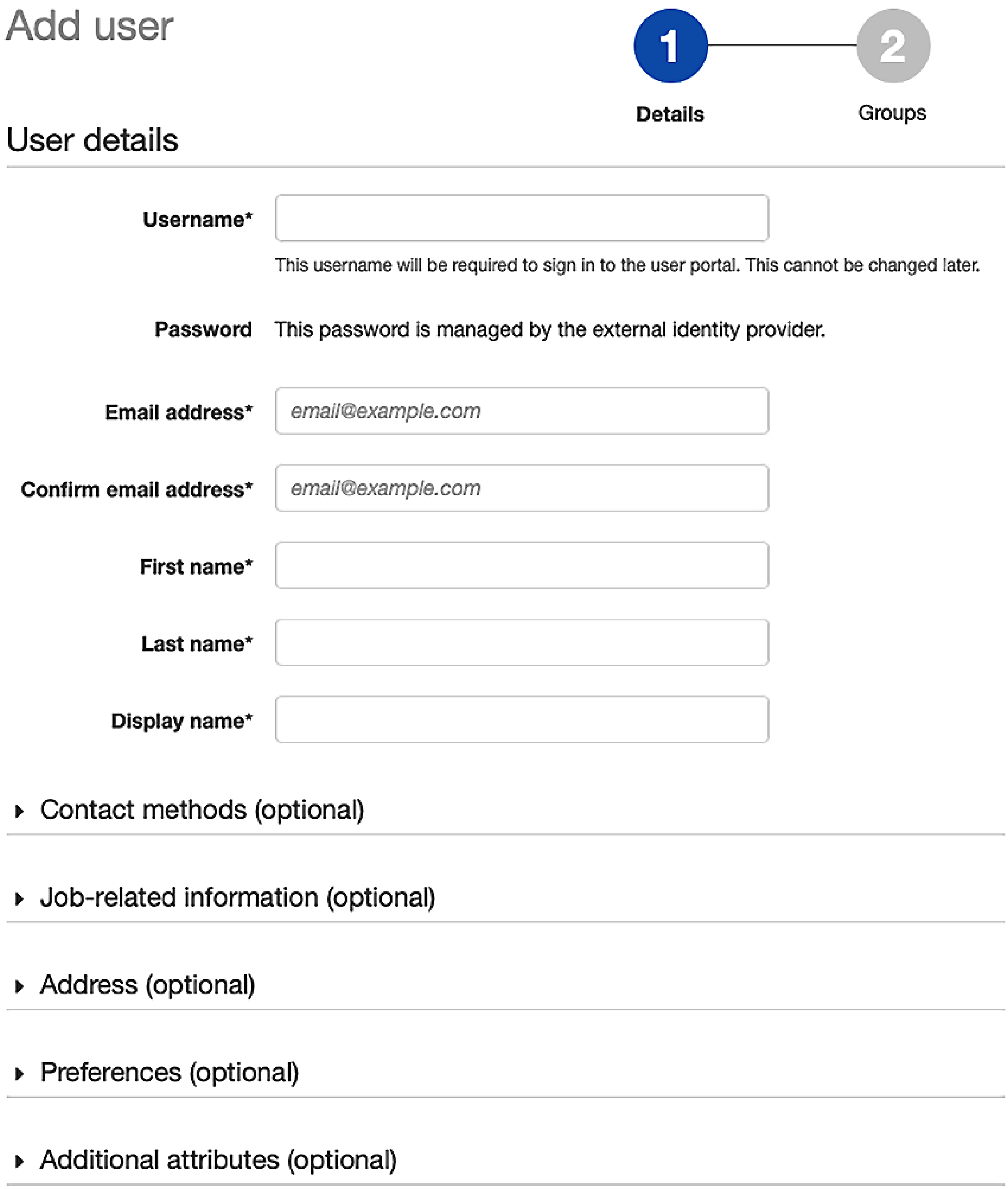
Settings

ARN arn:aws:sso:::instance/ssoins-7223ec67c031315d

Identity source

Your identity source is where you administer your users and groups, and where AWS SSO authenticates your users. You can choose between AWS SSO, SAML 2.0-compatible identity provider (IdP), or Active Directory (AD). Learn more

Identity source	External Identity Provider | Change
Authentication	SAML 2.0 | View details
Provisioning	Manual | Enable automatic provisioning
Identity store ID	d-9067650dfa
Attributes for access control	Enabled | View details



Add user

User details

Username*

This username will be required to sign in to the user portal. This cannot be changed later.

Password This password is managed by the external identity provider.

Email address* email@example.com

Confirm email address* email@example.com

First name*

Last name*

Display name*

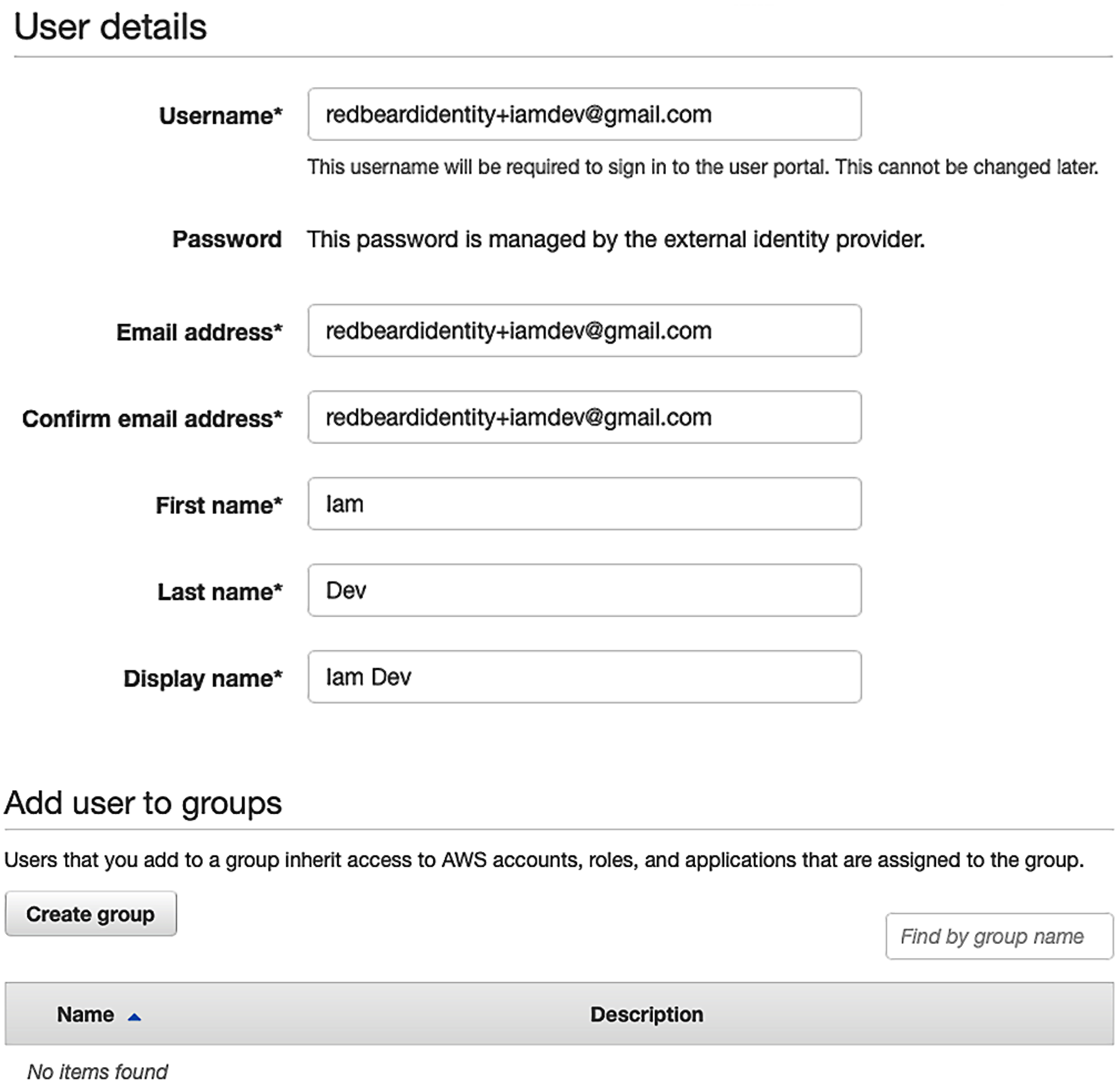
▸ Contact methods (optional)

▸ Job-related information (optional)

▸ Address (optional)

▸ Preferences (optional)

▸ Additional attributes (optional)



User details

Username* redbeardidentity+iamdev@gmail.com

This username will be required to sign in to the user portal. This cannot be changed later.

Password This password is managed by the external identity provider.

Email address* redbeardidentity+iamdev@gmail.com

Confirm email address* redbeardidentity+iamdev@gmail.com

First name* Iam

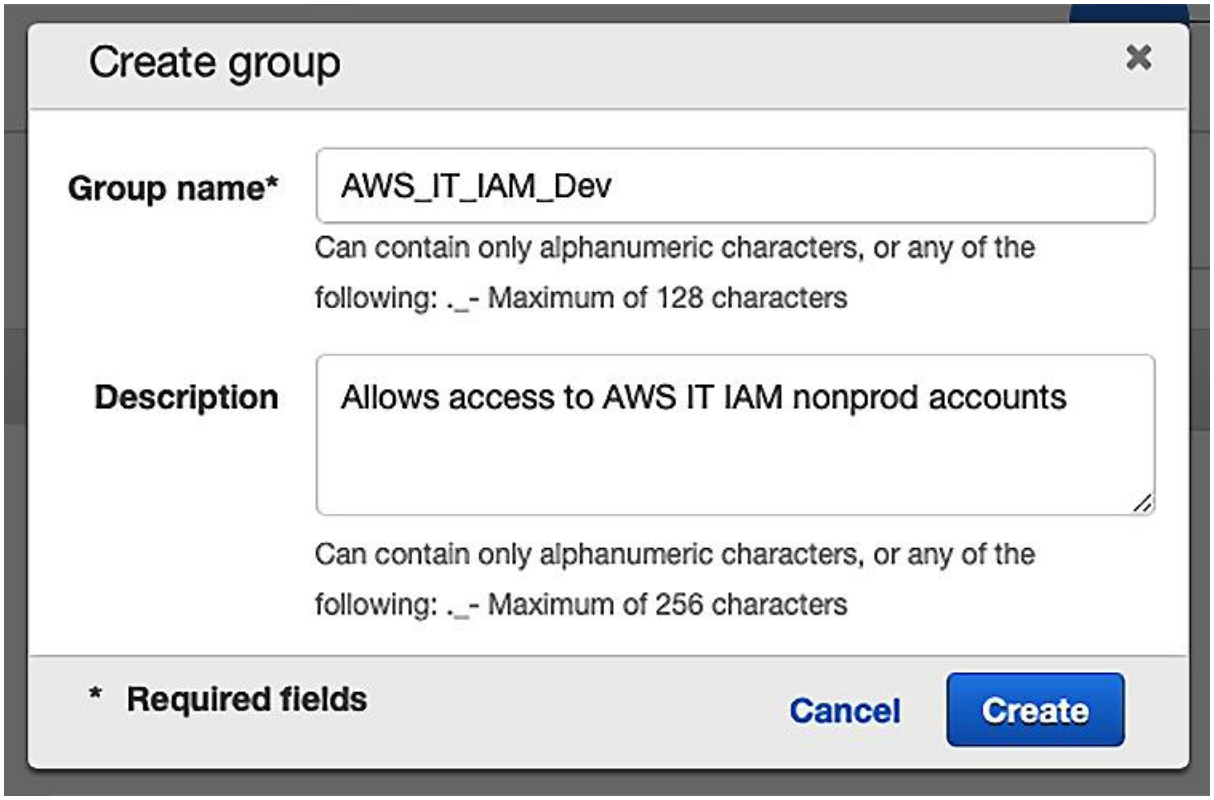
Last name* Dev

Display name* Iam Dev

Add user to groups

Users that you add to a group inherit access to AWS accounts, roles, and applications that are assigned to the group.

Name ▲	Description
No items found	



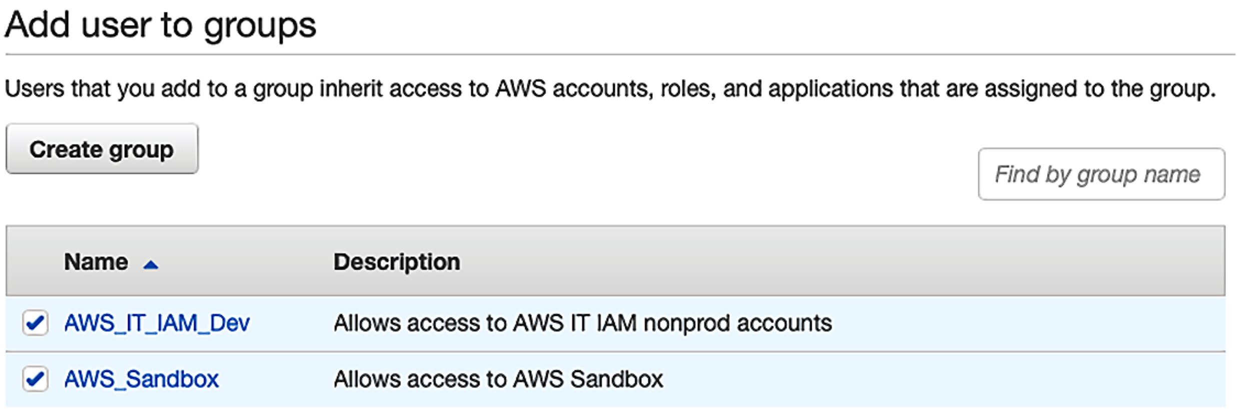
Group name*: AWS_IT_IAM_Dev

Can contain only alphanumeric characters, or any of the following: ._- Maximum of 128 characters

Description: Allows access to AWS IT IAM nonprod accounts

Can contain only alphanumeric characters, or any of the following: ._- Maximum of 256 characters

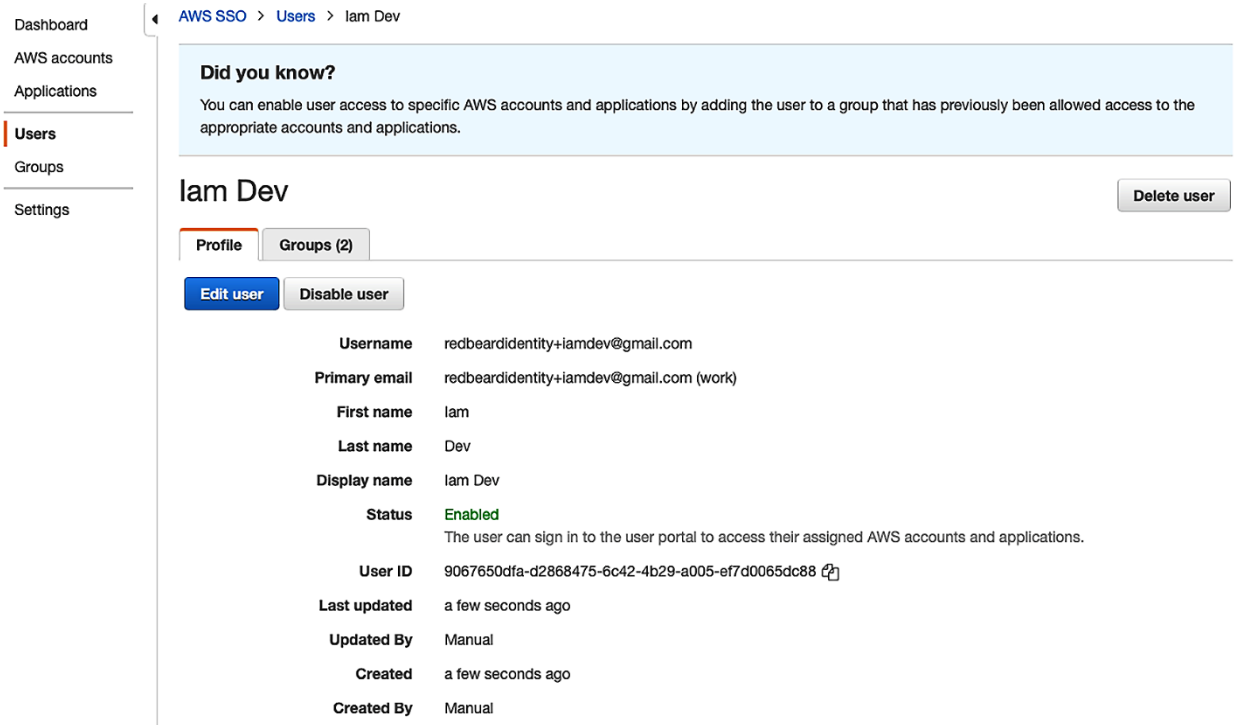
* **Required fields**



Add user to groups

Users that you add to a group inherit access to AWS accounts, roles, and applications that are assigned to the group.

	Name ▲	Description
☑	AWS_IT_IAM_Dev	Allows access to AWS IT IAM nonprod accounts
☑	AWS_Sandbox	Allows access to AWS Sandbox

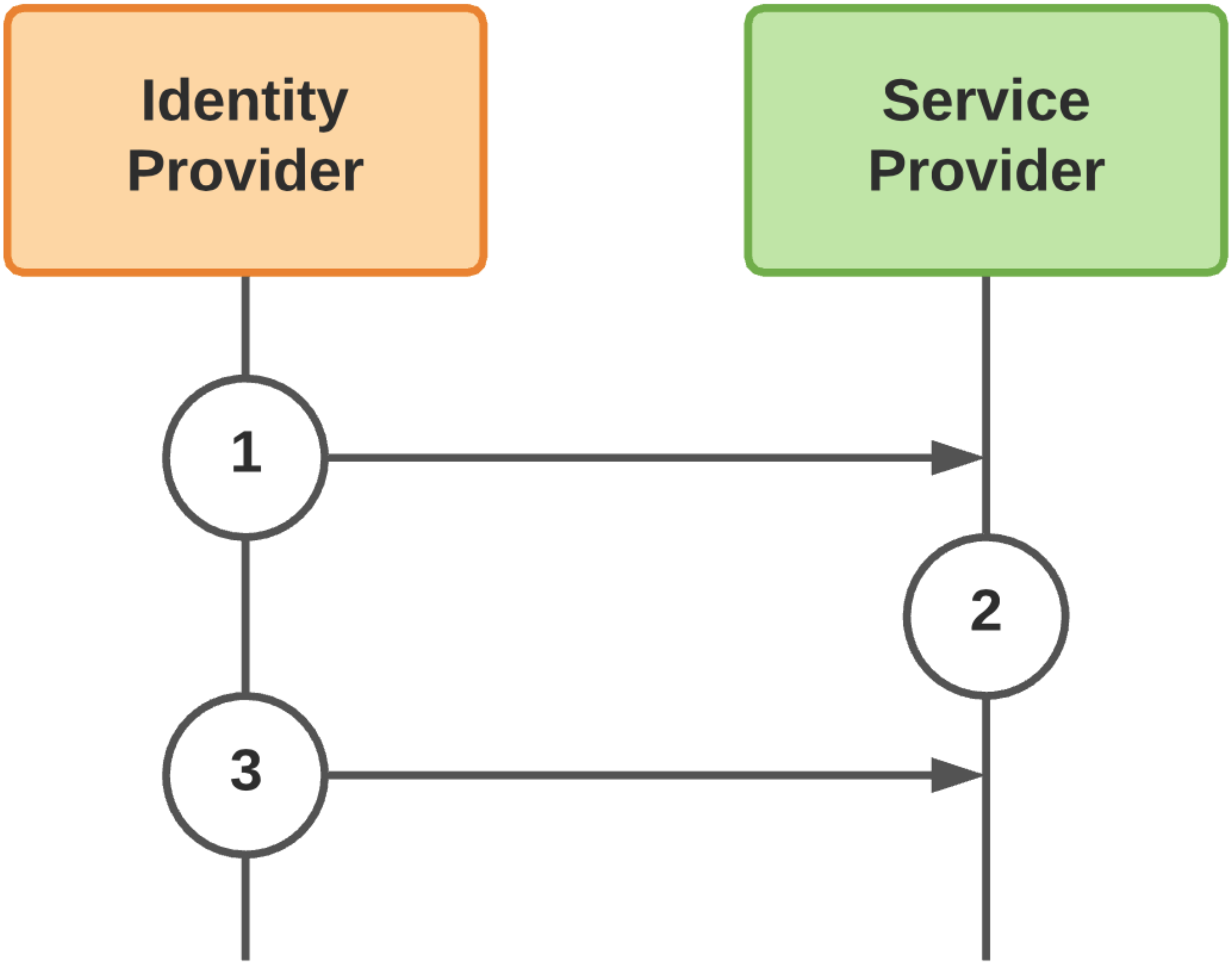


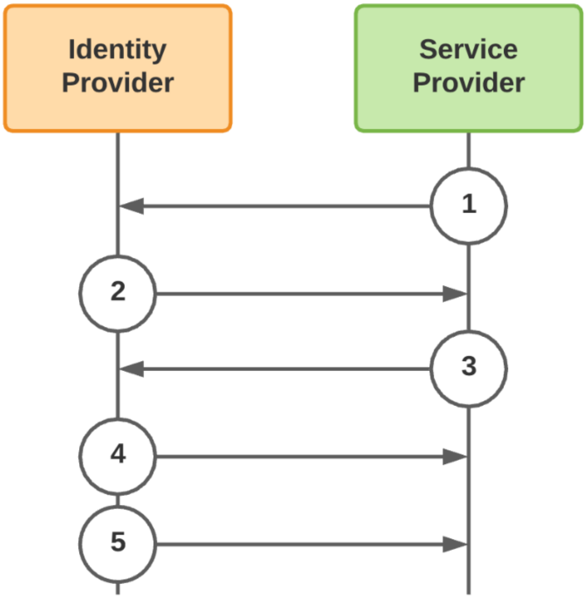
Did you know?

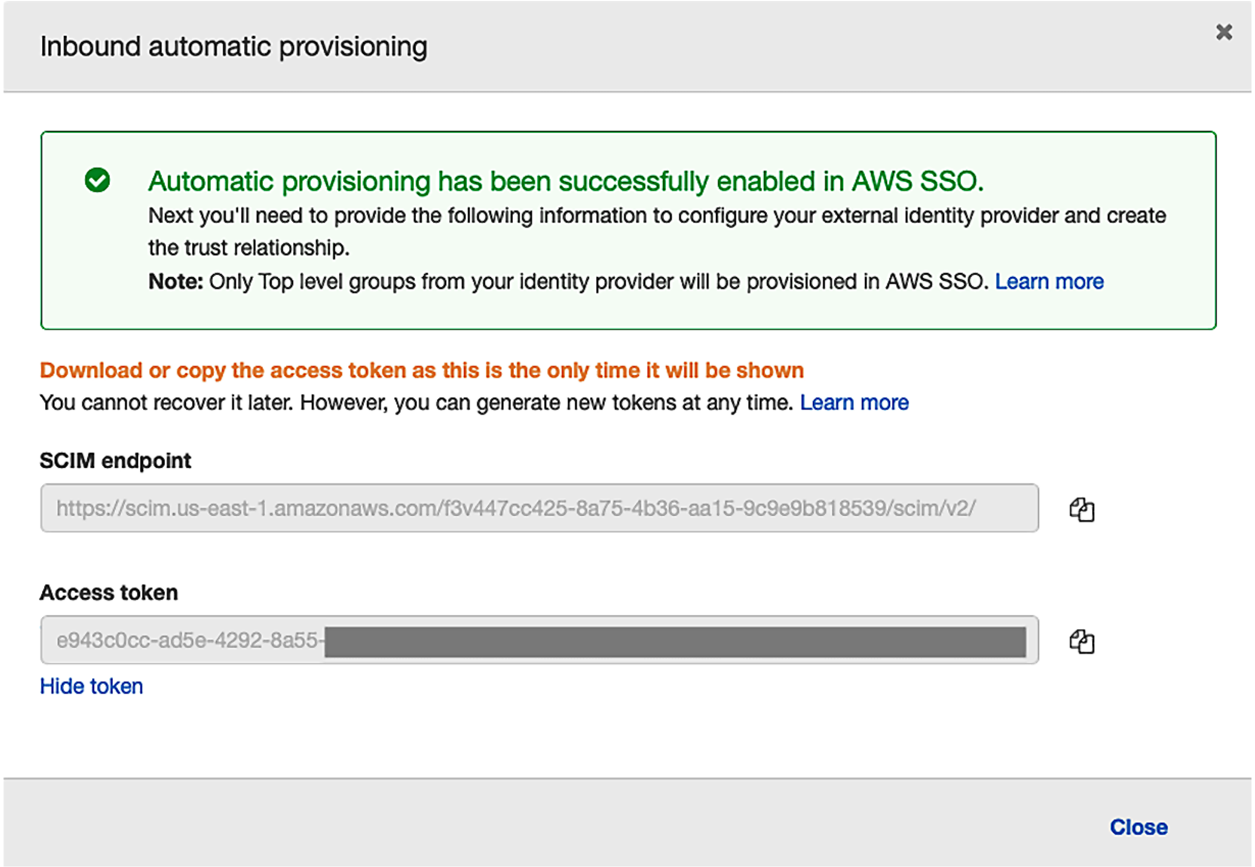
You can enable user access to specific AWS accounts and applications by adding the user to a group that has previously been allowed access to the appropriate accounts and applications.

Iam Dev

Username	redbeardidentity+iamdev@gmail.com
Primary email	redbeardidentity+iamdev@gmail.com (work)
First name	Iam
Last name	Dev
Display name	Iam Dev
Status	Enabled The user can sign in to the user portal to access their assigned AWS accounts and applications.
User ID	9067650dfa-d2868475-6c42-4b29-a005-ef7d0065dc88
Last updated	a few seconds ago
Updated By	Manual
Created	a few seconds ago
Created By	Manual


Identity Provider
Service Provider
1
2
3


Identity Provider
Service Provider
1
2
3
4
5



Inbound automatic provisioning

Automatic provisioning has been successfully enabled in AWS SSO.

Next you'll need to provide the following information to configure your external identity provider and create the trust relationship.

Note: Only Top level groups from your identity provider will be provisioned in AWS SSO. Learn more

Download or copy the access token as this is the only time it will be shown

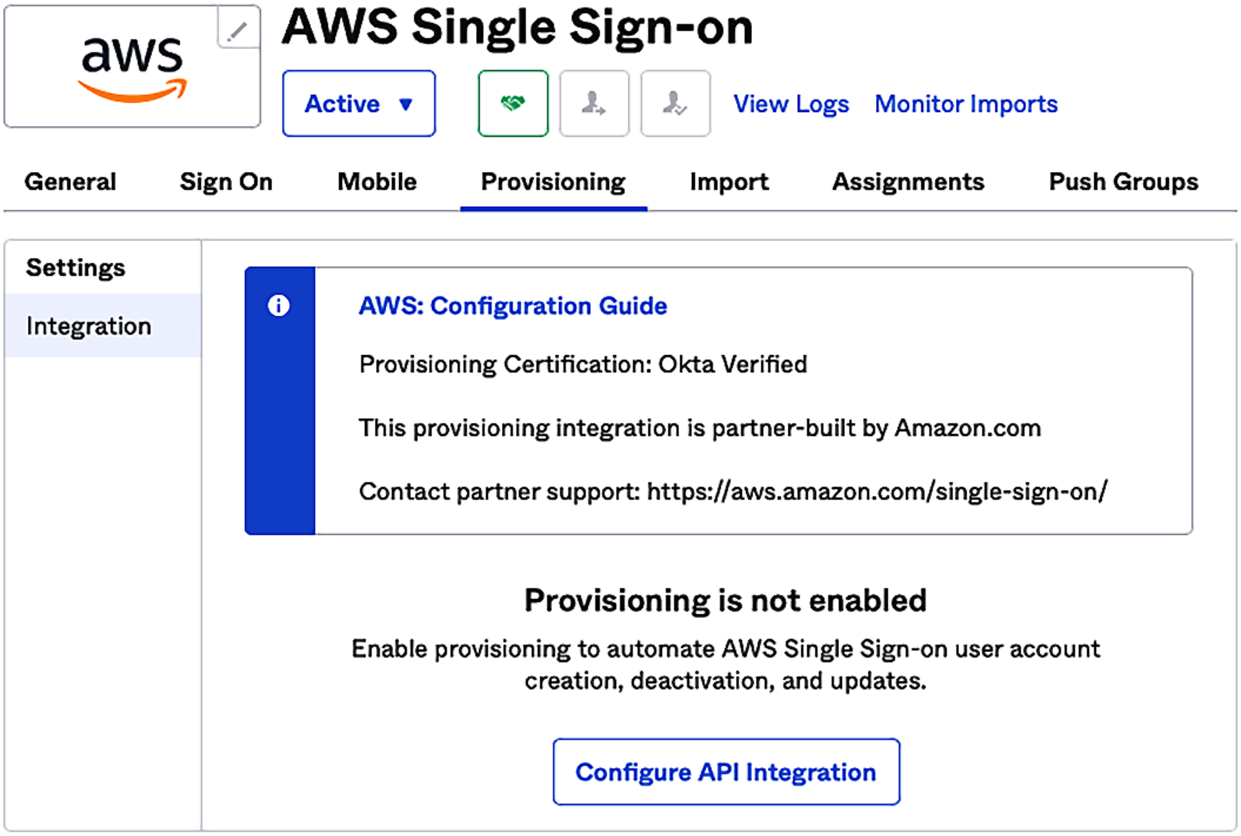
You cannot recover it later. However, you can generate new tokens at any time. Learn more

SCIM endpoint

https://scim.us-east-1.amazonaws.com/f3v447cc425-8a75-4b36-aa15-9c9e9b818539/scim/v2/

Access token

e943c0cc-ad5e-4292-8a55-[redacted]



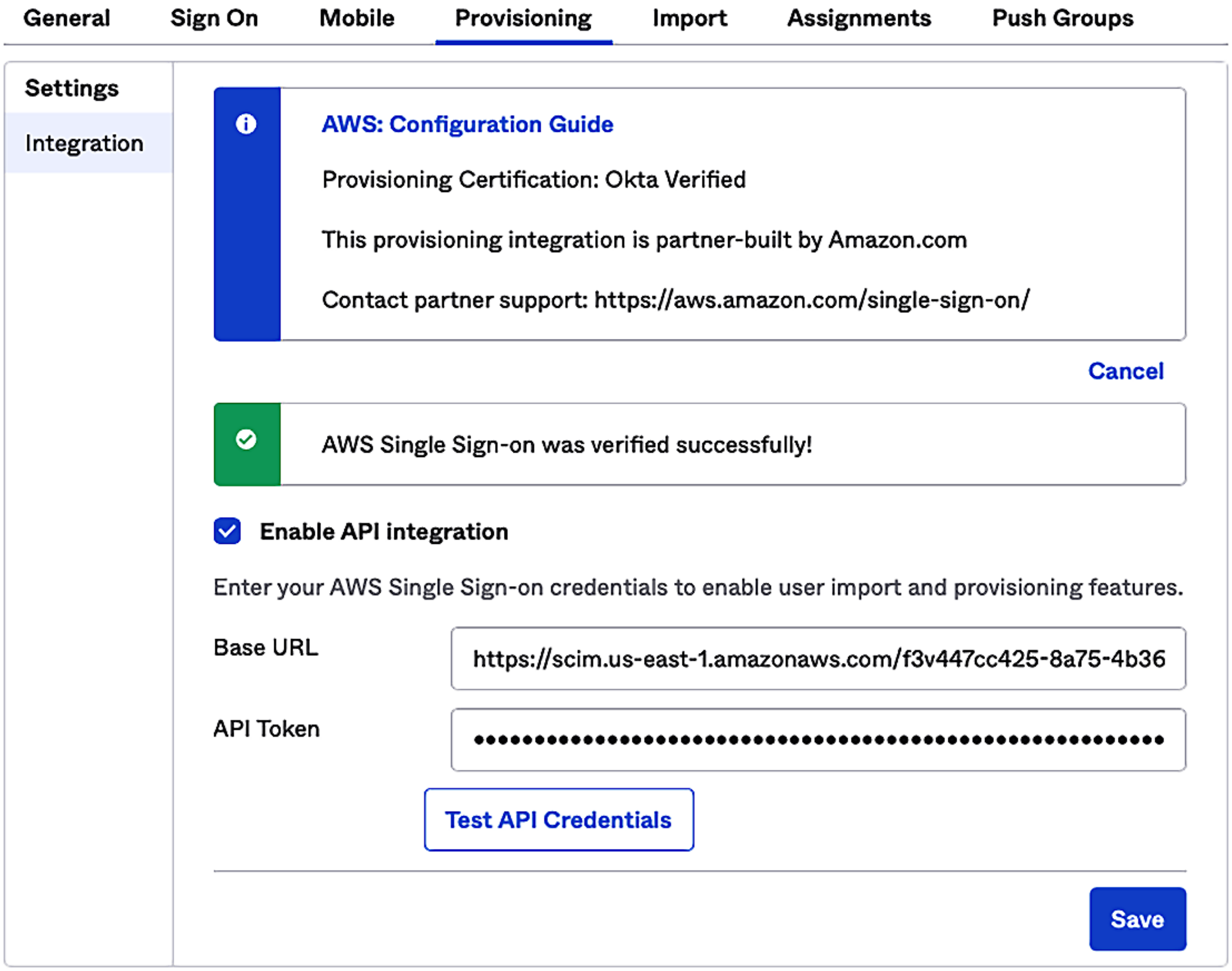
Provisioning Certification: Okta Verified

This provisioning integration is partner-built by Amazon.com

Contact partner support: https://aws.amazon.com/single-sign-on/

Provisioning is not enabled

Enable provisioning to automate AWS Single Sign-on user account creation, deactivation, and updates.



AWS: Configuration Guide

Provisioning Certification: Okta Verified

This provisioning integration is partner-built by Amazon.com

Contact partner support: https://aws.amazon.com/single-sign-on/

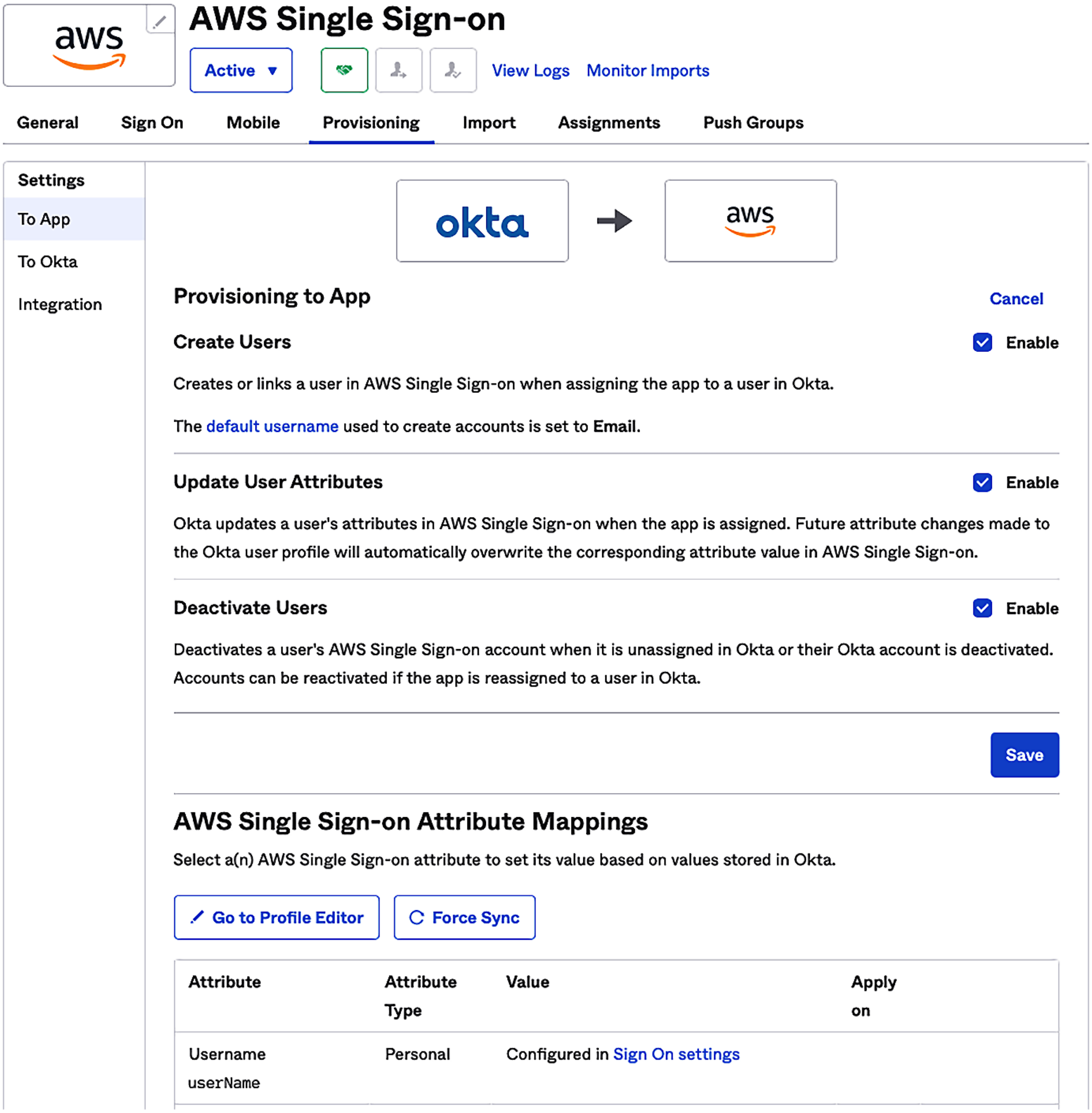
AWS Single Sign-on was verified successfully!

☑ **Enable API integration**

Enter your AWS Single Sign-on credentials to enable user import and provisioning features.

Base URL: https://scim.us-east-1.amazonaws.com/f3v447cc425-8a75-4b36

API Token: ••



AWS Single Sign-on

Provisioning to App

Create Users ☑ Enable

Creates or links a user in AWS Single Sign-on when assigning the app to a user in Okta.

The default username used to create accounts is set to **Email**.

Update User Attributes ☑ Enable

Okta updates a user's attributes in AWS Single Sign-on when the app is assigned. Future attribute changes made to the Okta user profile will automatically overwrite the corresponding attribute value in AWS Single Sign-on.

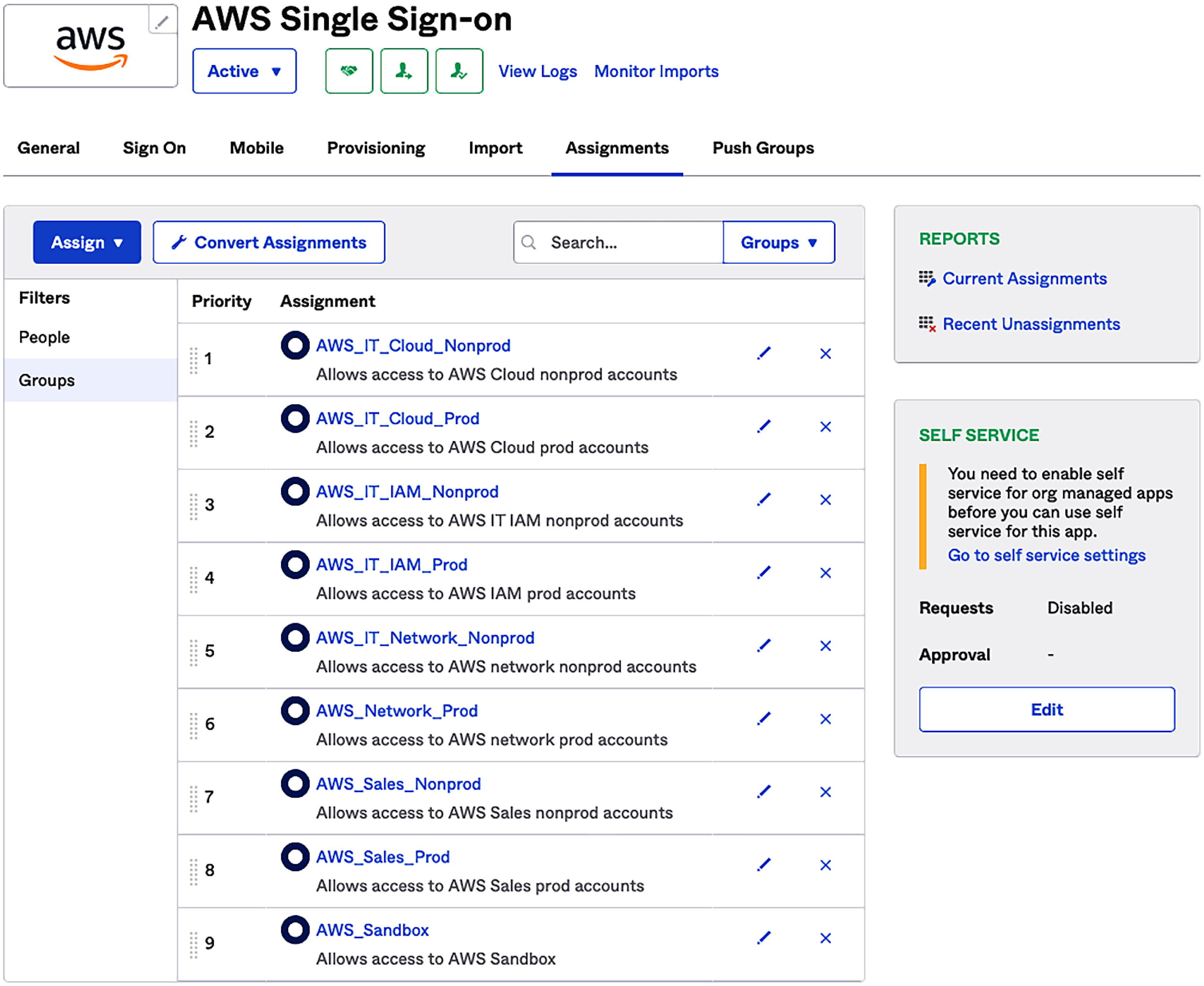
Deactivate Users ☑ Enable

Deactivates a user's AWS Single Sign-on account when it is unassigned in Okta or their Okta account is deactivated. Accounts can be reactivated if the app is reassigned to a user in Okta.

AWS Single Sign-on Attribute Mappings

Select a(n) AWS Single Sign-on attribute to set its value based on values stored in Okta.

Attribute	Attribute Type	Value	Apply on
Username `userName`	Personal	Configured in Sign On settings	



Priority	Assignment
1	AWS_IT_Cloud_Nonprod Allows access to AWS Cloud nonprod accounts
2	AWS_IT_Cloud_Prod Allows access to AWS Cloud prod accounts
3	AWS_IT_IAM_Nonprod Allows access to AWS IT IAM nonprod accounts
4	AWS_IT_IAM_Prod Allows access to AWS IAM prod accounts
5	AWS_IT_Network_Nonprod Allows access to AWS network nonprod accounts
6	AWS_Network_Prod Allows access to AWS network prod accounts
7	AWS_Sales_Nonprod Allows access to AWS Sales nonprod accounts
8	AWS_Sales_Prod Allows access to AWS Sales prod accounts
9	AWS_Sandbox Allows access to AWS Sandbox

REPORTS

Current Assignments

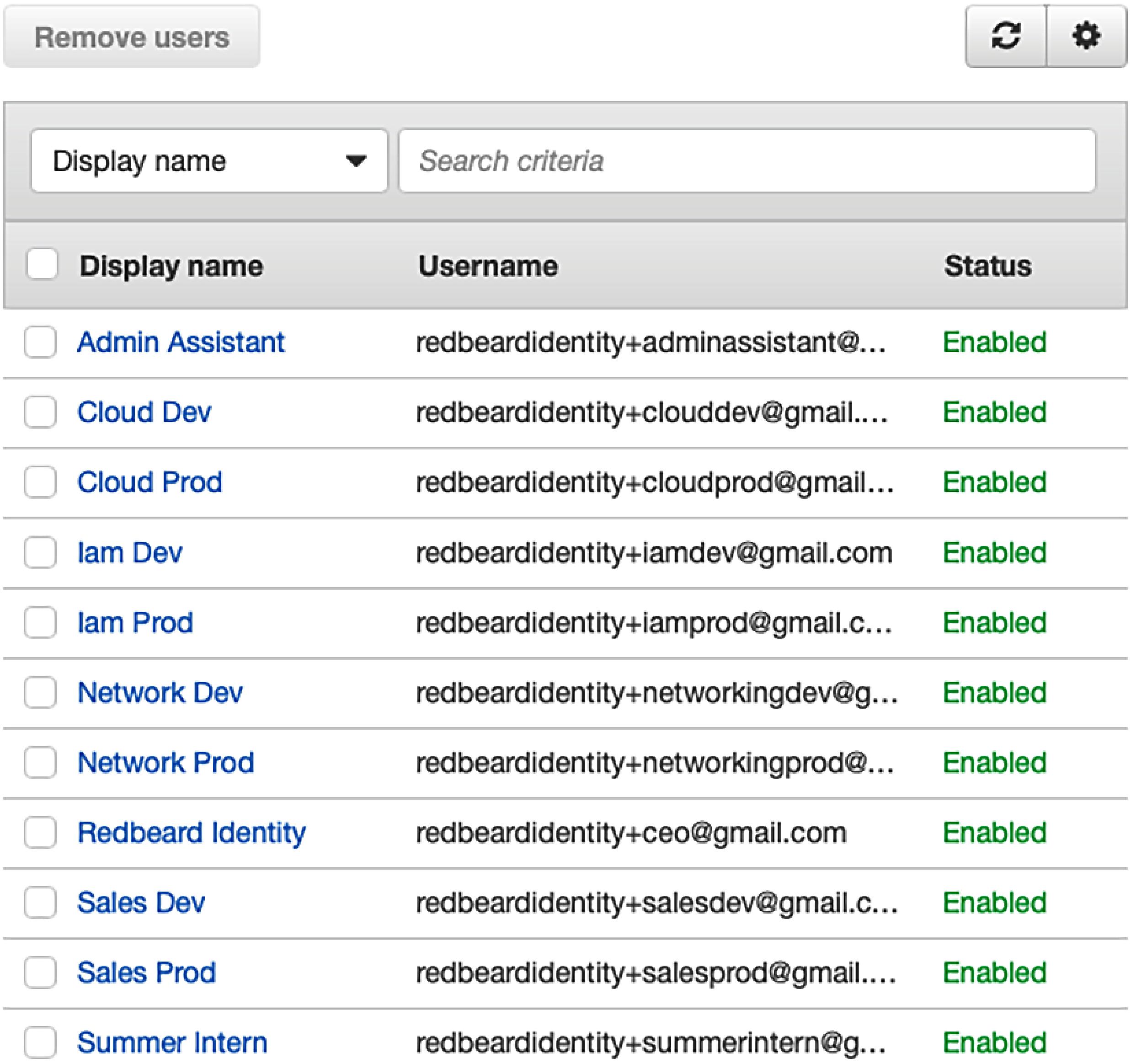
Recent Unassignments

SELF SERVICE

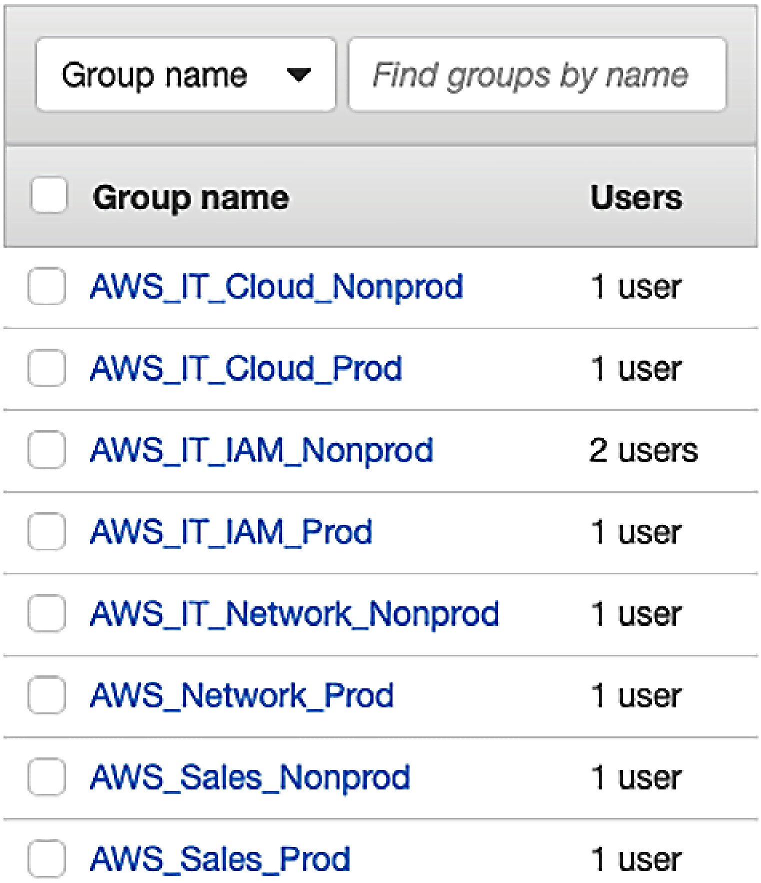
You need to enable self service for org managed apps before you can use self service for this app.

Go to self service settings

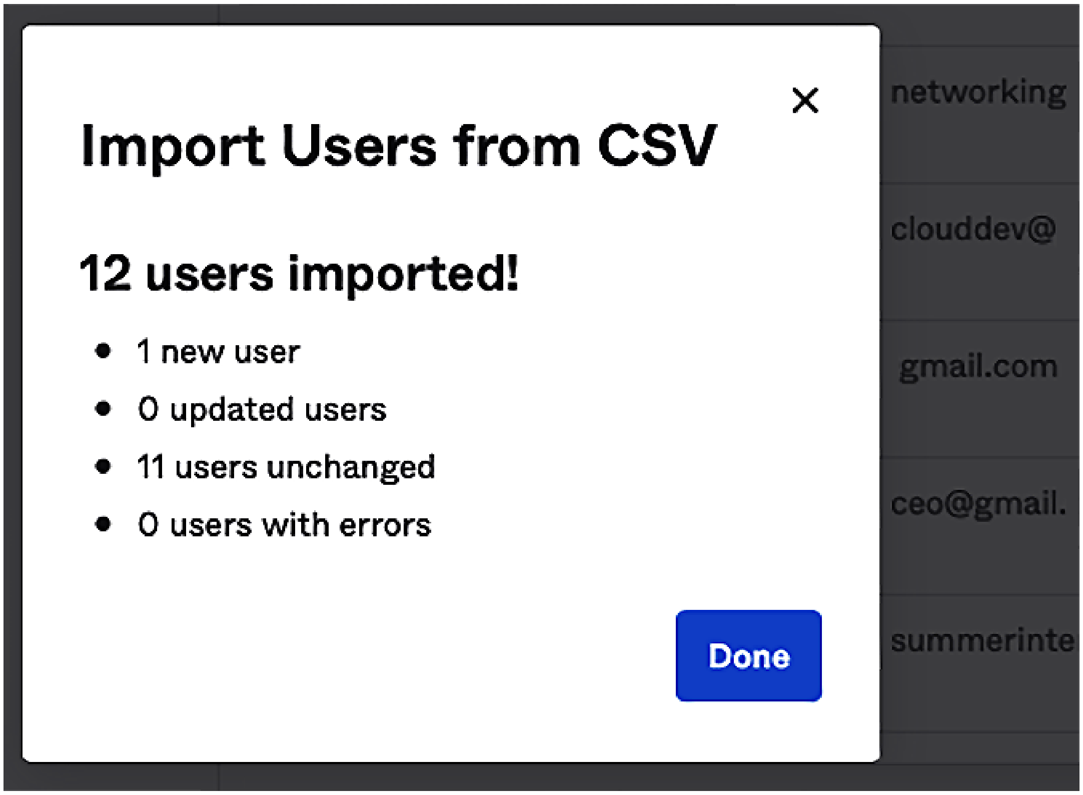
Requests	Disabled
Approval	-



□	Display name	Username	Status
□	Admin Assistant	redbeardidentity+adminassistant@...	Enabled
□	Cloud Dev	redbeardidentity+clouddev@gmail....	Enabled
□	Cloud Prod	redbeardidentity+cloudprod@gmail...	Enabled
□	Iam Dev	redbeardidentity+iamdev@gmail.com	Enabled
□	Iam Prod	redbeardidentity+iamprod@gmail.c...	Enabled
□	Network Dev	redbeardidentity+networkingdev@g...	Enabled
□	Network Prod	redbeardidentity+networkingprod@...	Enabled
□	Redbeard Identity	redbeardidentity+ceo@gmail.com	Enabled
□	Sales Dev	redbeardidentity+salesdev@gmail.c...	Enabled
□	Sales Prod	redbeardidentity+salesprod@gmail....	Enabled
□	Summer Intern	redbeardidentity+summerintern@g...	Enabled



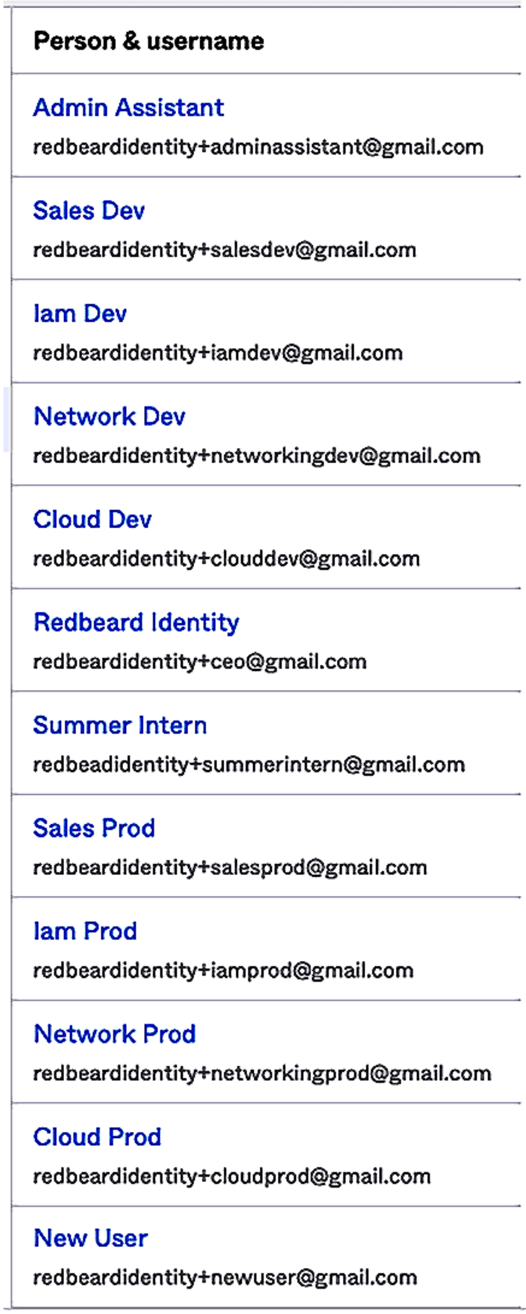
□	Group name	Users
□	AWS_IT_Cloud_Nonprod	1 user
□	AWS_IT_Cloud_Prod	1 user
□	AWS_IT_IAM_Nonprod	2 users
□	AWS_IT_IAM_Prod	1 user
□	AWS_IT_Network_Nonprod	1 user
□	AWS_Network_Prod	1 user
□	AWS_Sales_Nonprod	1 user
□	AWS_Sales_Prod	1 user



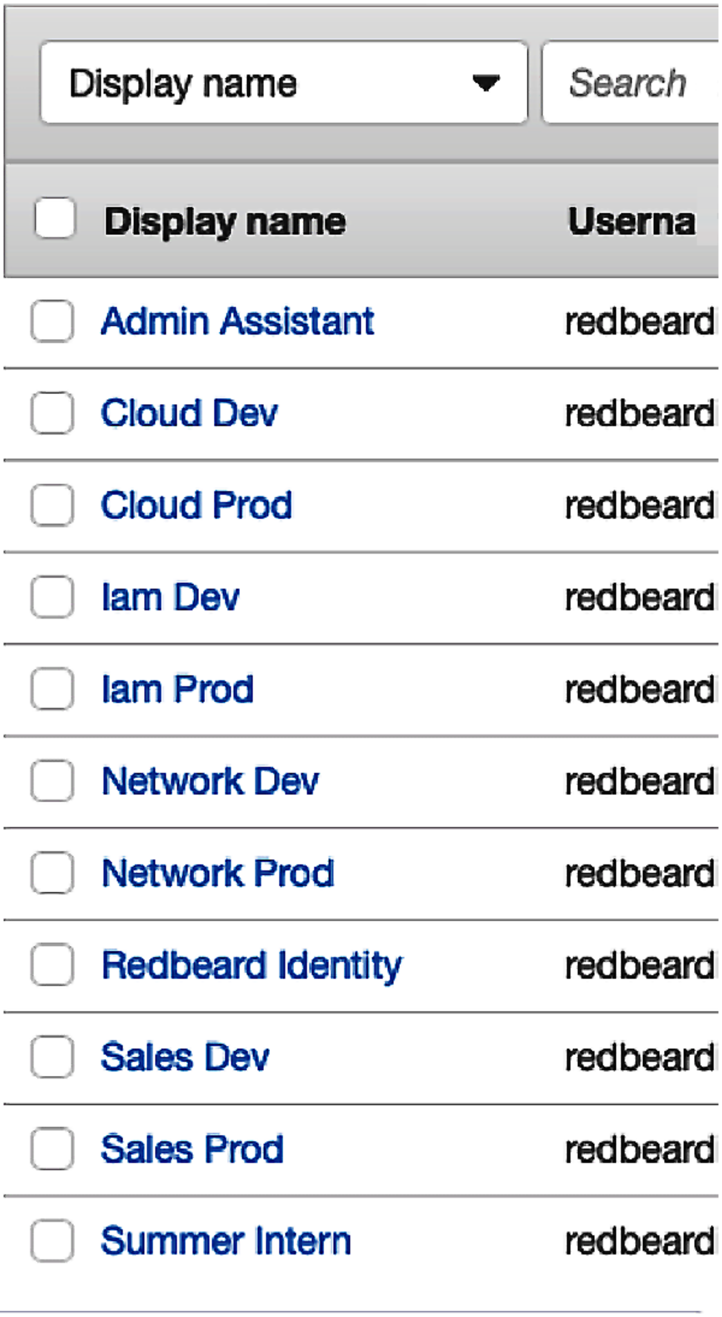
Import Users from CSV

12 users imported!

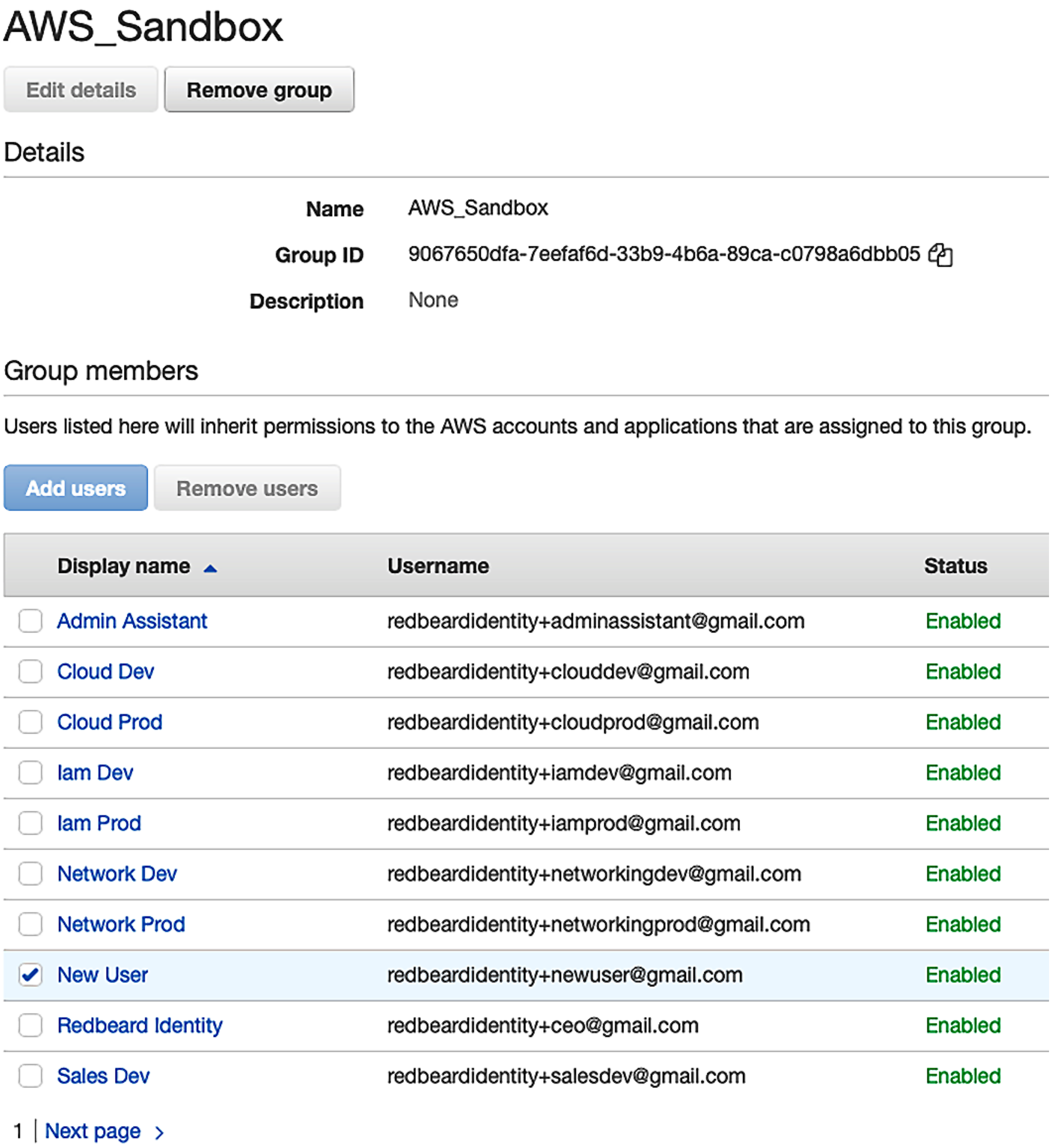
- 1 new user
- 0 updated users
- 11 users unchanged
- 0 users with errors



Person & username
Admin Assistant redbeardidentity+adminassistant@gmail.com
Sales Dev redbeardidentity+salesdev@gmail.com
Iam Dev redbeardidentity+iamdev@gmail.com
Network Dev redbeardidentity+networkingdev@gmail.com
Cloud Dev redbeardidentity+clouddev@gmail.com
Redbeard Identity redbeardidentity+ceo@gmail.com
Summer Intern redbeadidentity+summerintern@gmail.com
Sales Prod redbeardidentity+salesprod@gmail.com
Iam Prod redbeardidentity+iamprod@gmail.com
Network Prod redbeardidentity+networkingprod@gmail.com
Cloud Prod redbeardidentity+cloudprod@gmail.com
New User redbeardidentity+newuser@gmail.com



□	Display name	Userna
□	Admin Assistant	redbeard
□	Cloud Dev	redbeard
□	Cloud Prod	redbeard
□	Iam Dev	redbeard
□	Iam Prod	redbeard
□	Network Dev	redbeard
□	Network Prod	redbeard
□	Redbeard Identity	redbeard
□	Sales Dev	redbeard
□	Sales Prod	redbeard
□	Summer Intern	redbeard



AWS_Sandbox

Details

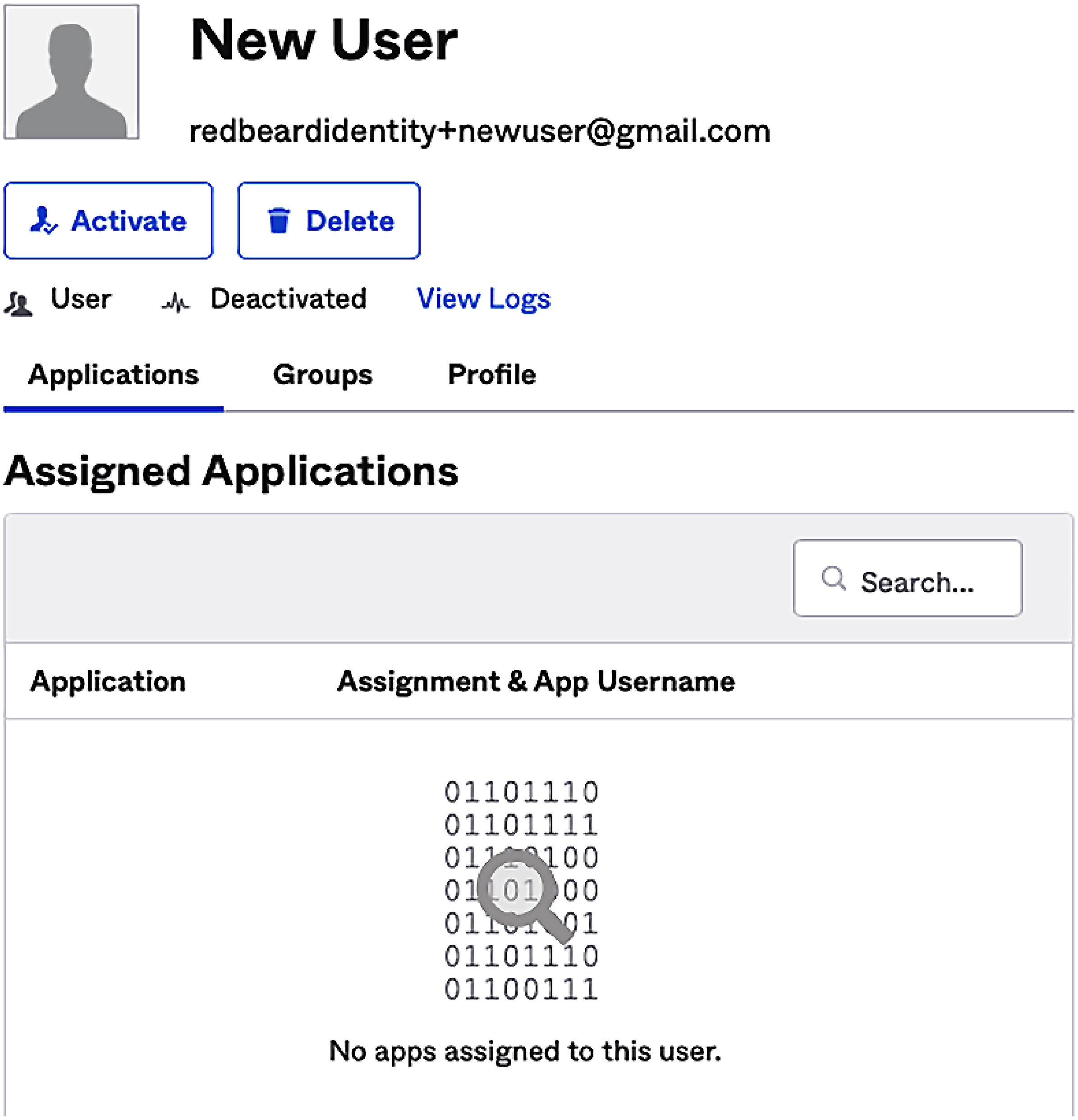
Name	AWS_Sandbox
Group ID	9067650dfa-7eefaf6d-33b9-4b6a-89ca-c0798a6dbb05
Description	None

Group members

Users listed here will inherit permissions to the AWS accounts and applications that are assigned to this group.

	Display name ▲	Username	Status
□	Admin Assistant	redbeardidentity+adminassistant@gmail.com	Enabled
□	Cloud Dev	redbeardidentity+clouddev@gmail.com	Enabled
□	Cloud Prod	redbeardidentity+cloudprod@gmail.com	Enabled
□	Iam Dev	redbeardidentity+iamdev@gmail.com	Enabled
□	Iam Prod	redbeardidentity+iamprod@gmail.com	Enabled
□	Network Dev	redbeardidentity+networkingdev@gmail.com	Enabled
□	Network Prod	redbeardidentity+networkingprod@gmail.com	Enabled
☑	New User	redbeardidentity+newuser@gmail.com	Enabled
□	Redbeard Identity	redbeardidentity+ceo@gmail.com	Enabled
□	Sales Dev	redbeardidentity+salesdev@gmail.com	Enabled

1 | Next page ›



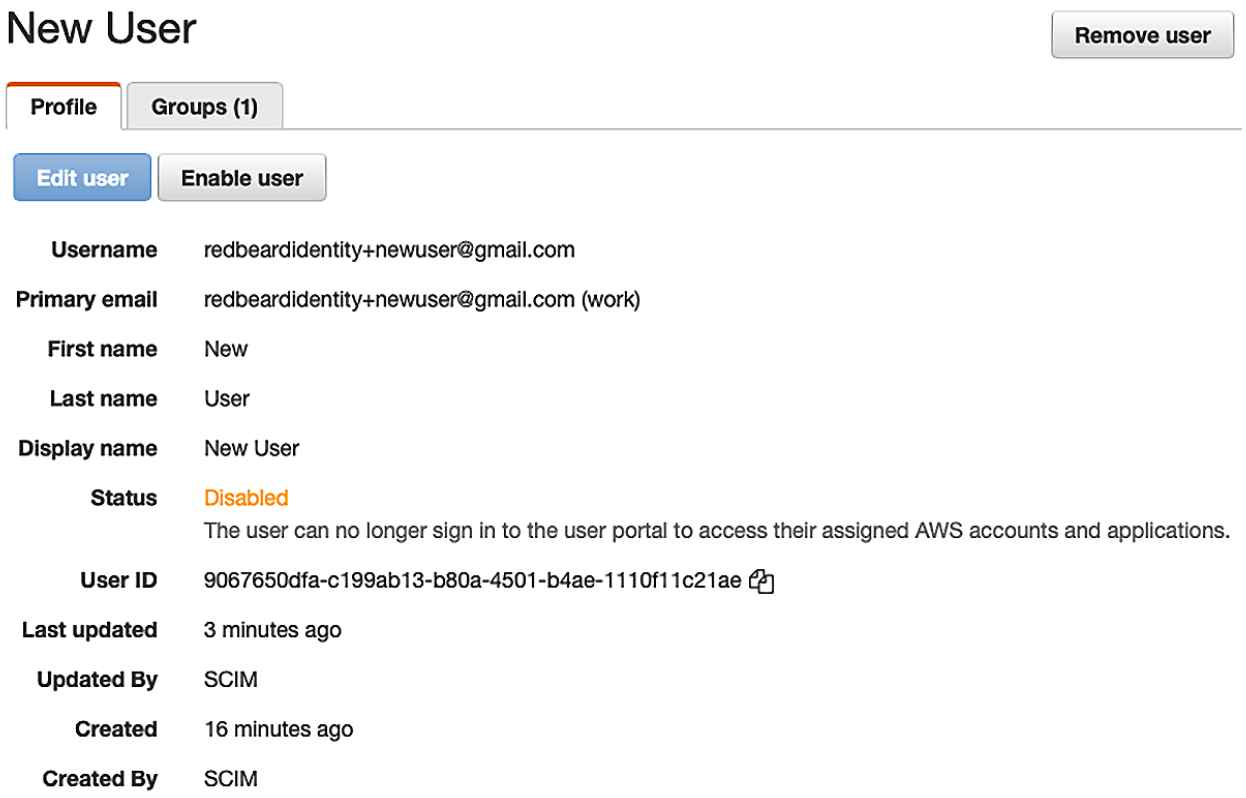
New User

redbeardidentity+newuser@gmail.com

Assigned Applications

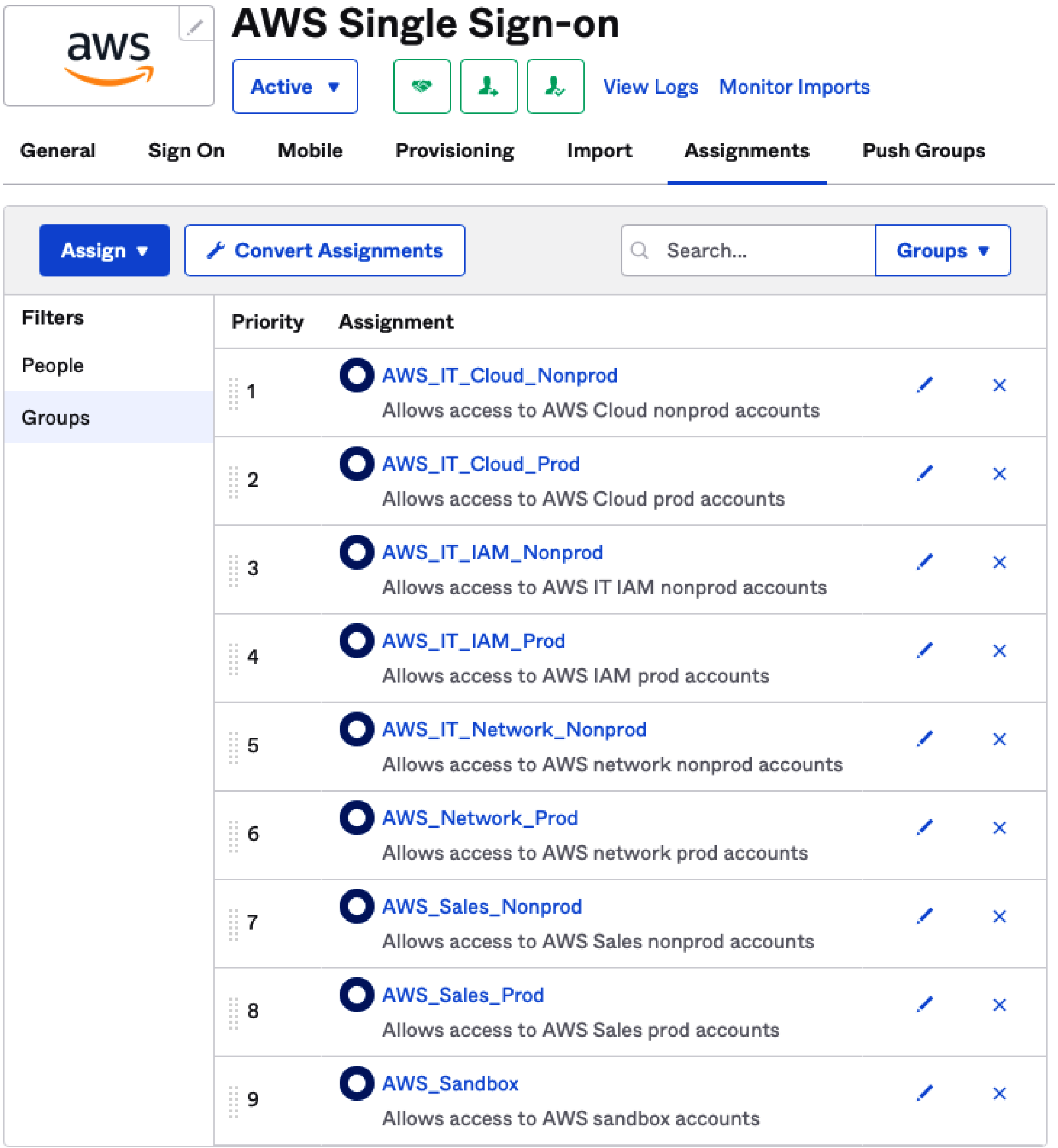
Application	Assignment & App Username

No apps assigned to this user.

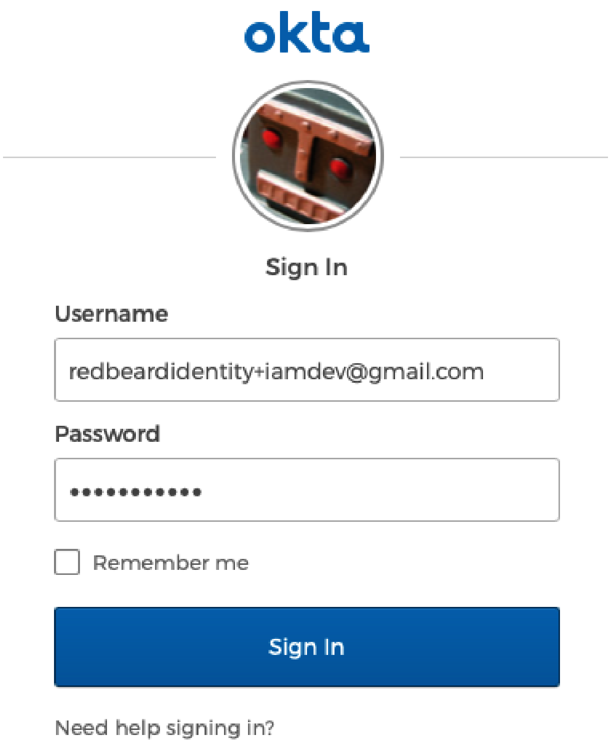


New User

Username	redbeardidentity+newuser@gmail.com
Primary email	redbeardidentity+newuser@gmail.com (work)
First name	New
Last name	User
Display name	New User
Status	Disabled The user can no longer sign in to the user portal to access their assigned AWS accounts and applications.
User ID	9067650dfa-c199ab13-b80a-4501-b4ae-1110f11c21ae
Last updated	3 minutes ago
Updated By	SCIM
Created	16 minutes ago
Created By	SCIM



Priority	Assignment
1	AWS_IT_Cloud_Nonprod Allows access to AWS Cloud nonprod accounts
2	AWS_IT_Cloud_Prod Allows access to AWS Cloud prod accounts
3	AWS_IT_IAM_Nonprod Allows access to AWS IT IAM nonprod accounts
4	AWS_IT_IAM_Prod Allows access to AWS IAM prod accounts
5	AWS_IT_Network_Nonprod Allows access to AWS network nonprod accounts
6	AWS_Network_Prod Allows access to AWS network prod accounts
7	AWS_Sales_Nonprod Allows access to AWS Sales nonprod accounts
8	AWS_Sales_Prod Allows access to AWS Sales prod accounts
9	AWS_Sandbox Allows access to AWS sandbox accounts



Sign In

Username

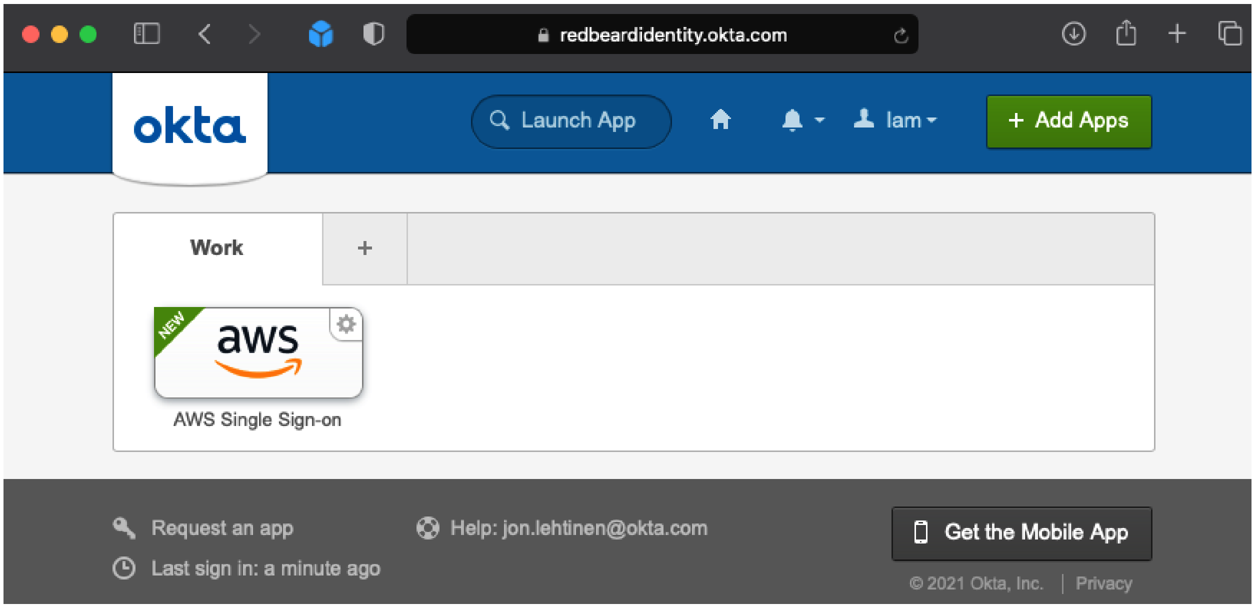
redbeardidentity+iamdev@gmail.com

Password

●●●●●●●●●●●

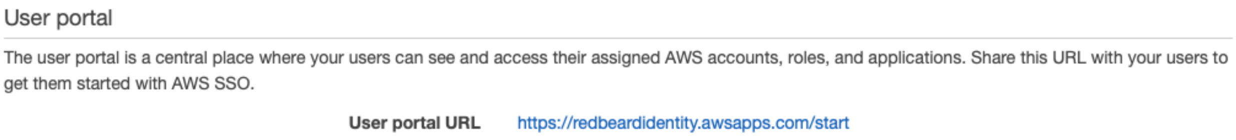
□ Remember me

Need help signing in?


redbeardidentity.okta.com
okta
Launch App
Iam
+ Add Apps
Work
+
NEW
aws

AWS Single Sign-on

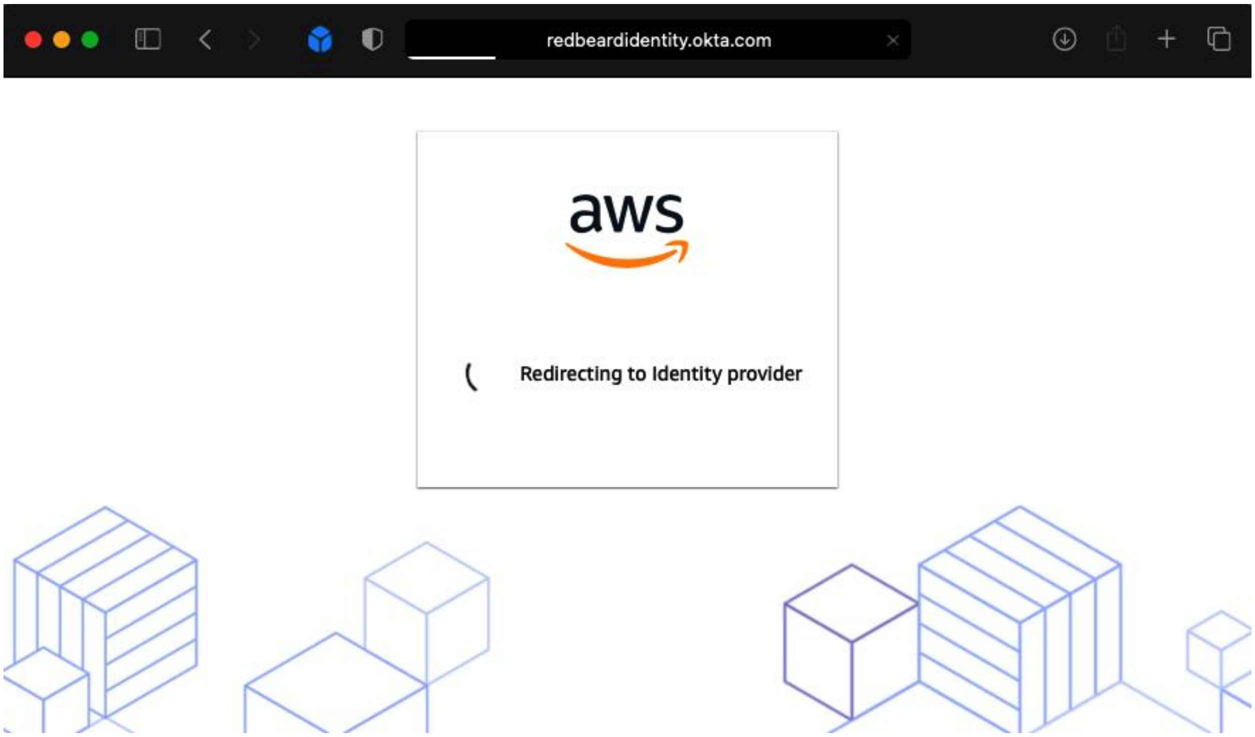
Request an app
Last sign in: a minute ago
Help: jon.lehtinen@okta.com
Get the Mobile App
© 2021 Okta, Inc. | Privacy



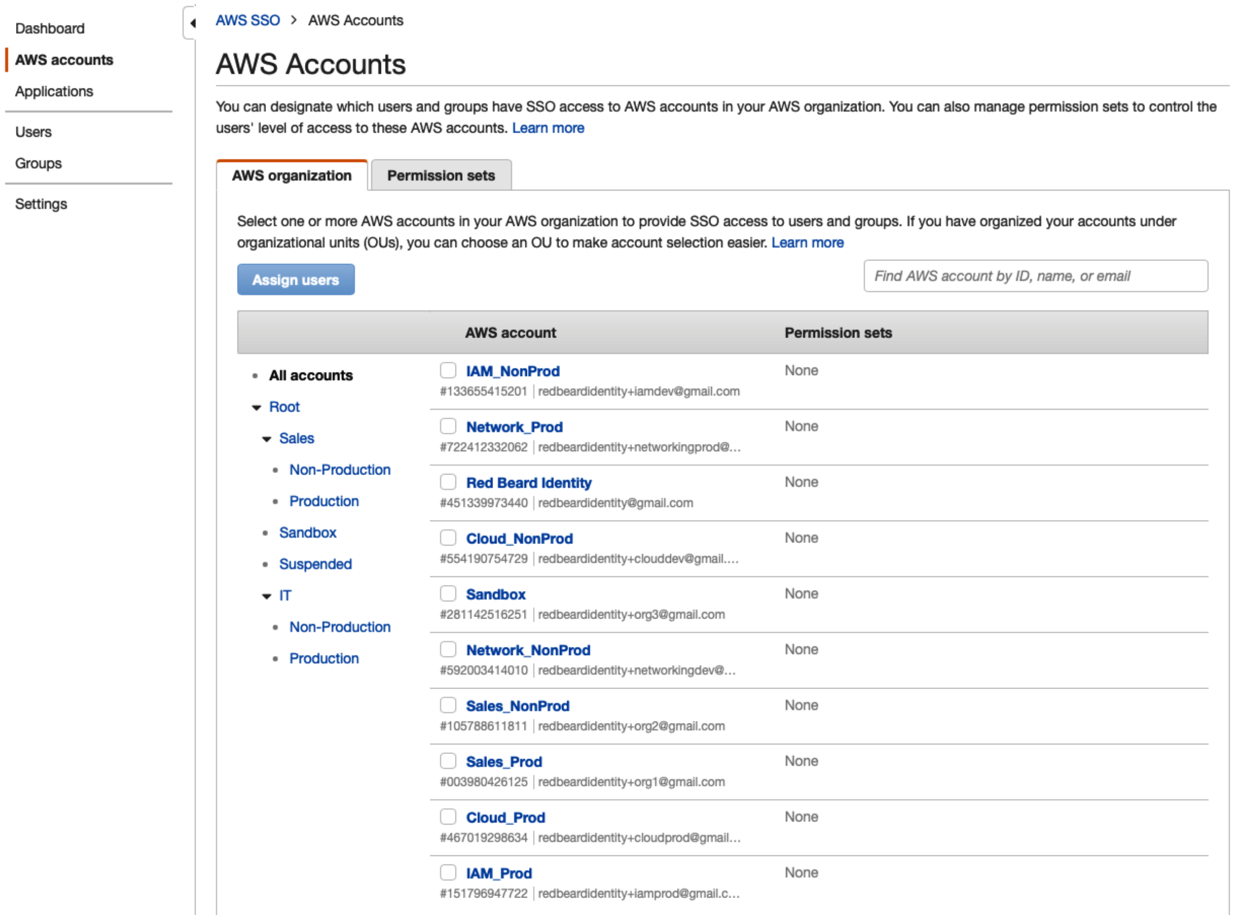
User portal

The user portal is a central place where your users can see and access their assigned AWS accounts, roles, and applications. Share this URL with your users to get them started with AWS SSO.

User portal URL https://redbeardidentity.awsapps.com/start



Redirecting to Identity provider



AWS SSO > AWS Accounts

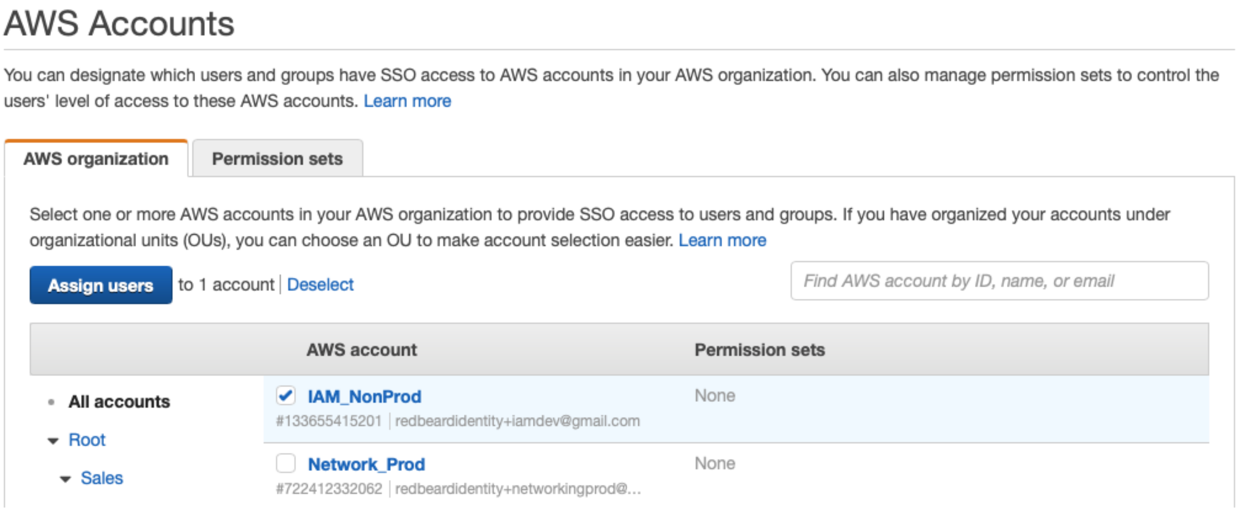
AWS Accounts

You can designate which users and groups have SSO access to AWS accounts in your AWS organization. You can also manage permission sets to control the users' level of access to these AWS accounts. Learn more

Select one or more AWS accounts in your AWS organization to provide SSO access to users and groups. If you have organized your accounts under organizational units (OUs), you can choose an OU to make account selection easier. Learn more

- All accounts
- Root
  - Sales
    - Non-Production
    - Production
  - Sandbox
  - Suspended
  - IT
    - Non-Production
    - Production

AWS account	Permission sets
□ IAM_NonProd #133655415201 | redbeardidentity+iamdev@gmail.com	None
□ Network_Prod #722412332062 | redbeardidentity+networkingprod@...	None
□ Red Beard Identity #451339973440 | redbeardidentity@gmail.com	None
□ Cloud_NonProd #554190754729 | redbeardidentity+clouddev@gmail....	None
□ Sandbox #281142516251 | redbeardidentity+org3@gmail.com	None
□ Network_NonProd #592003414010 | redbeardidentity+networkingdev@...	None
□ Sales_NonProd #105788611811 | redbeardidentity+org2@gmail.com	None
□ Sales_Prod #003980426125 | redbeardidentity+org1@gmail.com	None
□ Cloud_Prod #467019298634 | redbeardidentity+cloudprod@gmail...	None
□ IAM_Prod #151796947722 | redbeardidentity+iamprod@gmail.c...	None



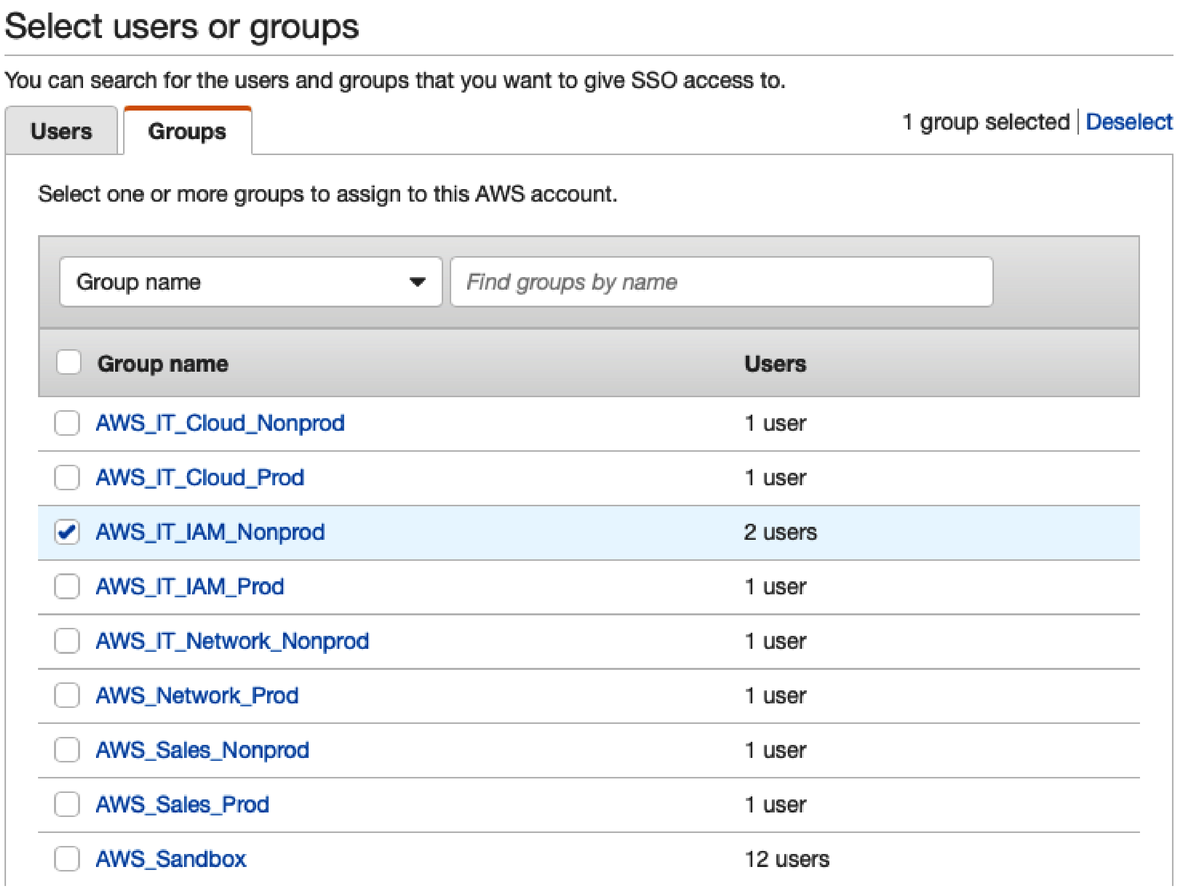
AWS Accounts

You can designate which users and groups have SSO access to AWS accounts in your AWS organization. You can also manage permission sets to control the users' level of access to these AWS accounts. Learn more

Select one or more AWS accounts in your AWS organization to provide SSO access to users and groups. If you have organized your accounts under organizational units (OUs), you can choose an OU to make account selection easier. Learn more

- All accounts
- Root
  - Sales

AWS account	Permission sets
☑ IAM_NonProd #133655415201 | redbeardidentity+iamdev@gmail.com	None
□ Network_Prod #722412332062 | redbeardidentity+networkingprod@...	None



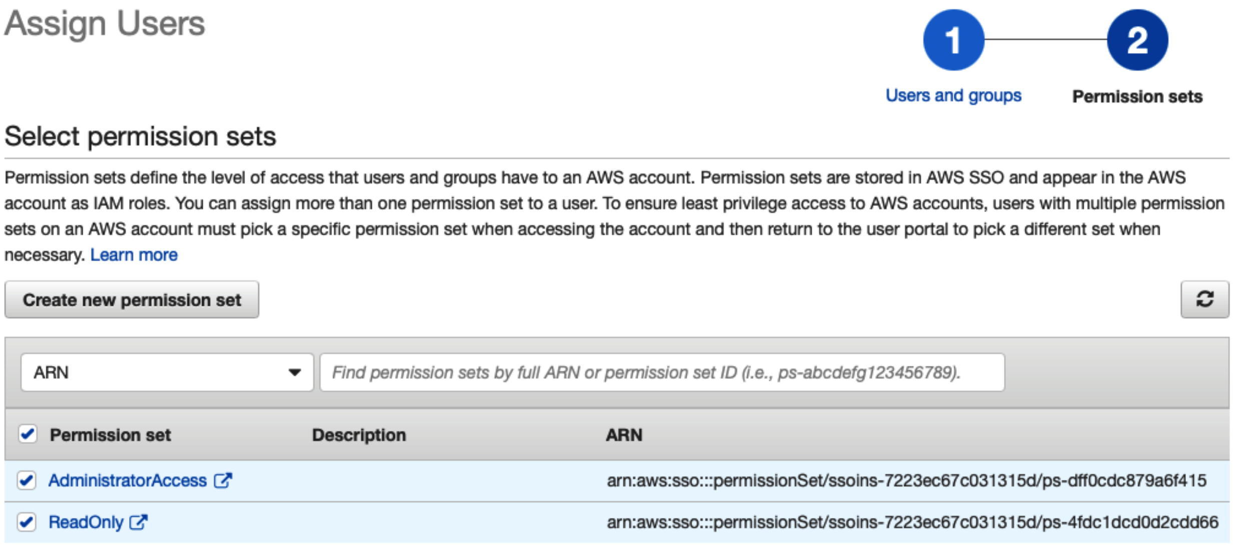
Select users or groups

You can search for the users and groups that you want to give SSO access to.

1 group selected | Deselect

Select one or more groups to assign to this AWS account.

☐ Group name	Users
☐ AWS_IT_Cloud_Nonprod	1 user
☐ AWS_IT_Cloud_Prod	1 user
☑ AWS_IT_IAM_Nonprod	2 users
☐ AWS_IT_IAM_Prod	1 user
☐ AWS_IT_Network_Nonprod	1 user
☐ AWS_Network_Prod	1 user
☐ AWS_Sales_Nonprod	1 user
☐ AWS_Sales_Prod	1 user
☐ AWS_Sandbox	12 users



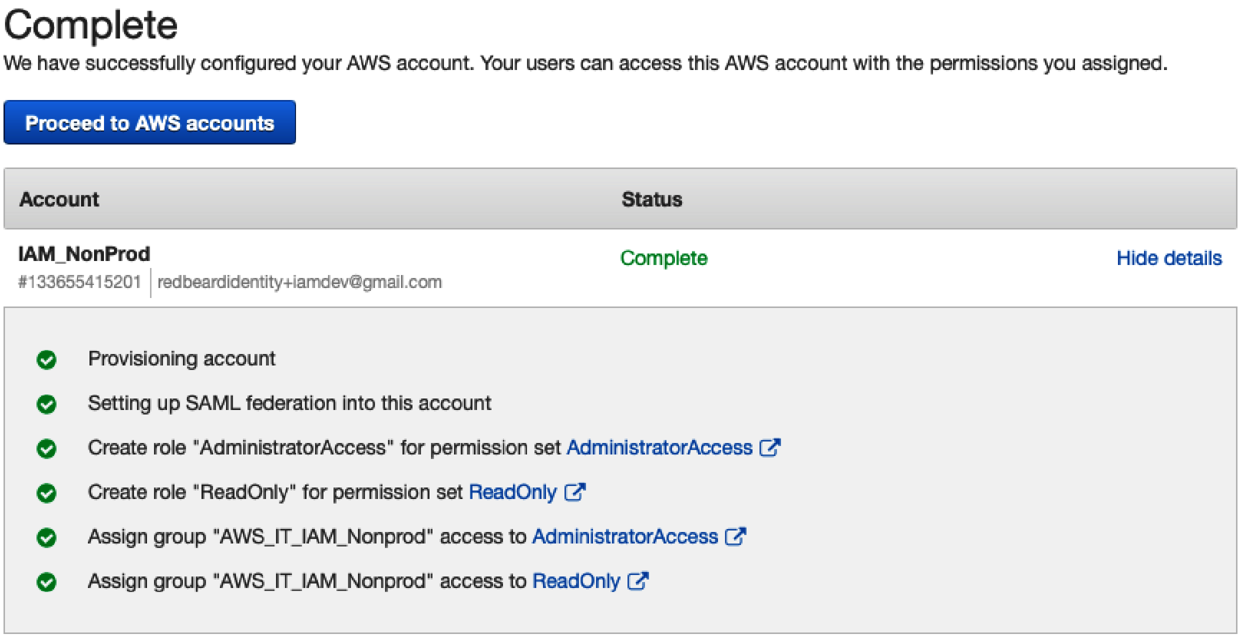
Assign Users

Select permission sets

Permission sets define the level of access that users and groups have to an AWS account. Permission sets are stored in AWS SSO and appear in the AWS account as IAM roles. You can assign more than one permission set to a user. To ensure least privilege access to AWS accounts, users with multiple permission sets on an AWS account must pick a specific permission set when accessing the account and then return to the user portal to pick a different set when necessary. Learn more

Create new permission set
ARN
Find permission sets by full ARN or permission set ID (i.e., ps-abcdefg123456789).

☑ Permission set	Description	ARN
☑ AdministratorAccess		arn:aws:sso:::permissionSet/ssoins-7223ec67c031315d/ps-dff0cdc879a6f415
☑ ReadOnly		arn:aws:sso:::permissionSet/ssoins-7223ec67c031315d/ps-4fdc1dcd0d2cdd66

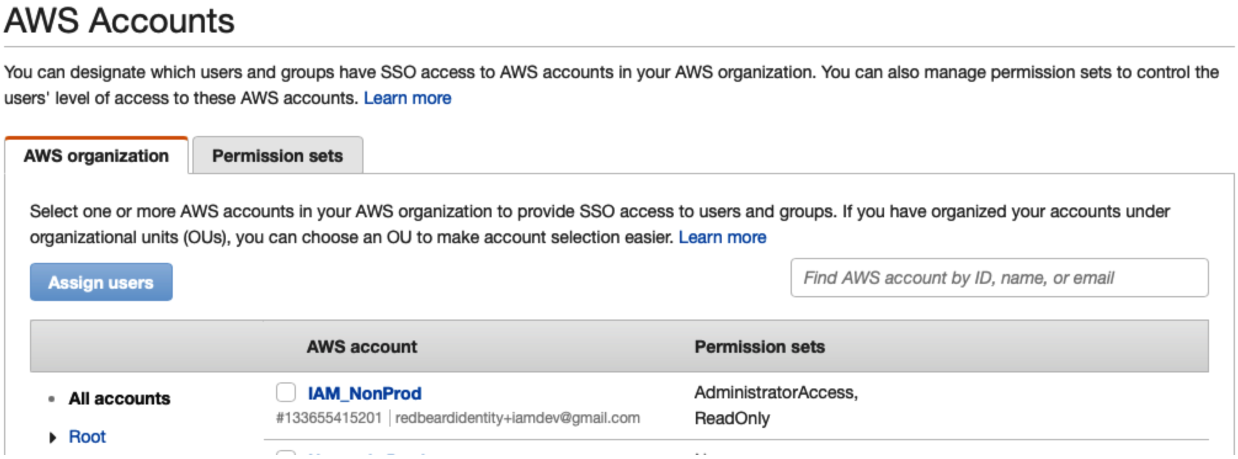


Complete

We have successfully configured your AWS account. Your users can access this AWS account with the permissions you assigned.

Account	Status	
IAM_NonProd #133655415201 | redbeardidentity+iamdev@gmail.com	Complete	Hide details

- ✓ Provisioning account
- ✓ Setting up SAML federation into this account
- ✓ Create role "AdministratorAccess" for permission set AdministratorAccess
- ✓ Create role "ReadOnly" for permission set ReadOnly
- ✓ Assign group "AWS_IT_IAM_Nonprod" access to AdministratorAccess
- ✓ Assign group "AWS_IT_IAM_Nonprod" access to ReadOnly

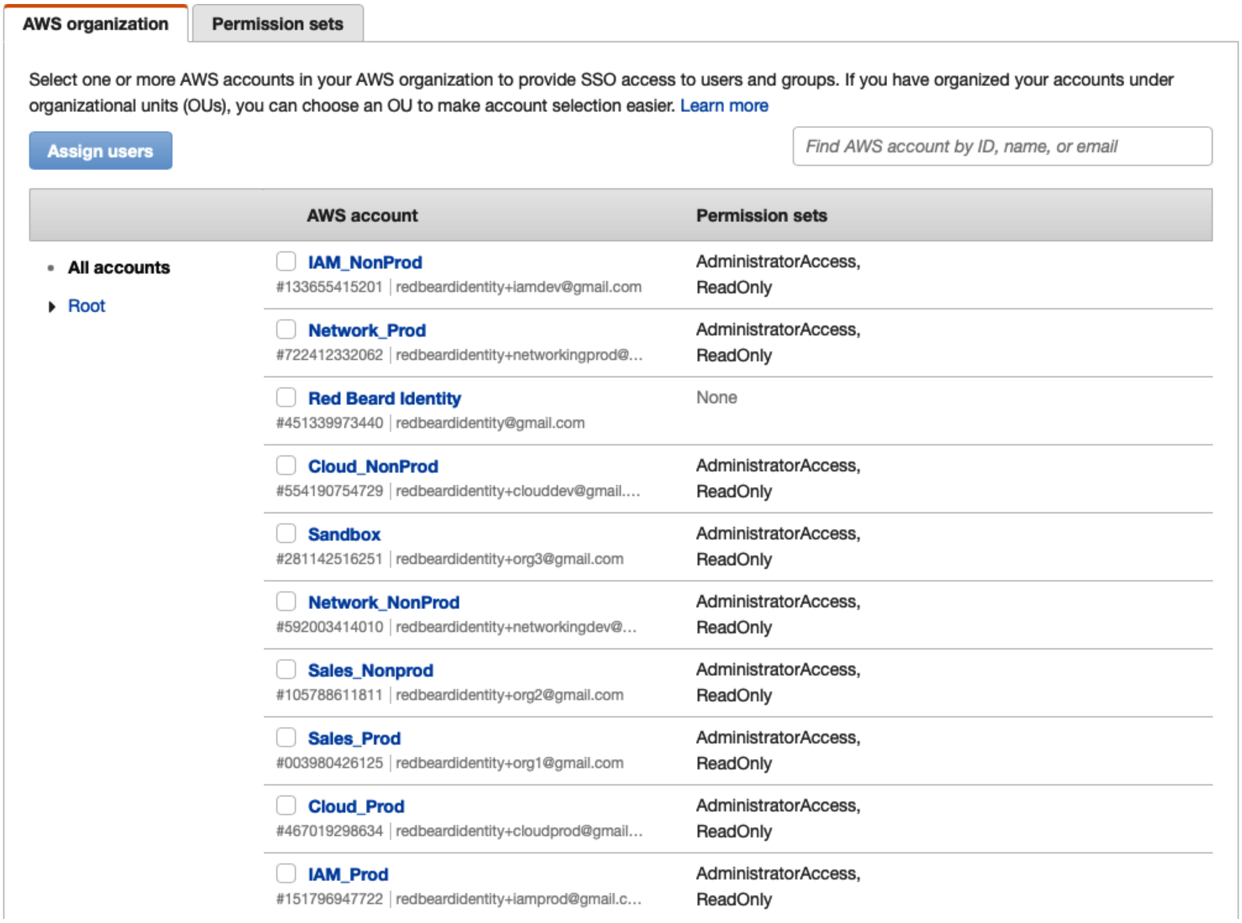


AWS Accounts

You can designate which users and groups have SSO access to AWS accounts in your AWS organization. You can also manage permission sets to control the users' level of access to these AWS accounts. Learn more

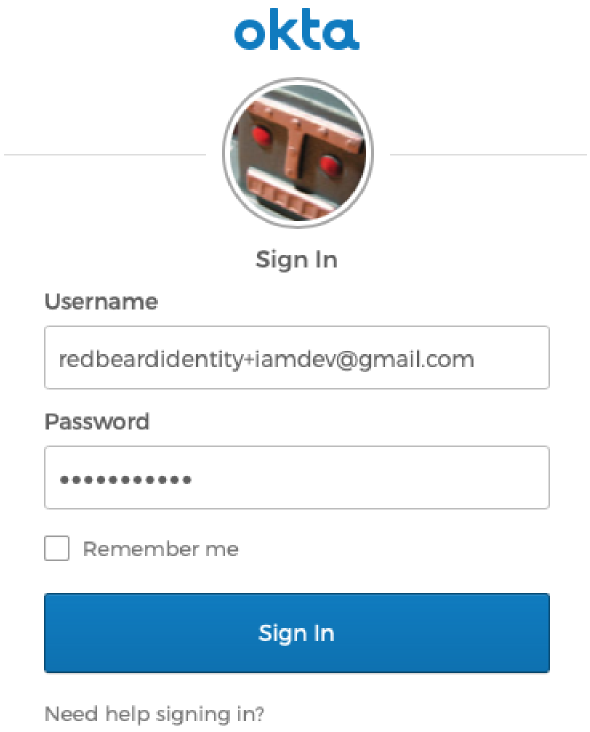
Select one or more AWS accounts in your AWS organization to provide SSO access to users and groups. If you have organized your accounts under organizational units (OUs), you can choose an OU to make account selection easier. Learn more

	AWS account	Permission sets
• **All accounts** ▸ Root	☐ **IAM_NonProd** #133655415201 | redbeardidentity+iamdev@gmail.com	AdministratorAccess, ReadOnly



Select one or more AWS accounts in your AWS organization to provide SSO access to users and groups. If you have organized your accounts under organizational units (OUs), you can choose an OU to make account selection easier. Learn more

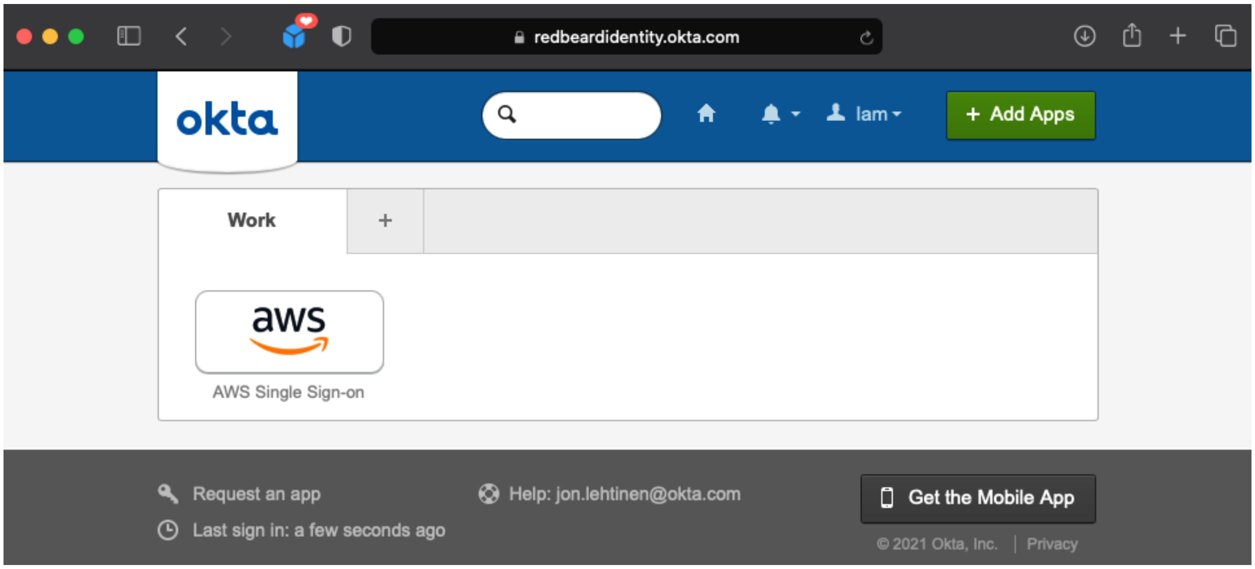
AWS account	Permission sets
□ IAM_NonProd #133655415201 | redbeardidentity+iamdev@gmail.com	AdministratorAccess, ReadOnly
□ Network_Prod #722412332062 | redbeardidentity+networkingprod@…	AdministratorAccess, ReadOnly
□ Red Beard Identity #451339973440 | redbeardidentity@gmail.com	None
□ Cloud_NonProd #554190754729 | redbeardidentity+clouddev@gmail.…	AdministratorAccess, ReadOnly
□ Sandbox #281142516251 | redbeardidentity+org3@gmail.com	AdministratorAccess, ReadOnly
□ Network_NonProd #592003414010 | redbeardidentity+networkingdev@…	AdministratorAccess, ReadOnly
□ Sales_Nonprod #105788611811 | redbeardidentity+org2@gmail.com	AdministratorAccess, ReadOnly
□ Sales_Prod #003980426125 | redbeardidentity+org1@gmail.com	AdministratorAccess, ReadOnly
□ Cloud_Prod #467019298634 | redbeardidentity+cloudprod@gmail…	AdministratorAccess, ReadOnly
□ IAM_Prod #151796947722 | redbeardidentity+iamprod@gmail.c…	AdministratorAccess, ReadOnly



Sign In

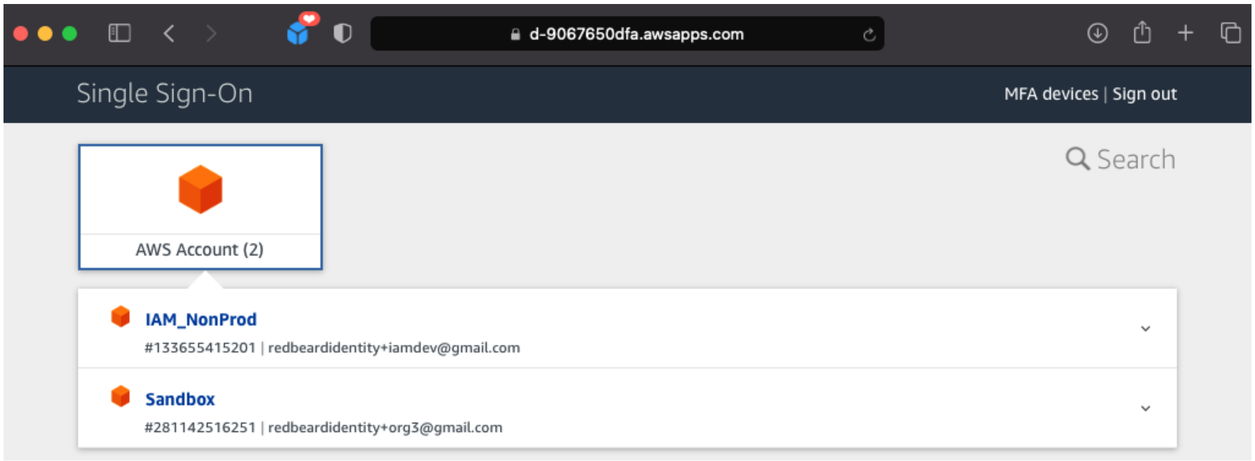
Username: redbeardidentity+iamdev@gmail.com

Password: ●●●●●●●●●●●●



redbeardidentity.okta.com

okta
Iam
+ Add Apps
Work
+
aws
AWS Single Sign-on
Request an app
Help: jon.lehtinen@okta.com
Last sign in: a few seconds ago
Get the Mobile App
© 2021 Okta, Inc. | Privacy



d-9067650dfa.awsapps.com

Single Sign-On

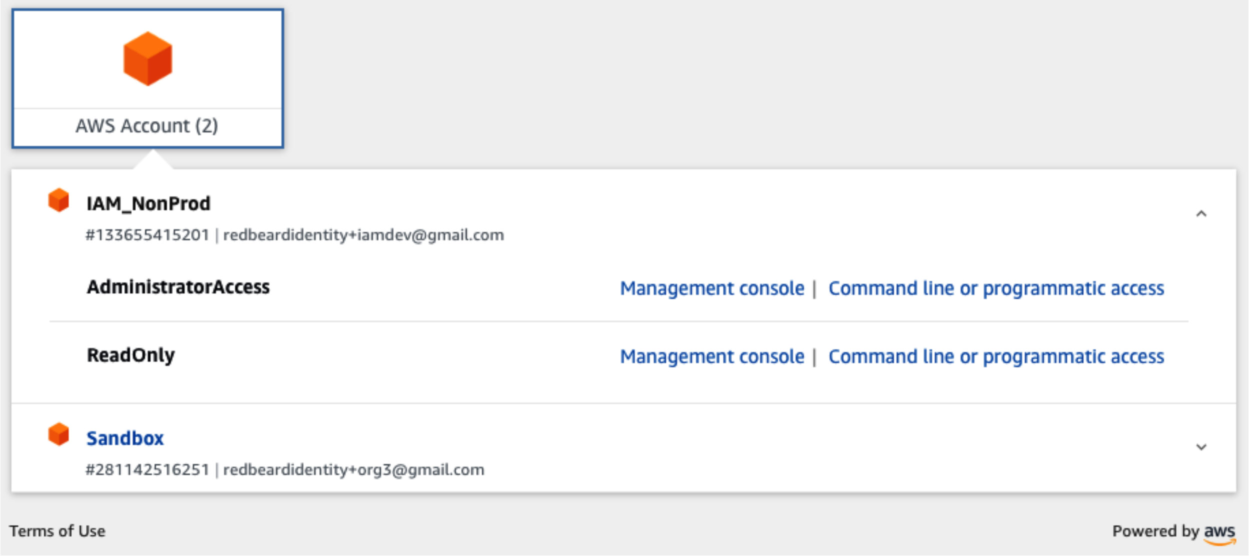
MFA devices | Sign out

Search

AWS Account (2)

IAM_NonProd
#133655415201 | redbeardidentity+iamdev@gmail.com

Sandbox
#281142516251 | redbeardidentity+org3@gmail.com



AWS Account (2)

IAM_NonProd
#133655415201 | redbeardidentity+iamdev@gmail.com

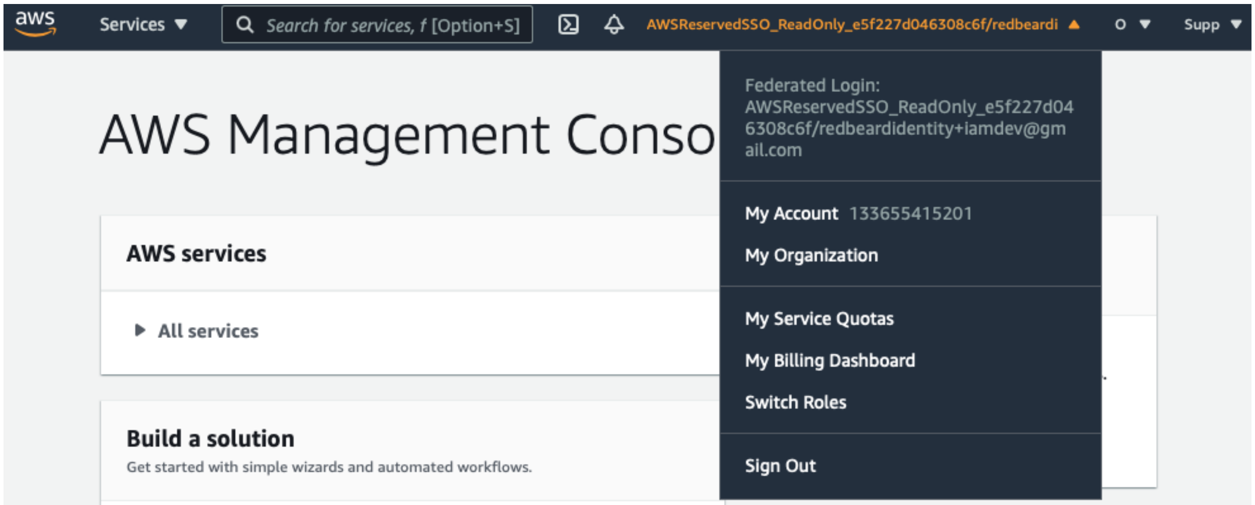
AdministratorAccess — Management console | Command line or programmatic access

ReadOnly — Management console | Command line or programmatic access

Sandbox
#281142516251 | redbeardidentity+org3@gmail.com

Terms of Use

Powered by aws



aws Services ▼ Search for services, f [Option+S]

AWSReservedSSO_ReadOnly_e5f227d046308c6f/redbeardi ▲ O ▼ Supp ▼

AWS Management Conso

AWS services

▶ All services

Build a solution

Get started with simple wizards and automated workflows.

Federated Login: AWSReservedSSO_ReadOnly_e5f227d046308c6f/redbeardidentity+iamdev@gmail.com

My Account 133655415201

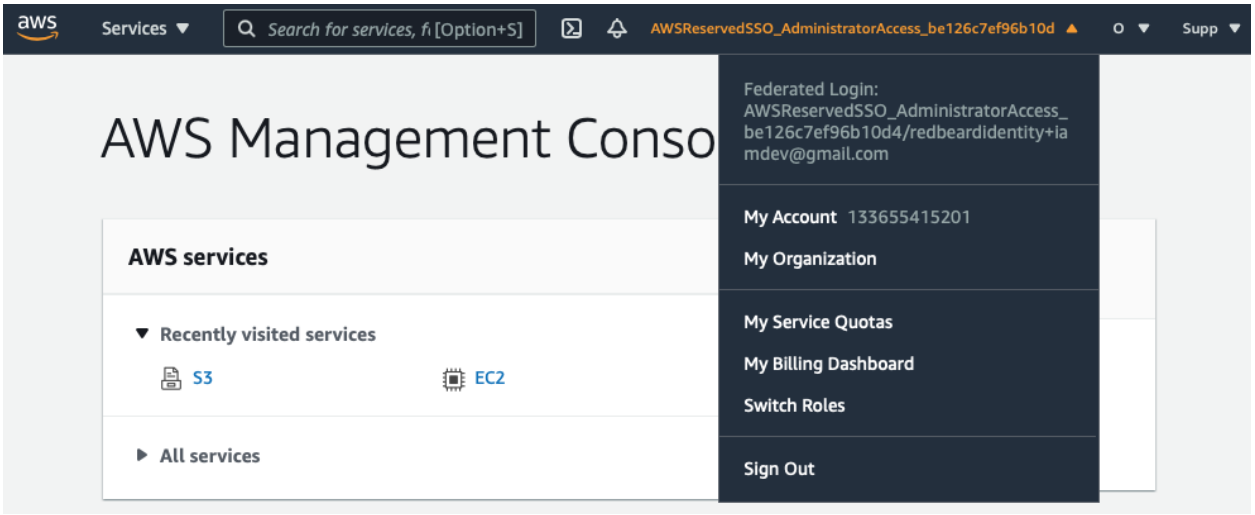
My Organization

My Service Quotas

My Billing Dashboard

Switch Roles

Sign Out



aws Services ▼ Search for services, fi [Option+S] AWSReservedSSO_AdministratorAccess_be126c7ef96b10d ▲ O ▼ Supp ▼

AWS Management Conso

AWS services

▼ Recently visited services

S3 EC2

▶ All services

Federated Login: AWSReservedSSO_AdministratorAccess_be126c7ef96b10d4/redbeardidentity+iamdev@gmail.com

My Account 133655415201

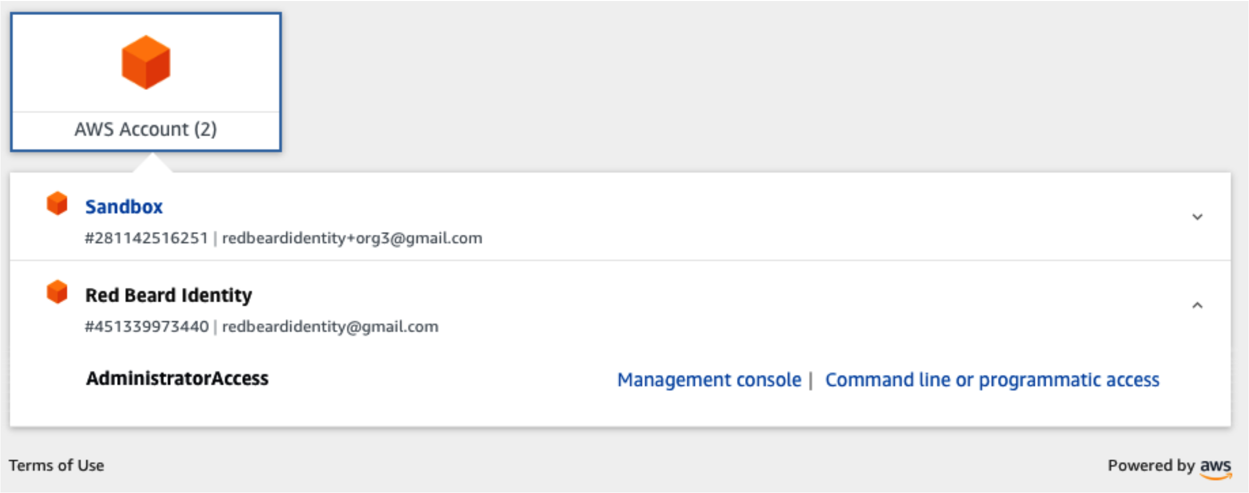
My Organization

My Service Quotas

My Billing Dashboard

Switch Roles

Sign Out



AWS Account (2)

Sandbox

#281142516251 | redbeardidentity+org3@gmail.com

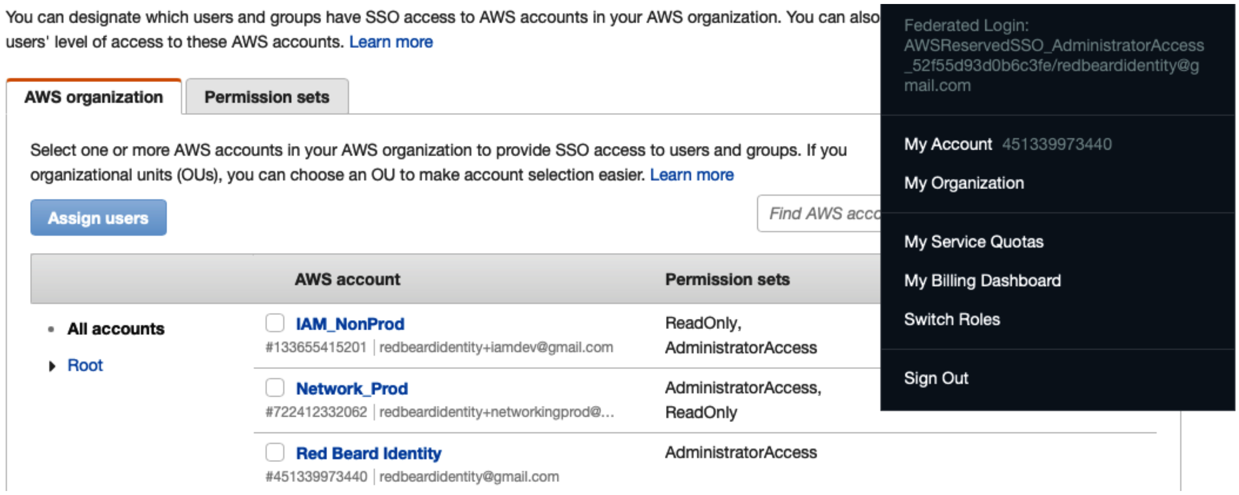
Red Beard Identity

#451339973440 | redbeardidentity@gmail.com

AdministratorAccess Management console | Command line or programmatic access

Terms of Use

Powered by aws



You can designate which users and groups have SSO access to AWS accounts in your AWS organization. You can also users' level of access to these AWS accounts. Learn more

AWS organization | Permission sets

Select one or more AWS accounts in your AWS organization to provide SSO access to users and groups. If you organizational units (OUs), you can choose an OU to make account selection easier. Learn more

Assign users

Find AWS acco

- **All accounts**
- ▸ Root

AWS account	Permission sets
□ **IAM_NonProd** #133655415201 | redbeardidentity+iamdev@gmail.com	ReadOnly, AdministratorAccess
□ **Network_Prod** #722412332062 | redbeardidentity+networkingprod@...	AdministratorAccess, ReadOnly
□ **Red Beard Identity** #451339973440 | redbeardidentity@gmail.com	AdministratorAccess

Federated Login: AWSReservedSSO_AdministratorAccess_52f55d93d0b6c3fe/redbeardidentity@gmail.com

My Account 451339973440

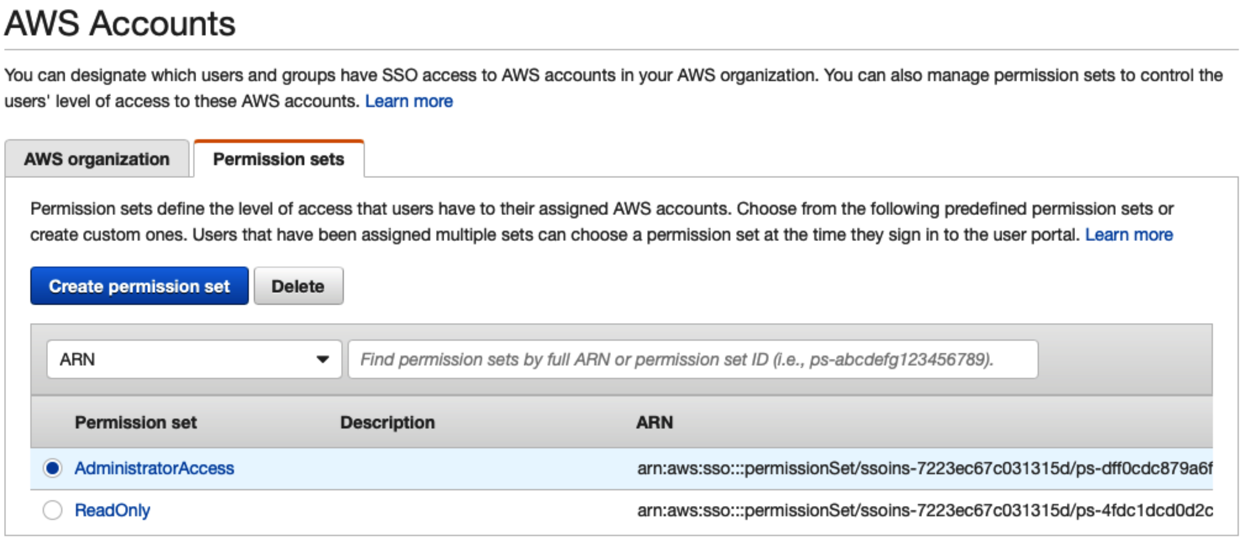
My Organization

My Service Quotas

My Billing Dashboard

Switch Roles

Sign Out



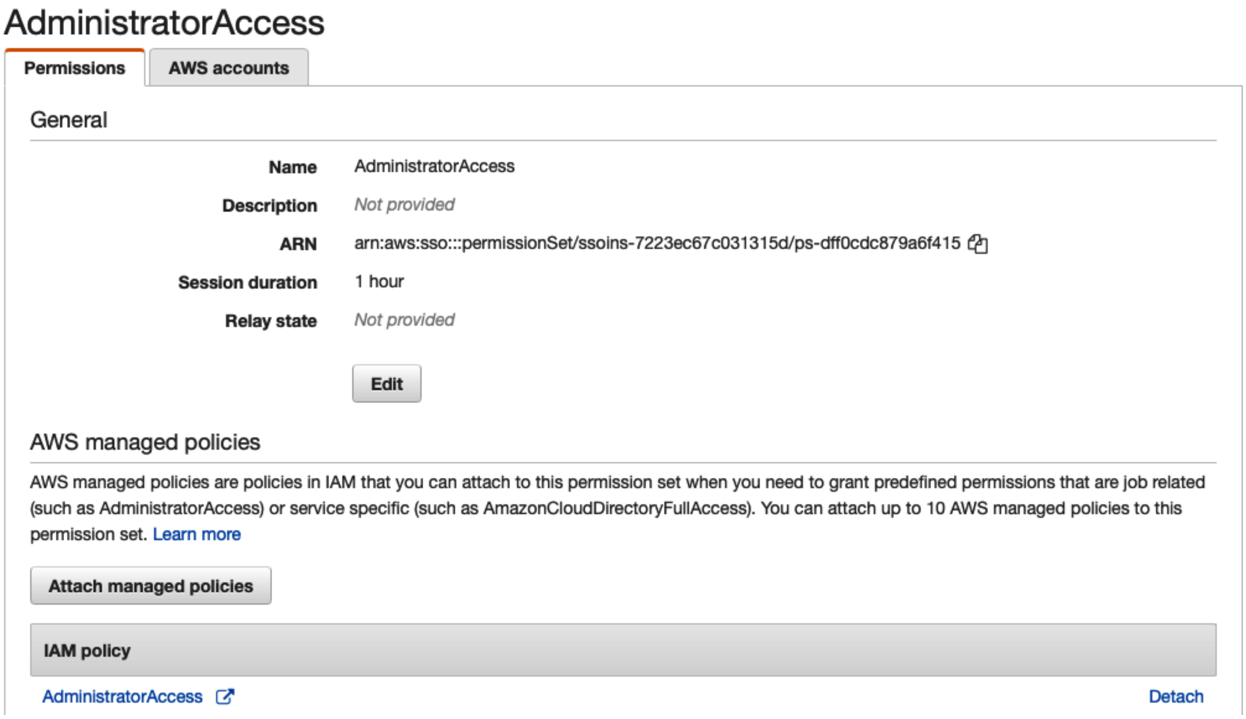
AWS Accounts

You can designate which users and groups have SSO access to AWS accounts in your AWS organization. You can also manage permission sets to control the users' level of access to these AWS accounts. Learn more

Permission sets define the level of access that users have to their assigned AWS accounts. Choose from the following predefined permission sets or create custom ones. Users that have been assigned multiple sets can choose a permission set at the time they sign in to the user portal. Learn more

Create permission set
Delete
ARN
Find permission sets by full ARN or permission set ID (i.e., ps-abcdefg123456789).

	Permission set	Description	ARN
●	AdministratorAccess		arn:aws:sso:::permissionSet/ssoins-7223ec67c031315d/ps-dff0cdc879a6f
○	ReadOnly		arn:aws:sso:::permissionSet/ssoins-7223ec67c031315d/ps-4fdc1dcd0d2c



AdministratorAccess

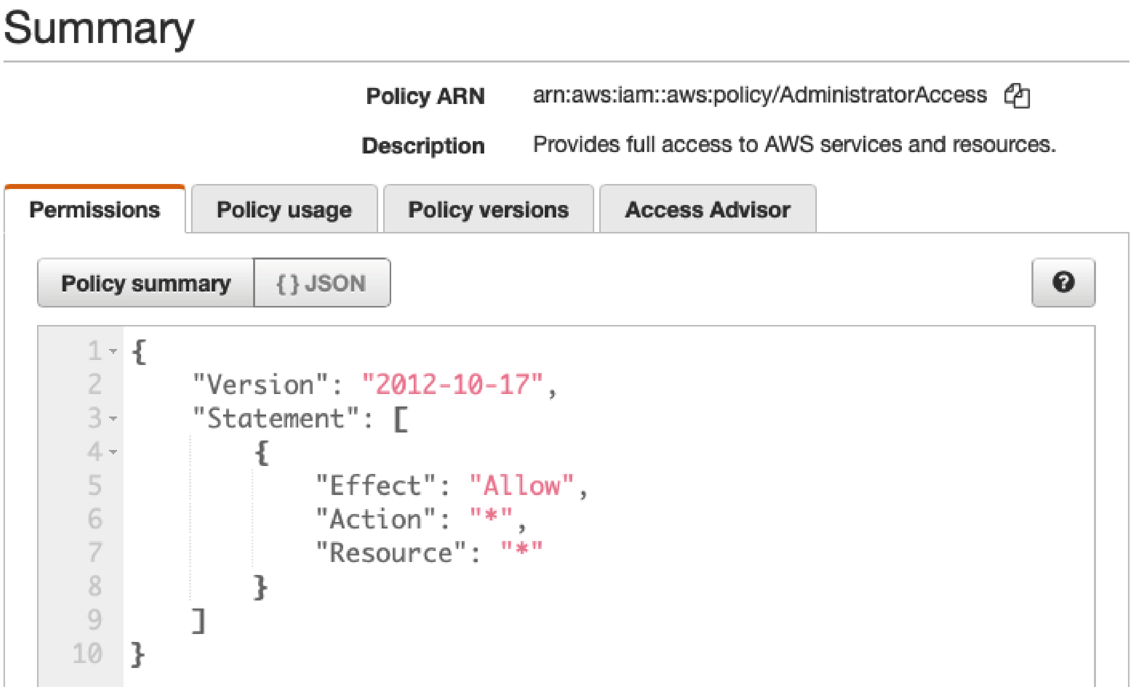
General

Name	AdministratorAccess
Description	*Not provided*
ARN	arn:aws:sso:::permissionSet/ssoins-7223ec67c031315d/ps-dff0cdc879a6f415
Session duration	1 hour
Relay state	*Not provided*

AWS managed policies

AWS managed policies are policies in IAM that you can attach to this permission set when you need to grant predefined permissions that are job related (such as AdministratorAccess) or service specific (such as AmazonCloudDirectoryFullAccess). You can attach up to 10 AWS managed policies to this permission set. Learn more

IAM policy	
AdministratorAccess	Detach

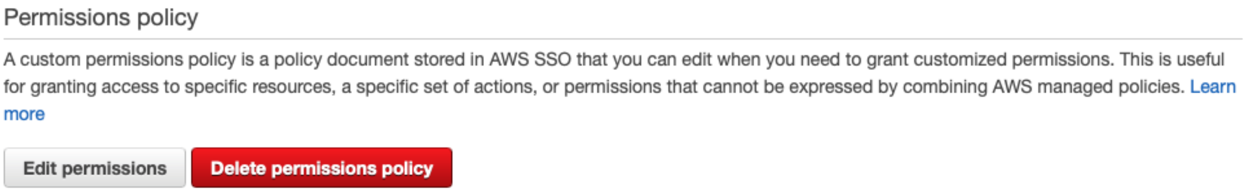


Summary

Policy ARN arn:aws:iam::aws:policy/AdministratorAccess

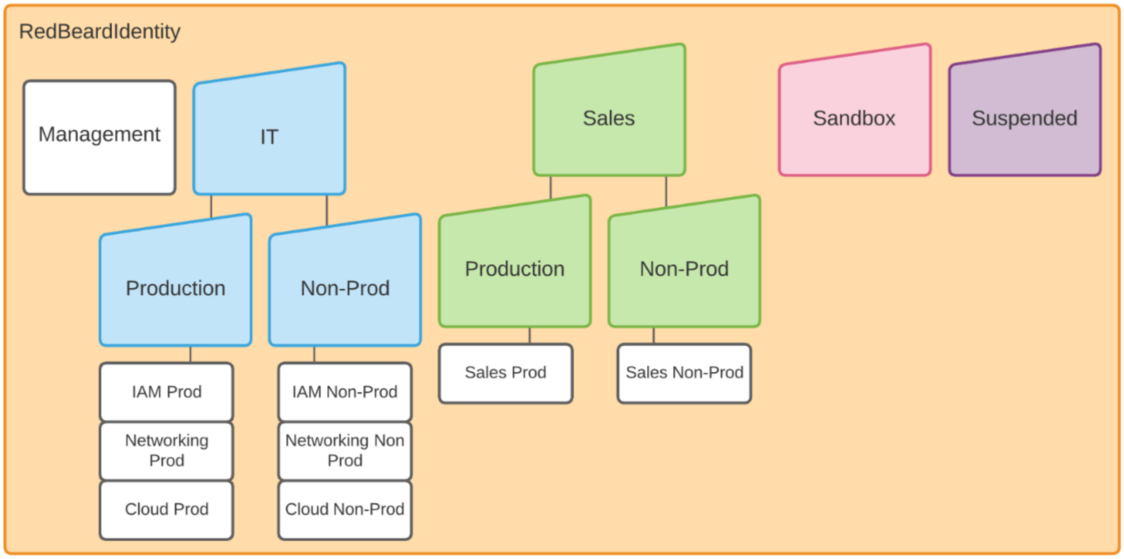
Description Provides full access to AWS services and resources.

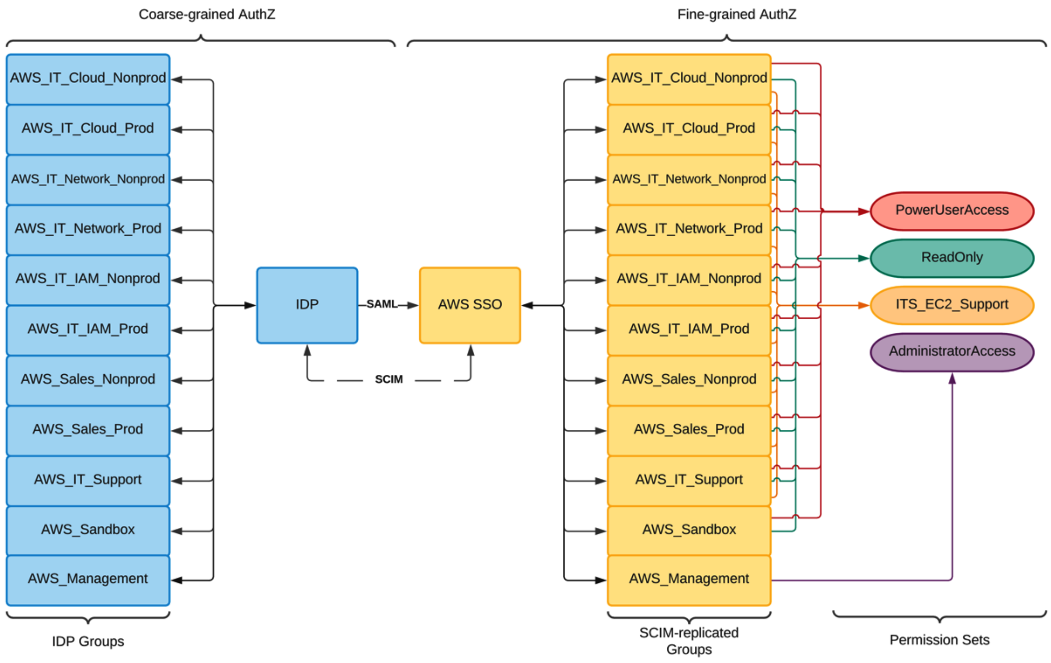
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

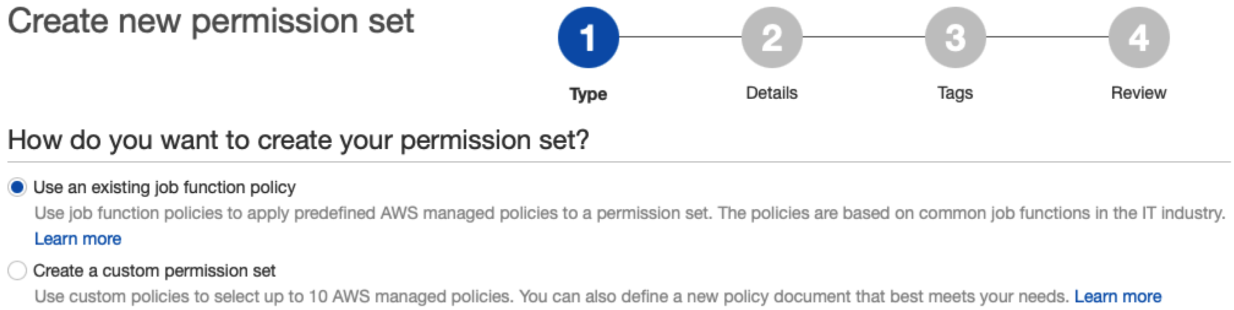


Permissions policy

A custom permissions policy is a policy document stored in AWS SSO that you can edit when you need to grant customized permissions. This is useful for granting access to specific resources, a specific set of actions, or permissions that cannot be expressed by combining AWS managed policies. Learn more





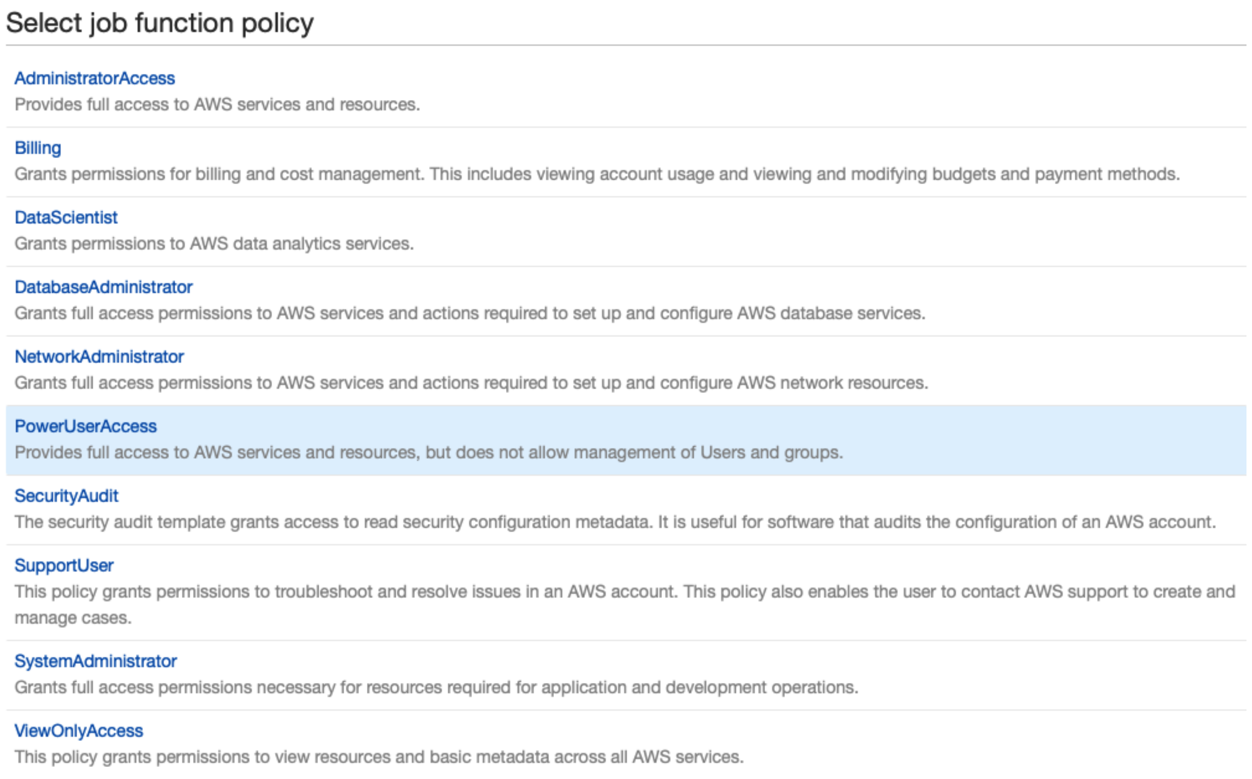


Create new permission set

How do you want to create your permission set?

● Use an existing job function policy
Use job function policies to apply predefined AWS managed policies to a permission set. The policies are based on common job functions in the IT industry. Learn more

○ Create a custom permission set
Use custom policies to select up to 10 AWS managed policies. You can also define a new policy document that best meets your needs. Learn more



Select job function policy

AdministratorAccess
Provides full access to AWS services and resources.

Billing
Grants permissions for billing and cost management. This includes viewing account usage and viewing and modifying budgets and payment methods.

DataScientist
Grants permissions to AWS data analytics services.

DatabaseAdministrator
Grants full access permissions to AWS services and actions required to set up and configure AWS database services.

NetworkAdministrator
Grants full access permissions to AWS services and actions required to set up and configure AWS network resources.

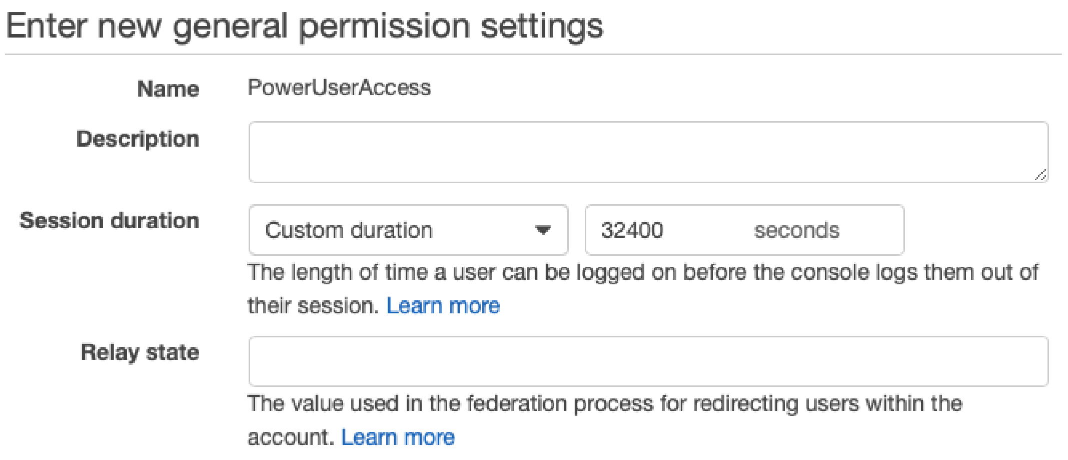
PowerUserAccess
Provides full access to AWS services and resources, but does not allow management of Users and groups.

SecurityAudit
The security audit template grants access to read security configuration metadata. It is useful for software that audits the configuration of an AWS account.

SupportUser
This policy grants permissions to troubleshoot and resolve issues in an AWS account. This policy also enables the user to contact AWS support to create and manage cases.

SystemAdministrator
Grants full access permissions necessary for resources required for application and development operations.

ViewOnlyAccess
This policy grants permissions to view resources and basic metadata across all AWS services.



Enter new general permission settings

Name PowerUserAccess

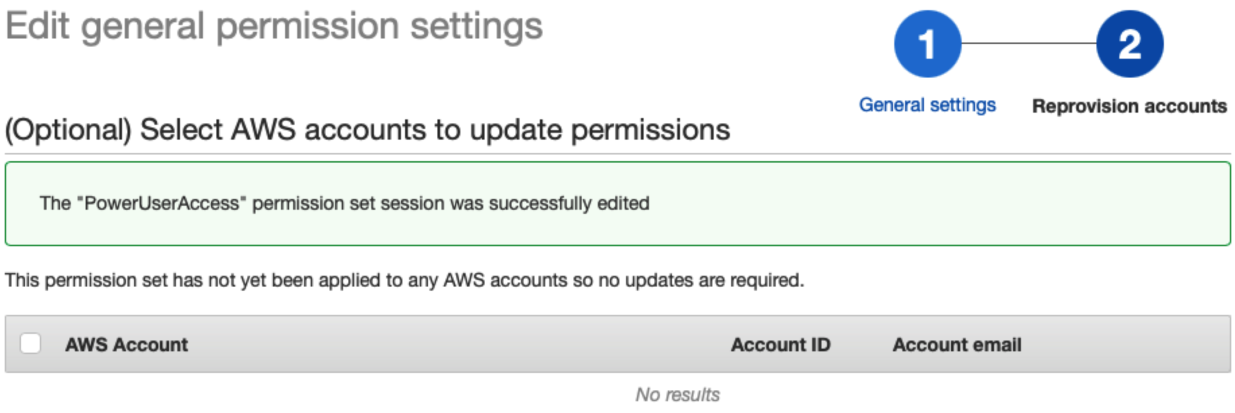
Description

Session duration Custom duration ▾ 32400 seconds

The length of time a user can be logged on before the console logs them out of their session. Learn more

Relay state

The value used in the federation process for redirecting users within the account. Learn more



Edit general permission settings

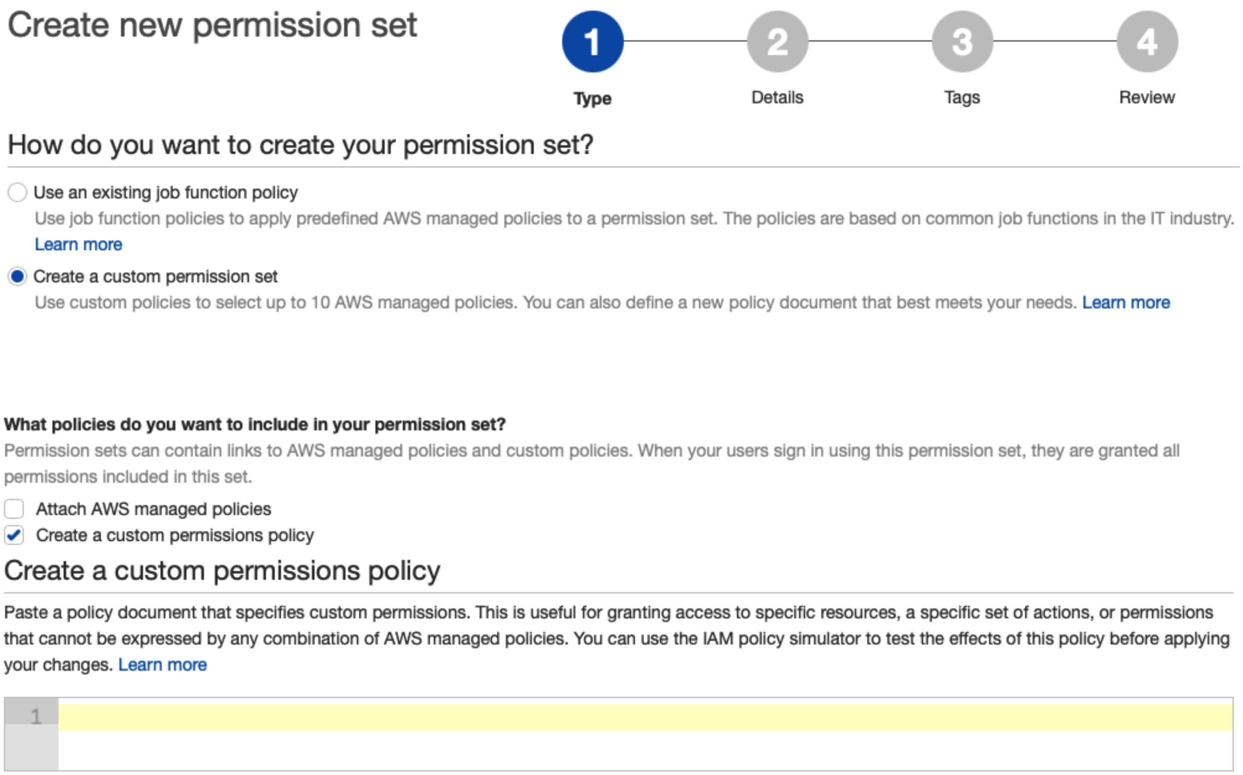
(Optional) Select AWS accounts to update permissions

The "PowerUserAccess" permission set session was successfully edited

This permission set has not yet been applied to any AWS accounts so no updates are required.

□ AWS Account	Account ID	Account email

No results



Create new permission set

How do you want to create your permission set?

○ Use an existing job function policy
Use job function policies to apply predefined AWS managed policies to a permission set. The policies are based on common job functions in the IT industry. Learn more

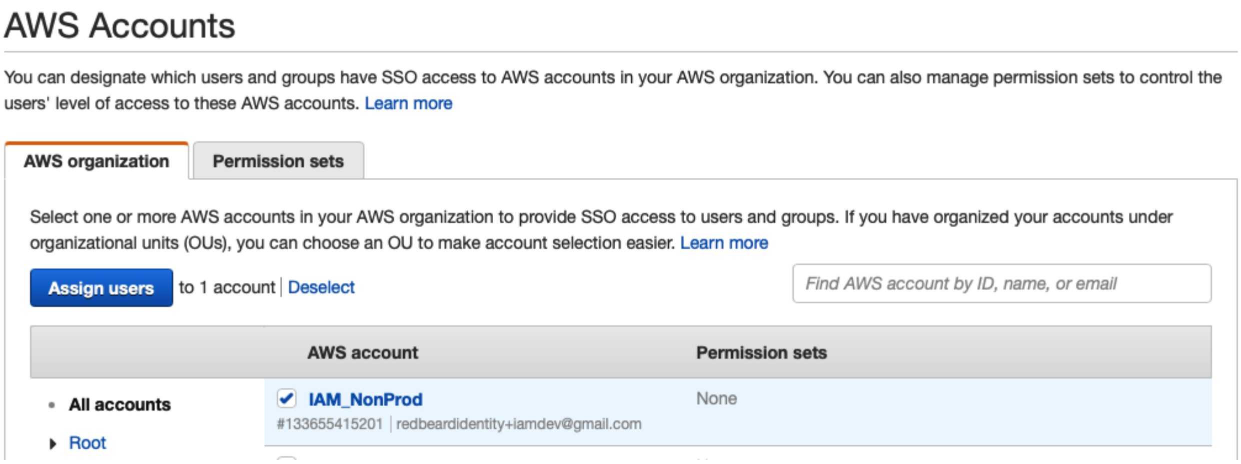
● Create a custom permission set
Use custom policies to select up to 10 AWS managed policies. You can also define a new policy document that best meets your needs. Learn more

What policies do you want to include in your permission set?
Permission sets can contain links to AWS managed policies and custom policies. When your users sign in using this permission set, they are granted all permissions included in this set.

□ Attach AWS managed policies
☑ Create a custom permissions policy

Create a custom permissions policy

Paste a policy document that specifies custom permissions. This is useful for granting access to specific resources, a specific set of actions, or permissions that cannot be expressed by any combination of AWS managed policies. You can use the IAM policy simulator to test the effects of this policy before applying your changes. Learn more



AWS Accounts

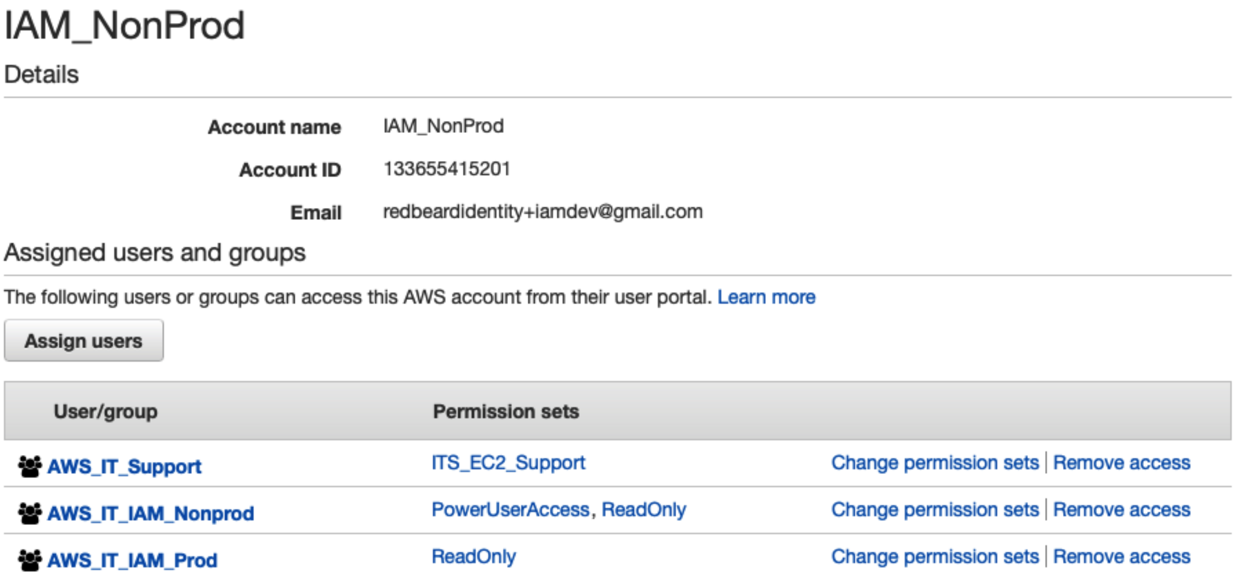
You can designate which users and groups have SSO access to AWS accounts in your AWS organization. You can also manage permission sets to control the users' level of access to these AWS accounts. Learn more

Select one or more AWS accounts in your AWS organization to provide SSO access to users and groups. If you have organized your accounts under organizational units (OUs), you can choose an OU to make account selection easier. Learn more

Assign users to 1 account | Deselect

- All accounts
- Root

AWS account	Permission sets
☑ IAM_NonProd #133655415201 | redbeardidentity+iamdev@gmail.com	None



IAM_NonProd

Details

Account name IAM_NonProd

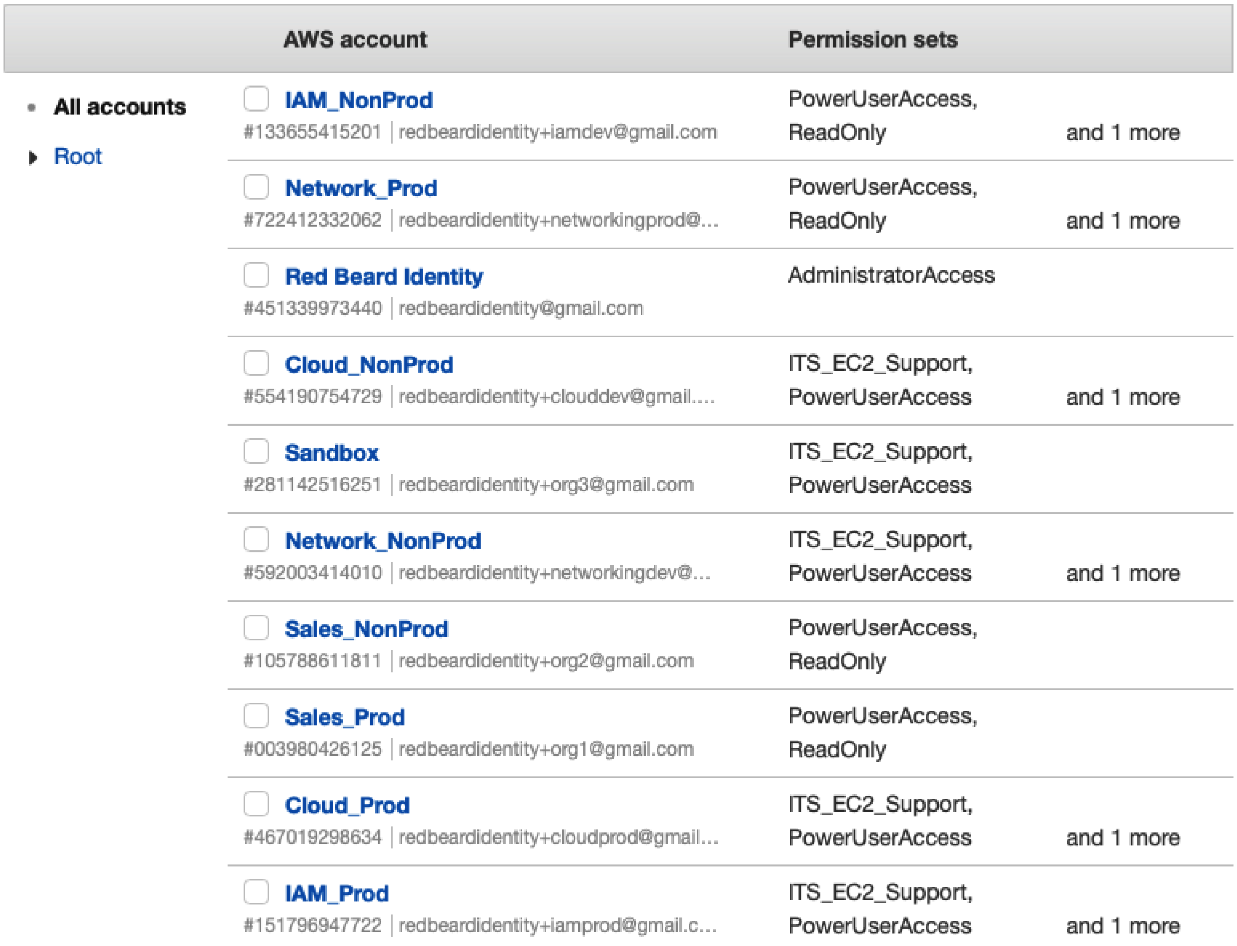
Account ID 133655415201

Email redbeardidentity+iamdev@gmail.com

Assigned users and groups

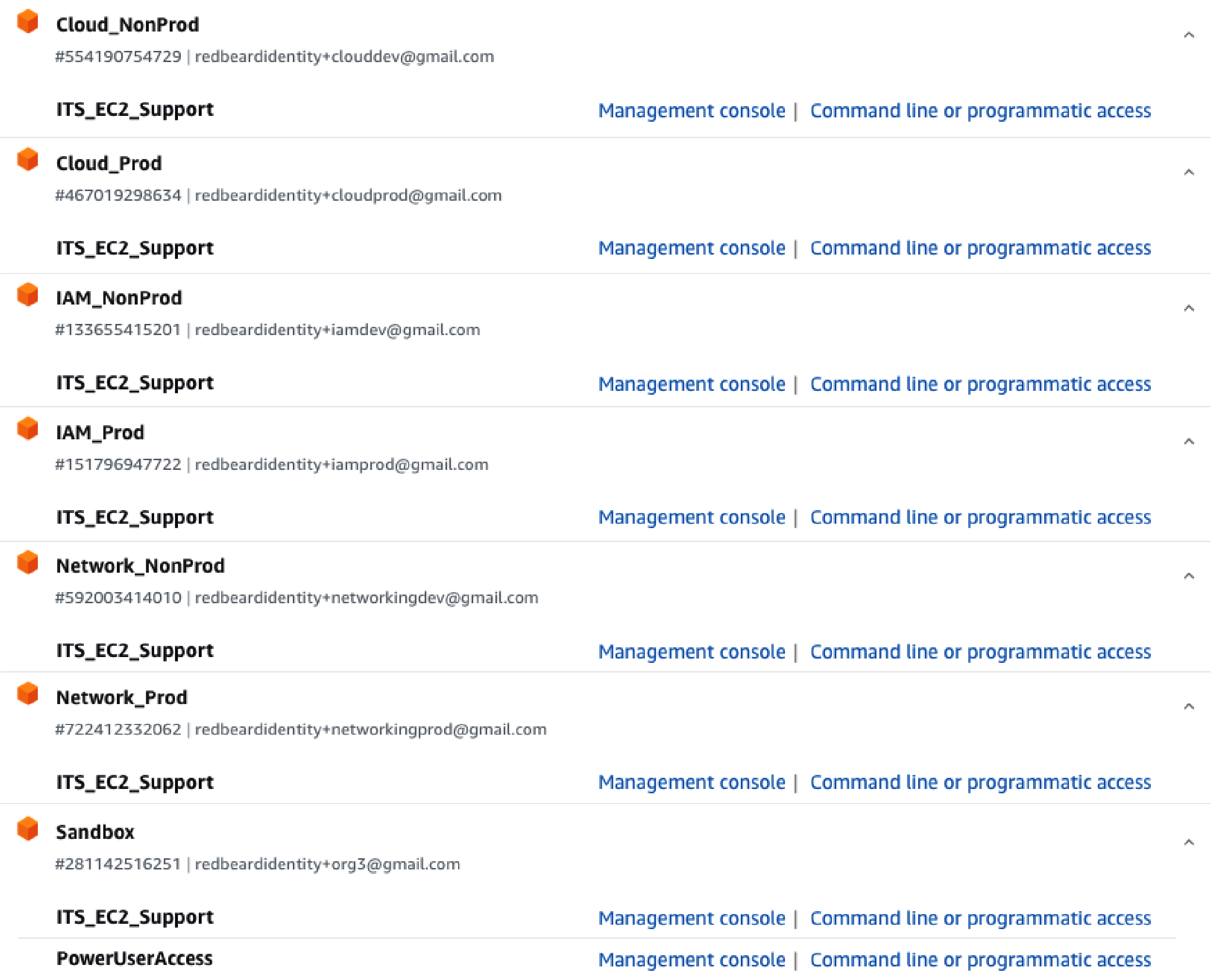
The following users or groups can access this AWS account from their user portal. Learn more

User/group	Permission sets	
AWS_IT_Support	ITS_EC2_Support	Change permission sets | Remove access
AWS_IT_IAM_Nonprod	PowerUserAccess, ReadOnly	Change permission sets | Remove access
AWS_IT_IAM_Prod	ReadOnly	Change permission sets | Remove access



- All accounts
- ▸ Root

AWS account	Permission sets	
□ **IAM_NonProd** #133655415201 | redbeardidentity+iamdev@gmail.com	PowerUserAccess, ReadOnly	and 1 more
□ **Network_Prod** #722412332062 | redbeardidentity+networkingprod@…	PowerUserAccess, ReadOnly	and 1 more
□ **Red Beard Identity** #451339973440 | redbeardidentity@gmail.com	AdministratorAccess	
□ **Cloud_NonProd** #554190754729 | redbeardidentity+clouddev@gmail.…	ITS_EC2_Support, PowerUserAccess	and 1 more
□ **Sandbox** #281142516251 | redbeardidentity+org3@gmail.com	ITS_EC2_Support, PowerUserAccess	
□ **Network_NonProd** #592003414010 | redbeardidentity+networkingdev@…	ITS_EC2_Support, PowerUserAccess	and 1 more
□ **Sales_NonProd** #105788611811 | redbeardidentity+org2@gmail.com	PowerUserAccess, ReadOnly	
□ **Sales_Prod** #003980426125 | redbeardidentity+org1@gmail.com	PowerUserAccess, ReadOnly	
□ **Cloud_Prod** #467019298634 | redbeardidentity+cloudprod@gmail…	ITS_EC2_Support, PowerUserAccess	and 1 more
□ **IAM_Prod** #151796947722 | redbeardidentity+iamprod@gmail.c…	ITS_EC2_Support, PowerUserAccess	and 1 more



Cloud_NonProd
#554190754729 | redbeardidentity+clouddev@gmail.com

ITS_EC2_Support Management console | Command line or programmatic access

Cloud_Prod
#467019298634 | redbeardidentity+cloudprod@gmail.com

ITS_EC2_Support Management console | Command line or programmatic access

IAM_NonProd
#133655415201 | redbeardidentity+iamdev@gmail.com

ITS_EC2_Support Management console | Command line or programmatic access

IAM_Prod
#151796947722 | redbeardidentity+iamprod@gmail.com

ITS_EC2_Support Management console | Command line or programmatic access

Network_NonProd
#592003414010 | redbeardidentity+networkingdev@gmail.com

ITS_EC2_Support Management console | Command line or programmatic access

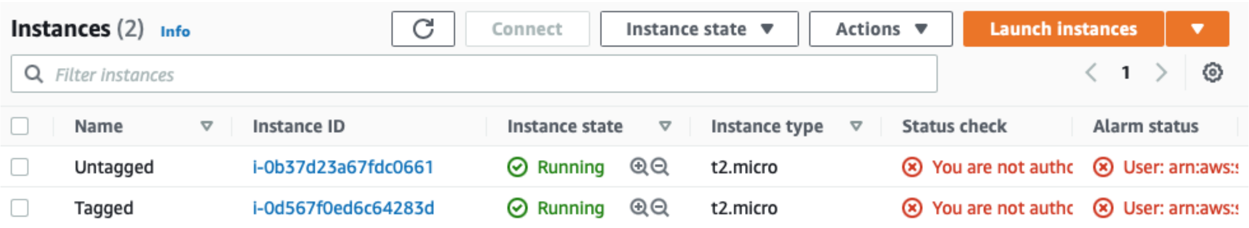
Network_Prod
#722412332062 | redbeardidentity+networkingprod@gmail.com

ITS_EC2_Support Management console | Command line or programmatic access

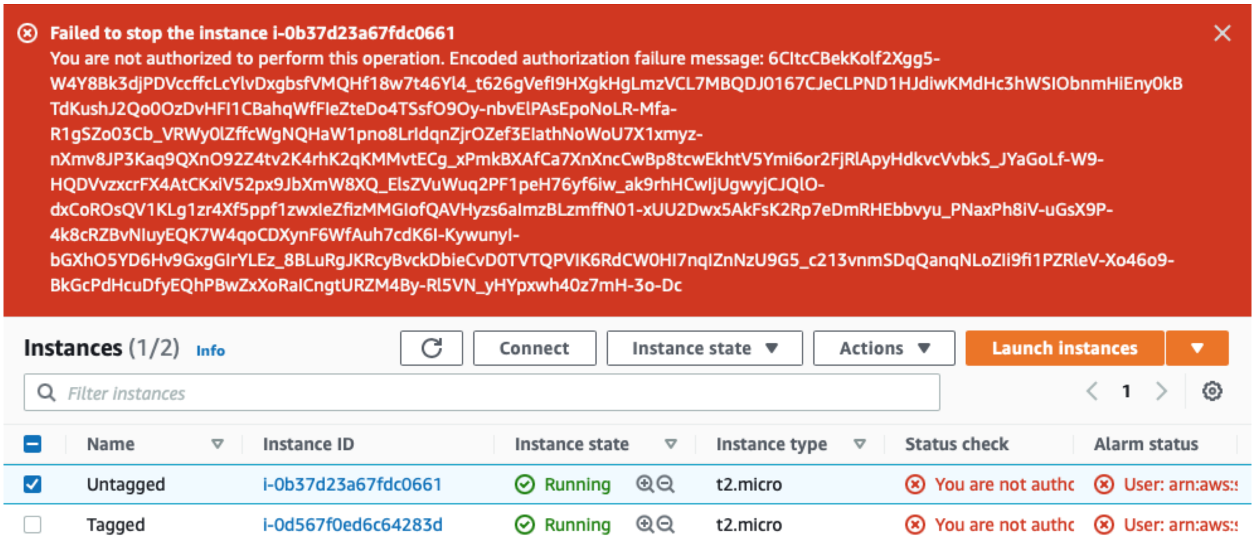
Sandbox
#281142516251 | redbeardidentity+org3@gmail.com

ITS_EC2_Support Management console | Command line or programmatic access

PowerUserAccess Management console | Command line or programmatic access



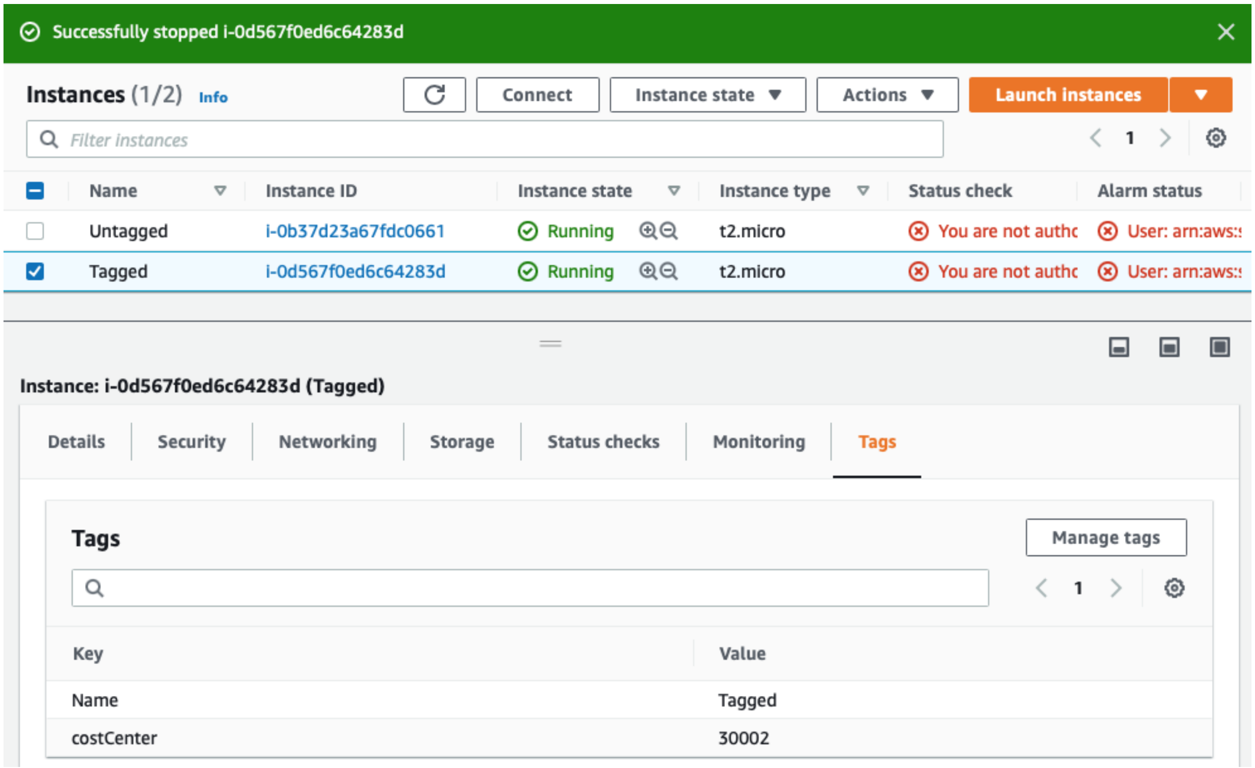
□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
□	Untagged	i-0b37d23a67fdc0661	✓ Running	t2.micro	⊗ You are not authc	⊗ User: arn:aws::
□	Tagged	i-0d567f0ed6c64283d	✓ Running	t2.micro	⊗ You are not authc	⊗ User: arn:aws::



Failed to stop the instance i-0b37d23a67fdc0661

You are not authorized to perform this operation. Encoded authorization failure message: 6CItcCBekKolf2Xgg5-W4Y8Bk3djPDVccffcLcYlvDxgbsfVMQHf18w7t46Yl4_t626gVefI9HXgkHgLmzVCL7MBQDJ0167CJeCLPND1HJdiwKMdHc3hWSIObnmHiEny0kBTdKushJ2Qo0OzDvHFI1CBahqWfFIeZteDo4TSsfO9Oy-nbvElPAsEpoNoLR-Mfa-R1gSZo03Cb_VRWy0lZffcWgNQHaW1pno8LrIdqnZjrOZef3ElathNoWoU7X1xmyz-nXmv8JP3Kaq9QXnO92Z4tv2K4rhK2qKMMvtECg_xPmkBXAfCa7XnXncCwBp8tcwEkhtV5Ymi6or2FjRlApyHdkvcVvbkS_JYaGoLf-W9-HQDVvzxcrFX4AtCKxiV52px9JbXmW8XQ_ElsZVuWuq2PF1peH76yf6iw_ak9rhHCwIjUgwyjCJQlO-dxCoROsQV1KLg1zr4Xf5ppf1zwxleZfizMMGlofQAVHyzs6aImzBLzmffN01-xUU2Dwx5AkFsK2Rp7eDmRHEbbvyu_PNaxPh8iV-uGsX9P-4k8cRZBvNIuyEQK7W4qoCDXynF6WfAuh7cdK6I-Kywunyl-bGXhO5YD6Hv9GxgGIrYLEz_8BLuRgJKRcyBvckDbieCvD0TVTQPVIK6RdCW0HI7nqIZnNzU9G5_c213vnmSDqQanqNLoZIi9fi1PZRleV-Xo46o9-BkGcPdHcuDfyEQhPBwZxXoRaICngtURZM4By-Rl5VN_yHYpxwh40z7mH-3o-Dc

▣	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
☑	Untagged	i-0b37d23a67fdc0661	✓ Running	t2.micro	☒ You are not authc	☒ User: arn:aws::
□	Tagged	i-0d567f0ed6c64283d	✓ Running	t2.micro	☒ You are not authc	☒ User: arn:aws::



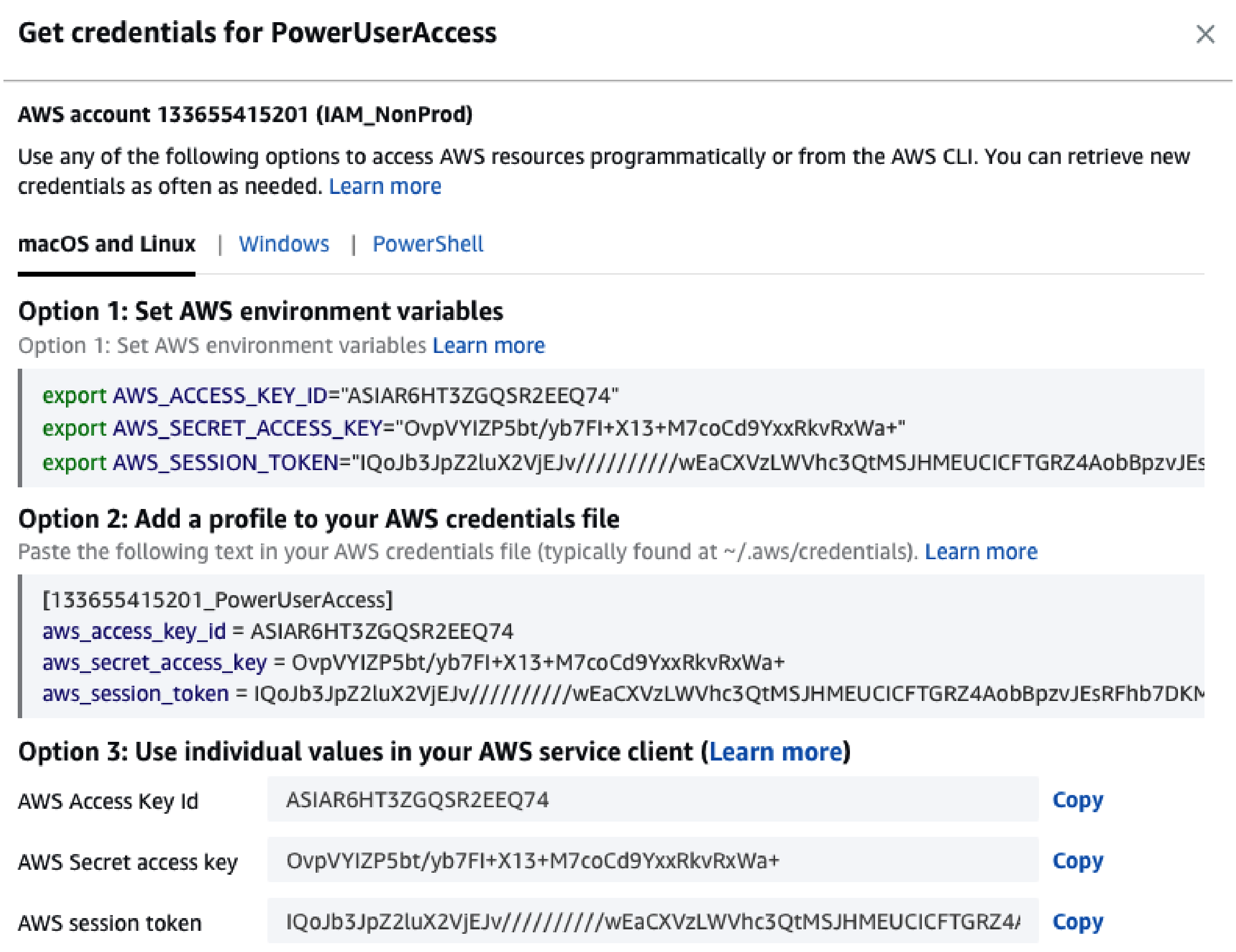
Successfully stopped i-0d567f0ed6c64283d

▣	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
□	Untagged	i-0b37d23a67fdc0661	✓ Running	t2.micro	☒ You are not authc	☒ User: arn:aws::
☑	Tagged	i-0d567f0ed6c64283d	✓ Running	t2.micro	☒ You are not authc	☒ User: arn:aws::

Instance: i-0d567f0ed6c64283d (Tagged)

Tags

Key	Value
Name	Tagged
costCenter	30002



Get credentials for PowerUserAccess

AWS account 133655415201 (IAM_NonProd)

Use any of the following options to access AWS resources programmatically or from the AWS CLI. You can retrieve new credentials as often as needed. Learn more

Option 1: Set AWS environment variables

Option 1: Set AWS environment variables Learn more

```
export AWS_ACCESS_KEY_ID="ASIAR6HT3ZGQSR2EEQ74"
export AWS_SECRET_ACCESS_KEY="OvpVYIZP5bt/yb7FI+X13+M7coCd9YxxRkvRxWa+"
export AWS_SESSION_TOKEN="IQoJb3JpZ2luX2VjEJv//////////wEaCXVzLWVhc3QtMSJHMEUCICFTGRZ4AobBpzvJEs
```

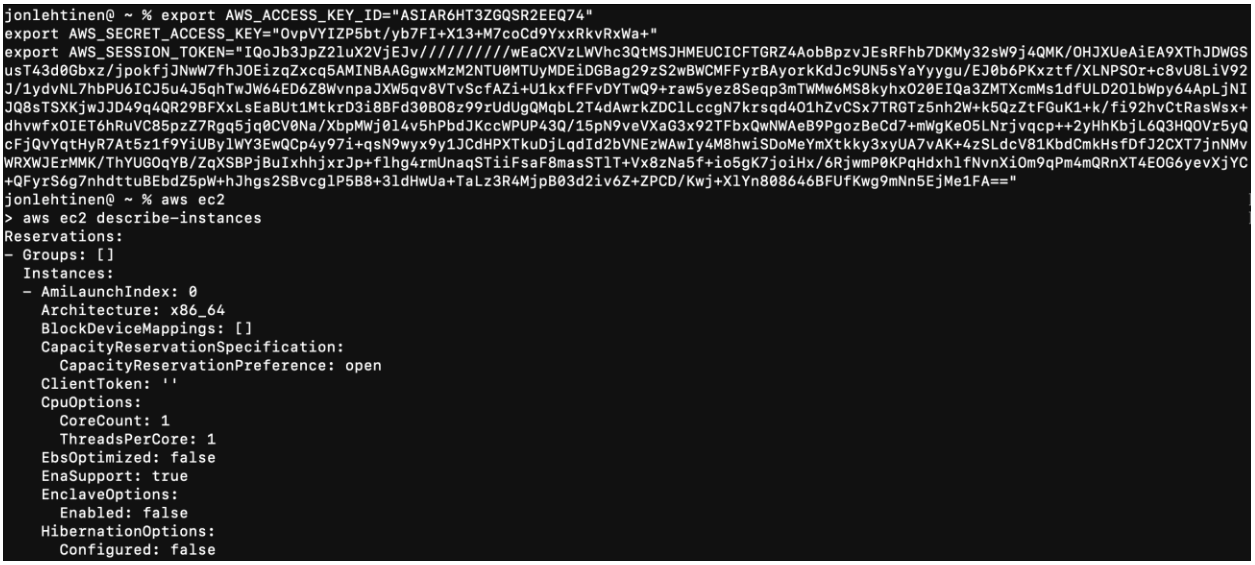
Option 2: Add a profile to your AWS credentials file

Paste the following text in your AWS credentials file (typically found at ~/.aws/credentials). Learn more

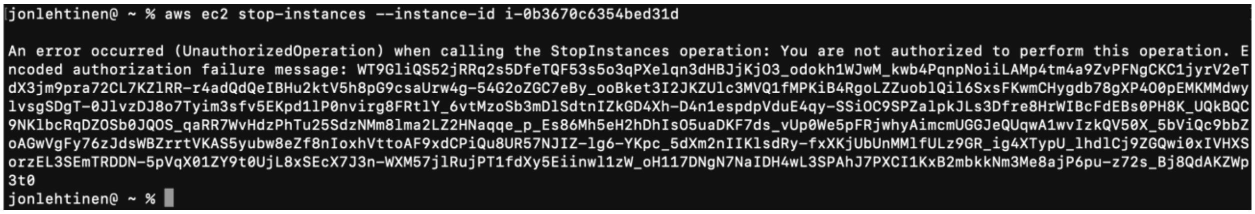
```
[133655415201_PowerUserAccess]
aws_access_key_id = ASIAR6HT3ZGQSR2EEQ74
aws_secret_access_key = OvpVYIZP5bt/yb7FI+X13+M7coCd9YxxRkvRxWa+
aws_session_token = IQoJb3JpZ2luX2VjEJv//////////wEaCXVzLWVhc3QtMSJHMEUCICFTGRZ4AobBpzvJEsRFhb7DKM
```

Option 3: Use individual values in your AWS service client (Learn more)

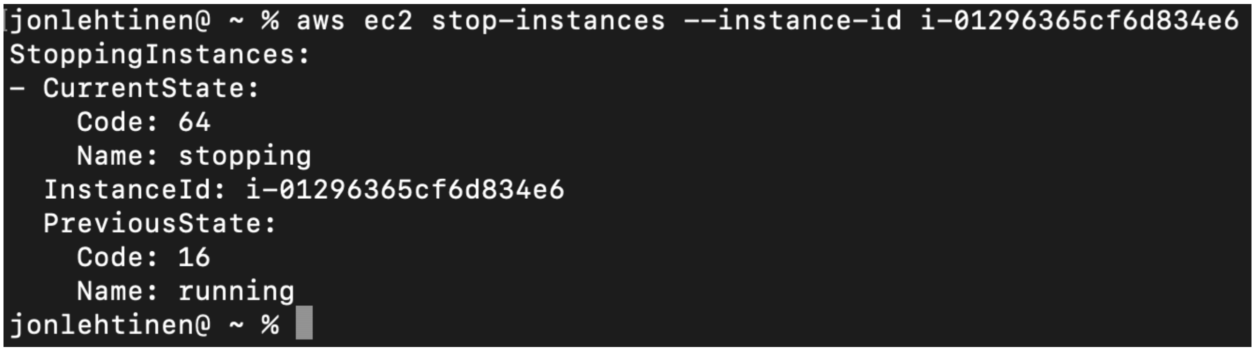
AWS Access Key Id	ASIAR6HT3ZGQSR2EEQ74	Copy
AWS Secret access key	OvpVYIZP5bt/yb7FI+X13+M7coCd9YxxRkvRxWa+	Copy
AWS session token	IQoJb3JpZ2luX2VjEJv//////////wEaCXVzLWVhc3QtMSJHMEUCICFTGRZ4/	Copy



```
jonlehtinen@ ~ % export AWS_ACCESS_KEY_ID="ASIAR6HT3ZGQSR2EEQ74"
export AWS_SECRET_ACCESS_KEY="OvpVYIZP5bt/yb7FI+X13+M7coCd9YxxRkvRxWa+"
export AWS_SESSION_TOKEN="IQoJb3JpZ2luX2VjEJv//////////wEaCXVzLWVhc3QtMSJHMEUCICFTGRZ4AobBpzvJEsRFhb7DKMy32sW9j4QMK/OHJXUeAiEA9XThJDWGS
usT43d0Gbxz/jpokfjJNwW7fhJOEizqZxcq5AMINBAAGgwxMzM2NTU0MTUyMDEiDGBag29zS2wBWCMFFyrBAyorkKdJc9UN5sYaYyygu/EJ0b6PKxztf/XLNPSOr+c8vU8LiV92
J/1ydvNL7hbPU6ICJ5u4J5qhTwJW64ED6Z8WvnpaJXW5qv8VTvScfAZi+U1kxfFFvDYTwQ9+raw5yez8Seqp3mTWMw6MS8kyhxO20EIQa3ZMTXcmMs1dfULD2OlbWpy64ApLjNI
JQ8sTSXKjwJJD49q4QR29BFXxLsEaBUt1MtkrD3i8BFd30BO8z99rUdUgQMqbL2T4dAwrkZDClLccgN7krsqd4O1hZvCSx7TRGTz5nh2W+k5QzZtFGuK1+k/fi92hvCtRasWsx+
dhvwfxOIET6hRuVC85pzZ7Rgq5jq0CV0Na/XbpMWj0l4v5hPbdJKccWPUP43Q/15pN9veVXaG3x92TFbxQwNWAeB9PgozBeCd7+mWgKeO5LNrjvqcp++2yHhKbjL6Q3HQOVr5yQ
cFjQvYqtHyR7At5z1f9YiUBylWY3EwQCp4y97i+qsN9wyx9y1JCdHPXTkuDjLqdId2bVNEzWAwIy4M8hwiSDoMeYmXtkky3xyUA7vAK+4zSLdcV81KbdCmkHsfDfJ2CXT7jnNMv
WRXWJErMMK/ThYUGOqYB/ZqXSBPjBuIxhhjxrJp+flhg4rmUnaqSTiiFsaF8masSTlT+Vx8zNa5f+io5gK7joiHx/6RjwmP0KPqHdxhlfNvnXiOm9qPm4mQRnXT4EOG6yevXjYC
+QFyrS6g7nhdttuBEbdZ5pW+hJhgs2SBvcglP5B8+3ldHwUa+TaLz3R4MjpB03d2iv6Z+ZPCD/Kwj+XlYn808646BFUfKwg9mNn5EjMe1FA=="
jonlehtinen@ ~ % aws ec2
> aws ec2 describe-instances
Reservations:
- Groups: []
  Instances:
  - AmiLaunchIndex: 0
    Architecture: x86_64
    BlockDeviceMappings: []
    CapacityReservationSpecification:
      CapacityReservationPreference: open
    ClientToken: ''
    CpuOptions:
      CoreCount: 1
      ThreadsPerCore: 1
    EbsOptimized: false
    EnaSupport: true
    EnclaveOptions:
      Enabled: false
    HibernationOptions:
      Configured: false
```

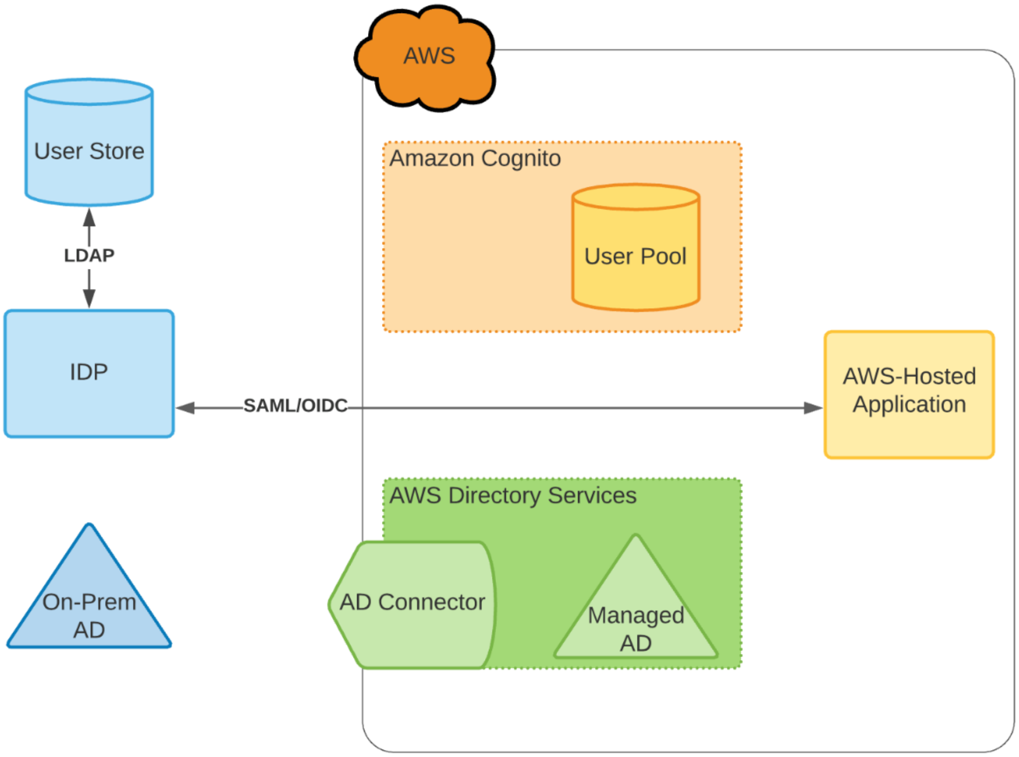


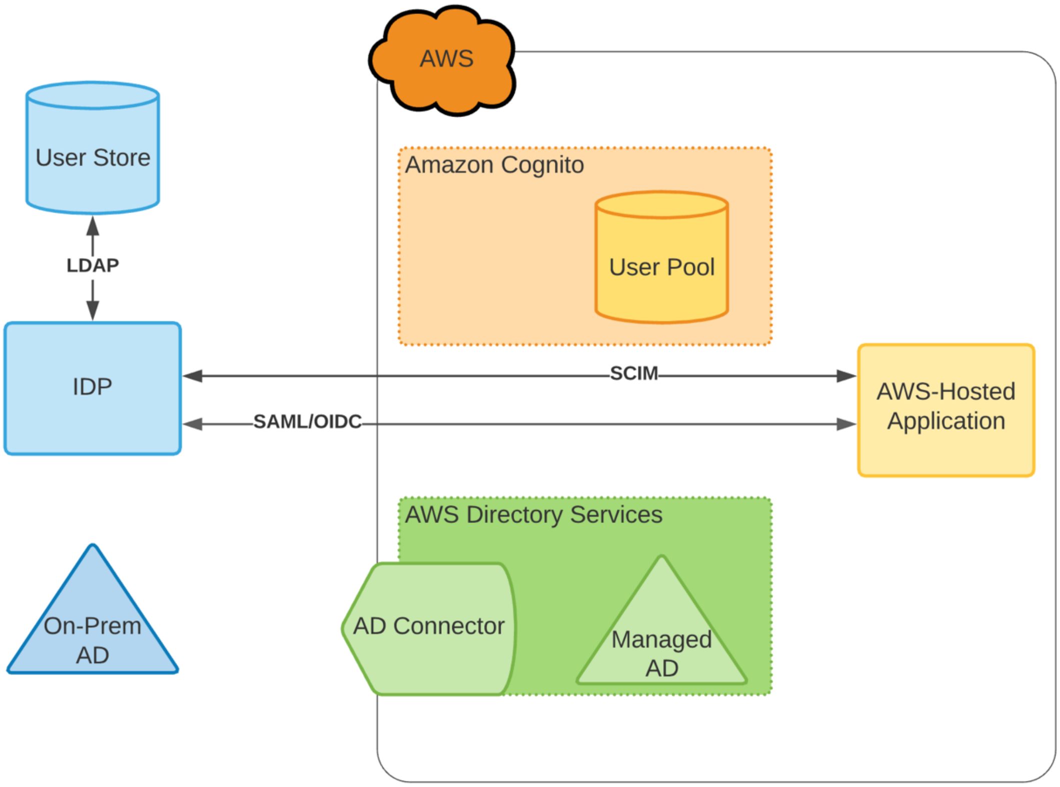
```
jonlehtinen@ ~ % aws ec2 stop-instances --instance-id i-0b3670c6354bed31d

An error occurred (UnauthorizedOperation) when calling the StopInstances operation: You are not authorized to perform this operation. E
ncoded authorization failure message: WT9GliQS52jRRq2s5DfeTQF53s5o3qPXelqn3dHBJjKjO3_odokh1WJwM_kwb4PqnpNoiiLAMp4tm4a9ZvPFNgCKC1jyrV2eT
dX3jm9pra72CL7KZlRR-r4adQdQeIBHu2ktV5h8pG9csaUrw4g-54G2oZGC7eBy_ooBket3I2JKZUlc3MVQ1fMPKiB4RgoLZZuoblQil6SxsFKwmCHygdb78gXP4O0pEMKMMdwy
lvsgSDgT-0JlvzDJ8o7Tyim3sfv5EKpd1lP0nvirg8FRtlY_6vtMzoSb3mDlSdtnIZkGD4Xh-D4n1espdpVduE4qy-SSiOC9SPZalpkJLs3Dfre8HrWIBcFdEBs0PH8K_UQkBQC
9NKlbcRqDZOSb0JQOS_qaRR7WvHdzPhTu25SdzNMm8lma2LZ2HNaqqe_p_Es86Mh5eH2hDhIsO5uaDKF7ds_vUp0We5pFRjwhyAimcmUGGJeQUqwA1wvIzkQV50X_5bViQc9bbZ
oAGwVgFy76zJdsWBZrrtVKAS5yubw8eZf8nIoxhVttoAF9xdCPiQu8UR57NJIZ-lg6-YKpc_5dXm2nIIKlsdRy-fxXKjUbUnMMlfULz9GR_ig4XTypU_lhdlCj9ZGQwi0xIVHXS
orzEL3SEmTRDDN-5pVqX01ZY9t0UjL8xSEcX7J3n-WXM57jlRujPT1fdXy5Eiinwl1zW_oH117DNgN7NaIDH4wL3SPAhJ7PXCI1KxB2mbkkNm3Me8ajP6pu-z72s_Bj8QdAKZWp
3t0
jonlehtinen@ ~ %
```

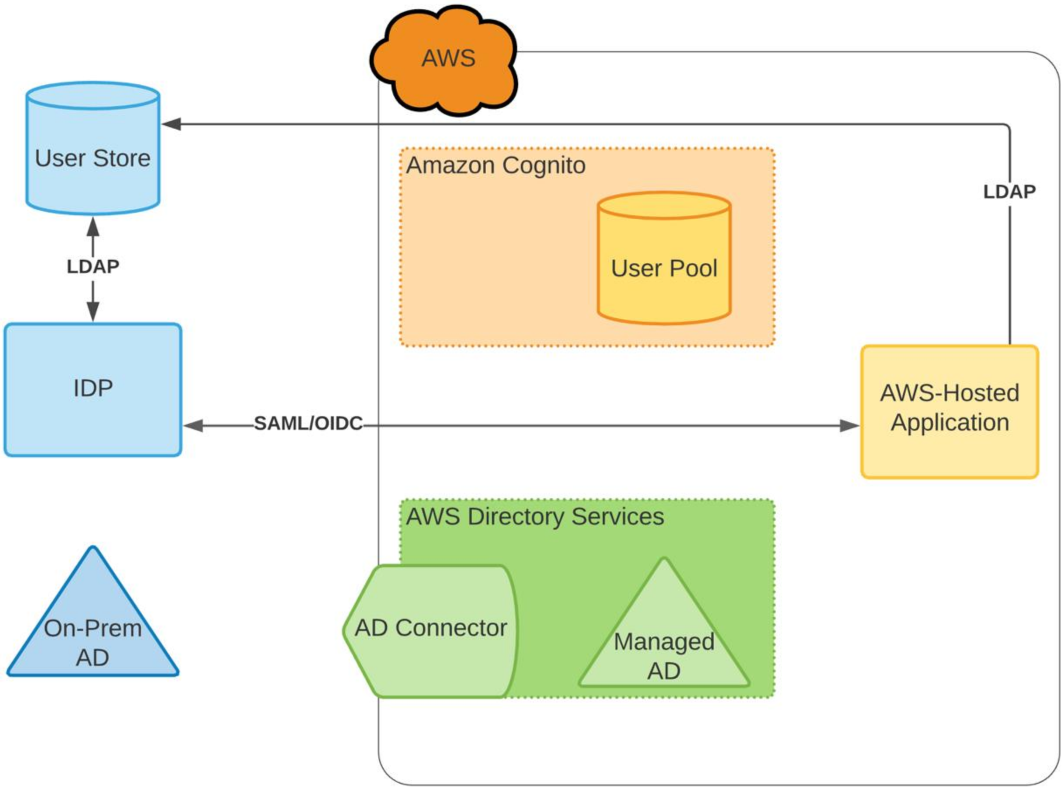


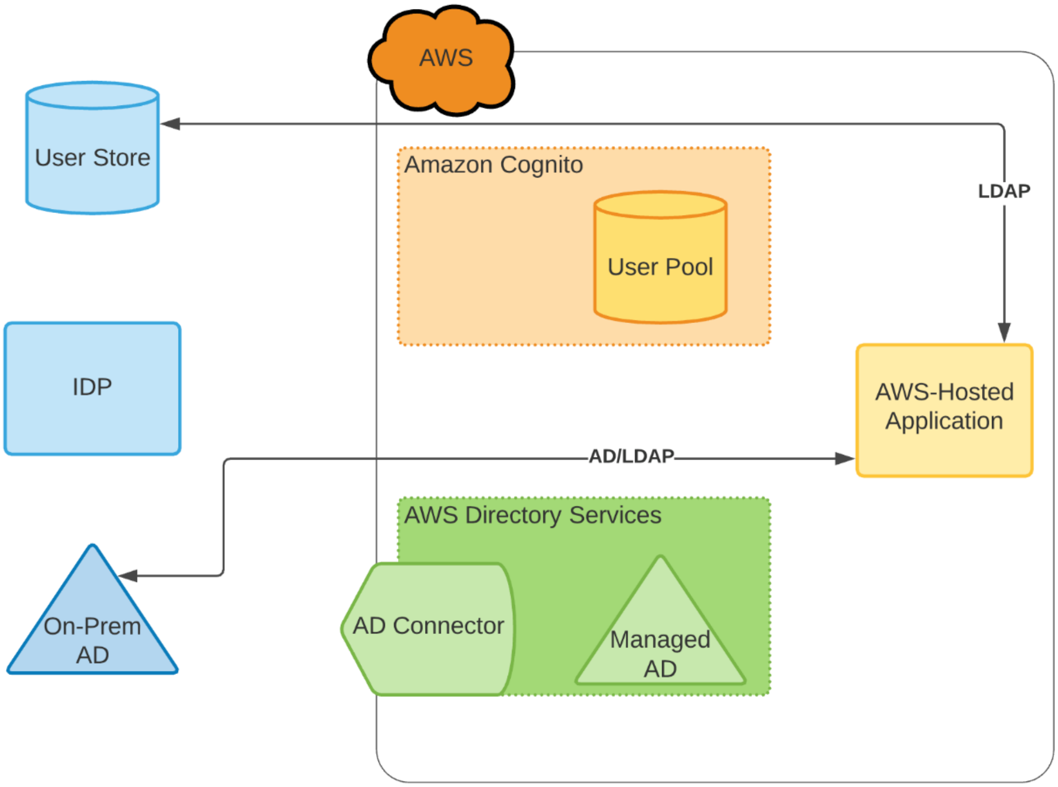
```
jonlehtinen@ ~ % aws ec2 stop-instances --instance-id i-01296365cf6d834e6
StoppingInstances:
- CurrentState:
    Code: 64
    Name: stopping
  InstanceId: i-01296365cf6d834e6
  PreviousState:
    Code: 16
    Name: running
jonlehtinen@ ~ %
```

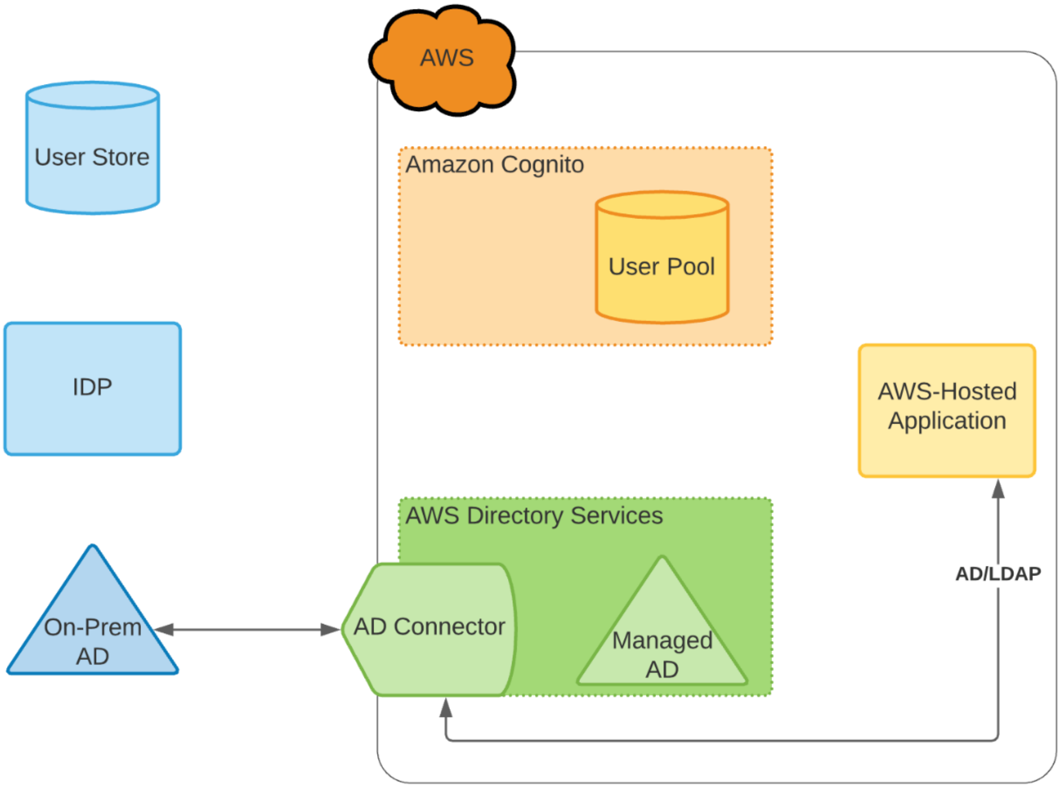
Chapter 11: Bringing Your Users into AWS

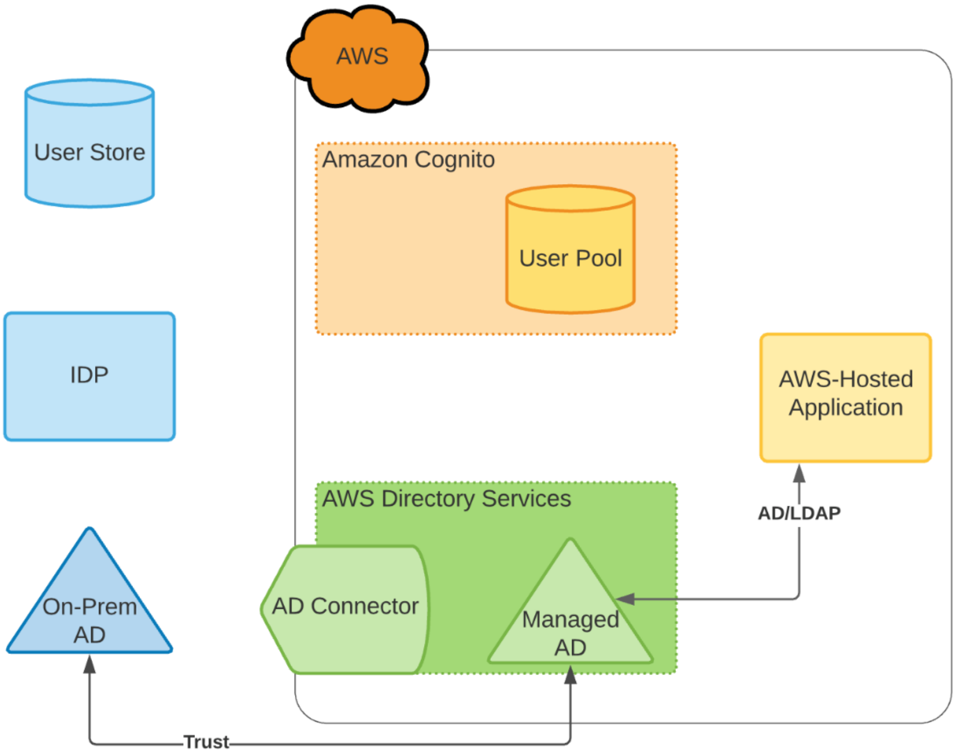


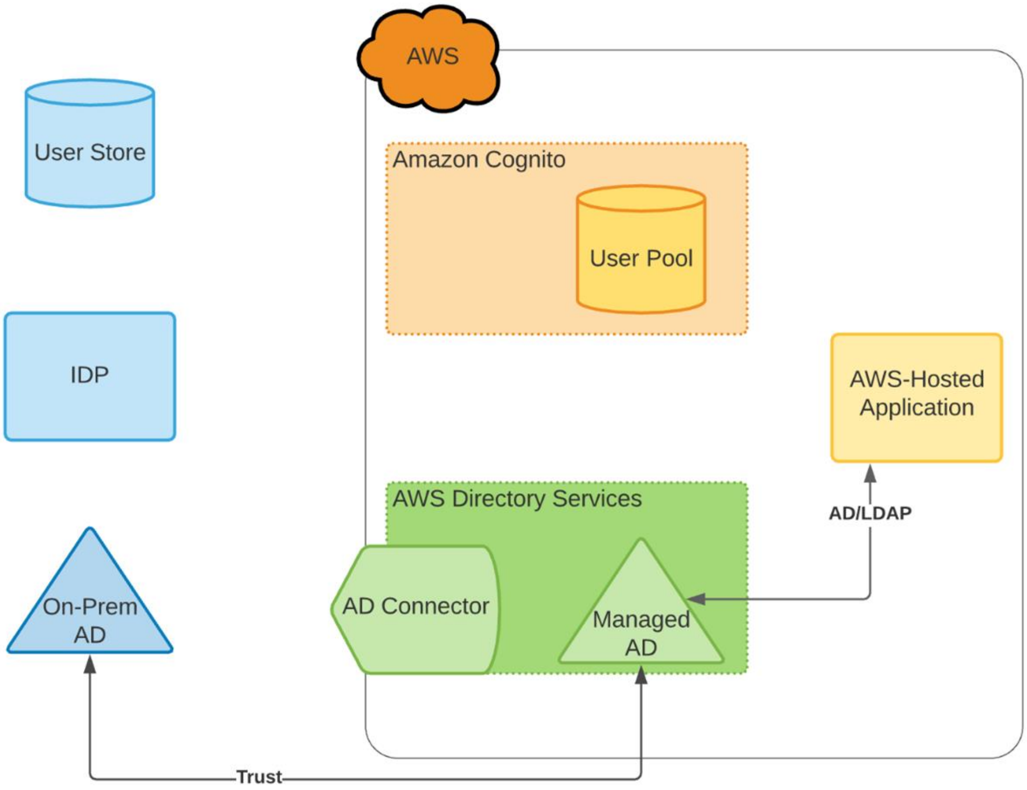

AWS
User Store
LDAP
Amazon Cognito
User Pool
IDP
SCIM
SAML/OIDC
AWS-Hosted Application
AWS Directory Services
On-Prem AD
AD Connector
Managed AD

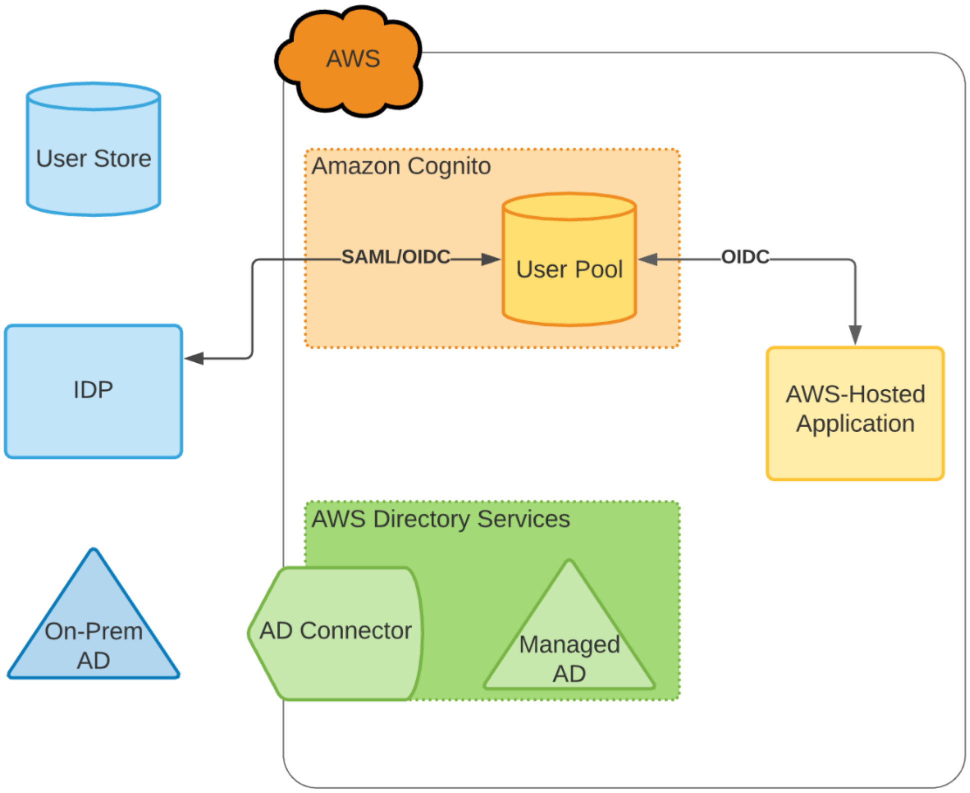

AWS
User Store
LDAP
Amazon Cognito
User Pool
LDAP
IDP
SAML/OIDC
AWS-Hosted Application
AWS Directory Services
On-Prem AD
AD Connector
Managed AD

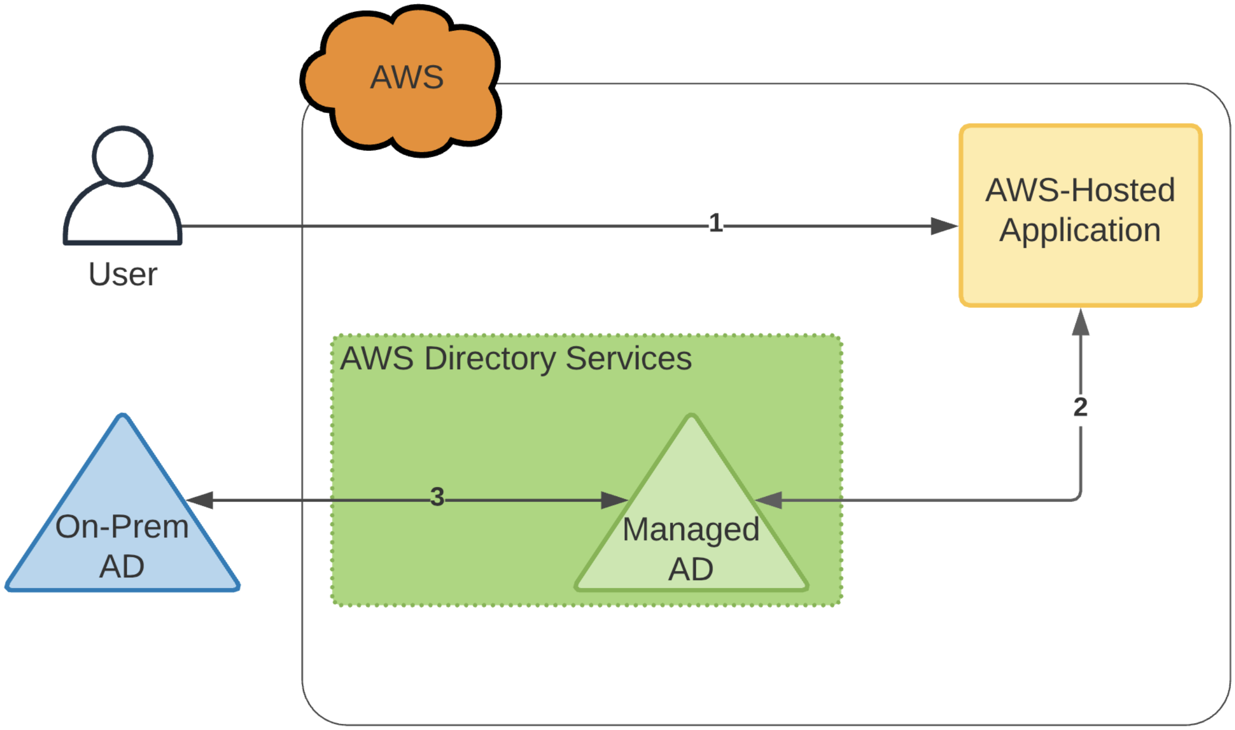

AWS
User Store
LDAP
Amazon Cognito
User Pool
IDP
AWS-Hosted Application
AD/LDAP
AWS Directory Services
On-Prem AD
AD Connector
Managed AD

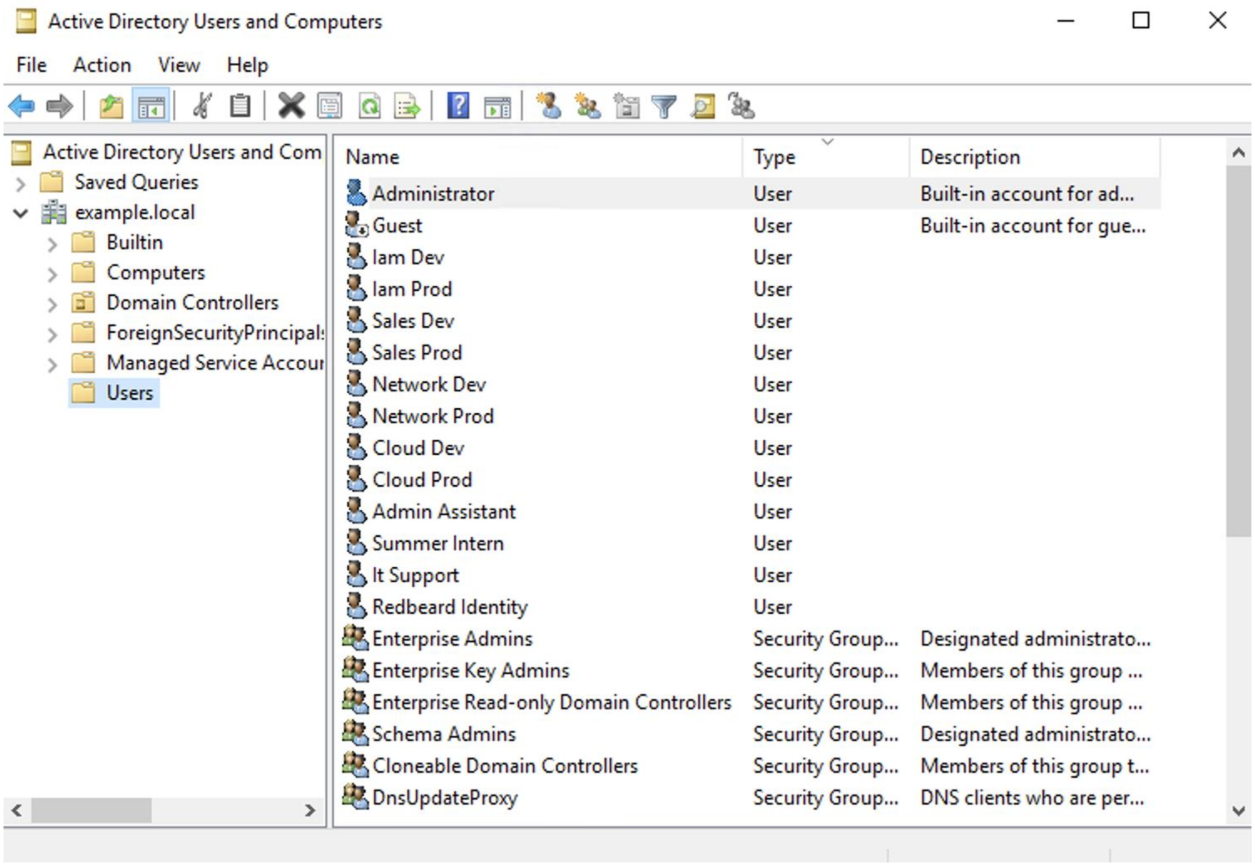

AWS
User Store
Amazon Cognito
User Pool
IDP
AWS-Hosted Application
AWS Directory Services
AD/LDAP
On-Prem AD
AD Connector
Managed AD


AWS
User Store
Amazon Cognito
User Pool
IDP
AWS-Hosted Application
AWS Directory Services
AD/LDAP
AD Connector
Managed AD
On-Prem AD
Trust


AWS
User Store
Amazon Cognito
User Pool
IDP
AWS-Hosted Application
AWS Directory Services
AD/LDAP
AD Connector
Managed AD
On-Prem AD
Trust


AWS
User Store
Amazon Cognito
SAML/OIDC
User Pool
OIDC
IDP
AWS-Hosted Application
AWS Directory Services
On-Prem AD
AD Connector
Managed AD


AWS
User
1
AWS-Hosted Application
AWS Directory Services
2
On-Prem AD
3
Managed AD

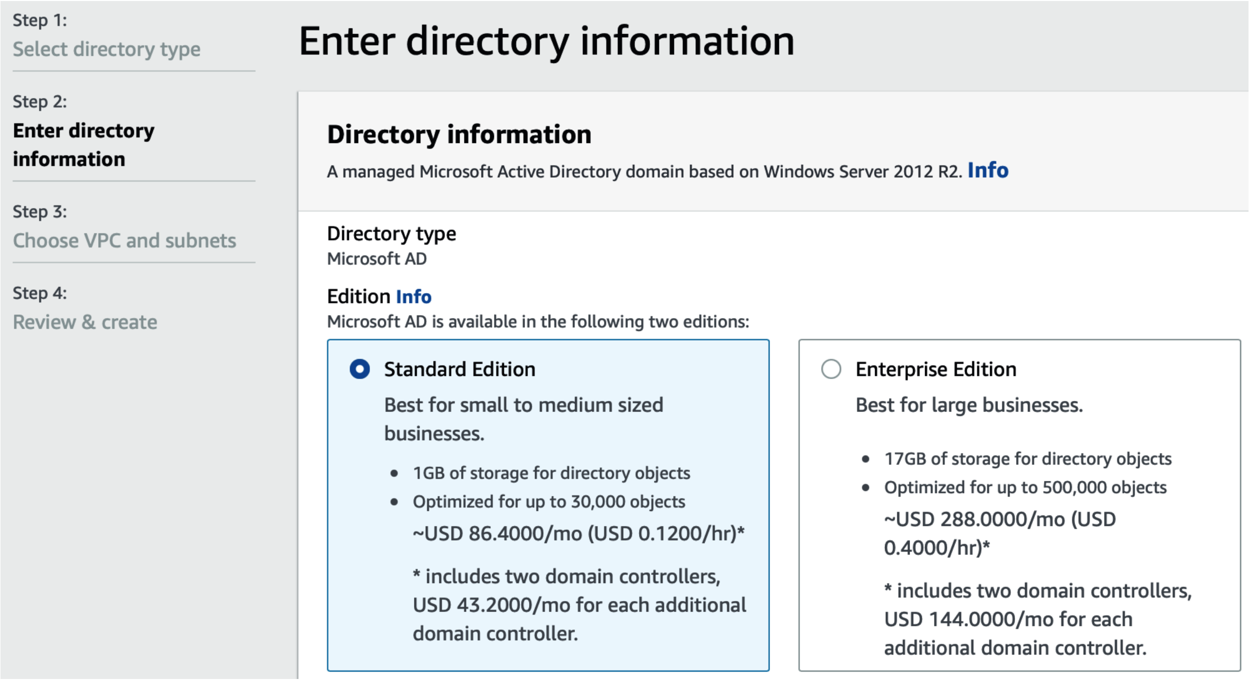


Active Directory Users and Computers

File Action View Help

- Active Directory Users and Com
  - Saved Queries
  - example.local
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipal:
    - Managed Service Accour
    - Users

Name	Type	Description
Administrator	User	Built-in account for ad...
Guest	User	Built-in account for gue...
Iam Dev	User	
Iam Prod	User	
Sales Dev	User	
Sales Prod	User	
Network Dev	User	
Network Prod	User	
Cloud Dev	User	
Cloud Prod	User	
Admin Assistant	User	
Summer Intern	User	
It Support	User	
Redbeard Identity	User	
Enterprise Admins	Security Group...	Designated administrato...
Enterprise Key Admins	Security Group...	Members of this group ...
Enterprise Read-only Domain Controllers	Security Group...	Members of this group ...
Schema Admins	Security Group...	Designated administrato...
Cloneable Domain Controllers	Security Group...	Members of this group t...
DnsUpdateProxy	Security Group...	DNS clients who are per...



Step 1:
Select directory type

Step 2:
Enter directory information

Step 3:
Choose VPC and subnets

Step 4:
Review & create

Enter directory information

Directory information

A managed Microsoft Active Directory domain based on Windows Server 2012 R2. Info

Directory type
Microsoft AD

Edition Info
Microsoft AD is available in the following two editions:

● Standard Edition

Best for small to medium sized businesses.

- 1GB of storage for directory objects
- Optimized for up to 30,000 objects

~USD 86.4000/mo (USD 0.1200/hr)*

* includes two domain controllers, USD 43.2000/mo for each additional domain controller.

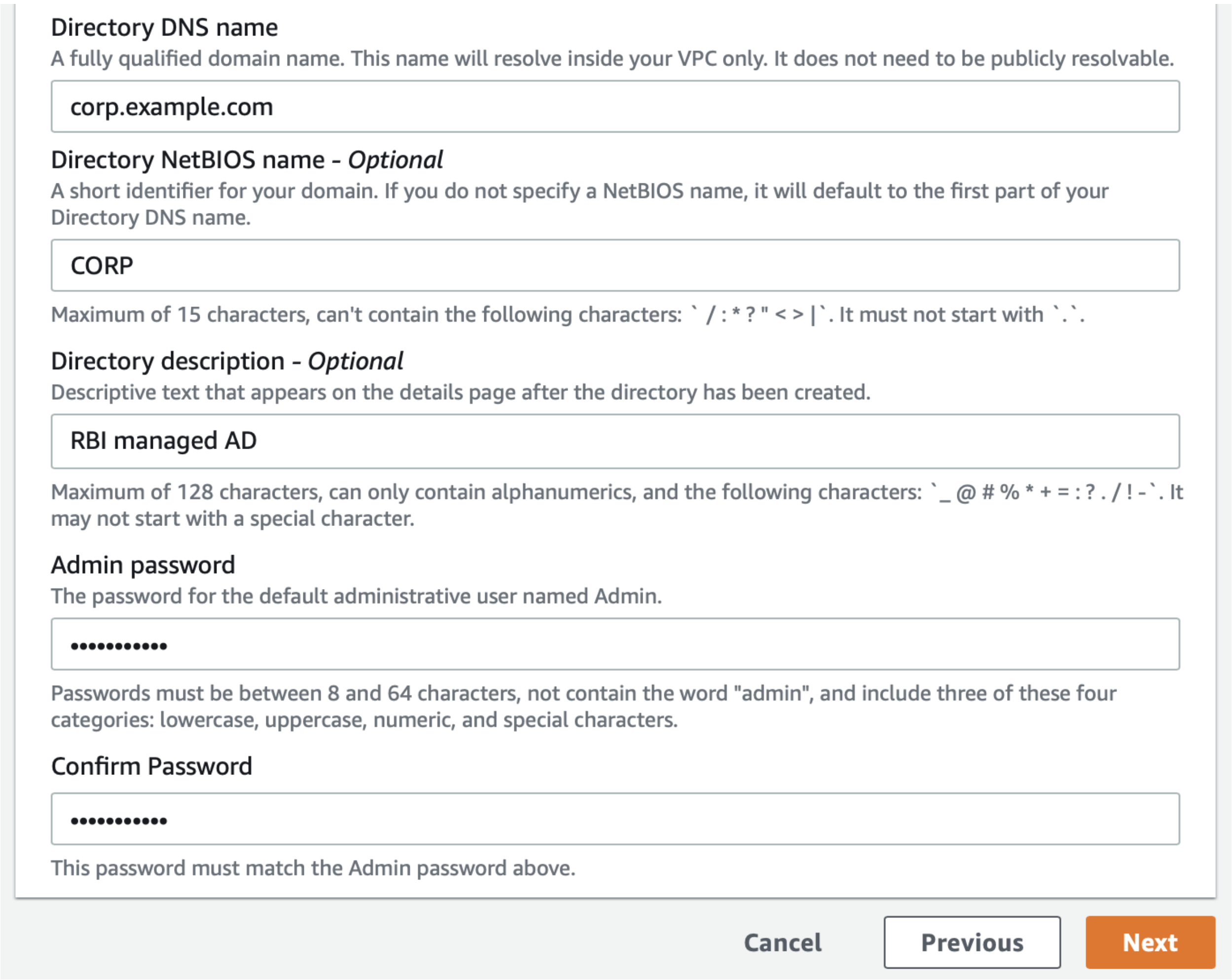
○ Enterprise Edition

Best for large businesses.

- 17GB of storage for directory objects
- Optimized for up to 500,000 objects

~USD 288.0000/mo (USD 0.4000/hr)*

* includes two domain controllers, USD 144.0000/mo for each additional domain controller.



Directory DNS name

A fully qualified domain name. This name will resolve inside your VPC only. It does not need to be publicly resolvable.

corp.example.com

Directory NetBIOS name - *Optional*

A short identifier for your domain. If you do not specify a NetBIOS name, it will default to the first part of your Directory DNS name.

CORP

Maximum of 15 characters, can't contain the following characters: ` / : * ? " < > |`. It must not start with `.`.

Directory description - *Optional*

Descriptive text that appears on the details page after the directory has been created.

RBI managed AD

Maximum of 128 characters, can only contain alphanumerics, and the following characters: `_ @ # % * + = : ? . / ! -`. It may not start with a special character.

Admin password

The password for the default administrative user named Admin.

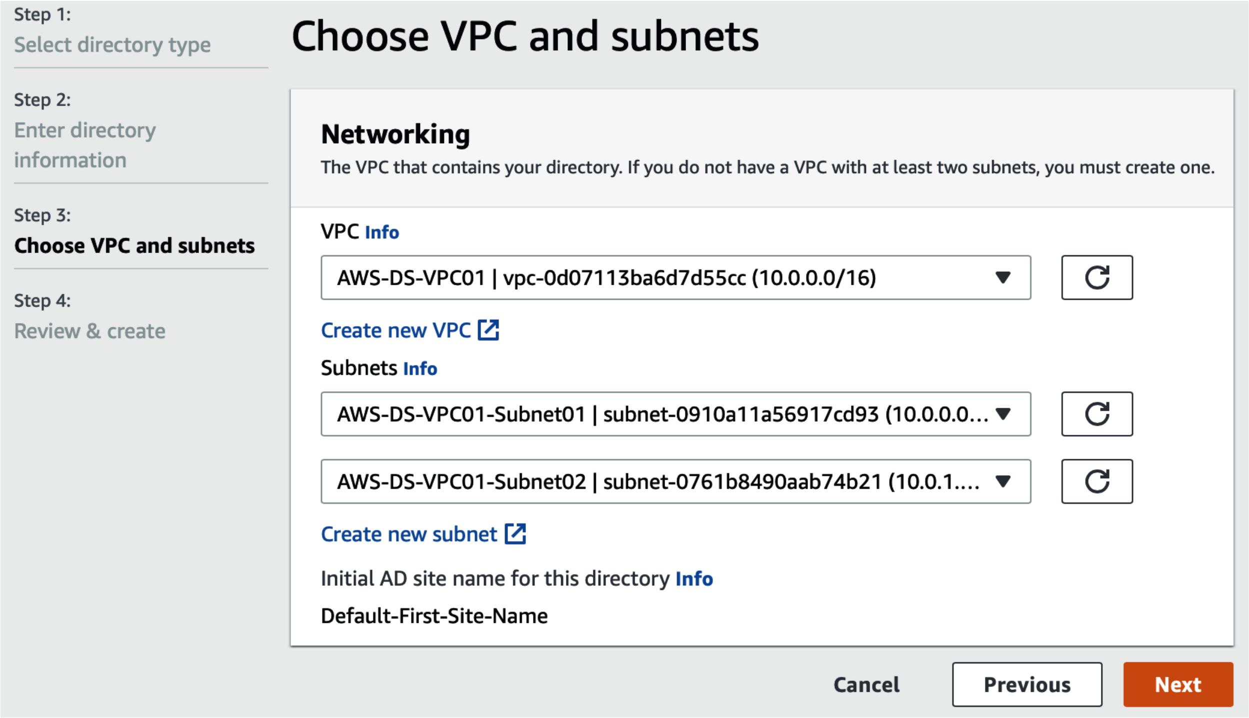
•••••••••••

Passwords must be between 8 and 64 characters, not contain the word "admin", and include three of these four categories: lowercase, uppercase, numeric, and special characters.

Confirm Password

•••••••••••

This password must match the Admin password above.



Choose VPC and subnets

Networking

The VPC that contains your directory. If you do not have a VPC with at least two subnets, you must create one.

VPC Info

AWS-DS-VPC01 | vpc-0d07113ba6d7d55cc (10.0.0.0/16)

Create new VPC

Subnets Info

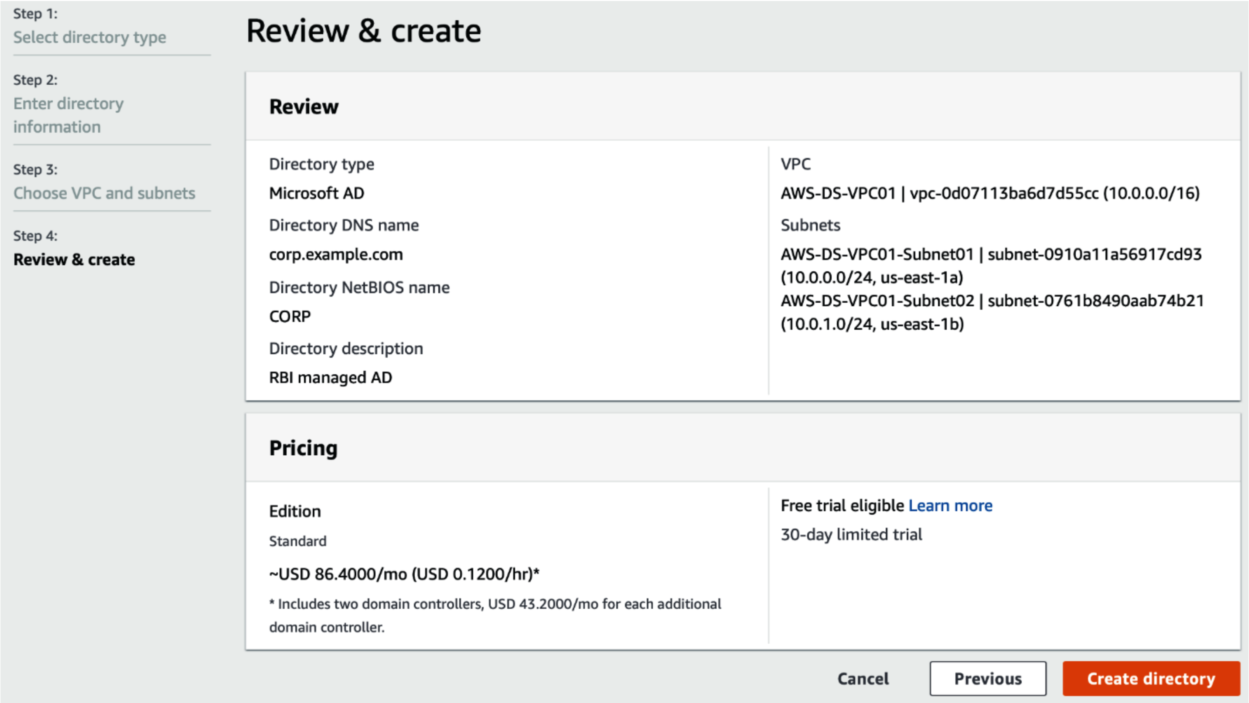
AWS-DS-VPC01-Subnet01 | subnet-0910a11a56917cd93 (10.0.0.0…

AWS-DS-VPC01-Subnet02 | subnet-0761b8490aab74b21 (10.0.1.…

Create new subnet

Initial AD site name for this directory Info

Default-First-Site-Name



Review & create

Review

Directory type
Microsoft AD

Directory DNS name
corp.example.com

Directory NetBIOS name
CORP

Directory description
RBI managed AD

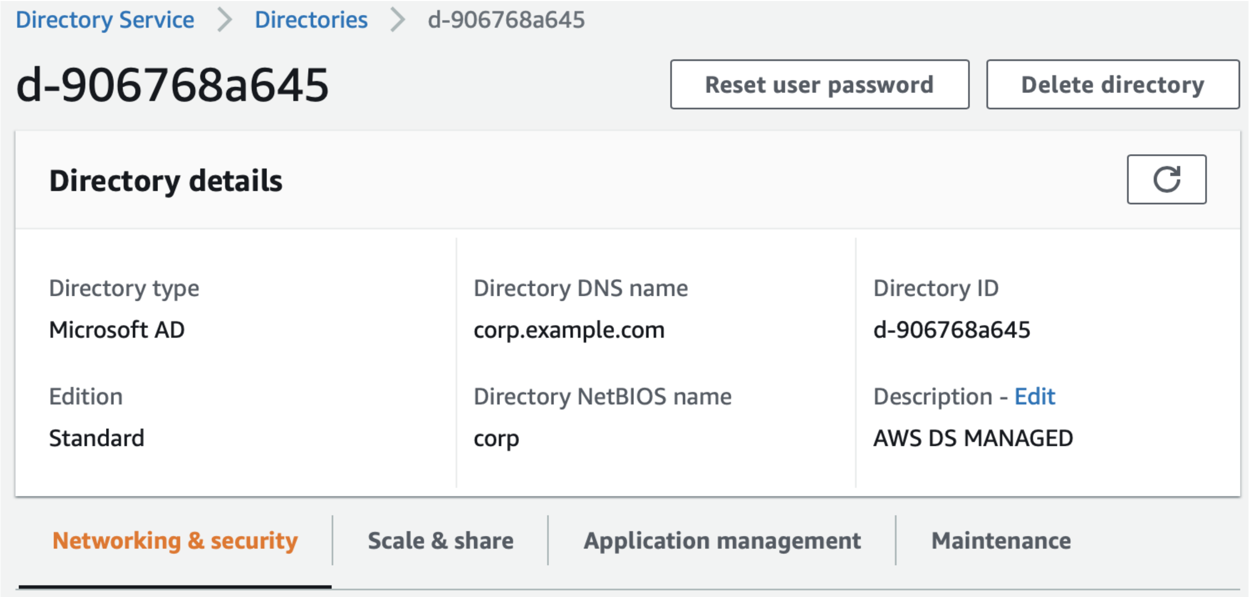
VPC
AWS-DS-VPC01 | vpc-0d07113ba6d7d55cc (10.0.0.0/16)

Subnets
AWS-DS-VPC01-Subnet01 | subnet-0910a11a56917cd93 (10.0.0.0/24, us-east-1a)
AWS-DS-VPC01-Subnet02 | subnet-0761b8490aab74b21 (10.0.1.0/24, us-east-1b)

Pricing

Edition
Standard
~USD 86.4000/mo (USD 0.1200/hr)*
* Includes two domain controllers, USD 43.2000/mo for each additional domain controller.

Free trial eligible Learn more
30-day limited trial



d-906768a645

Directory details

Directory type
Microsoft AD

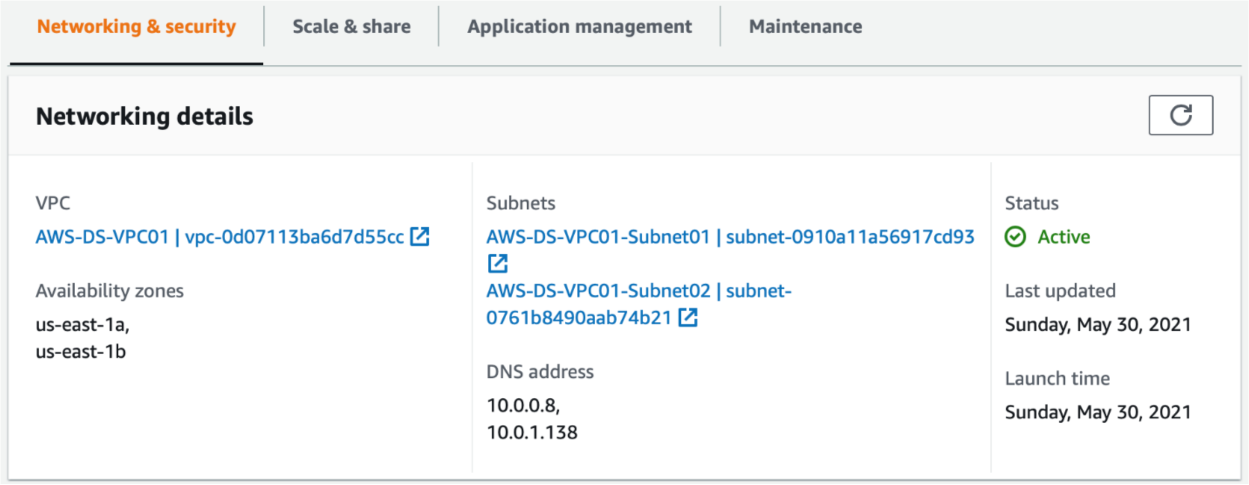
Edition
Standard

Directory DNS name
corp.example.com

Directory NetBIOS name
corp

Directory ID
d-906768a645

Description - Edit
AWS DS MANAGED



Networking details

VPC
AWS-DS-VPC01 | vpc-0d07113ba6d7d55cc

Availability zones
us-east-1a,
us-east-1b

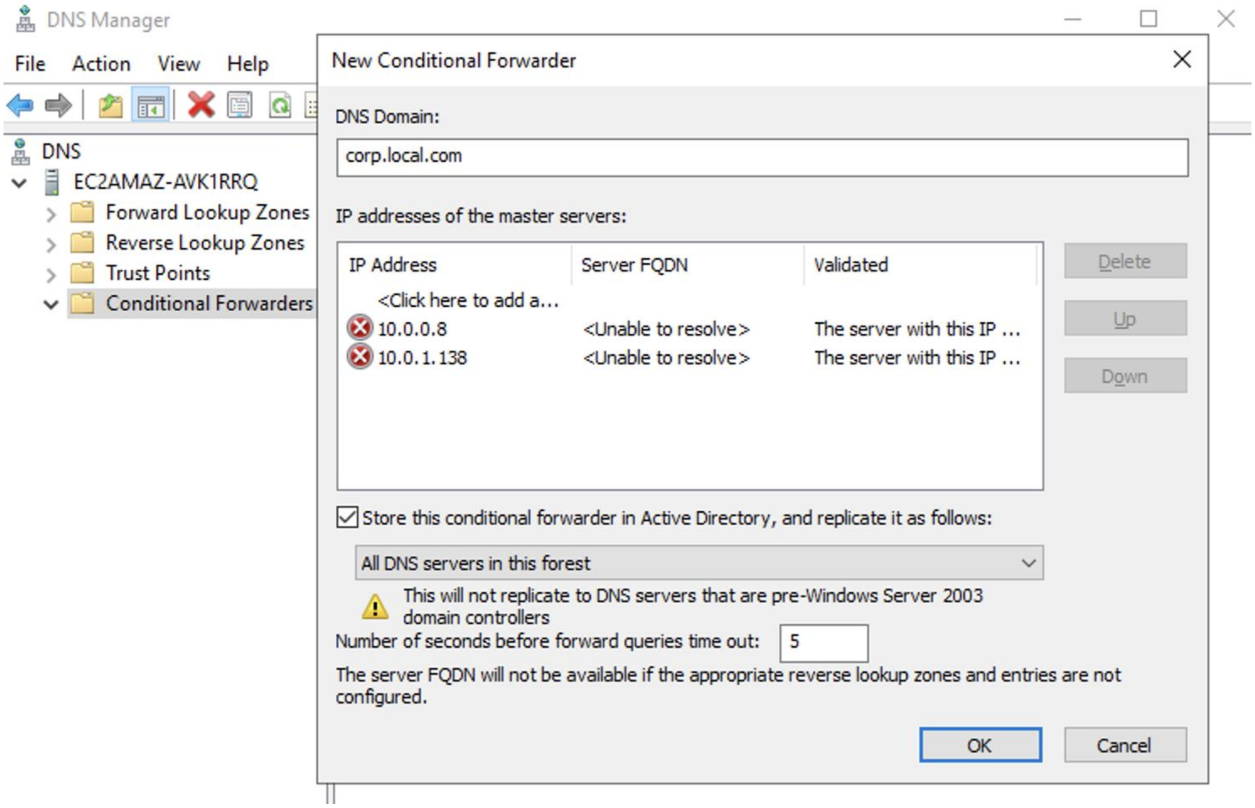
Subnets
AWS-DS-VPC01-Subnet01 | subnet-0910a11a56917cd93
AWS-DS-VPC01-Subnet02 | subnet-0761b8490aab74b21

DNS address
10.0.0.8,
10.0.1.138

Status
Active

Last updated
Sunday, May 30, 2021

Launch time
Sunday, May 30, 2021



New Conditional Forwarder

DNS Domain:

corp.local.com

IP addresses of the master servers:

IP Address	Server FQDN	Validated
<Click here to add a...		
☒ 10.0.0.8	<Unable to resolve>	The server with this IP ...
☒ 10.0.1.138	<Unable to resolve>	The server with this IP ...

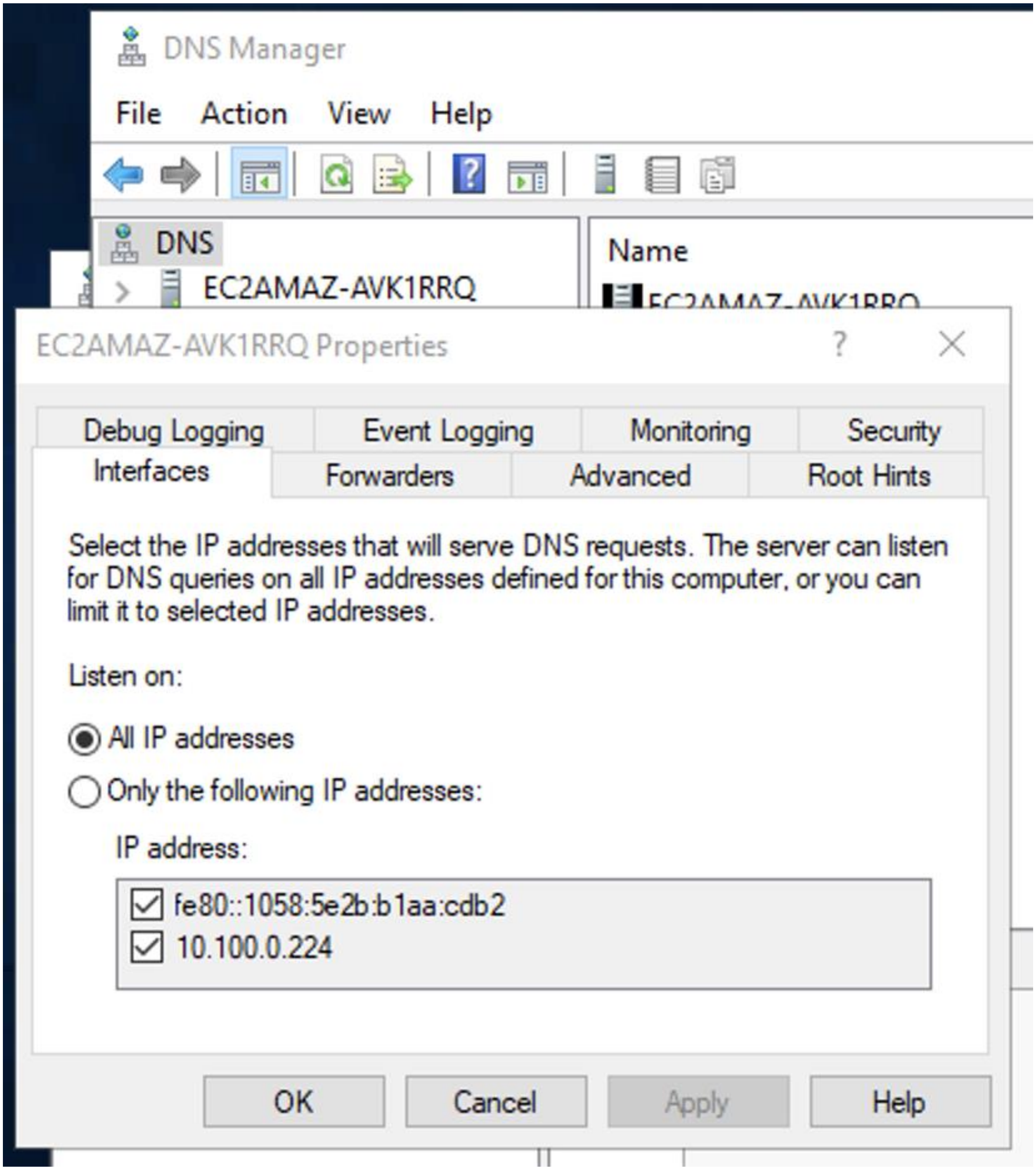
☑ Store this conditional forwarder in Active Directory, and replicate it as follows:

All DNS servers in this forest

⚠ This will not replicate to DNS servers that are pre-Windows Server 2003 domain controllers

Number of seconds before forward queries time out: 5

The server FQDN will not be available if the appropriate reverse lookup zones and entries are not configured.



EC2AMAZ-AVK1RRQ Properties

Select the IP addresses that will serve DNS requests. The server can listen for DNS queries on all IP addresses defined for this computer, or you can limit it to selected IP addresses.

Listen on:

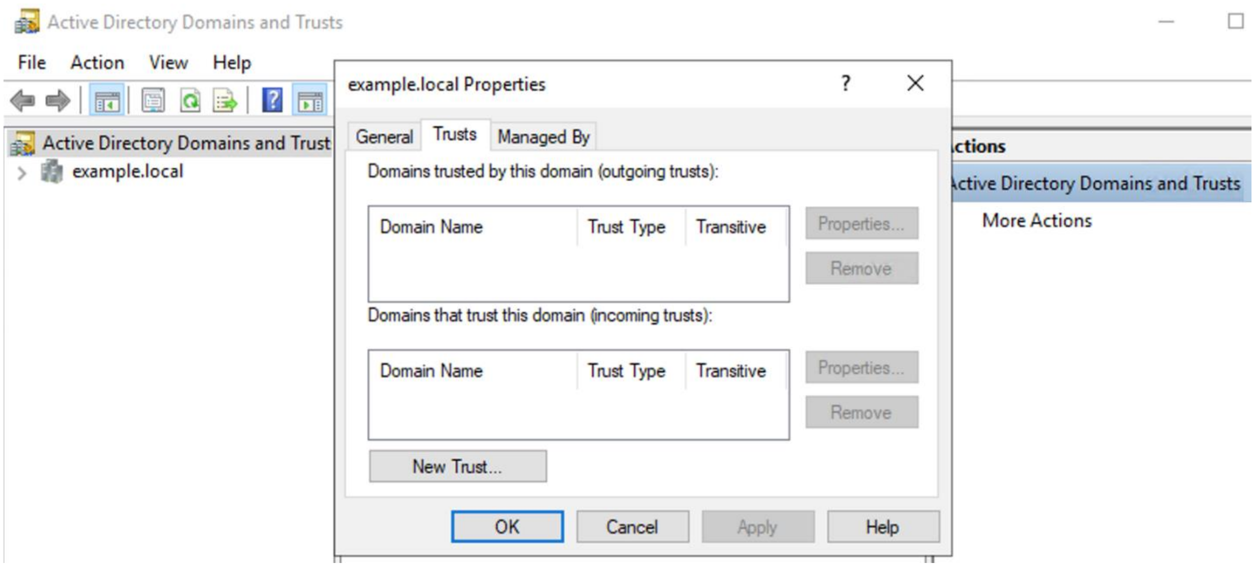
● All IP addresses

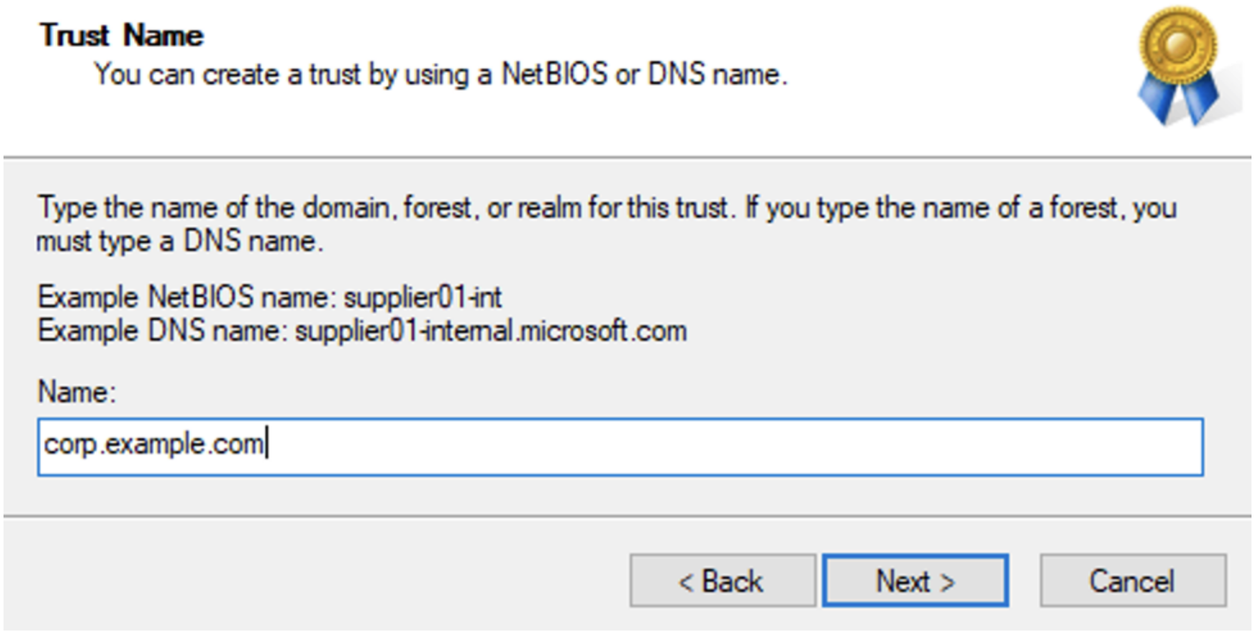
○ Only the following IP addresses:

IP address:

☑ fe80::1058:5e2b:b1aa:cdb2

☑ 10.100.0.224





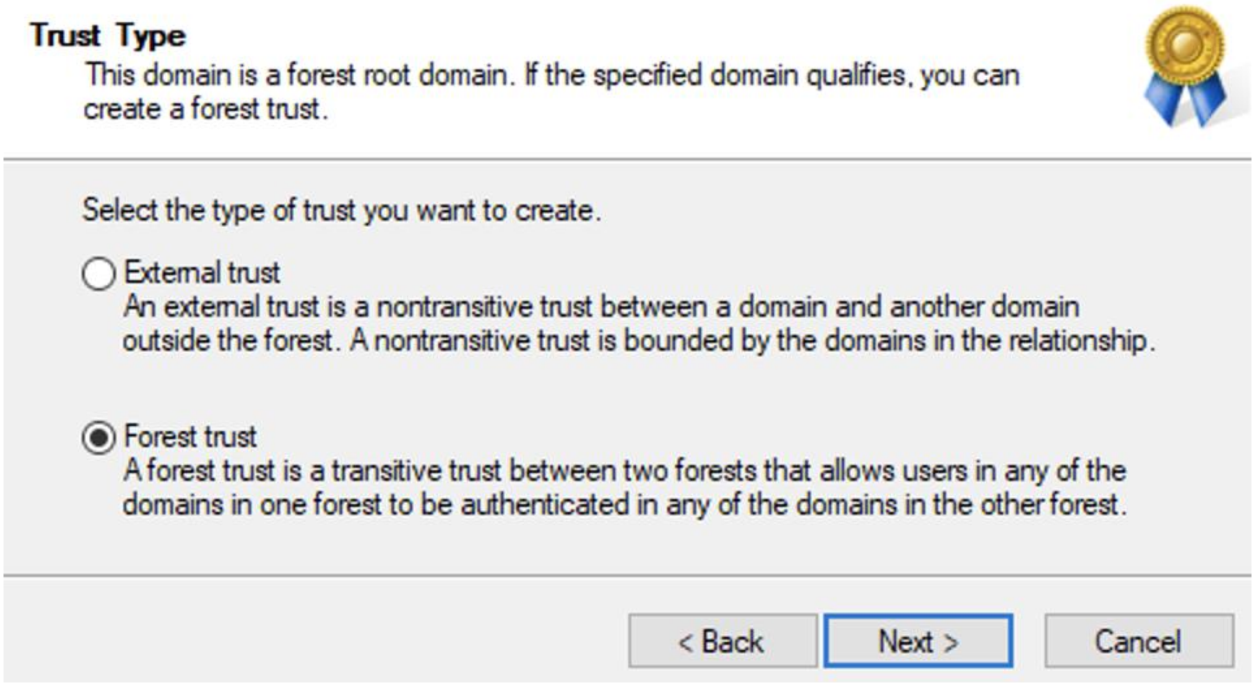
Trust Name

You can create a trust by using a NetBIOS or DNS name.

Type the name of the domain, forest, or realm for this trust. If you type the name of a forest, you must type a DNS name.

Example NetBIOS name: supplier01-int
Example DNS name: supplier01-internal.microsoft.com

Name:
corp.example.com



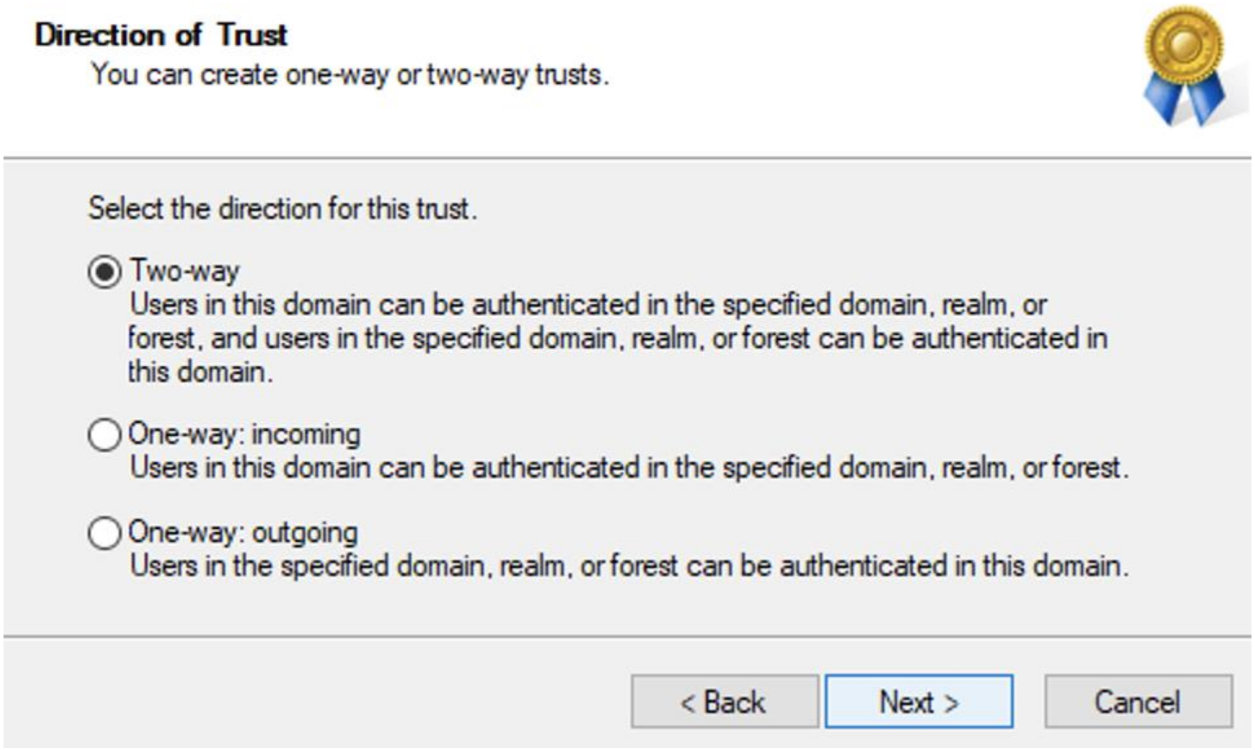
Trust Type

This domain is a forest root domain. If the specified domain qualifies, you can create a forest trust.

Select the type of trust you want to create.

○ External trust
An external trust is a nontransitive trust between a domain and another domain outside the forest. A nontransitive trust is bounded by the domains in the relationship.

● Forest trust
A forest trust is a transitive trust between two forests that allows users in any of the domains in one forest to be authenticated in any of the domains in the other forest.



Direction of Trust

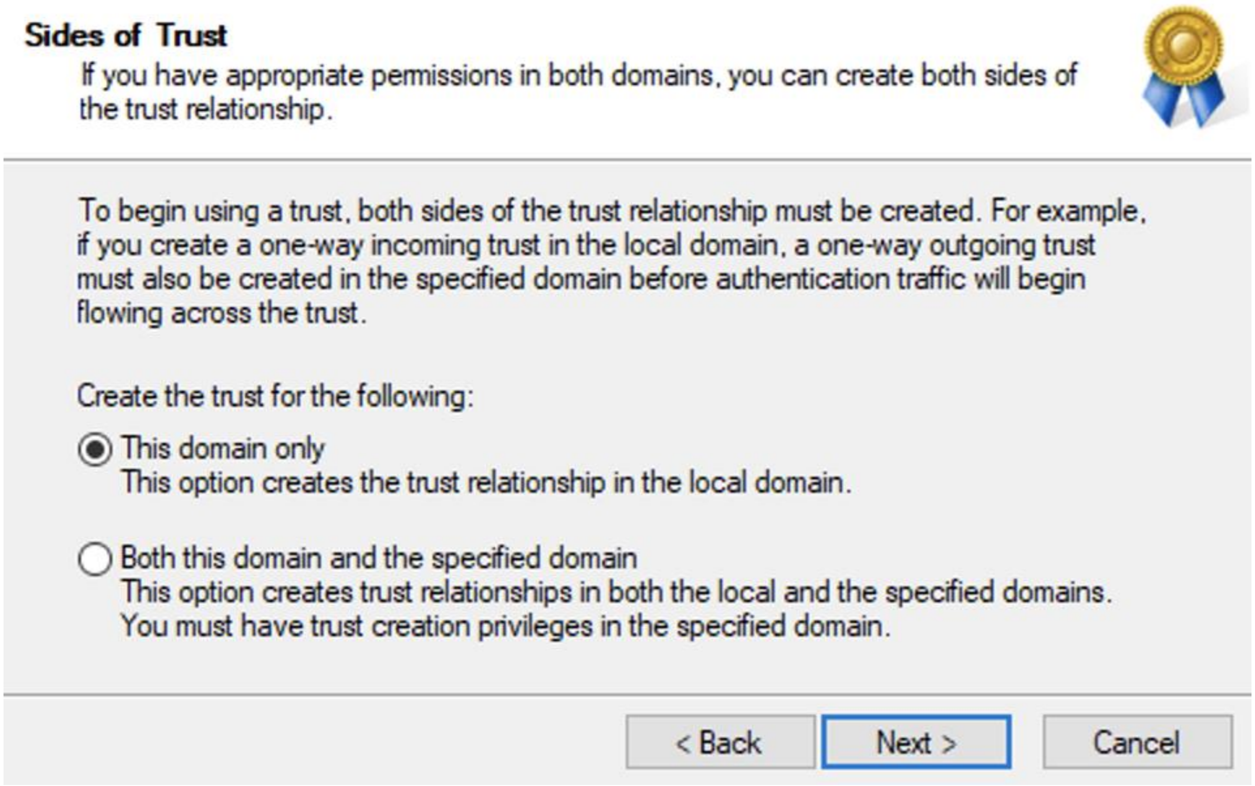
You can create one-way or two-way trusts.

Select the direction for this trust.

● Two-way
Users in this domain can be authenticated in the specified domain, realm, or forest, and users in the specified domain, realm, or forest can be authenticated in this domain.

○ One-way: incoming
Users in this domain can be authenticated in the specified domain, realm, or forest.

○ One-way: outgoing
Users in the specified domain, realm, or forest can be authenticated in this domain.



Sides of Trust

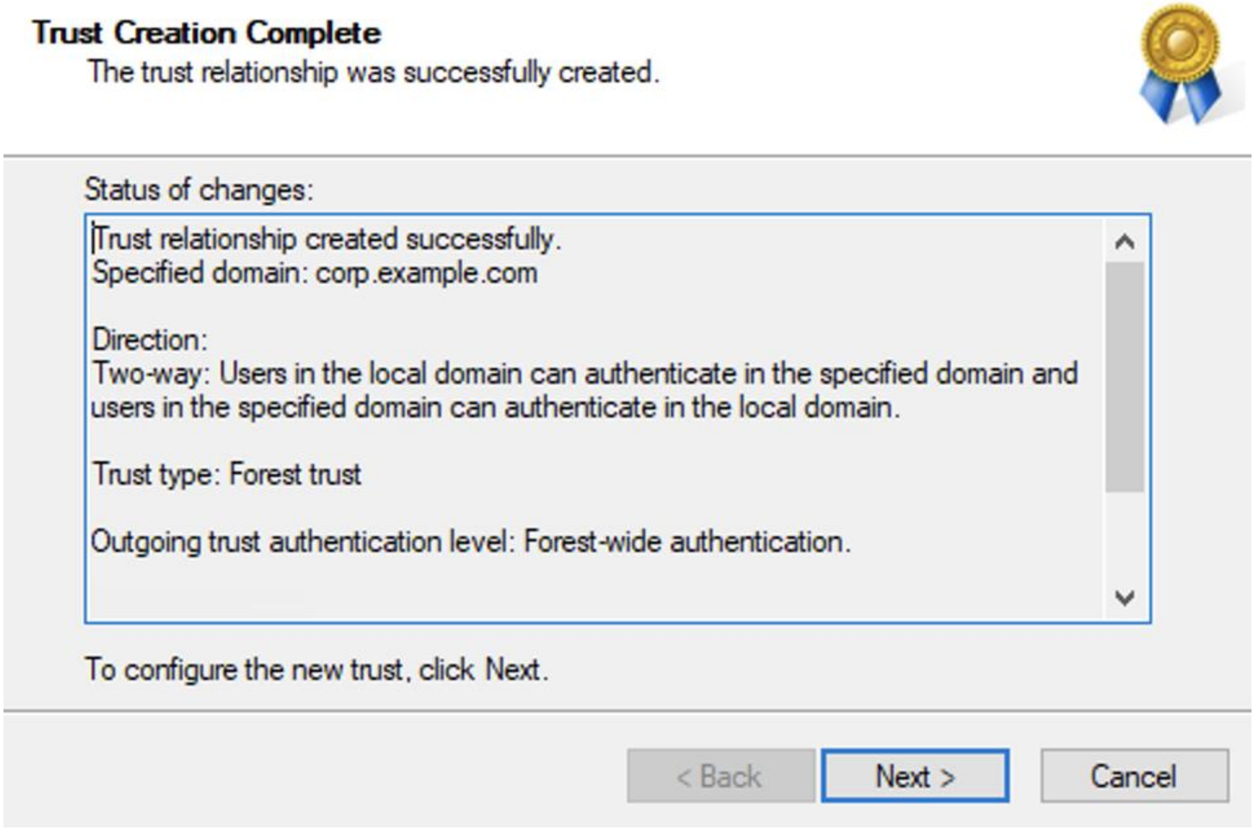
If you have appropriate permissions in both domains, you can create both sides of the trust relationship.

To begin using a trust, both sides of the trust relationship must be created. For example, if you create a one-way incoming trust in the local domain, a one-way outgoing trust must also be created in the specified domain before authentication traffic will begin flowing across the trust.

Create the trust for the following:

● This domain only
This option creates the trust relationship in the local domain.

○ Both this domain and the specified domain
This option creates trust relationships in both the local and the specified domains. You must have trust creation privileges in the specified domain.



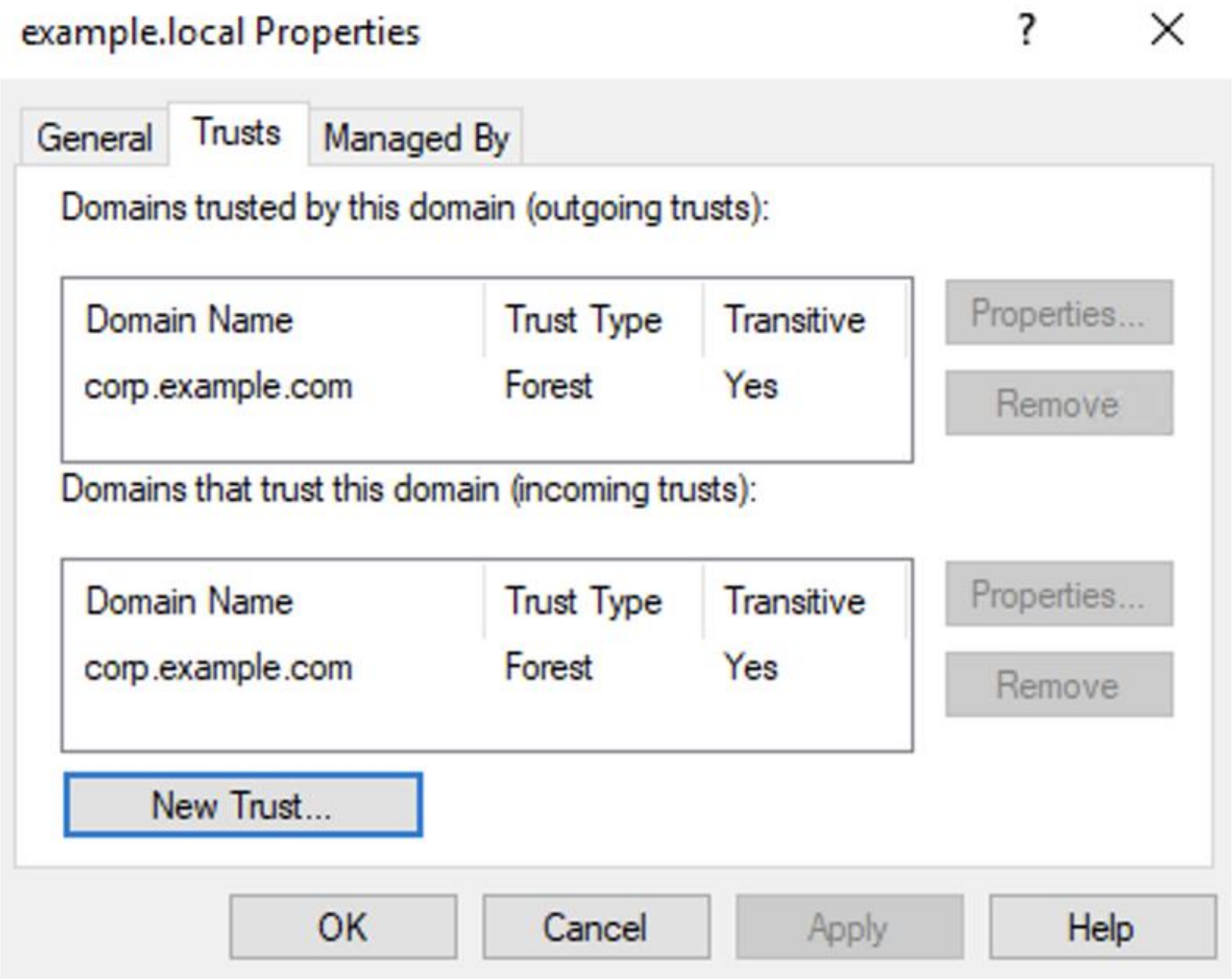
Trust Creation Complete

The trust relationship was successfully created.

Status of changes:

```
Trust relationship created successfully.
Specified domain: corp.example.com

Direction:
Two-way: Users in the local domain can authenticate in the specified domain and
users in the specified domain can authenticate in the local domain.

Trust type: Forest trust

Outgoing trust authentication level: Forest-wide authentication.
```

To configure the new trust, click Next.



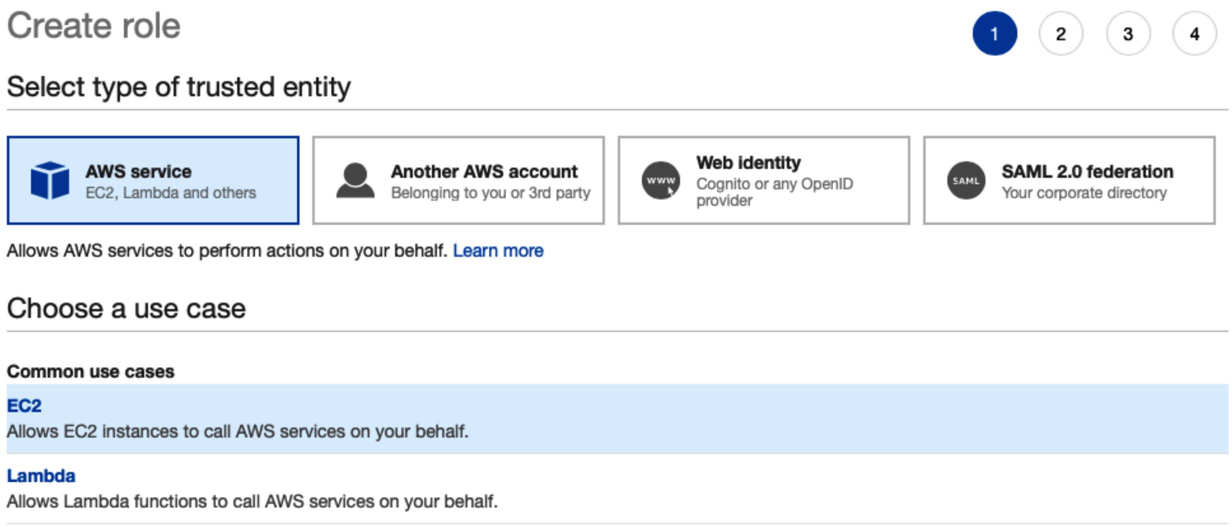
example.local Properties

Domains trusted by this domain (outgoing trusts):

Domain Name	Trust Type	Transitive
corp.example.com	Forest	Yes

Domains that trust this domain (incoming trusts):

Domain Name	Trust Type	Transitive
corp.example.com	Forest	Yes



Create role

Select type of trusted entity

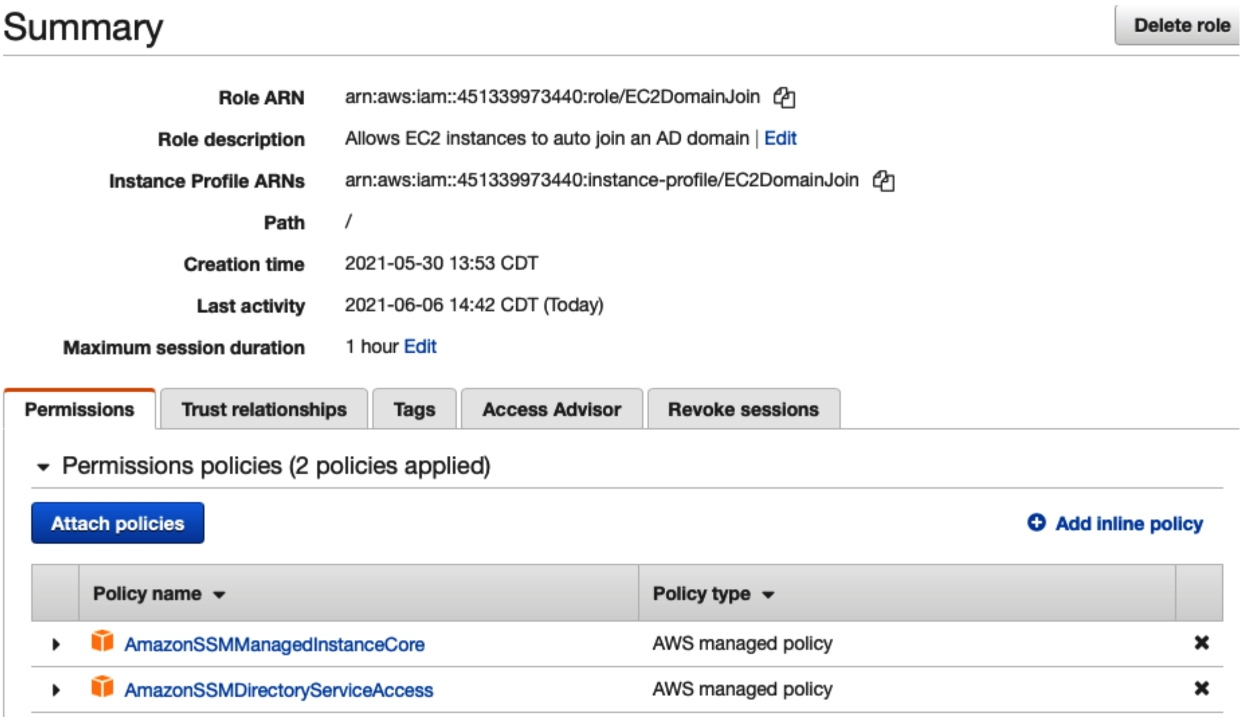
Allows AWS services to perform actions on your behalf. Learn more

Choose a use case

Common use cases

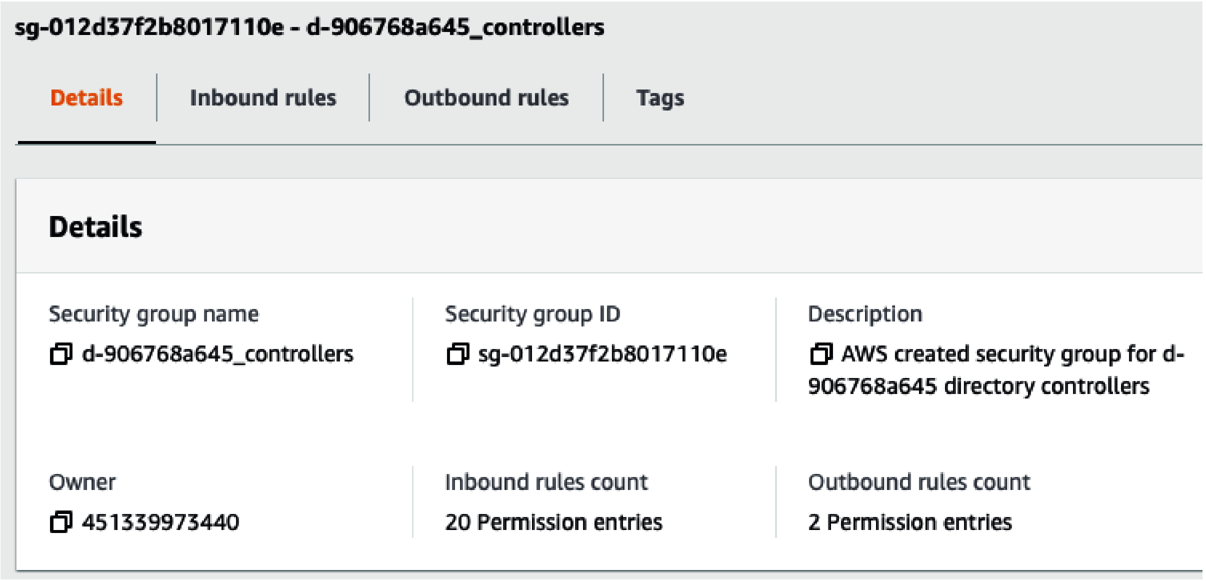
EC2
Allows EC2 instances to call AWS services on your behalf.

Lambda
Allows Lambda functions to call AWS services on your behalf.

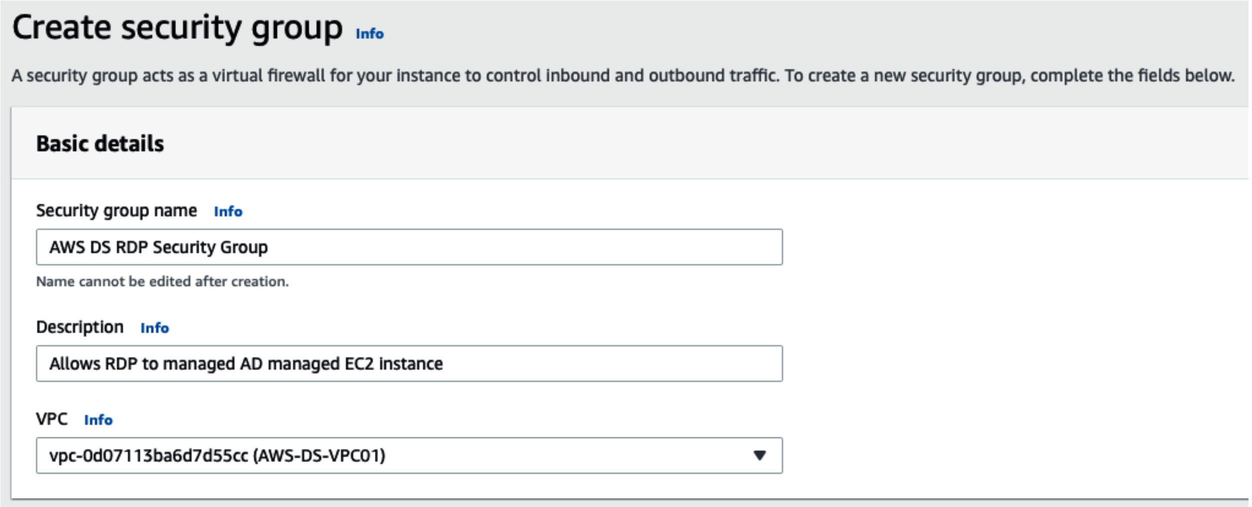


Role ARN	arn:aws:iam::451339973440:role/EC2DomainJoin
Role description	Allows EC2 instances to auto join an AD domain | Edit
Instance Profile ARNs	arn:aws:iam::451339973440:instance-profile/EC2DomainJoin
Path	/
Creation time	2021-05-30 13:53 CDT
Last activity	2021-06-06 14:42 CDT (Today)
Maximum session duration	1 hour Edit

	Policy name	Policy type	
▸	AmazonSSMManagedInstanceCore	AWS managed policy	✖
▸	AmazonSSMDirectoryServiceAccess	AWS managed policy	✖



Security group name	Security group ID	Description
d-906768a645_controllers	sg-012d37f2b8017110e	AWS created security group for d-906768a645 directory controllers
Owner	Inbound rules count	Outbound rules count
451339973440	20 Permission entries	2 Permission entries



Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info

AWS DS RDP Security Group

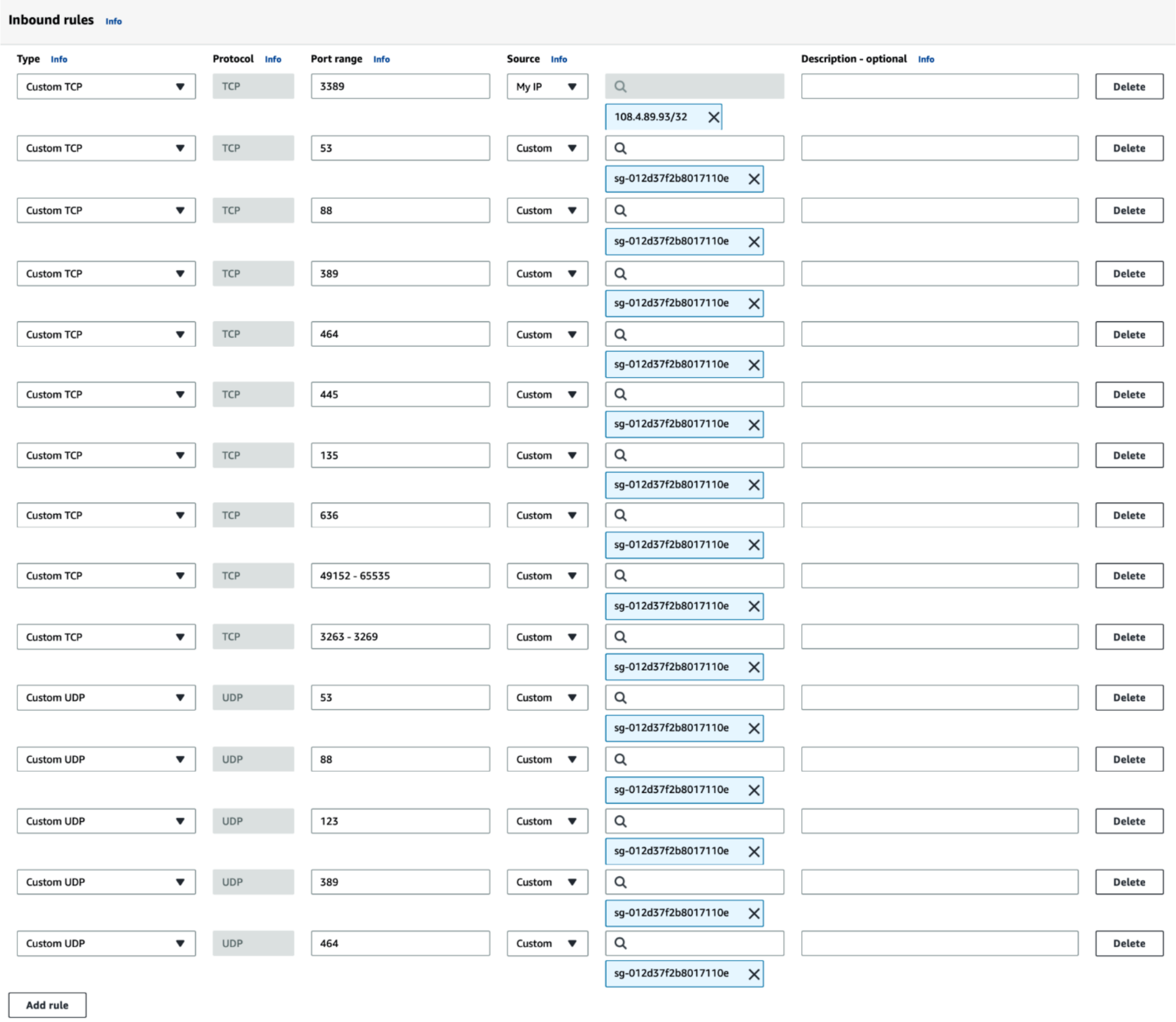
Name cannot be edited after creation.

Description Info

Allows RDP to managed AD managed EC2 instance

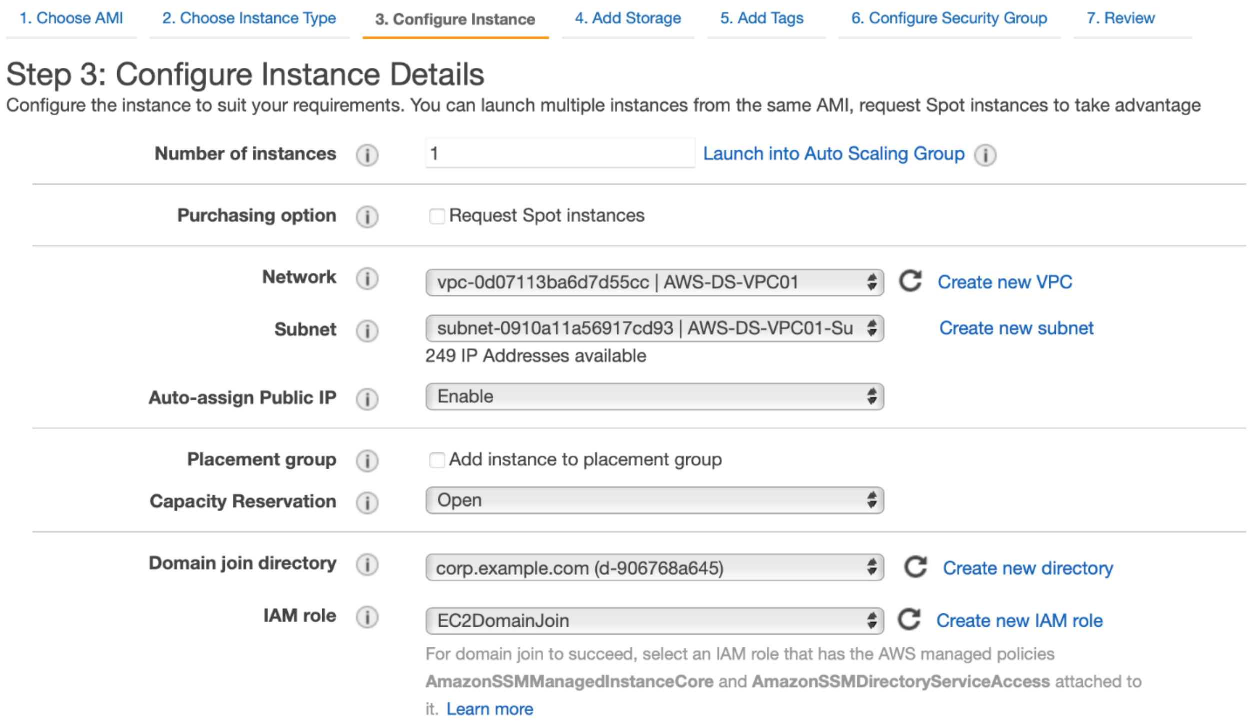
VPC Info

vpc-0d07113ba6d7d55cc (AWS-DS-VPC01) ▼



Inbound rules Info

Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
Custom TCP ▼	TCP	3389	My IP ▼	108.4.89.93/32 ×		Delete
Custom TCP ▼	TCP	53	Custom ▼	sg-012d37f2b8017110e ×		Delete
Custom TCP ▼	TCP	88	Custom ▼	sg-012d37f2b8017110e ×		Delete
Custom TCP ▼	TCP	389	Custom ▼	sg-012d37f2b8017110e ×		Delete
Custom TCP ▼	TCP	464	Custom ▼	sg-012d37f2b8017110e ×		Delete
Custom TCP ▼	TCP	445	Custom ▼	sg-012d37f2b8017110e ×		Delete
Custom TCP ▼	TCP	135	Custom ▼	sg-012d37f2b8017110e ×		Delete
Custom TCP ▼	TCP	636	Custom ▼	sg-012d37f2b8017110e ×		Delete
Custom TCP ▼	TCP	49152 - 65535	Custom ▼	sg-012d37f2b8017110e ×		Delete
Custom TCP ▼	TCP	3263 - 3269	Custom ▼	sg-012d37f2b8017110e ×		Delete
Custom UDP ▼	UDP	53	Custom ▼	sg-012d37f2b8017110e ×		Delete
Custom UDP ▼	UDP	88	Custom ▼	sg-012d37f2b8017110e ×		Delete
Custom UDP ▼	UDP	123	Custom ▼	sg-012d37f2b8017110e ×		Delete
Custom UDP ▼	UDP	389	Custom ▼	sg-012d37f2b8017110e ×		Delete
Custom UDP ▼	UDP	464	Custom ▼	sg-012d37f2b8017110e ×		Delete



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage

Number of instances: 1

Purchasing option: □ Request Spot instances

Network: vpc-0d07113ba6d7d55cc | AWS-DS-VPC01

Subnet: subnet-0910a11a56917cd93 | AWS-DS-VPC01-Su

249 IP Addresses available

Auto-assign Public IP: Enable

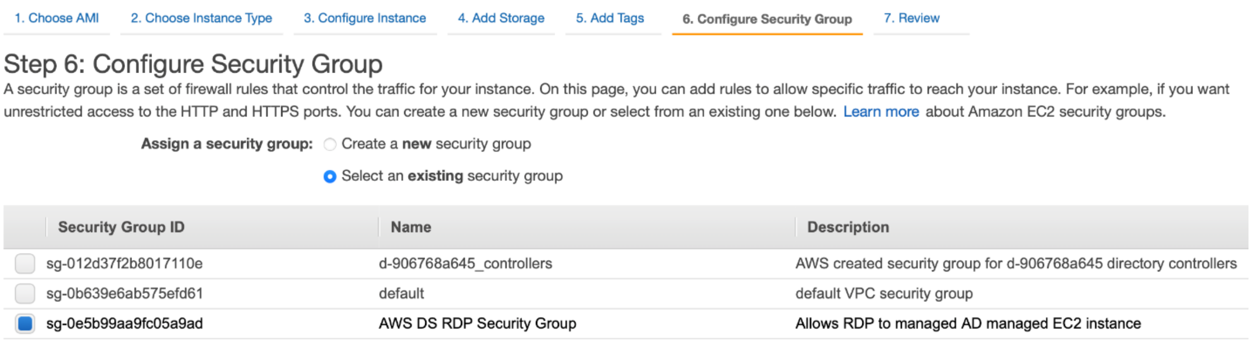
Placement group: □ Add instance to placement group

Capacity Reservation: Open

Domain join directory: corp.example.com (d-906768a645)

IAM role: EC2DomainJoin

For domain join to succeed, select an IAM role that has the AWS managed policies **AmazonSSMManagedInstanceCore** and **AmazonSSMDirectoryServiceAccess** attached to it. Learn more



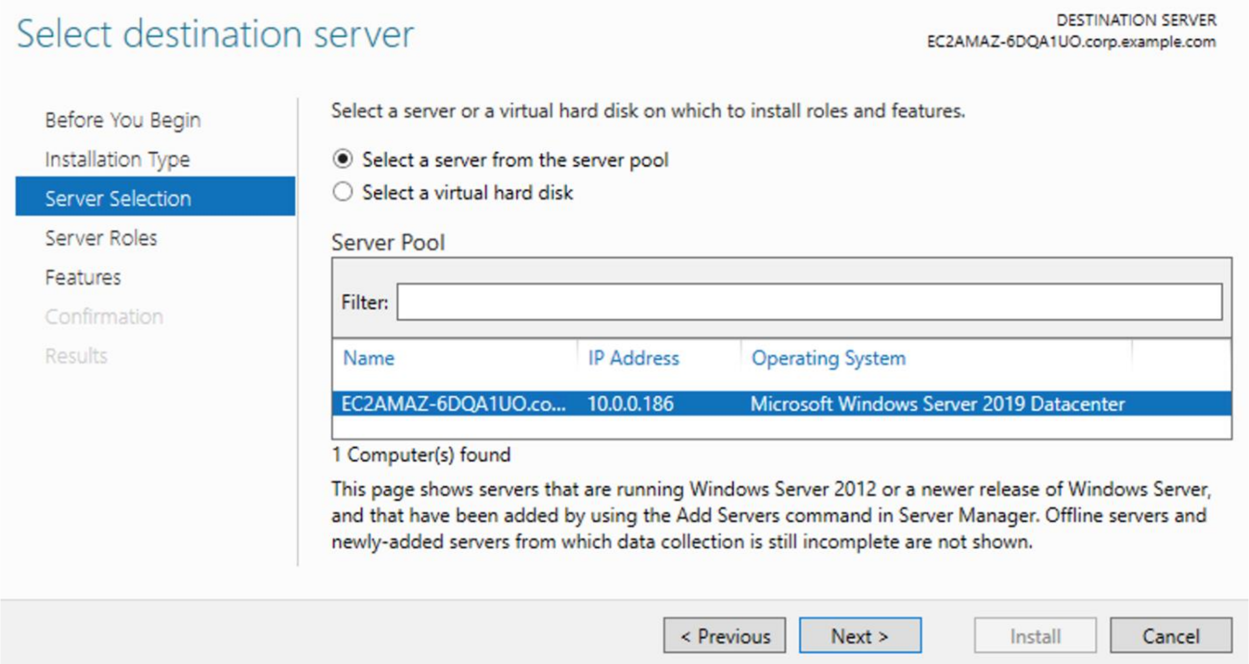
Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ○ Create a **new** security group

● Select an **existing** security group

	Security Group ID	Name	Description
□	sg-012d37f2b8017110e	d-906768a645_controllers	AWS created security group for d-906768a645 directory controllers
□	sg-0b639e6ab575efd61	default	default VPC security group
☑	sg-0e5b99aa9fc05a9ad	AWS DS RDP Security Group	Allows RDP to managed AD managed EC2 instance



Select destination server

DESTINATION SERVER
EC2AMAZ-6DQA1UO.corp.example.com

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

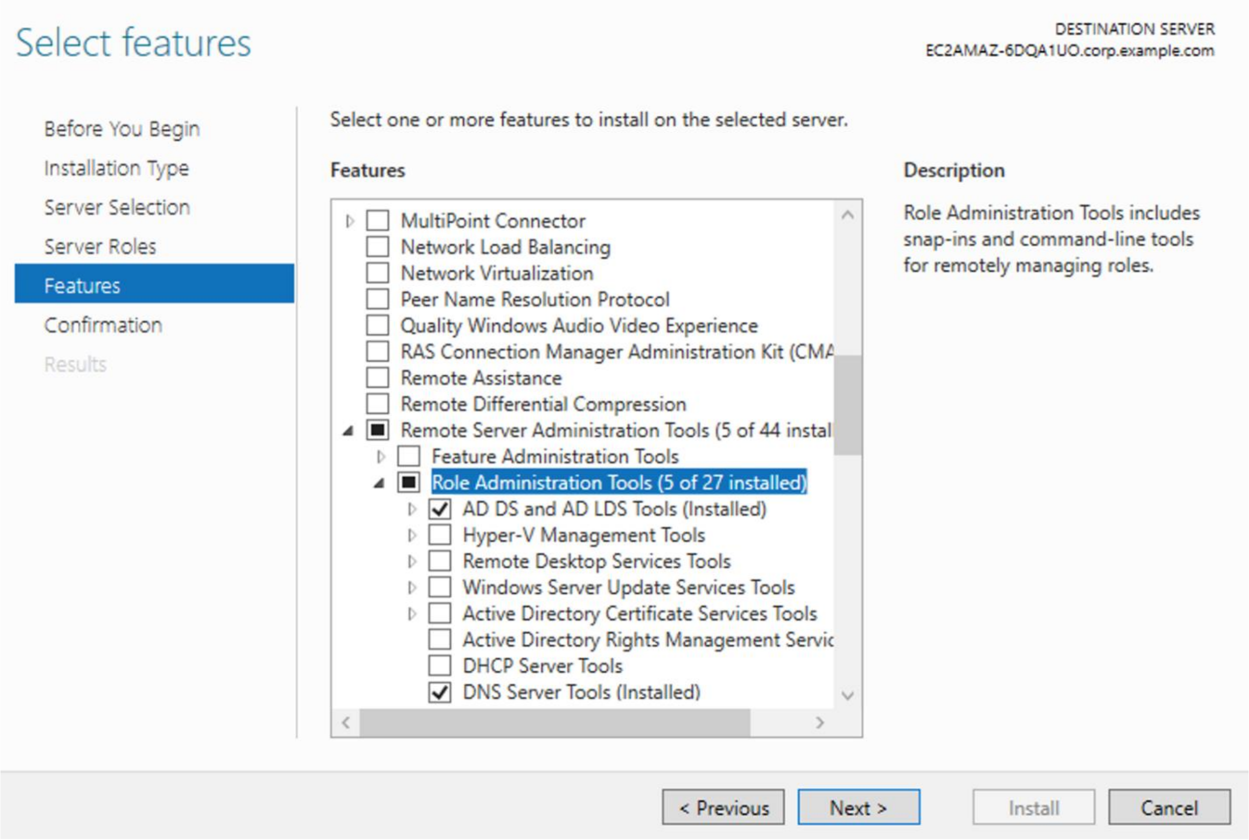
Server Pool

Filter:

Name	IP Address	Operating System
EC2AMAZ-6DQA1UO.co...	10.0.0.186	Microsoft Windows Server 2019 Datacenter

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.



Select features

DESTINATION SERVER
EC2AMAZ-6DQA1UO.corp.example.com

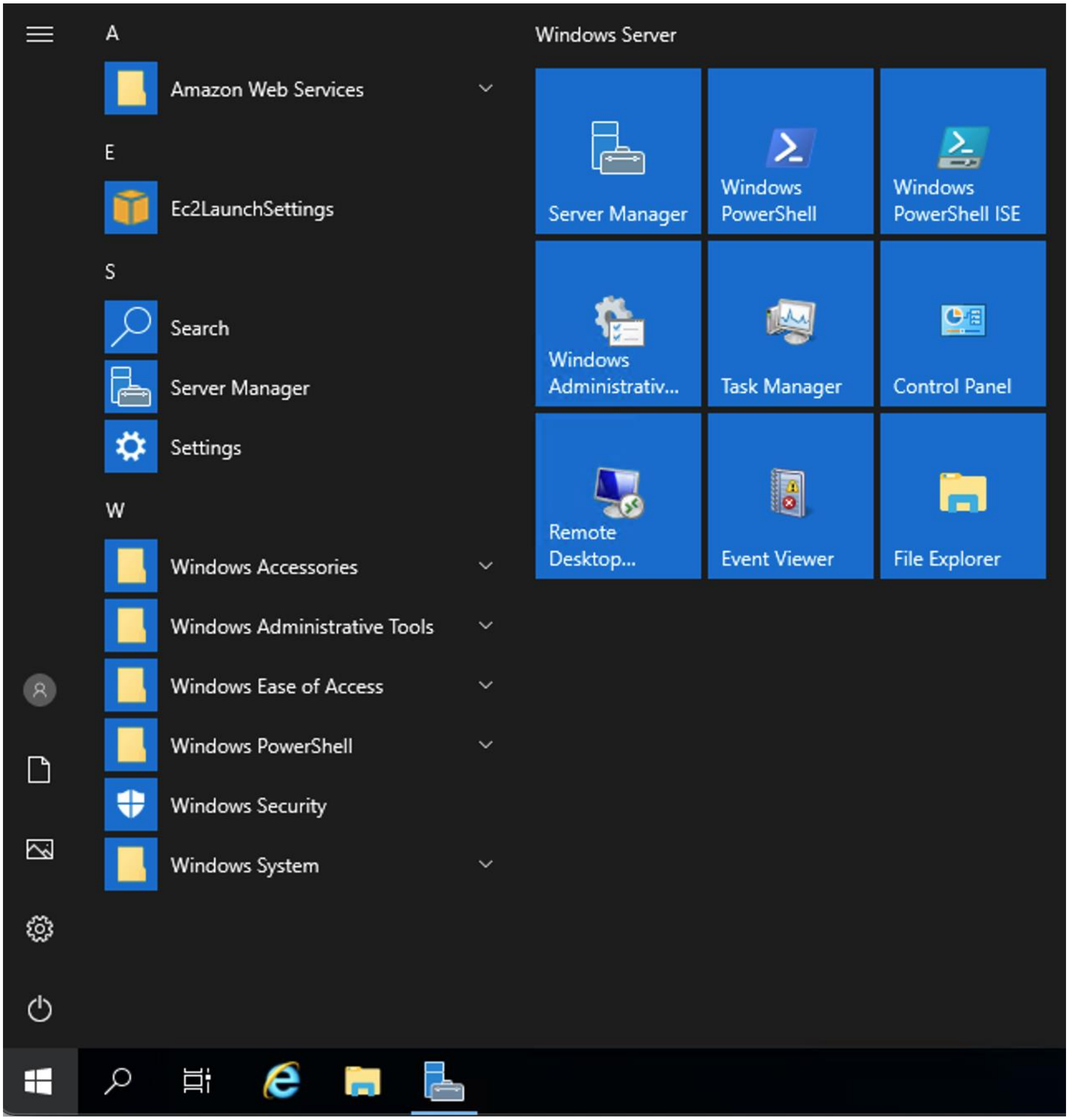
Select one or more features to install on the selected server.

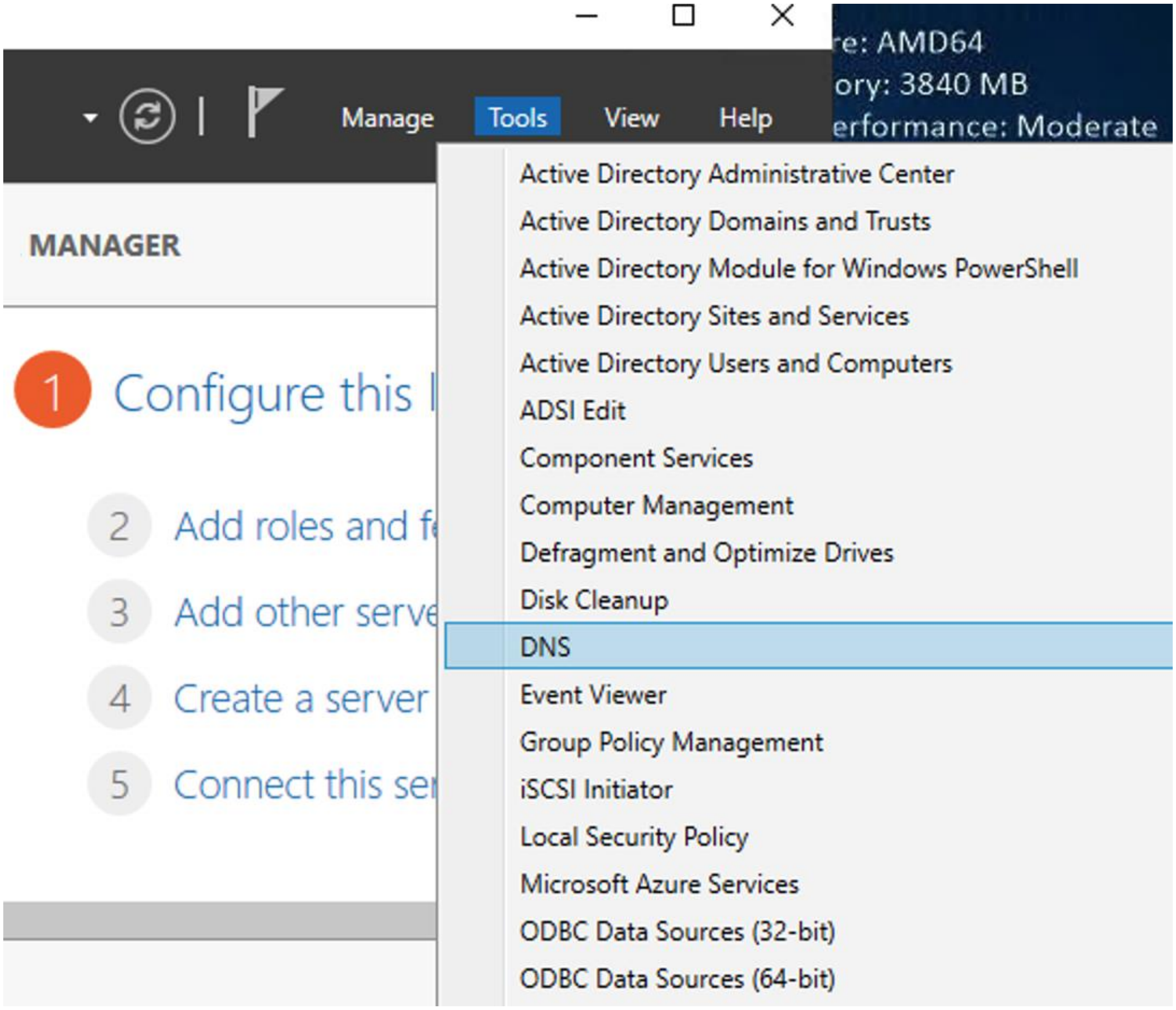
Features

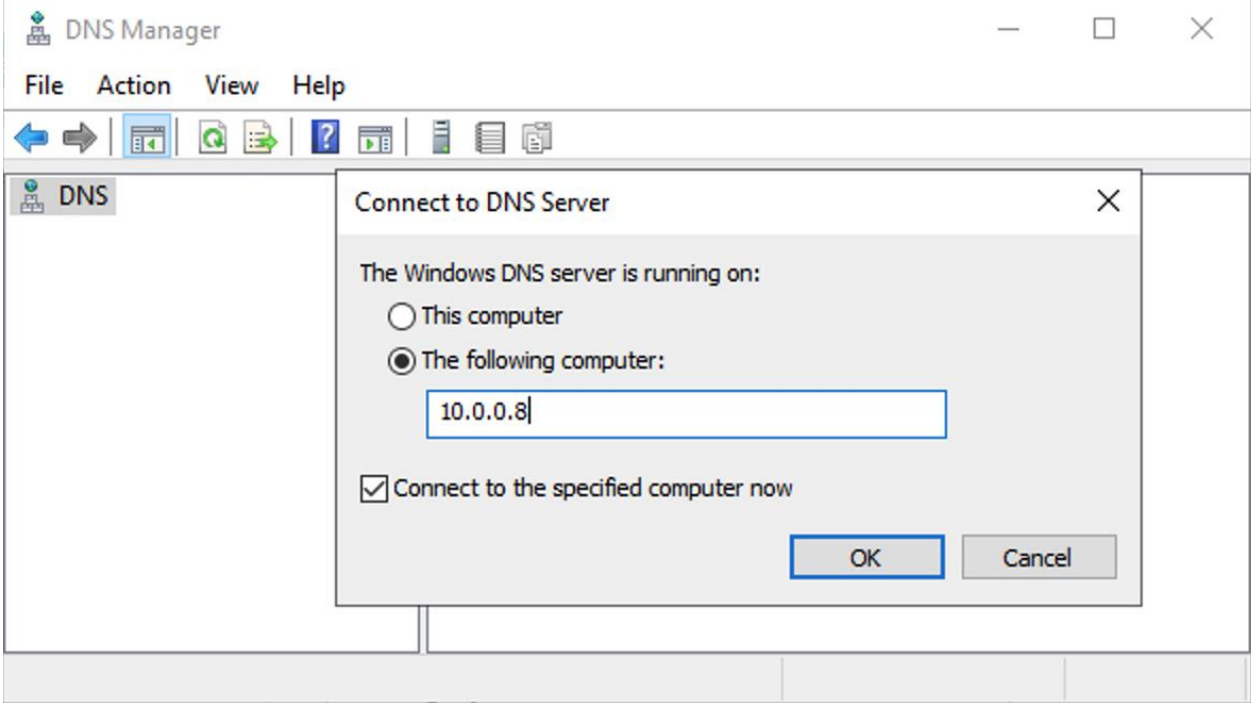
- ▷ □ MultiPoint Connector
- □ Network Load Balancing
- □ Network Virtualization
- □ Peer Name Resolution Protocol
- □ Quality Windows Audio Video Experience
- □ RAS Connection Manager Administration Kit (CMA
- □ Remote Assistance
- □ Remote Differential Compression
- ◢ ■ Remote Server Administration Tools (5 of 44 instal
  - ▷ □ Feature Administration Tools
  - ◢ ■ Role Administration Tools (5 of 27 installed)
    - ▷ ☑ AD DS and AD LDS Tools (Installed)
    - ▷ □ Hyper-V Management Tools
    - ▷ □ Remote Desktop Services Tools
    - ▷ □ Windows Server Update Services Tools
    - ▷ □ Active Directory Certificate Services Tools
    - □ Active Directory Rights Management Servic
    - □ DHCP Server Tools
    - ☑ DNS Server Tools (Installed)

Description

Role Administration Tools includes snap-ins and command-line tools for remotely managing roles.


A
Amazon Web Services
E
Ec2LaunchSettings
S
Search
Server Manager
Settings
W
Windows Accessories
Windows Administrative Tools
Windows Ease of Access
Windows PowerShell
Windows Security
Windows System
Windows Server
Server Manager
Windows PowerShell
Windows PowerShell ISE
Windows Administrativ...
Task Manager
Control Panel
Remote Desktop...
Event Viewer
File Explorer


re: AMD64
ory: 3840 MB
erformance: Moderate
Manage
Tools
View
Help
MANAGER
1 Configure this l
2 Add roles and f
3 Add other serve
4 Create a server
5 Connect this se
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
DNS
Event Viewer
Group Policy Management
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)



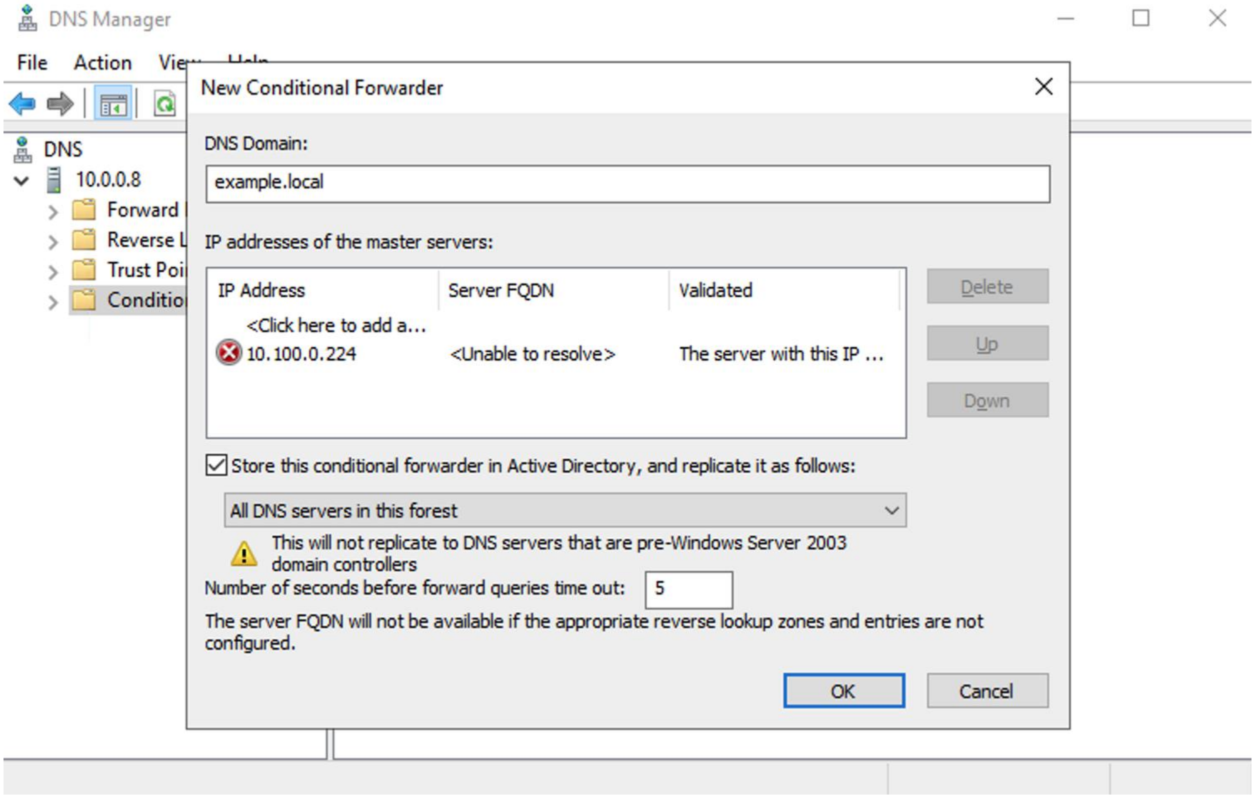
The Windows DNS server is running on:

○ This computer

● The following computer:

10.0.0.8

☑ Connect to the specified computer now



DNS Domain:

example.local

IP addresses of the master servers:

IP Address	Server FQDN	Validated
<Click here to add a...		
☒ 10.100.0.224	<Unable to resolve>	The server with this IP ...

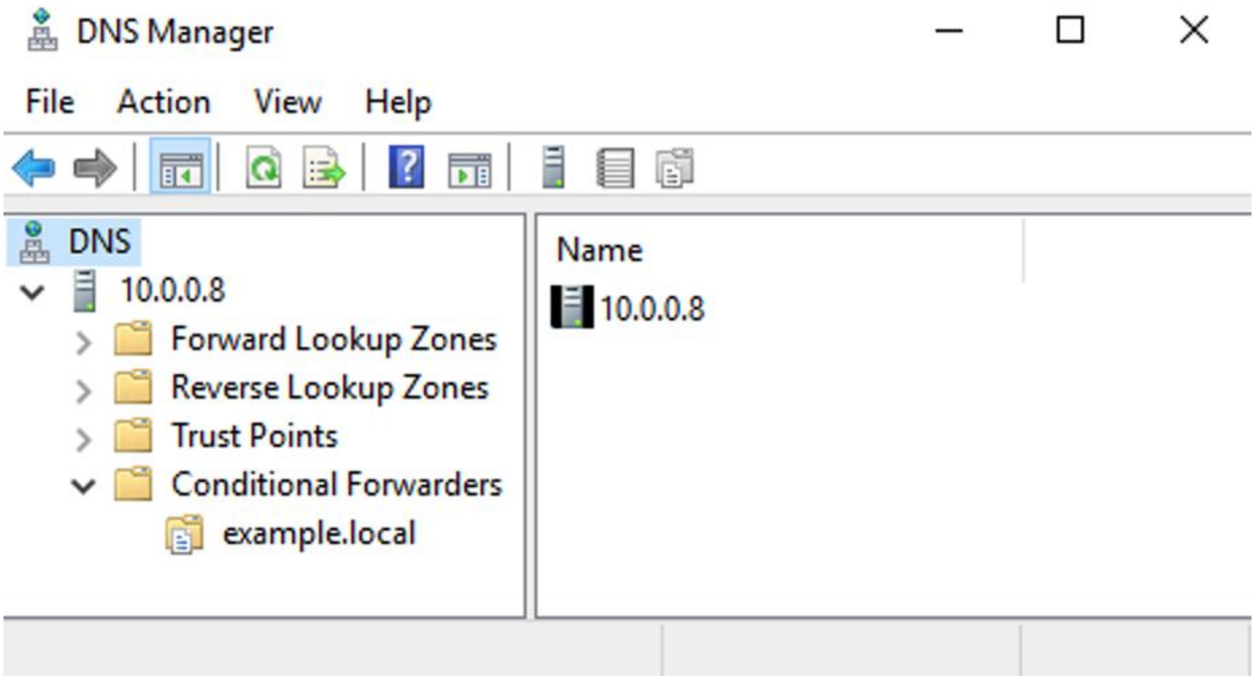
☑ Store this conditional forwarder in Active Directory, and replicate it as follows:

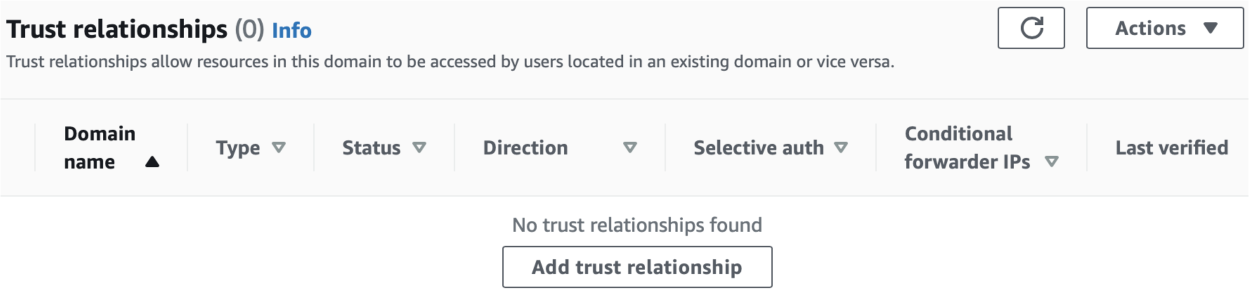
All DNS servers in this forest

⚠ This will not replicate to DNS servers that are pre-Windows Server 2003 domain controllers

Number of seconds before forward queries time out: 5

The server FQDN will not be available if the appropriate reverse lookup zones and entries are not configured.

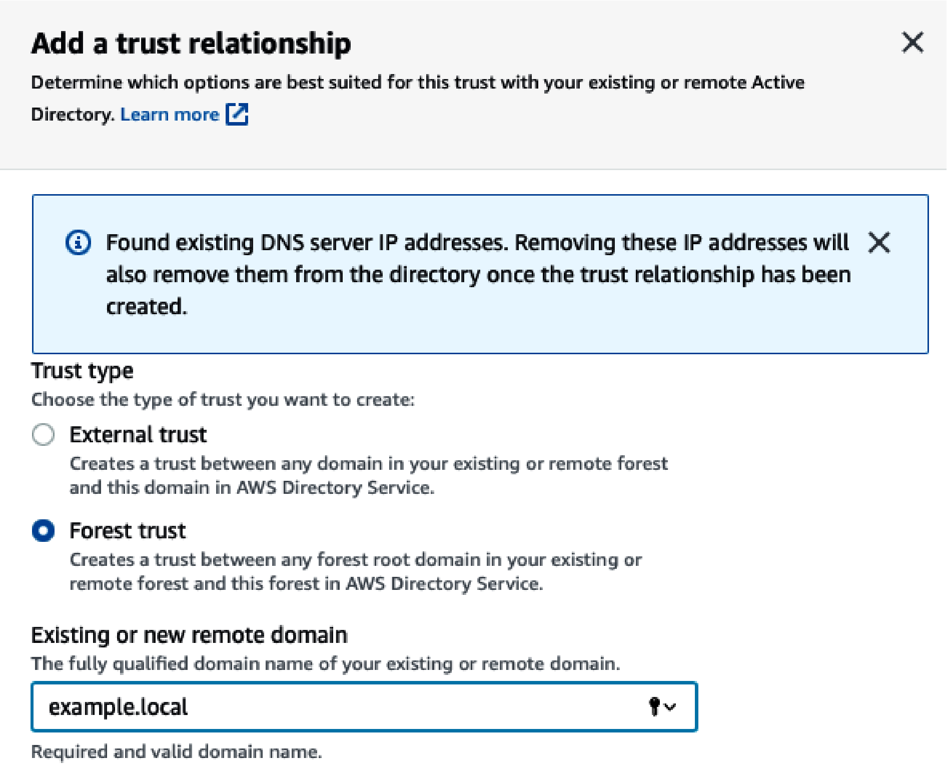



Trust relationships (0) Info

Trust relationships allow resources in this domain to be accessed by users located in an existing domain or vice versa.

Domain name ▲	Type ▽	Status ▽	Direction ▽	Selective auth ▽	Conditional forwarder IPs ▽	Last verified

No trust relationships found



Add a trust relationship

Determine which options are best suited for this trust with your existing or remote Active Directory. Learn more

Found existing DNS server IP addresses. Removing these IP addresses will also remove them from the directory once the trust relationship has been created.

Trust type

Choose the type of trust you want to create:

○ External trust

Creates a trust between any domain in your existing or remote forest and this domain in AWS Directory Service.

● Forest trust

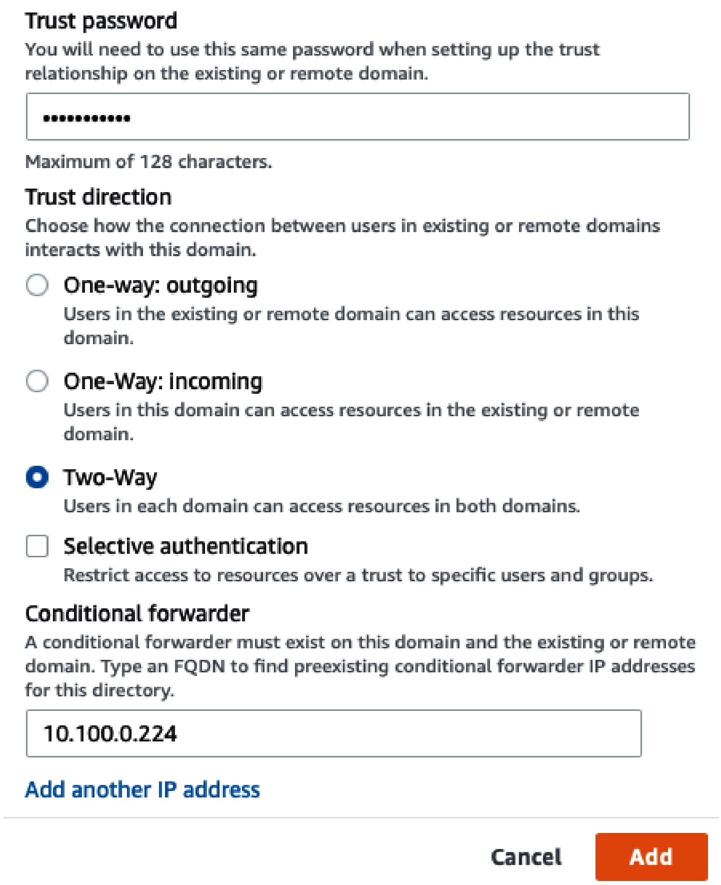
Creates a trust between any forest root domain in your existing or remote forest and this forest in AWS Directory Service.

Existing or new remote domain

The fully qualified domain name of your existing or remote domain.

example.local

Required and valid domain name.



Trust password

You will need to use this same password when setting up the trust relationship on the existing or remote domain.

••••••••••••

Maximum of 128 characters.

Trust direction

Choose how the connection between users in existing or remote domains interacts with this domain.

○ One-way: outgoing
Users in the existing or remote domain can access resources in this domain.

○ One-Way: incoming
Users in this domain can access resources in the existing or remote domain.

● Two-Way
Users in each domain can access resources in both domains.

□ Selective authentication
Restrict access to resources over a trust to specific users and groups.

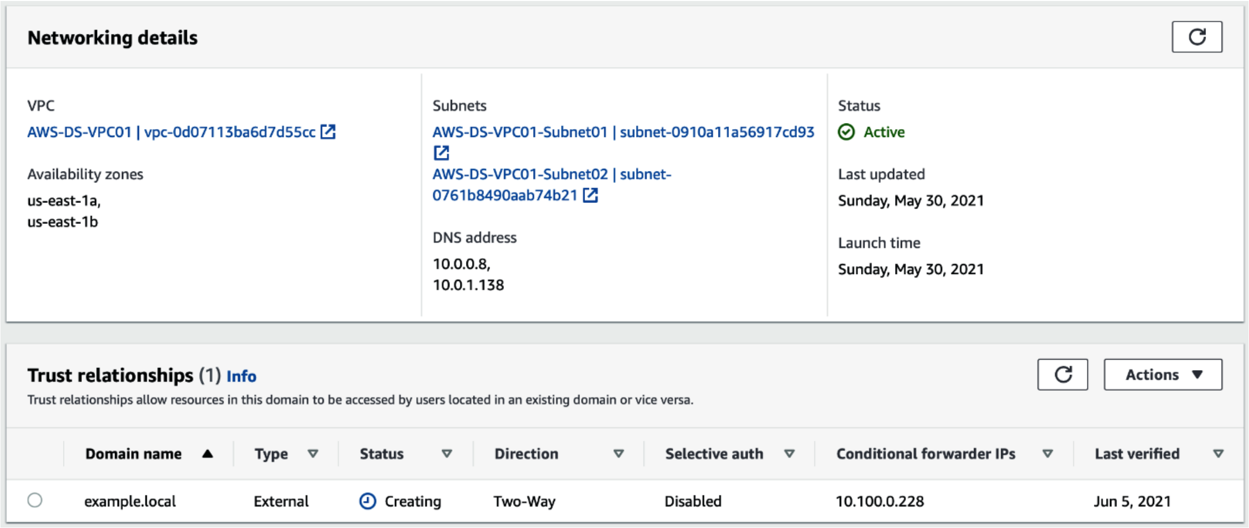
Conditional forwarder

A conditional forwarder must exist on this domain and the existing or remote domain. Type an FQDN to find preexisting conditional forwarder IP addresses for this directory.

10.100.0.224

Add another IP address

Cancel Add



Networking details

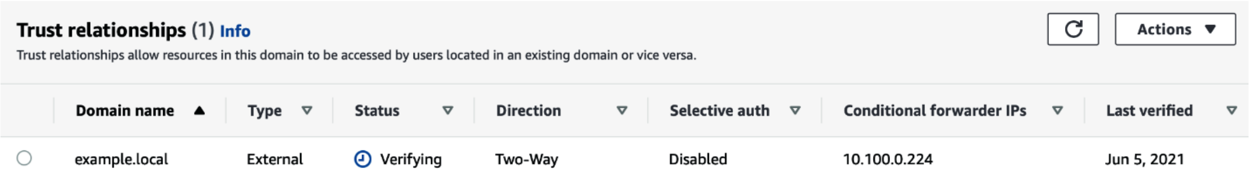
VPC	Subnets	Status
AWS-DS-VPC01 | vpc-0d07113ba6d7d55cc	AWS-DS-VPC01-Subnet01 | subnet-0910a11a56917cd93 AWS-DS-VPC01-Subnet02 | subnet-0761b8490aab74b21	✓ Active
Availability zones	DNS address	Last updated
us-east-1a, us-east-1b	10.0.0.8, 10.0.1.138	Sunday, May 30, 2021
		Launch time
		Sunday, May 30, 2021

Trust relationships (1) Info

Trust relationships allow resources in this domain to be accessed by users located in an existing domain or vice versa.

Actions ▼

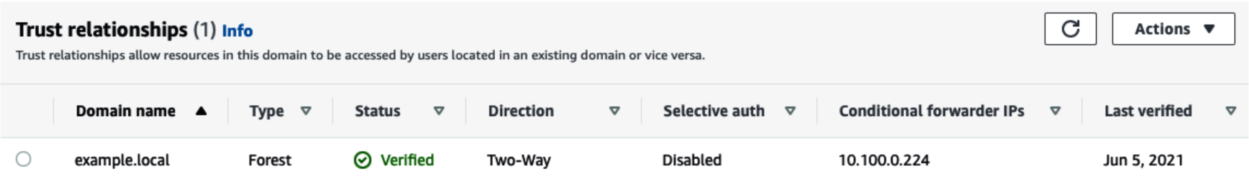
	Domain name ▲	Type ▽	Status ▽	Direction ▽	Selective auth ▽	Conditional forwarder IPs ▽	Last verified ▽
○	example.local	External	Creating	Two-Way	Disabled	10.100.0.228	Jun 5, 2021



Trust relationships (1) Info

Trust relationships allow resources in this domain to be accessed by users located in an existing domain or vice versa.

	Domain name ▲	Type	Status	Direction	Selective auth	Conditional forwarder IPs	Last verified
○	example.local	External	Verifying	Two-Way	Disabled	10.100.0.224	Jun 5, 2021

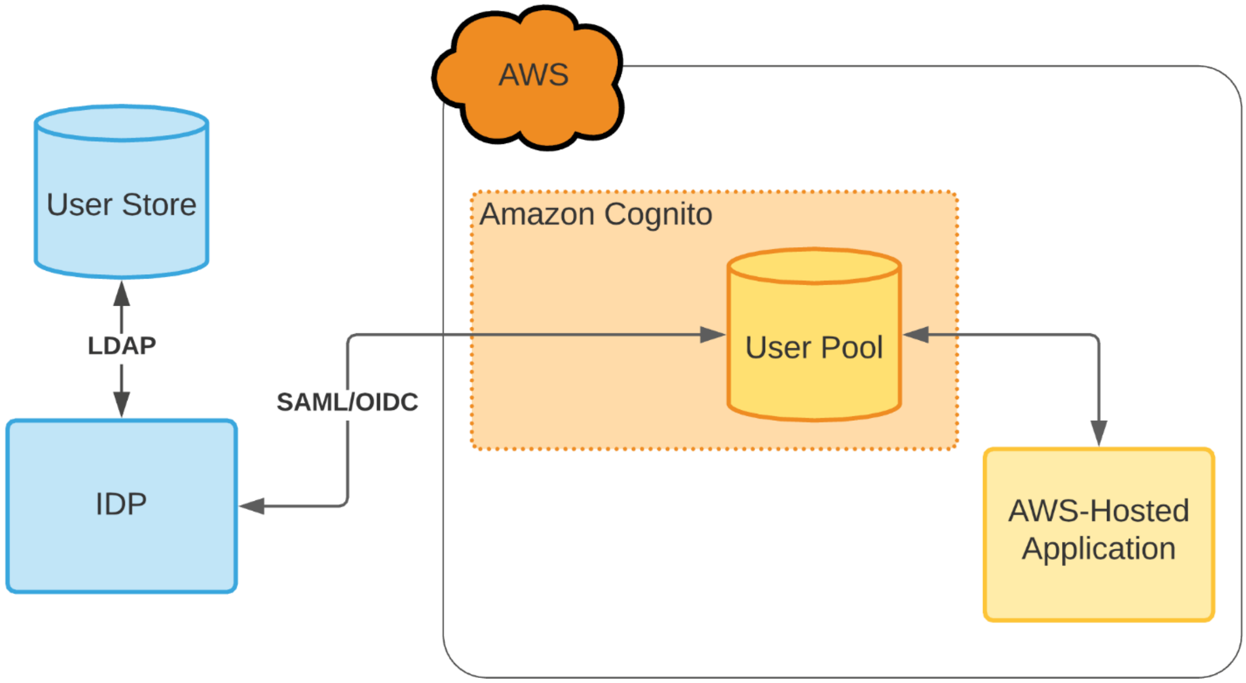


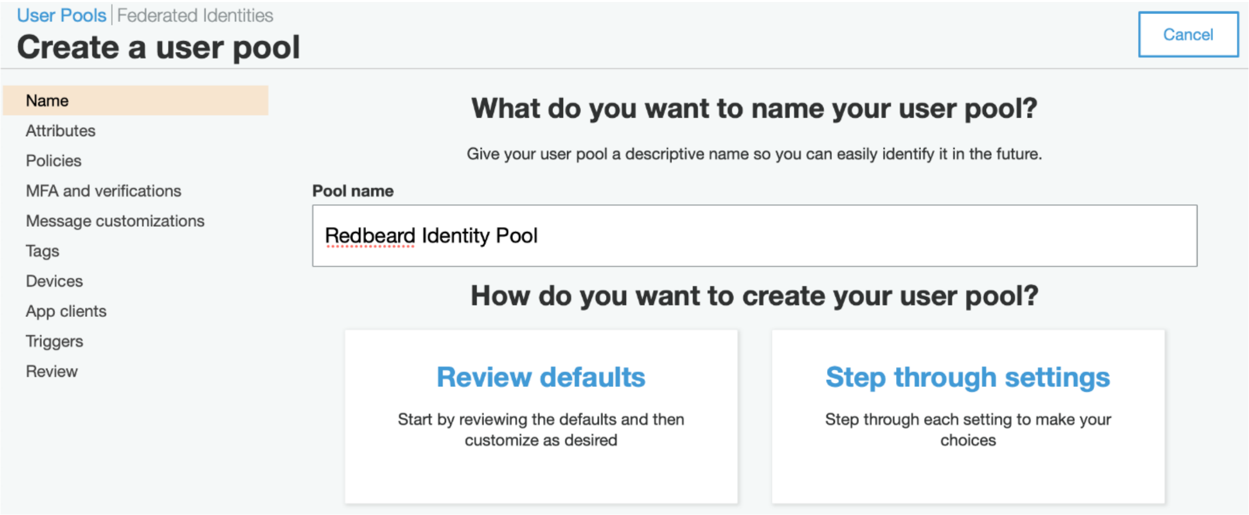
Trust relationships (1) Info

Trust relationships allow resources in this domain to be accessed by users located in an existing domain or vice versa.

	Domain name ▲	Type	Status	Direction	Selective auth	Conditional forwarder IPs	Last verified
○	example.local	Forest	✓ Verified	Two-Way	Disabled	10.100.0.224	Jun 5, 2021

Chapter 12: AWS-Hosted Application Single Sign-On Using an Existing Identity Provider





Create a user pool

What do you want to name your user pool?

Give your user pool a descriptive name so you can easily identify it in the future.

Pool name

Redbeard Identity Pool

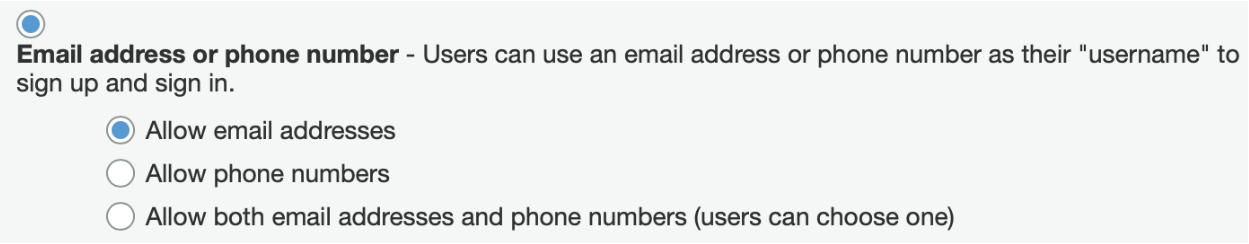
How do you want to create your user pool?

Review defaults

Start by reviewing the defaults and then customize as desired

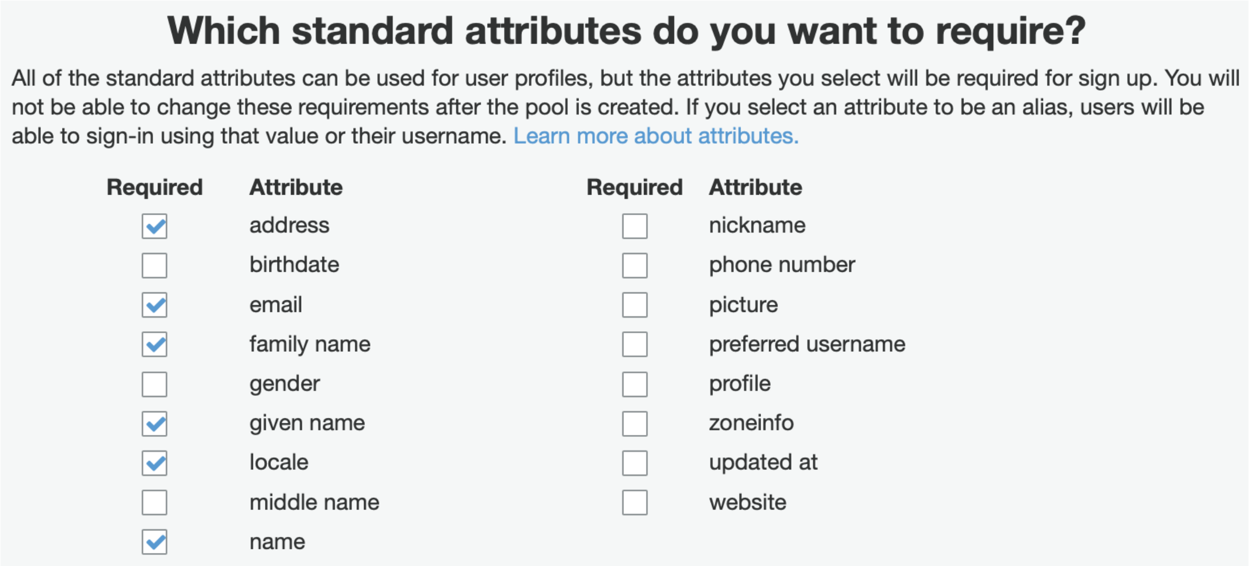
Step through settings

Step through each setting to make your choices



●
Email address or phone number - Users can use an email address or phone number as their "username" to sign up and sign in.

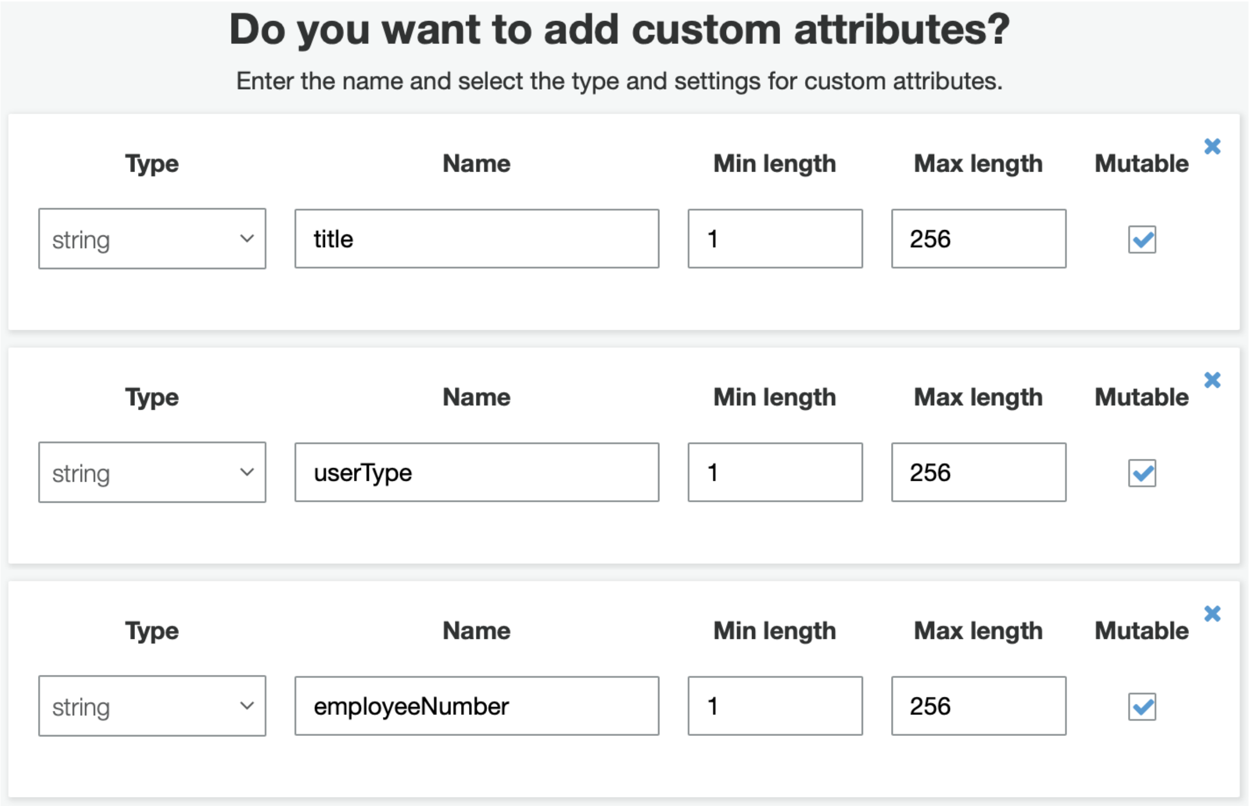
- ● Allow email addresses
- ○ Allow phone numbers
- ○ Allow both email addresses and phone numbers (users can choose one)



Which standard attributes do you want to require?

All of the standard attributes can be used for user profiles, but the attributes you select will be required for sign up. You will not be able to change these requirements after the pool is created. If you select an attribute to be an alias, users will be able to sign-in using that value or their username. Learn more about attributes.

Required	Attribute	Required	Attribute
☑	address	□	nickname
□	birthdate	□	phone number
☑	email	□	picture
☑	family name	□	preferred username
□	gender	□	profile
☑	given name	□	zoneinfo
☑	locale	□	updated at
□	middle name	□	website
☑	name		



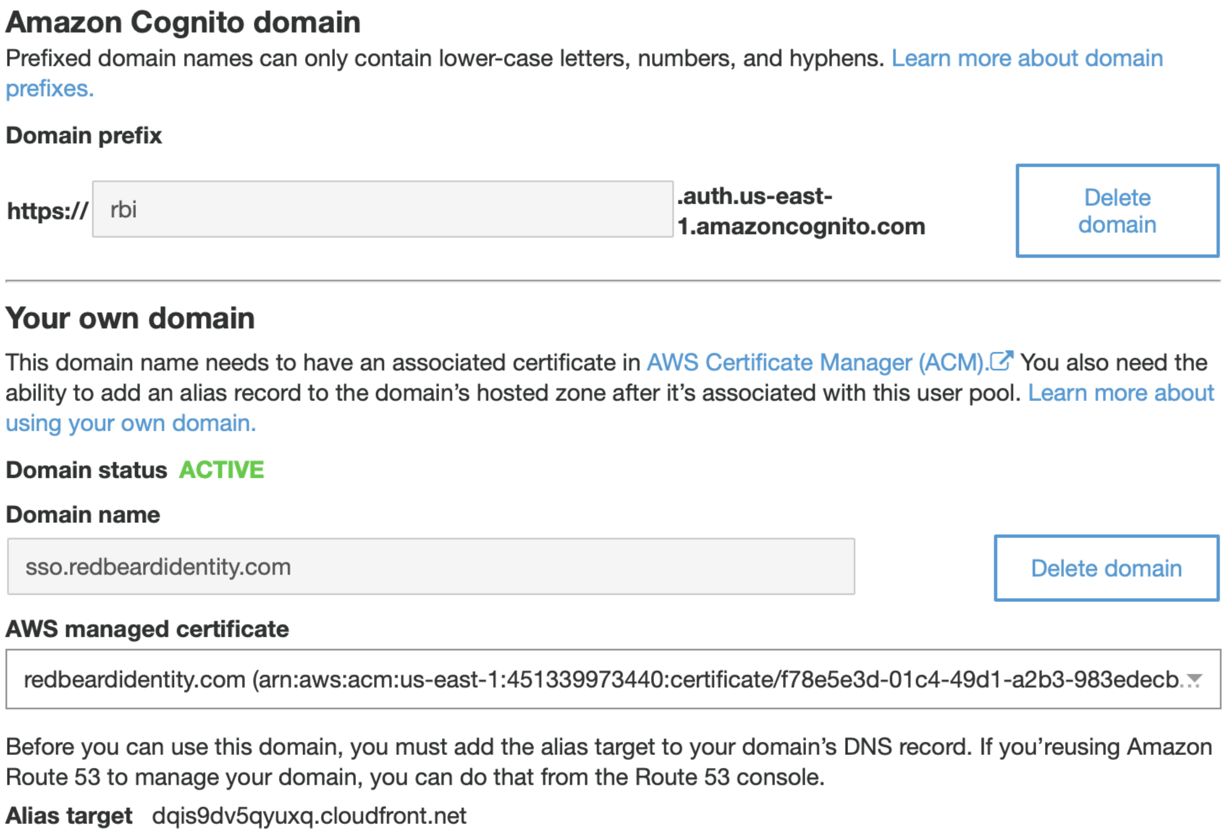
Do you want to add custom attributes?

Enter the name and select the type and settings for custom attributes.

Type	Name	Min length	Max length	Mutable
string	title	1	256	☑

Type	Name	Min length	Max length	Mutable
string	userType	1	256	☑

Type	Name	Min length	Max length	Mutable
string	employeeNumber	1	256	☑



Amazon Cognito domain

Prefixed domain names can only contain lower-case letters, numbers, and hyphens. Learn more about domain prefixes.

Domain prefix

https:// rbi **.auth.us-east-1.amazoncognito.com**

Your own domain

This domain name needs to have an associated certificate in AWS Certificate Manager (ACM). You also need the ability to add an alias record to the domain's hosted zone after it's associated with this user pool. Learn more about using your own domain.

Domain status ACTIVE

Domain name

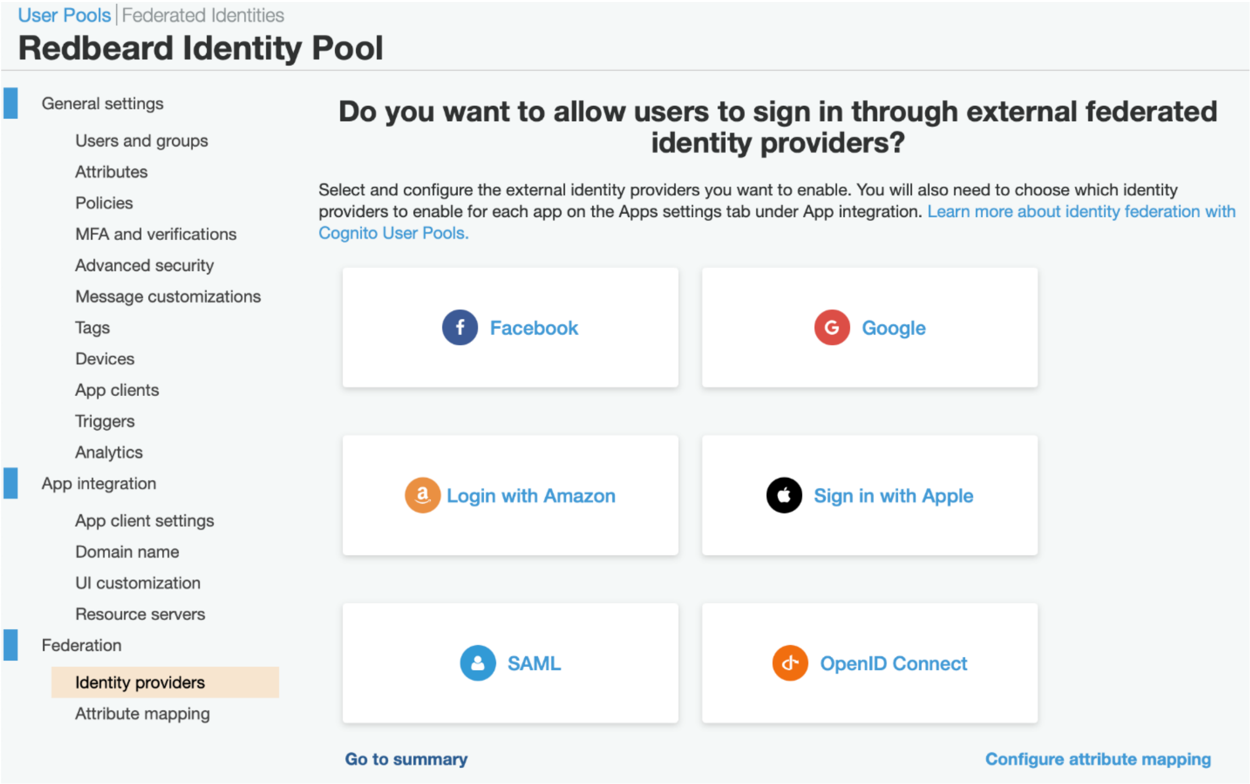
sso.redbeardidentity.com

AWS managed certificate

redbeardidentity.com (arn:aws:acm:us-east-1:451339973440:certificate/f78e5e3d-01c4-49d1-a2b3-983edecb...

Before you can use this domain, you must add the alias target to your domain's DNS record. If you'reusing Amazon Route 53 to manage your domain, you can do that from the Route 53 console.

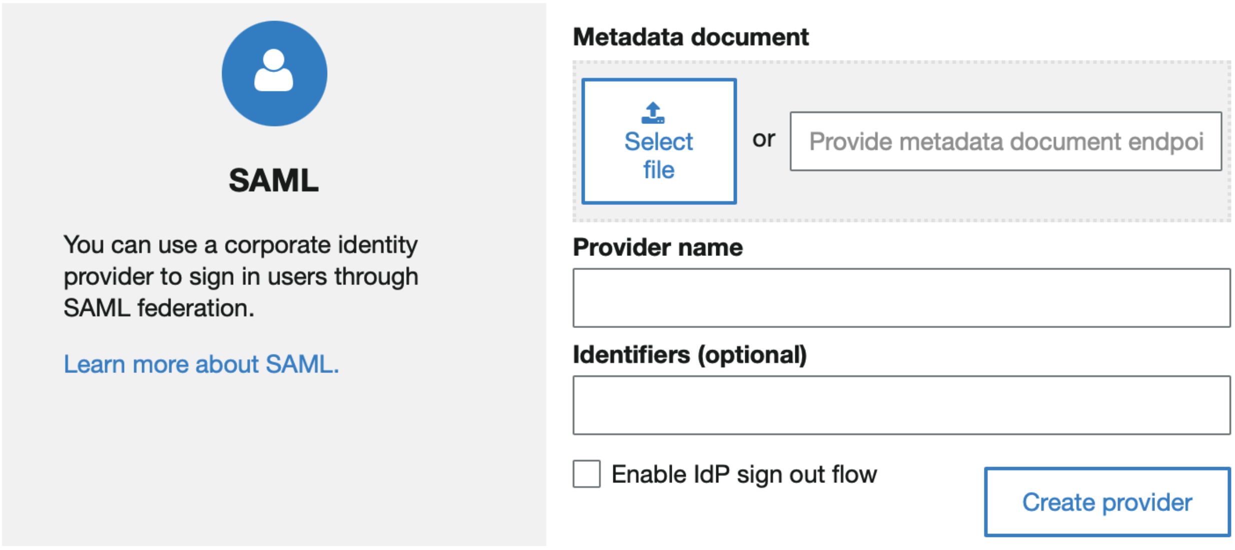
Alias target dqis9dv5qyuxq.cloudfront.net



Redbeard Identity Pool

Do you want to allow users to sign in through external federated identity providers?

Select and configure the external identity providers you want to enable. You will also need to choose which identity providers to enable for each app on the Apps settings tab under App integration. Learn more about identity federation with Cognito User Pools.



SAML

You can use a corporate identity provider to sign in users through SAML federation.

Learn more about SAML.

Metadata document

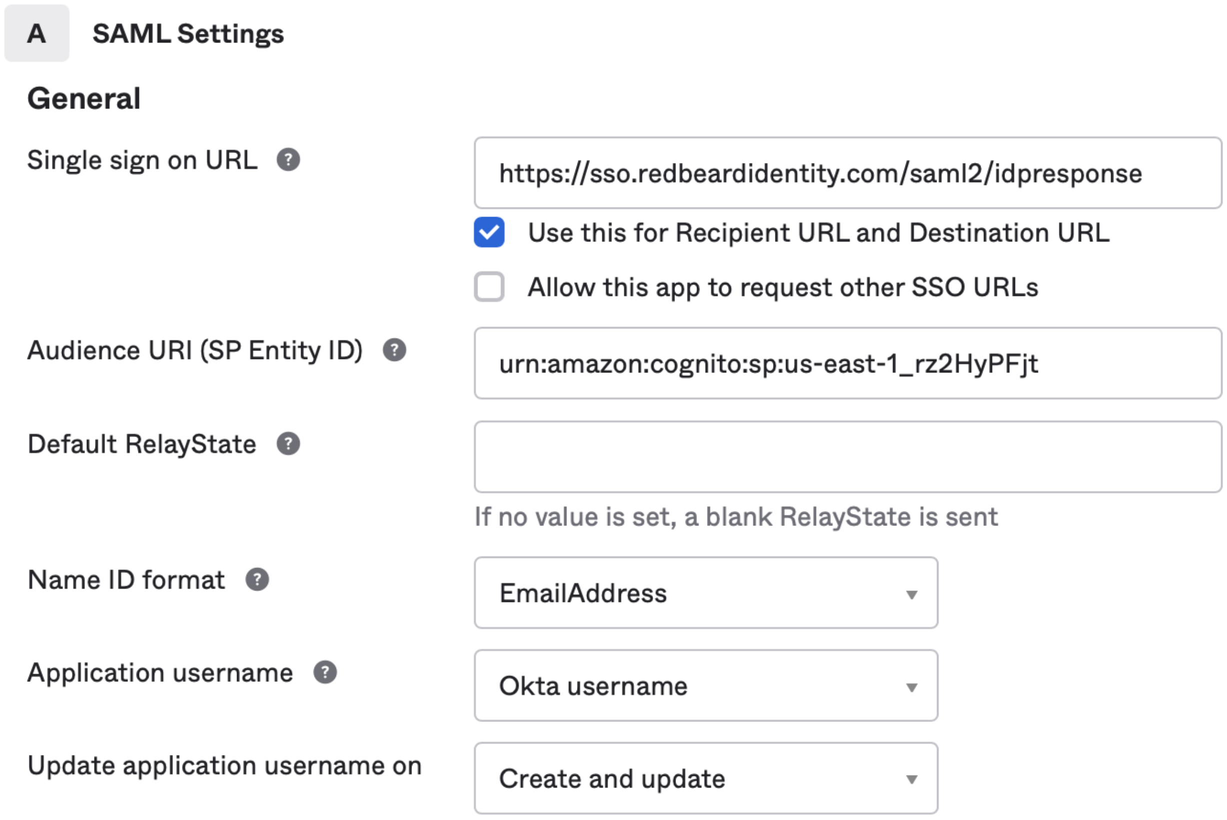
Select file or Provide metadata document endpoi

Provider name

Identifiers (optional)

□ Enable IdP sign out flow

Create provider



A SAML Settings

General

Single sign on URL: https://sso.redbeardidentity.com/saml2/idpresponse

☑ Use this for Recipient URL and Destination URL

□ Allow this app to request other SSO URLs

Audience URI (SP Entity ID): urn:amazon:cognito:sp:us-east-1_rz2HyPFjt

Default RelayState:

If no value is set, a blank RelayState is sent

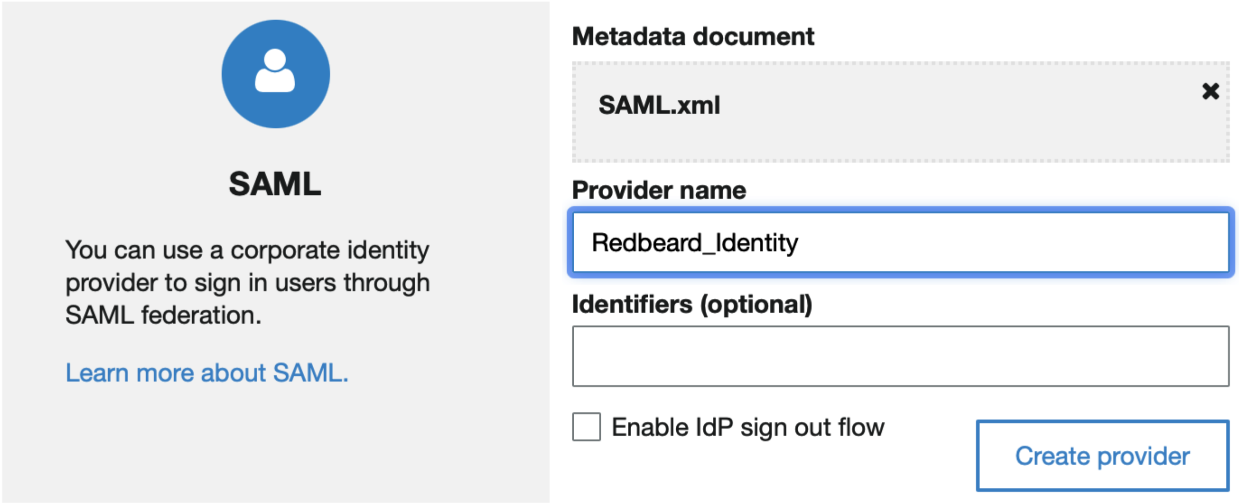
Name ID format: EmailAddress

Application username: Okta username

Update application username on: Create and update

ATTRIBUTE STATEMENTS

Name	Name Format	Value
email	Unspecified	user.email
name	Unspecified	user.displayName
given_name	Unspecified	user.firstName
family_name	Unspecified	user.lastName
address	Unspecified	user.postalAddress
custom:title	Unspecified	user.title
custom:userType	Unspecified	user.userType
custom:employeeNumber	Unspecified	user.employeeNumber
custom:costCenter	Unspecified	user.costCenter
custom:organization	Unspecified	user.organization
custom:division	Unspecified	user.division
custom:department	Unspecified	user.department
custom.managerid	Unspecified	user.managerId
locale	Unspecified	user.city



SAML

You can use a corporate identity provider to sign in users through SAML federation.

Learn more about SAML.

Metadata document

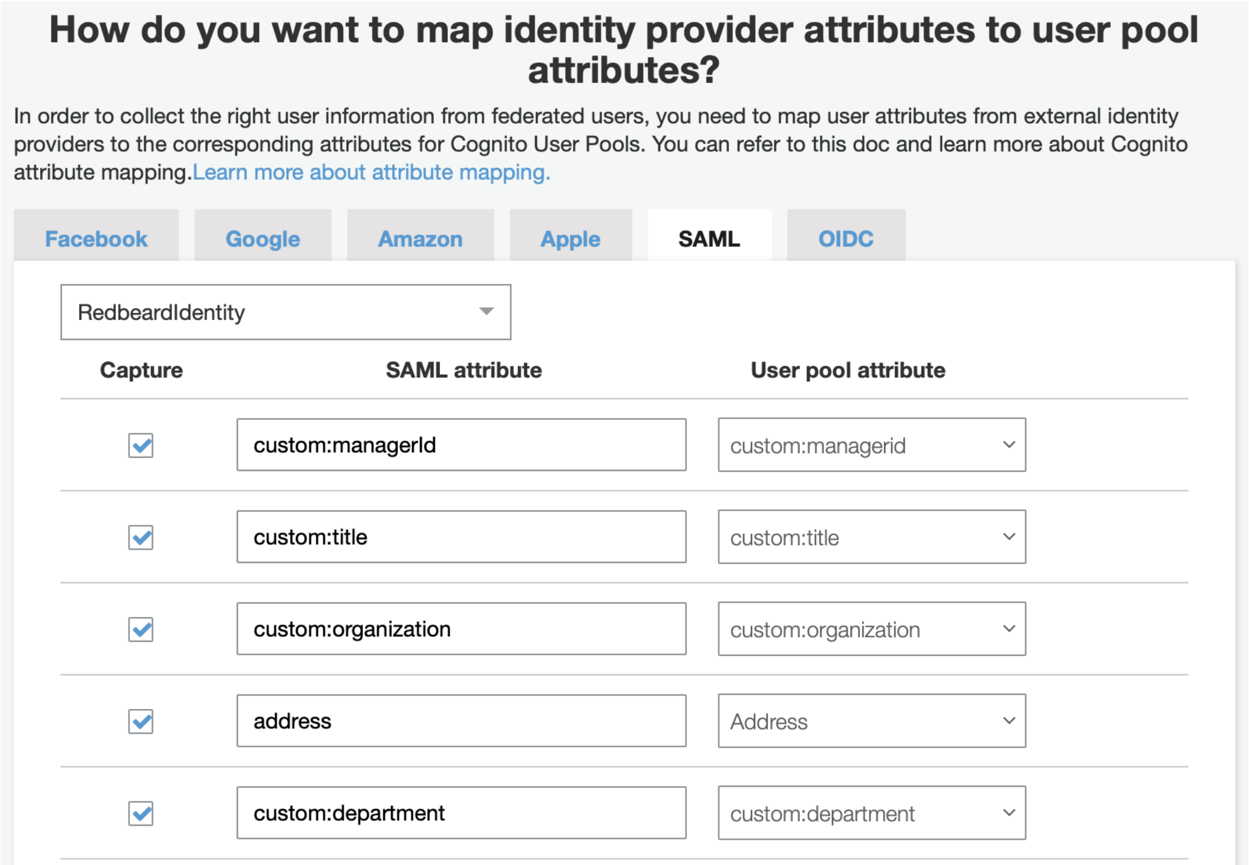
SAML.xml

Provider name

Redbeard_Identity

Identifiers (optional)

☐ Enable IdP sign out flow

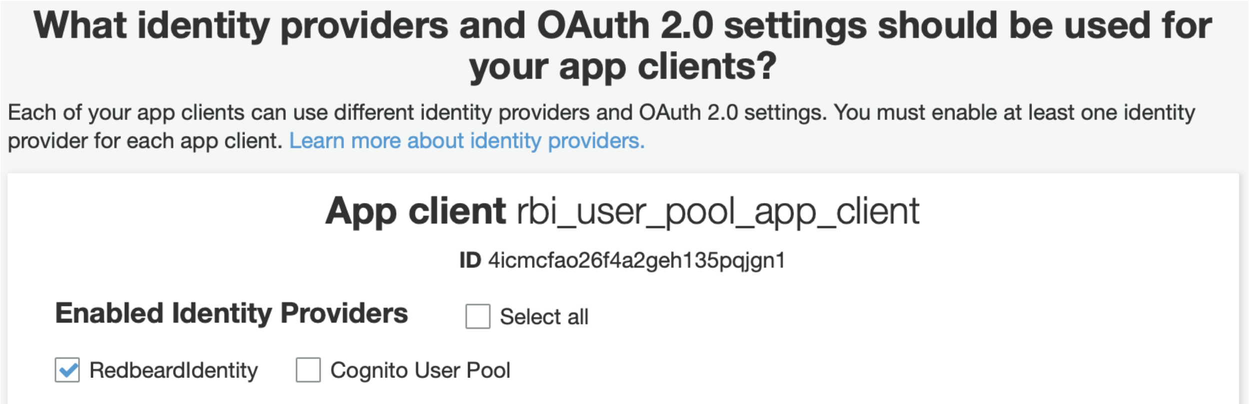


How do you want to map identity provider attributes to user pool attributes?

In order to collect the right user information from federated users, you need to map user attributes from external identity providers to the corresponding attributes for Cognito User Pools. You can refer to this doc and learn more about Cognito attribute mapping.Learn more about attribute mapping.

RedbeardIdentity

Capture	SAML attribute	User pool attribute
☑	custom:managerId	custom:managerid
☑	custom:title	custom:title
☑	custom:organization	custom:organization
☑	address	Address
☑	custom:department	custom:department



What identity providers and OAuth 2.0 settings should be used for your app clients?

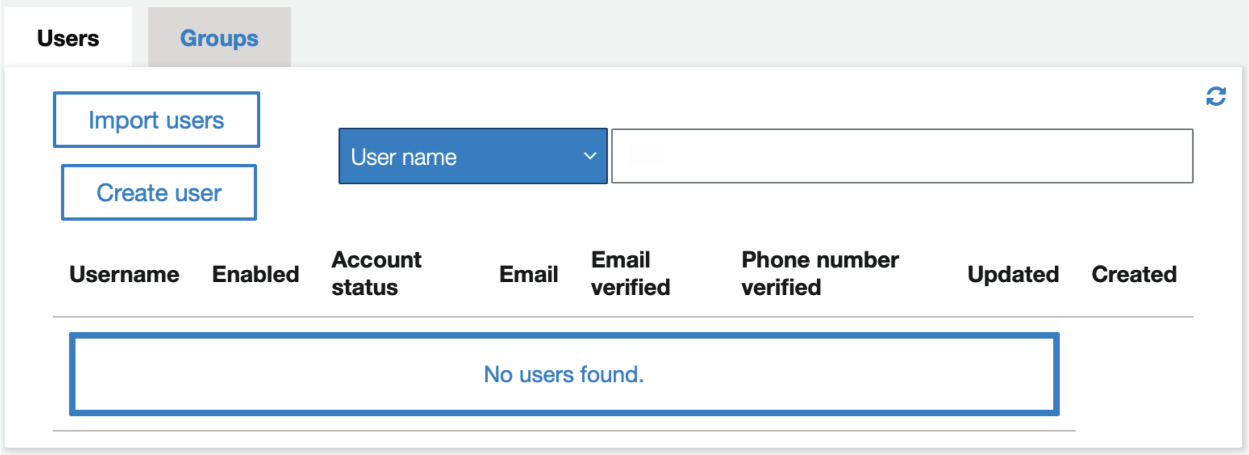
Each of your app clients can use different identity providers and OAuth 2.0 settings. You must enable at least one identity provider for each app client. Learn more about identity providers.

App client rbi_user_pool_app_client

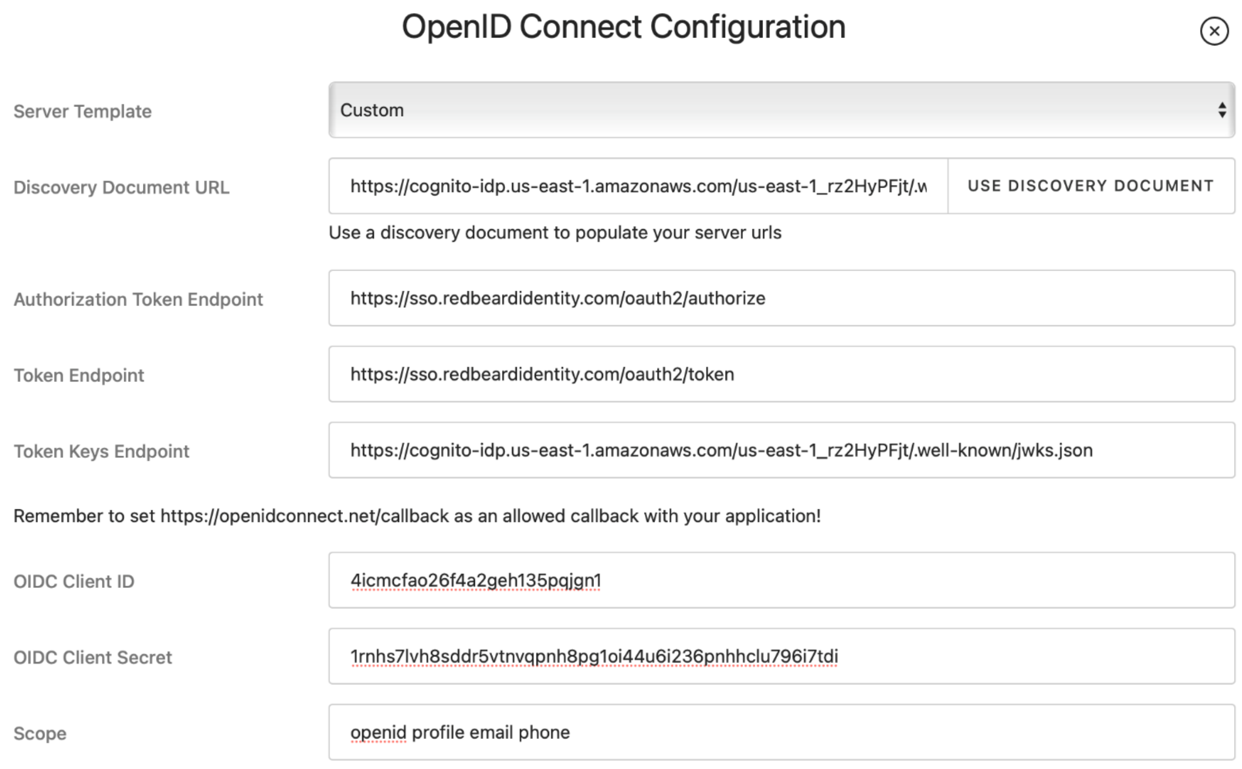
ID 4icmcfao26f4a2geh135pqjgn1

Enabled Identity Providers □ Select all

☑ RedbeardIdentity □ Cognito User Pool



Username	Enabled	Account status	Email	Email verified	Phone number verified	Updated	Created
No users found.							



OpenID Connect Configuration

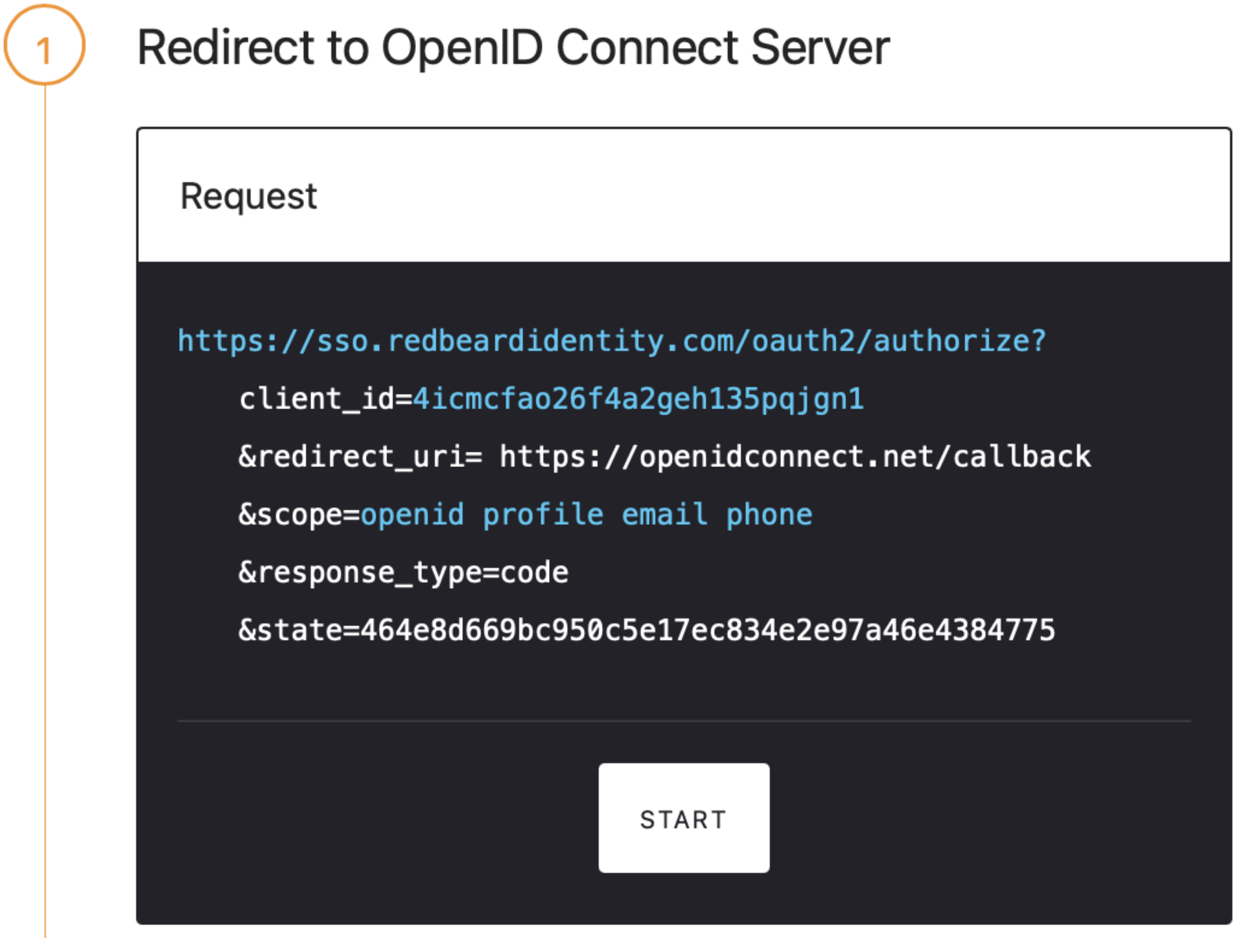
Server Template	Custom
Discovery Document URL	https://cognito-idp.us-east-1.amazonaws.com/us-east-1_rz2HyPFjt/.w

Use a discovery document to populate your server urls

Authorization Token Endpoint	https://sso.redbeardidentity.com/oauth2/authorize
Token Endpoint	https://sso.redbeardidentity.com/oauth2/token
Token Keys Endpoint	https://cognito-idp.us-east-1.amazonaws.com/us-east-1_rz2HyPFjt/.well-known/jwks.json

Remember to set https://openidconnect.net/callback as an allowed callback with your application!

OIDC Client ID	4icmcfao26f4a2geh135pqjgn1
OIDC Client Secret	1rnhs7lvh8sddr5vtnvqpnh8pg1oi44u6i236pnhhclu796i7tdi
Scope	openid profile email phone

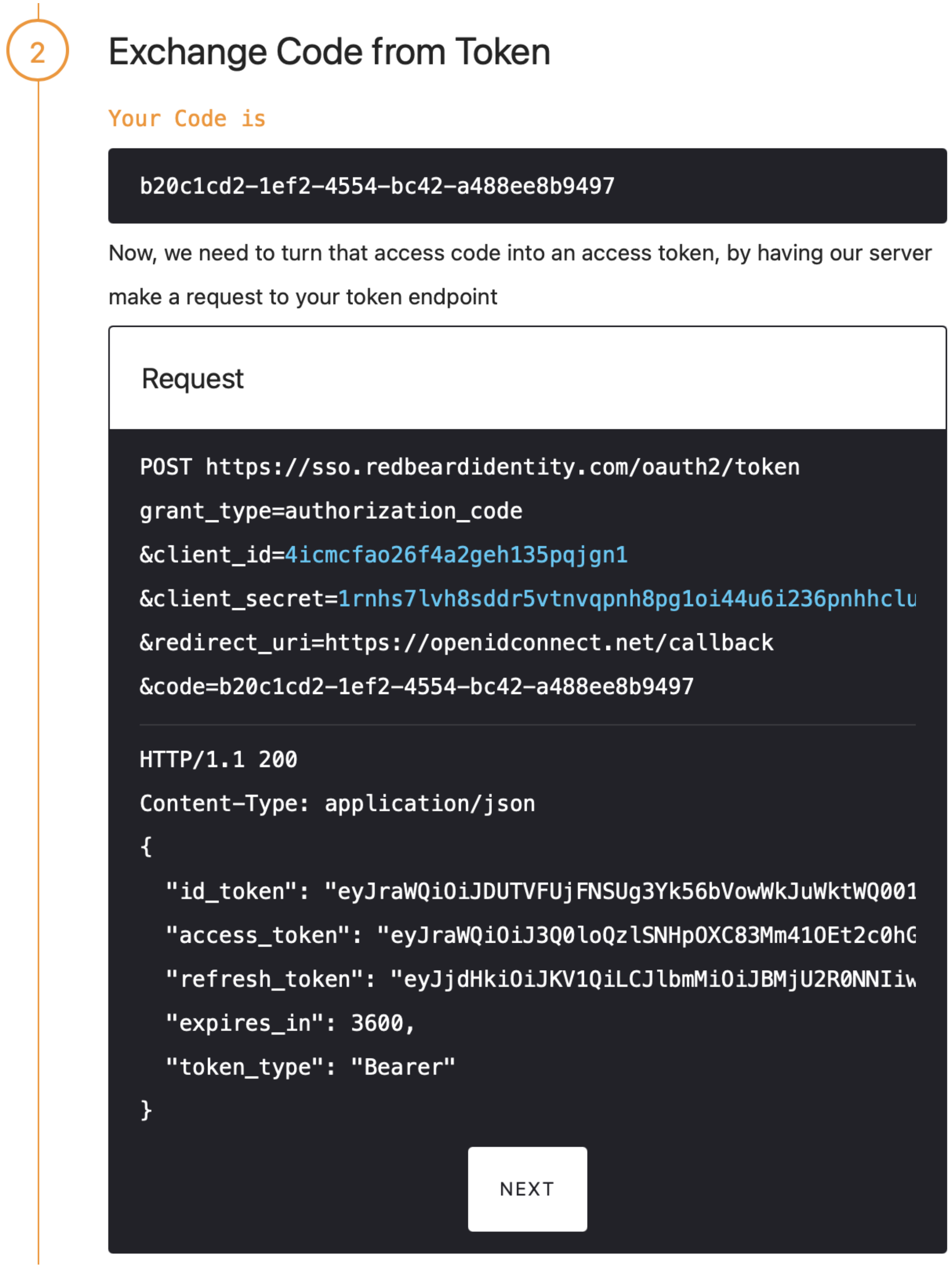


1

Redirect to OpenID Connect Server

Request

```
https://sso.redbeardidentity.com/oauth2/authorize?
    client_id=4icmcfao26f4a2geh135pqjgn1
    &redirect_uri= https://openidconnect.net/callback
    &scope=openid profile email phone
    &response_type=code
    &state=464e8d669bc950c5e17ec834e2e97a46e4384775
```



2

Exchange Code from Token

Your Code is

```
b20c1cd2-1ef2-4554-bc42-a488ee8b9497
```

Now, we need to turn that access code into an access token, by having our server make a request to your token endpoint

Request

```
POST https://sso.redbeardidentity.com/oauth2/token
grant_type=authorization_code
&client_id=4icmcfao26f4a2geh135pqjgn1
&client_secret=1rnhs7lvh8sddr5vtnvqpnh8pg1oi44u6i236pnhhclu
&redirect_uri=https://openidconnect.net/callback
&code=b20c1cd2-1ef2-4554-bc42-a488ee8b9497
```

```
HTTP/1.1 200
Content-Type: application/json
{
  "id_token": "eyJraWQiOiJDUTVFUjFNSUg3Yk56bVowWkJuWktWQ001
  "access_token": "eyJraWQiOiJ3Q0loQzlSNHpOXC83Mm41OEt2c0hG
  "refresh_token": "eyJjdHkiOiJKV1QiLCJlbmMiOiJBMjU2R0NNIiw
  "expires_in": 3600,
  "token_type": "Bearer"
}
```

3 Verify User Token

Now, we need to verify that the ID Token sent was from the correct place by validating the JWT's signature

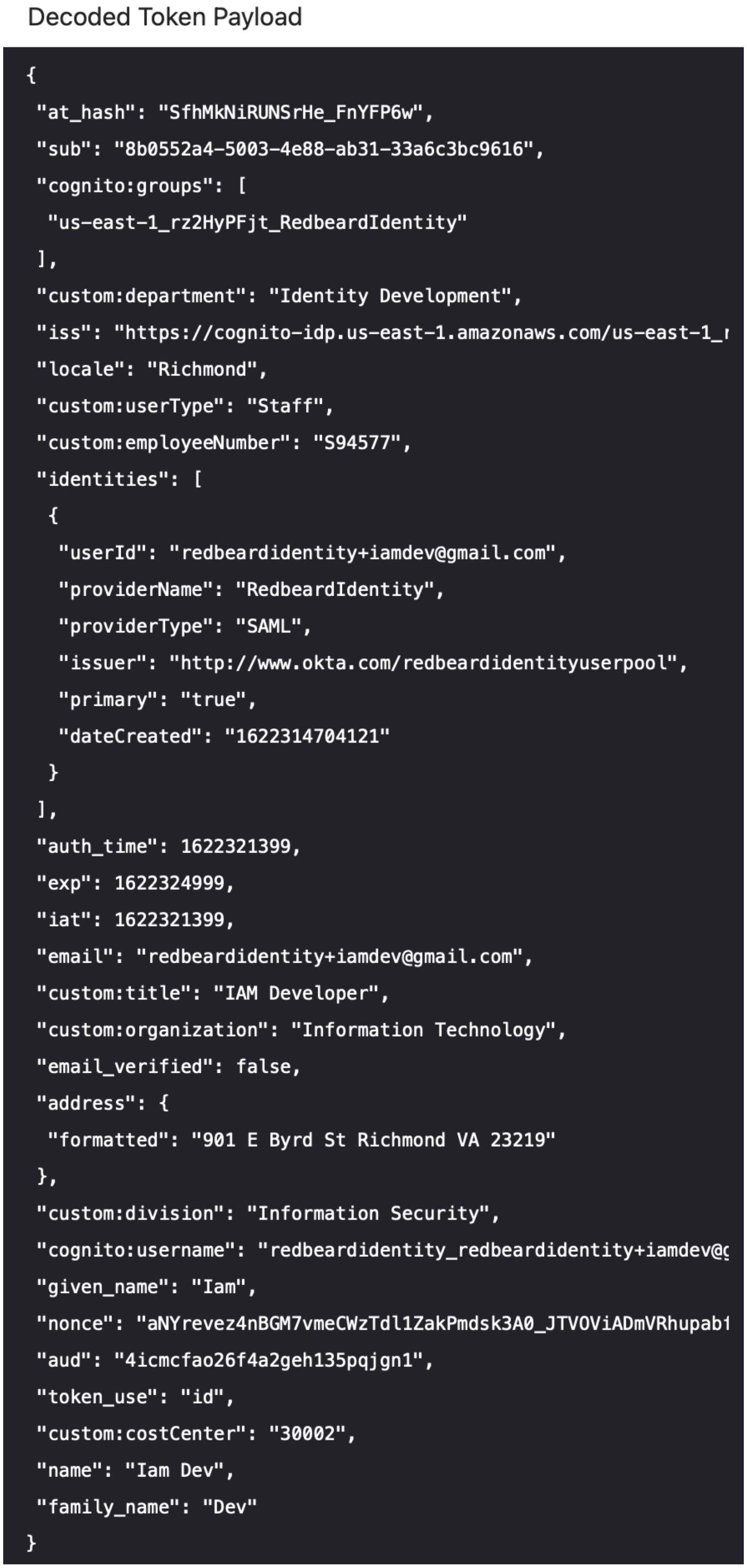
Your “id_token” is

VIEW ON JWT.IO

```
eyJraWQiOiJDUTVFUjFNSUg3Yk56bVowWkJuWktWQ001QW42ZUtmblA0ek5MS
0DXvPrLmm_ph73K9lM4-
xFSVv9PN6OV9n_g4HHNxiBxP_7gfYT7CF1_WJnRLEvL7VamL28zzA0WhGmP1M
aSli3LQqhA0UxAP1fULA3I362-
_oGqtQ7MJsXWlOvVYYS1MUfvfWqf3V4v-GMZ-
uYqu6FoUN6_wlKbgLqUbDTq8voZjeeboLiSwaglAMkm-MhV_Wfg-
t9dBCjaEpOYtQarEkZfE4uL7_2XiXRP2FQBFoDQzE8LZgtKsgHzvmzbjisWDw
```

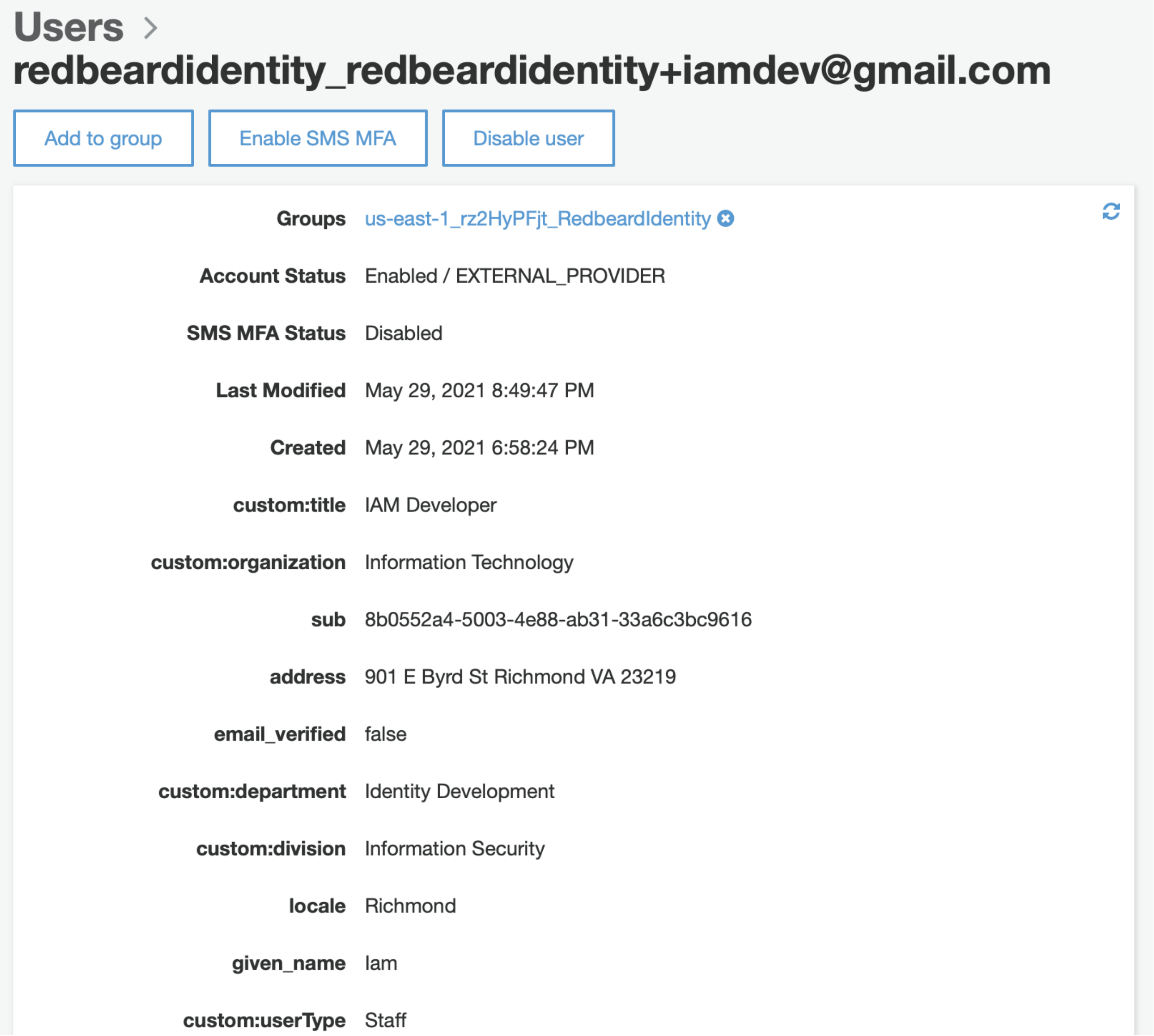
This token is cryptographically signed with the **RS256** algorithim. We'll use the public key of the OpenID Connect server to validate it. In order to do that, we'll fetch the public key from **https://cognito-idp.us-east-1.amazonaws.com/us-east-1_rz2HyPFjt/.well-known/jwks.json**, which is found in the discovery document or configuration menu options.

VERIFY



Decoded Token Payload

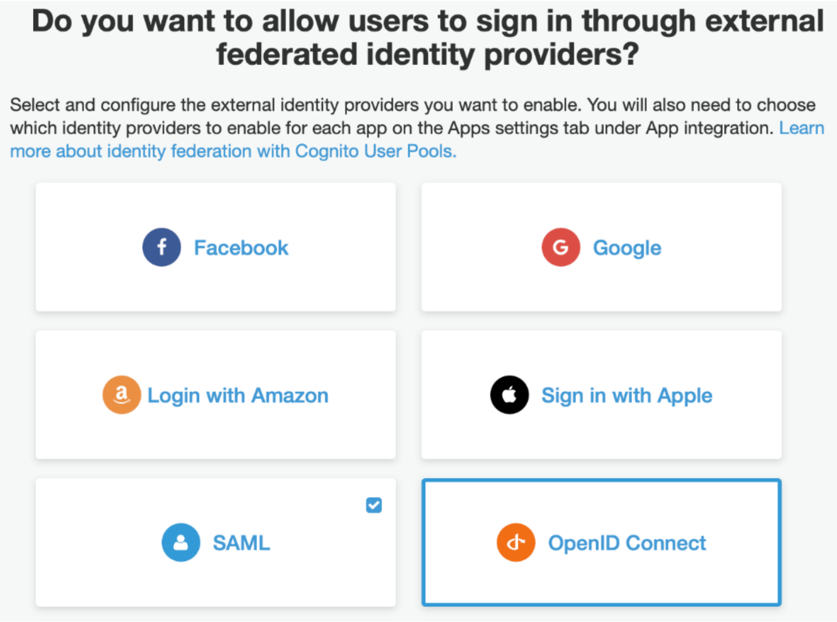
```
{
 "at_hash": "SfhMkNiRUNSrHe_FnYFP6w",
 "sub": "8b0552a4-5003-4e88-ab31-33a6c3bc9616",
 "cognito:groups": [
  "us-east-1_rz2HyPFjt_RedbeardIdentity"
 ],
 "custom:department": "Identity Development",
 "iss": "https://cognito-idp.us-east-1.amazonaws.com/us-east-1_r
 "locale": "Richmond",
 "custom:userType": "Staff",
 "custom:employeeNumber": "S94577",
 "identities": [
  {
   "userId": "redbeardidentity+iamdev@gmail.com",
   "providerName": "RedbeardIdentity",
   "providerType": "SAML",
   "issuer": "http://www.okta.com/redbeardidentityuserpool",
   "primary": "true",
   "dateCreated": "1622314704121"
  }
 ],
 "auth_time": 1622321399,
 "exp": 1622324999,
 "iat": 1622321399,
 "email": "redbeardidentity+iamdev@gmail.com",
 "custom:title": "IAM Developer",
 "custom:organization": "Information Technology",
 "email_verified": false,
 "address": {
  "formatted": "901 E Byrd St Richmond VA 23219"
 },
 "custom:division": "Information Security",
 "cognito:username": "redbeardidentity_redbeardidentity+iamdev@g
 "given_name": "Iam",
 "nonce": "aNYrevez4nBGM7vmeCWzTdl1ZakPmdsk3A0_JTVOViADmVRhupab1
 "aud": "4icmcfao26f4a2geh135pqjgn1",
 "token_use": "id",
 "custom:costCenter": "30002",
 "name": "Iam Dev",
 "family_name": "Dev"
}
```



Users >

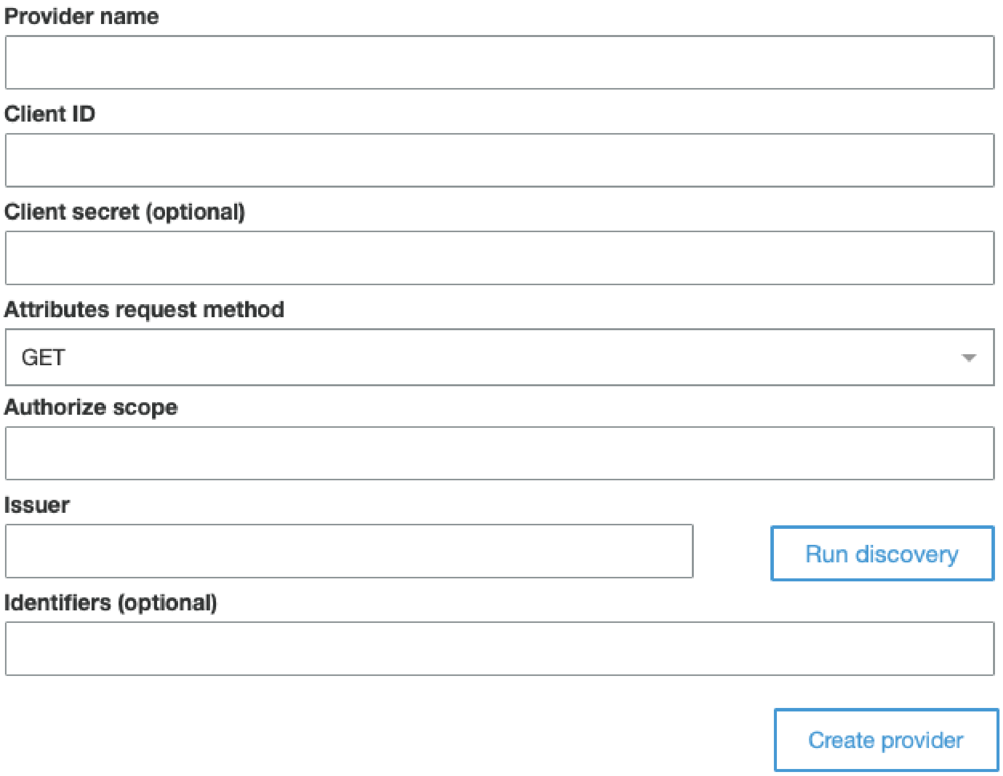
redbeardidentity_redbeardidentity+iamdev@gmail.com

Groups	us-east-1_rz2HyPFjt_RedbeardIdentity
Account Status	Enabled / EXTERNAL_PROVIDER
SMS MFA Status	Disabled
Last Modified	May 29, 2021 8:49:47 PM
Created	May 29, 2021 6:58:24 PM
custom:title	IAM Developer
custom:organization	Information Technology
sub	8b0552a4-5003-4e88-ab31-33a6c3bc9616
address	901 E Byrd St Richmond VA 23219
email_verified	false
custom:department	Identity Development
custom:division	Information Security
locale	Richmond
given_name	Iam
custom:userType	Staff



Do you want to allow users to sign in through external federated identity providers?

Select and configure the external identity providers you want to enable. You will also need to choose which identity providers to enable for each app on the Apps settings tab under App integration. Learn more about identity federation with Cognito User Pools.



Provider name

Client ID

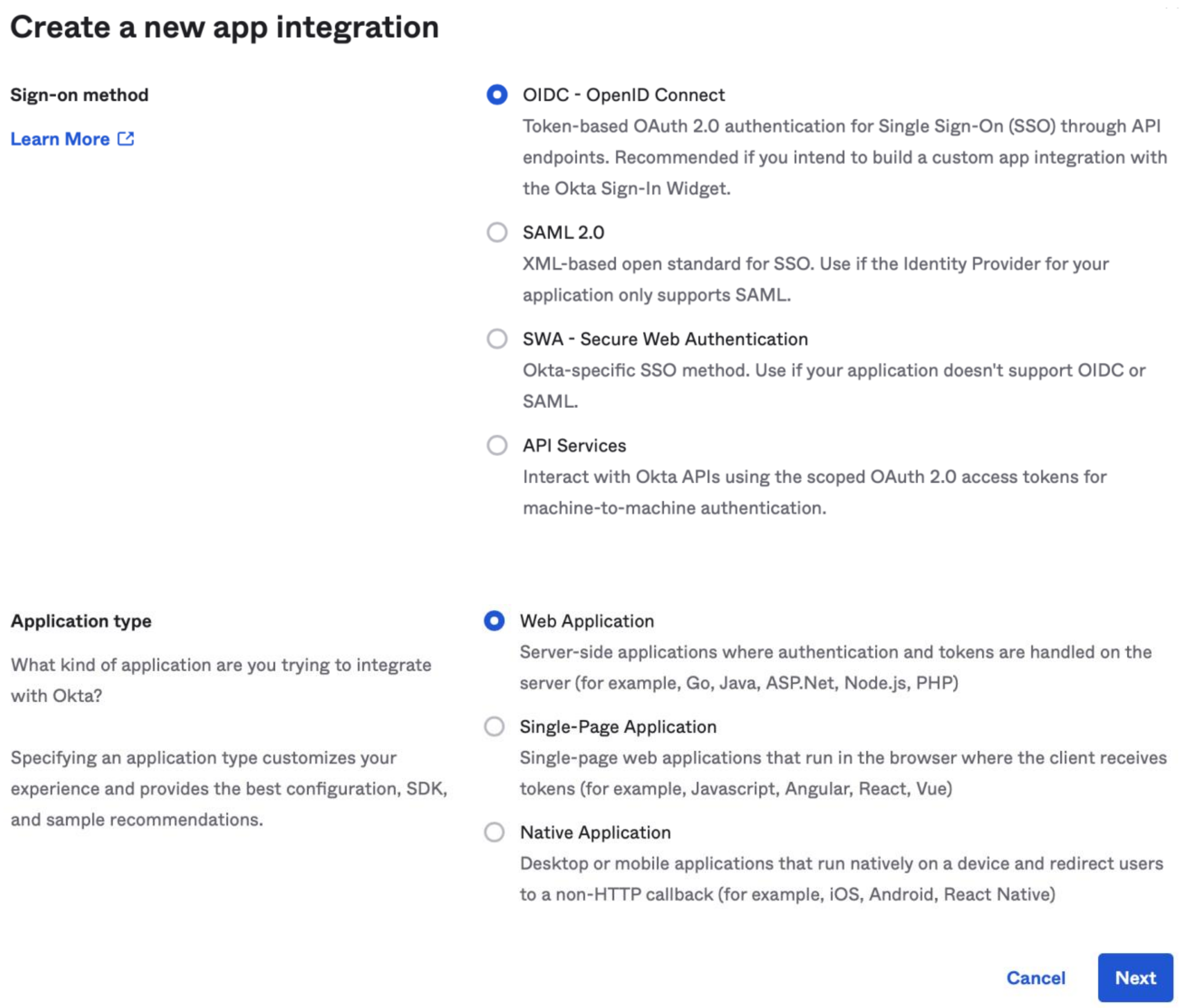
Client secret (optional)

Attributes request method: GET

Authorize scope

Issuer

Identifiers (optional)



Create a new app integration

Sign-on method

Learn More

● OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

○ SAML 2.0
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

○ SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

○ API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Application type

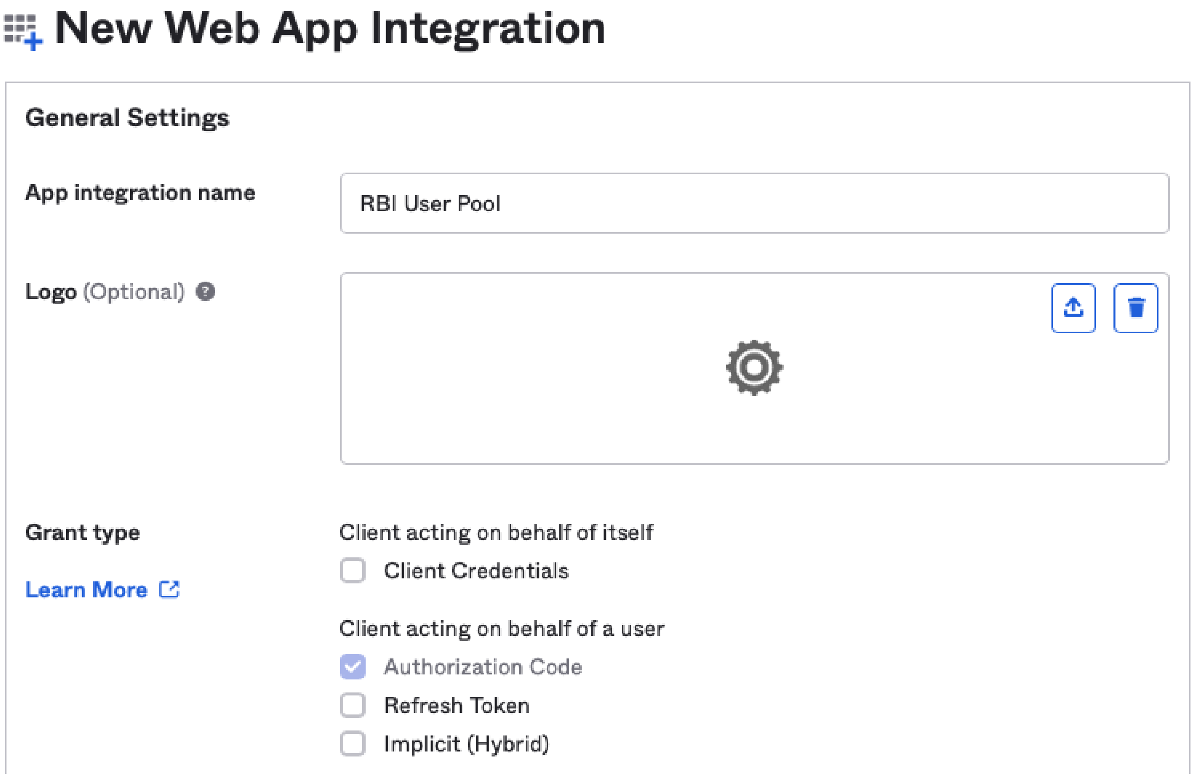
What kind of application are you trying to integrate with Okta?

Specifying an application type customizes your experience and provides the best configuration, SDK, and sample recommendations.

● Web Application
Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)

○ Single-Page Application
Single-page web applications that run in the browser where the client receives tokens (for example, Javascript, Angular, React, Vue)

○ Native Application
Desktop or mobile applications that run natively on a device and redirect users to a non-HTTP callback (for example, iOS, Android, React Native)



New Web App Integration

General Settings

App integration name: RBI User Pool

Logo (Optional)

Grant type

Learn More

Client acting on behalf of itself

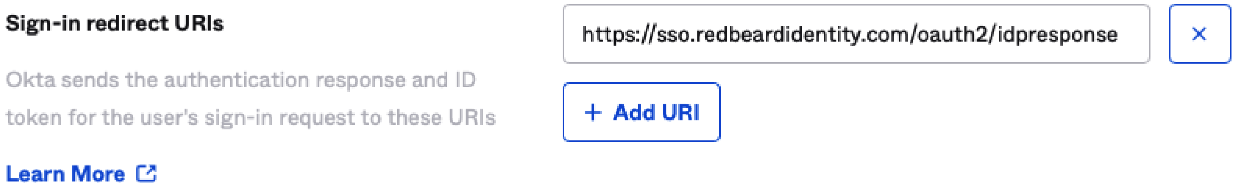
□ Client Credentials

Client acting on behalf of a user

☑ Authorization Code

□ Refresh Token

□ Implicit (Hybrid)

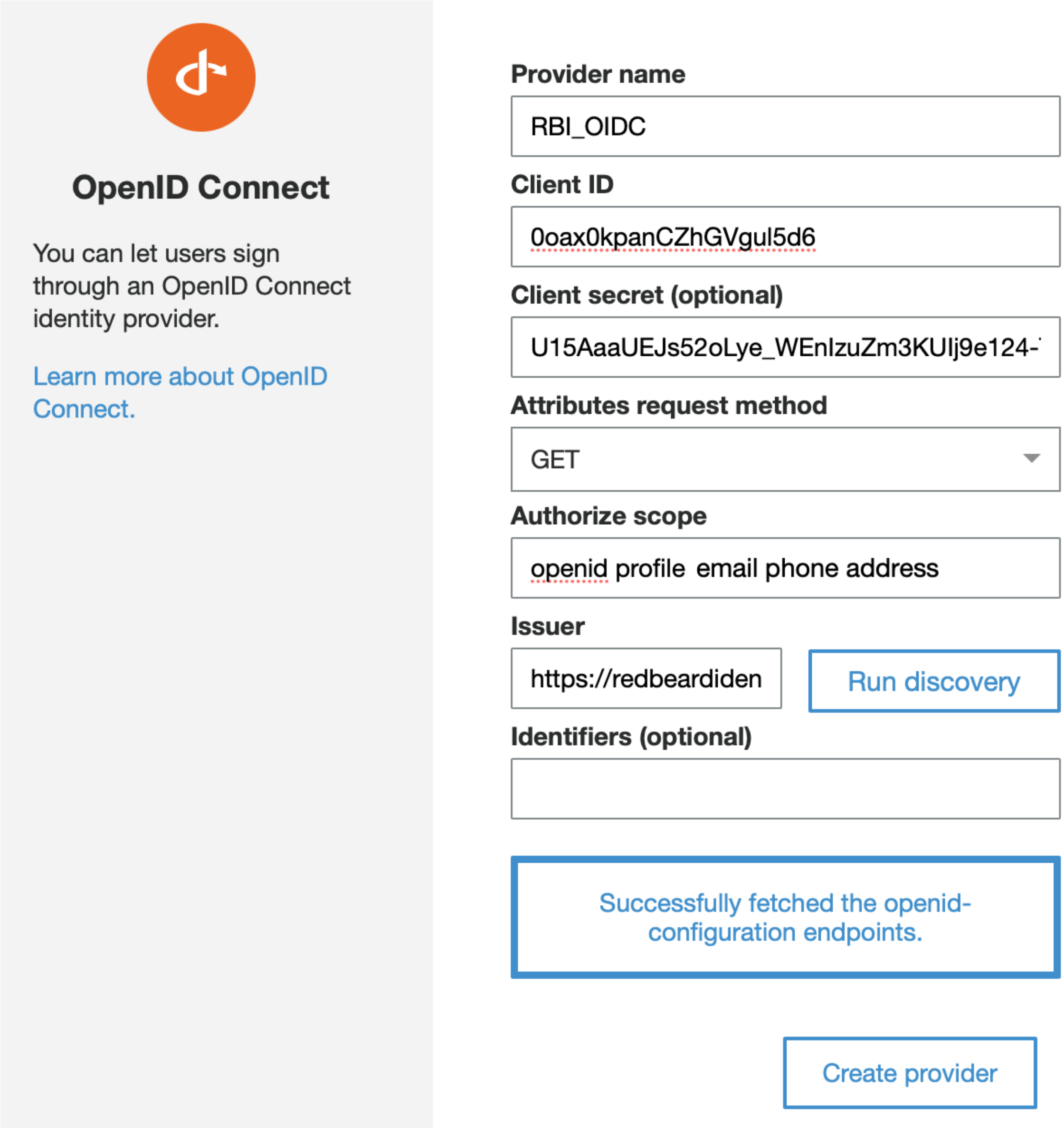


Sign-in redirect URIs

Okta sends the authentication response and ID token for the user's sign-in request to these URIs

Learn More

https://sso.redbeardidentity.com/oauth2/idpresponse



OpenID Connect

You can let users sign through an OpenID Connect identity provider.

Learn more about OpenID Connect.

Provider name: RBI_OIDC

Client ID: 0oax0kpanCZhGVgul5d6

Client secret (optional): U15AaaUEJs52oLye_WEnIzuZm3KUIj9e124-

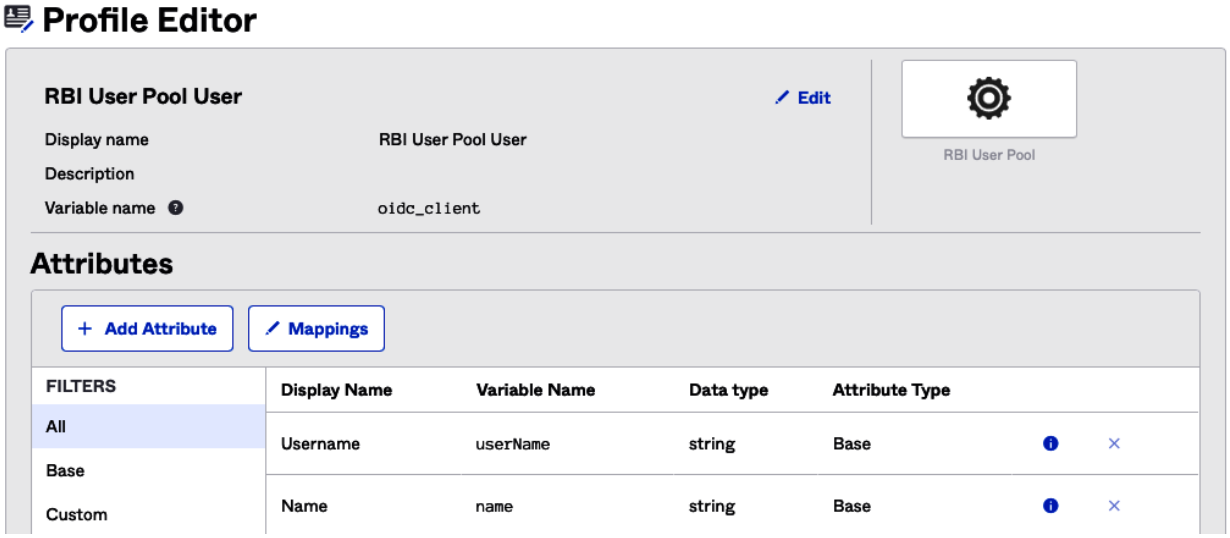
Attributes request method: GET

Authorize scope: openid profile email phone address

Issuer: https://redbeardiden

Identifiers (optional):

Successfully fetched the openid-configuration endpoints.



Profile Editor

RBI User Pool User

Display name: RBI User Pool User

Description:

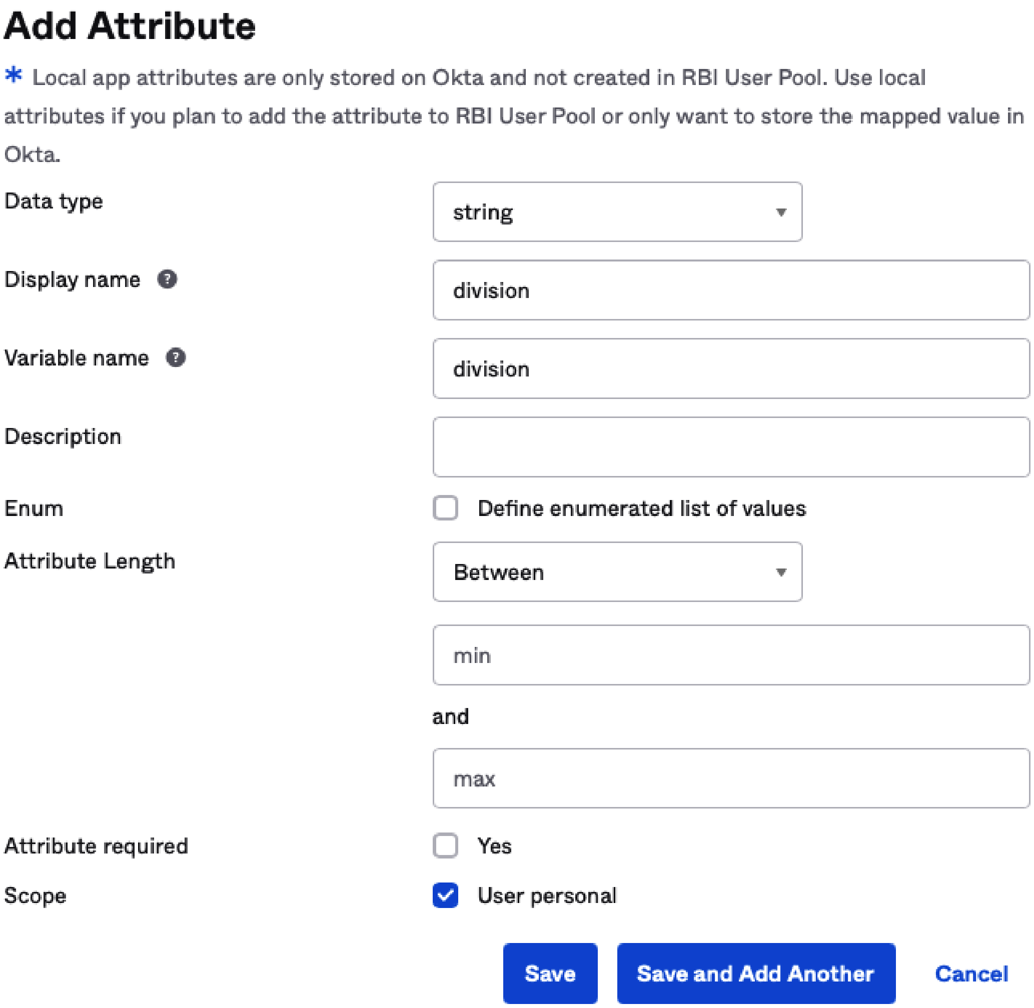
Variable name: oidc_client

Attributes

FILTERS

- All
- Base
- Custom

Display Name	Variable Name	Data type	Attribute Type
Username	userName	string	Base
Name	name	string	Base



Add Attribute

* Local app attributes are only stored on Okta and not created in RBI User Pool. Use local attributes if you plan to add the attribute to RBI User Pool or only want to store the mapped value in Okta.

Data type: string

Display name: division

Variable name: division

Description:

Enum: □ Define enumerated list of values

Attribute Length: Between

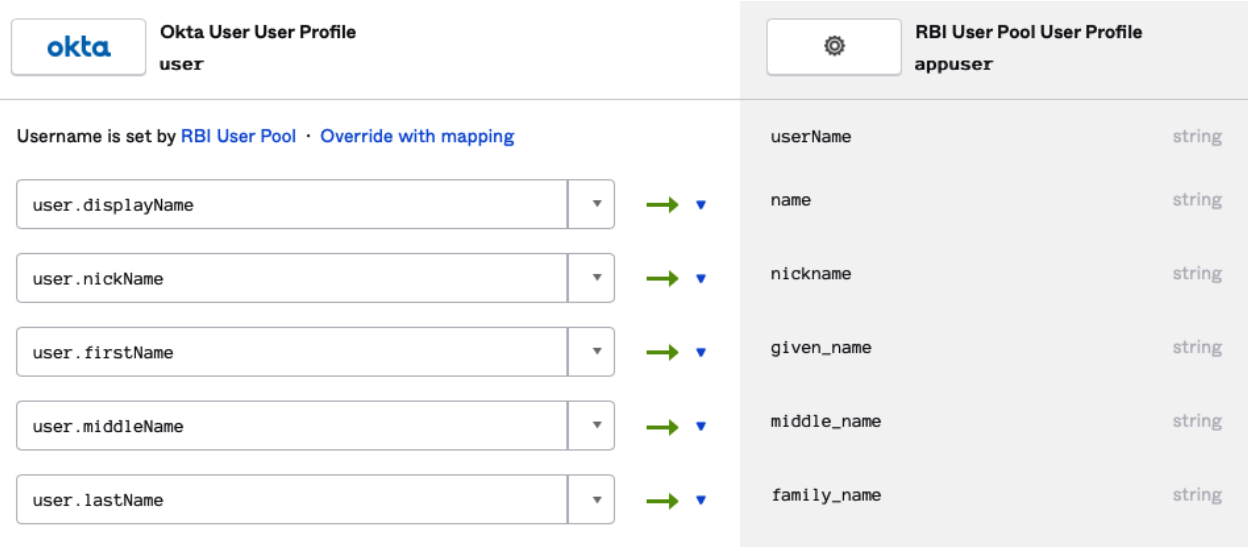
min

and

max

Attribute required: □ Yes

Scope: ☑ User personal

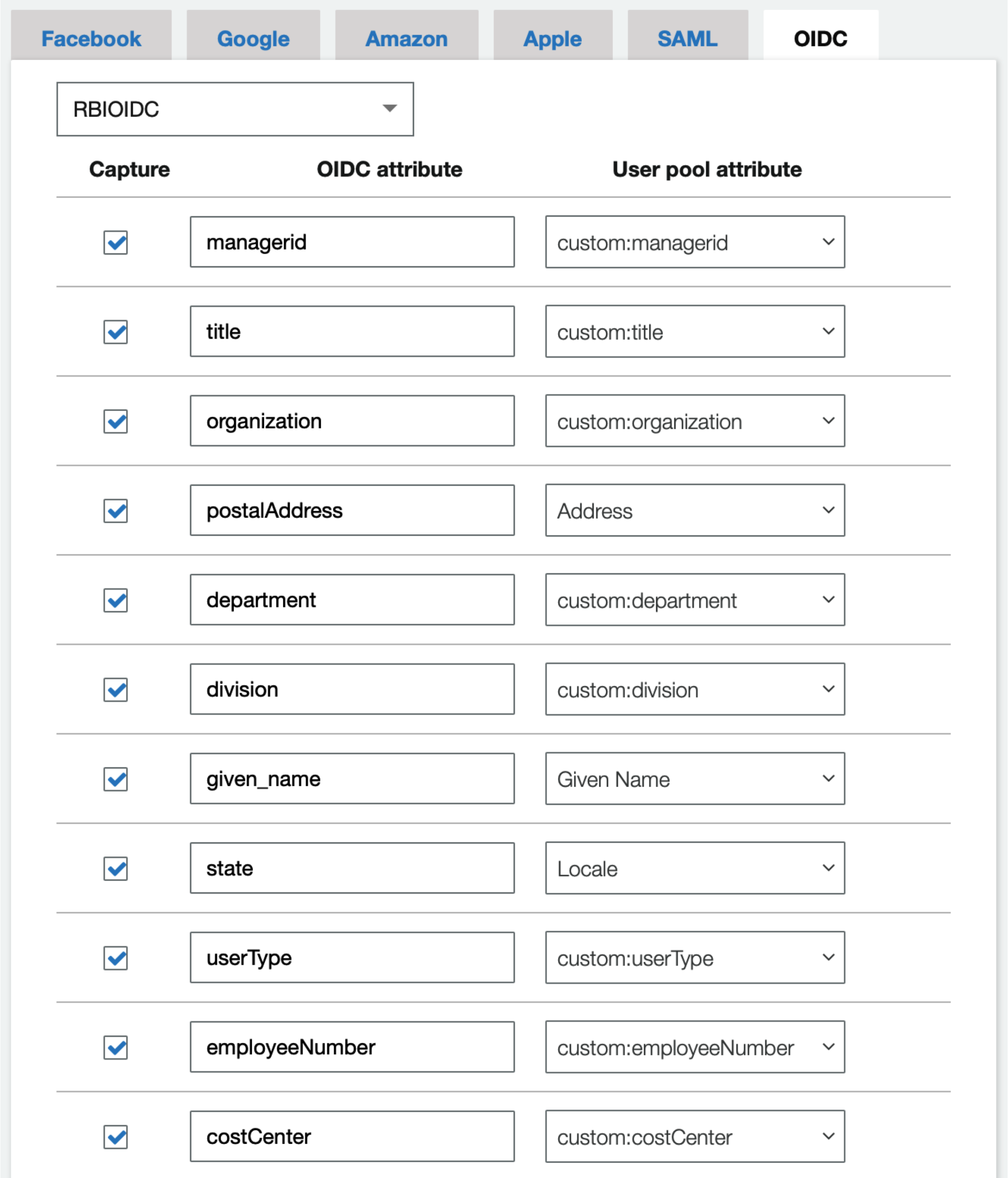


Okta User User Profile
user

RBI User Pool User Profile
appuser

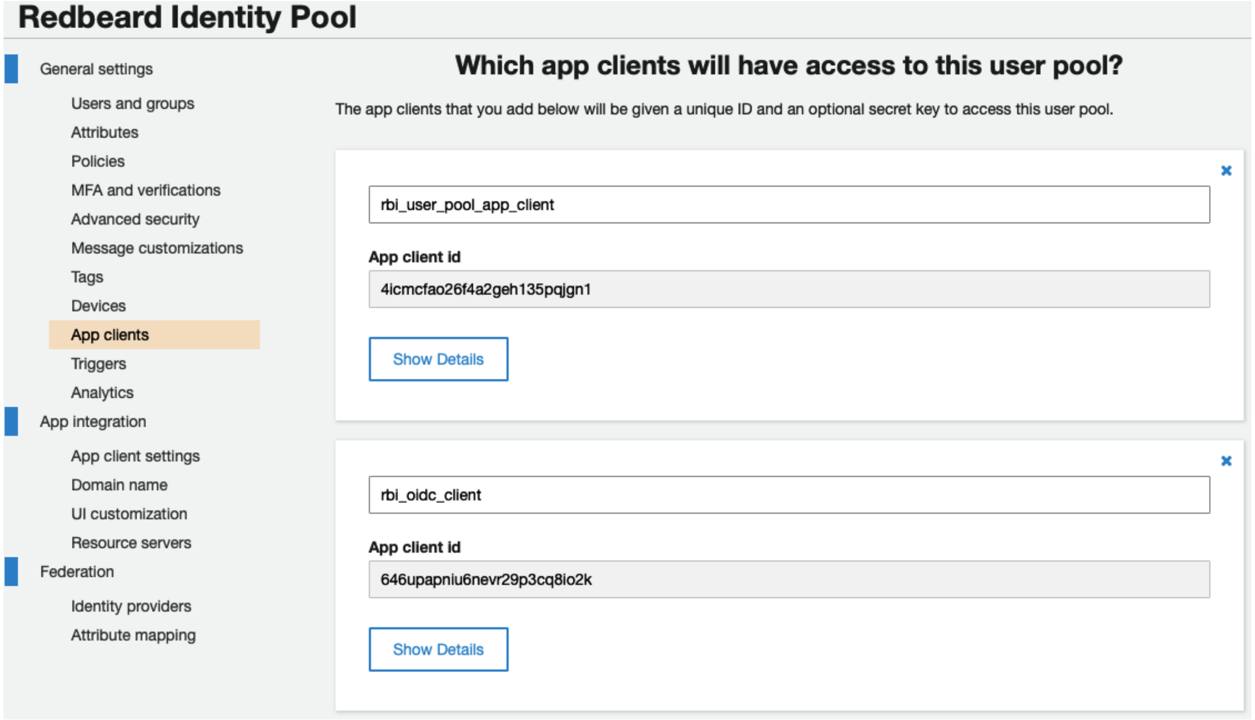
Username is set by RBI User Pool · Override with mapping

		userName	string
user.displayName	→	name	string
user.nickName	→	nickname	string
user.firstName	→	given_name	string
user.middleName	→	middle_name	string
user.lastName	→	family_name	string



RBIOIDC

Capture	OIDC attribute	User pool attribute
☑	managerid	custom:managerid
☑	title	custom:title
☑	organization	custom:organization
☑	postalAddress	Address
☑	department	custom:department
☑	division	custom:division
☑	given_name	Given Name
☑	state	Locale
☑	userType	custom:userType
☑	employeeNumber	custom:employeeNumber
☑	costCenter	custom:costCenter



Redbeard Identity Pool

Which app clients will have access to this user pool?

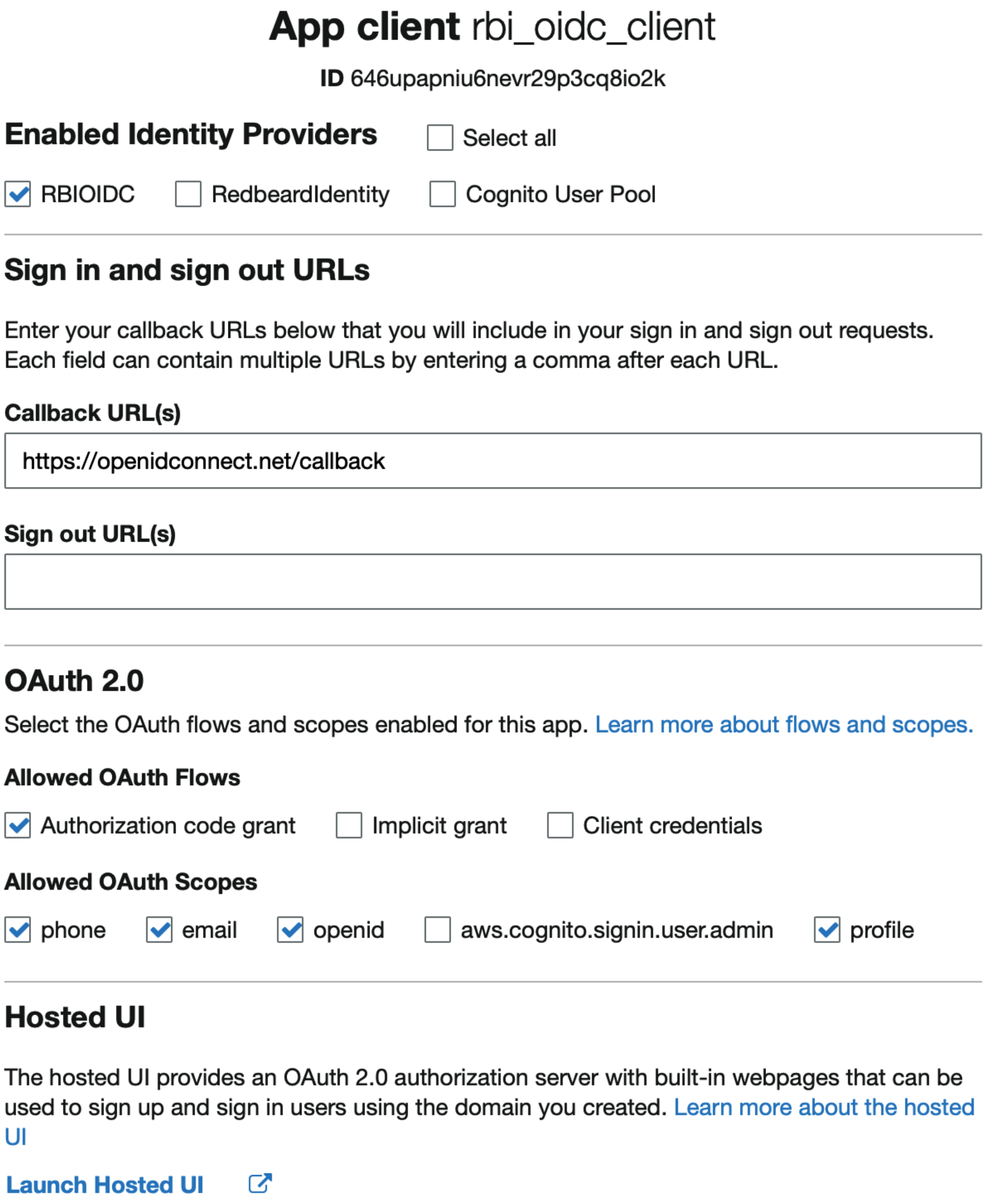
The app clients that you add below will be given a unique ID and an optional secret key to access this user pool.

rbi_user_pool_app_client

App client id: 4icmcfao26f4a2geh135pqjgn1

rbi_oidc_client

App client id: 646upapniu6nevr29p3cq8io2k



App client rbi_oidc_client

ID 646upapniu6nevr29p3cq8io2k

Enabled Identity Providers

□ Select all

☑ RBIOIDC □ RedbeardIdentity □ Cognito User Pool

Sign in and sign out URLs

Enter your callback URLs below that you will include in your sign in and sign out requests. Each field can contain multiple URLs by entering a comma after each URL.

Callback URL(s)

https://openidconnect.net/callback

Sign out URL(s)

OAuth 2.0

Select the OAuth flows and scopes enabled for this app. Learn more about flows and scopes.

Allowed OAuth Flows

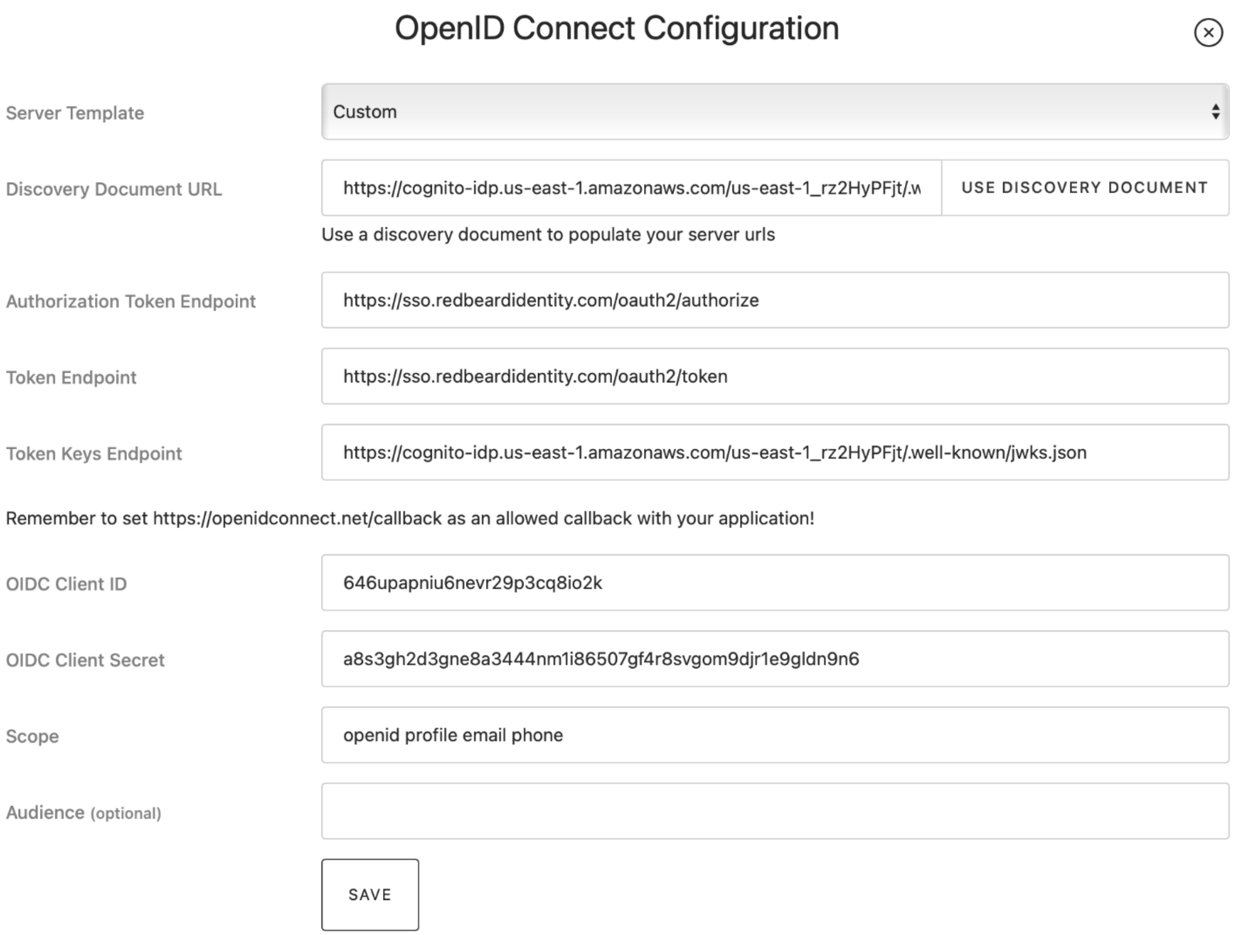
☑ Authorization code grant □ Implicit grant □ Client credentials

Allowed OAuth Scopes

☑ phone ☑ email ☑ openid □ aws.cognito.signin.user.admin ☑ profile

Hosted UI

The hosted UI provides an OAuth 2.0 authorization server with built-in webpages that can be used to sign up and sign in users using the domain you created. Learn more about the hosted UI



OpenID Connect Configuration

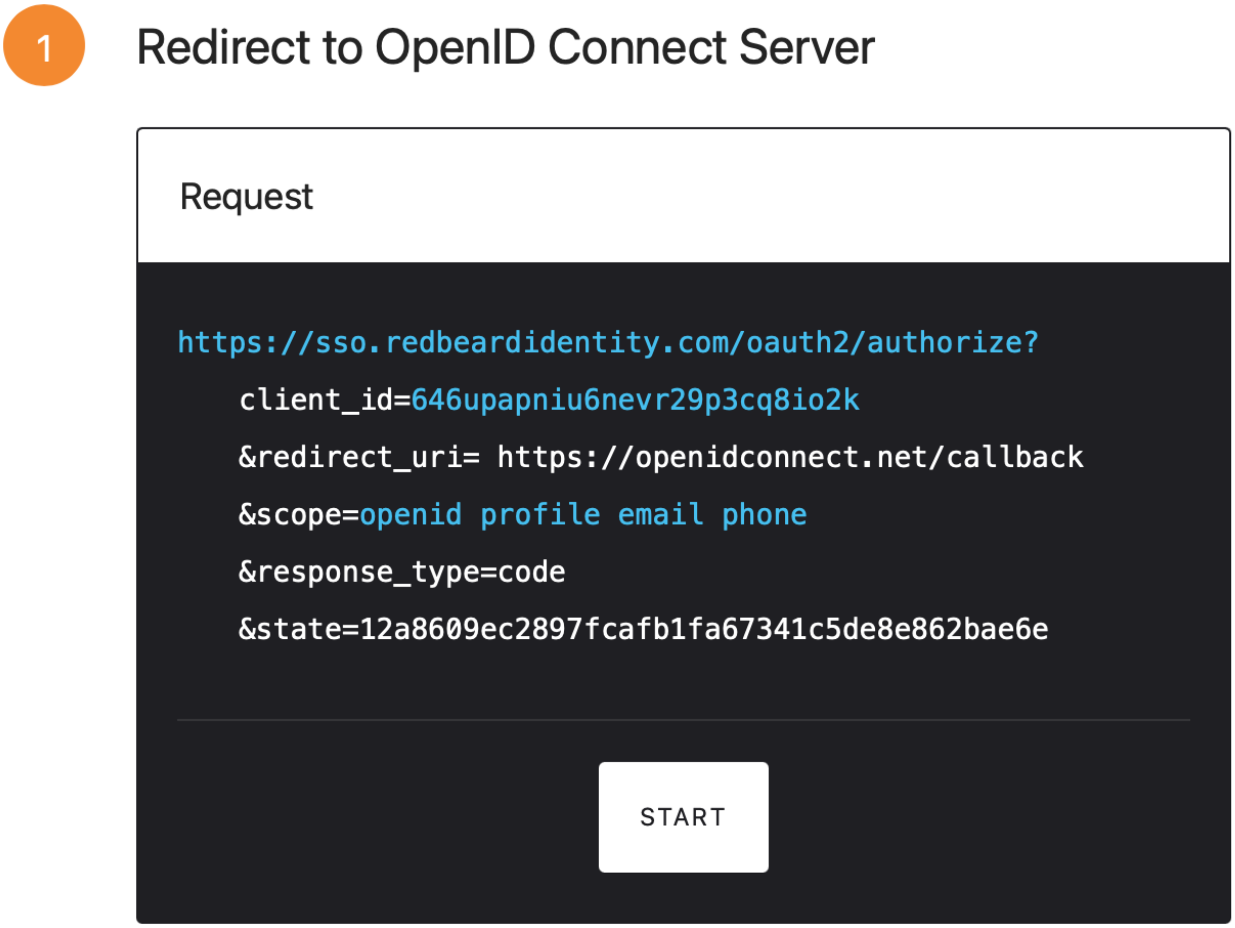
Server Template	Custom
Discovery Document URL	https://cognito-idp.us-east-1.amazonaws.com/us-east-1_rz2HyPFjt/.w

Use a discovery document to populate your server urls

Authorization Token Endpoint	https://sso.redbeardidentity.com/oauth2/authorize
Token Endpoint	https://sso.redbeardidentity.com/oauth2/token
Token Keys Endpoint	https://cognito-idp.us-east-1.amazonaws.com/us-east-1_rz2HyPFjt/.well-known/jwks.json

Remember to set https://openidconnect.net/callback as an allowed callback with your application!

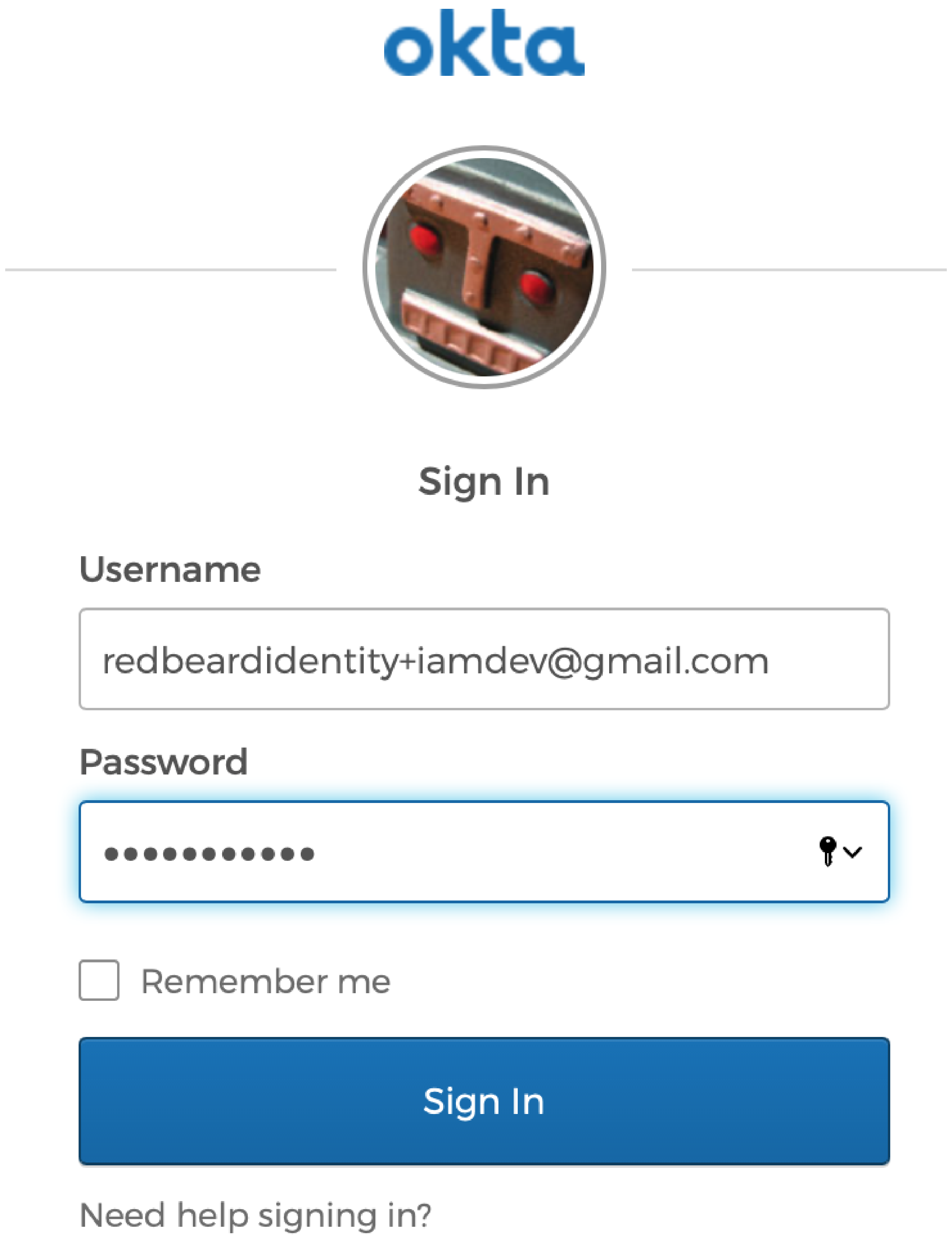
OIDC Client ID	646upapniu6nevr29p3cq8io2k
OIDC Client Secret	a8s3gh2d3gne8a3444nm1i86507gf4r8svgom9djr1e9gldn9n6
Scope	openid profile email phone
Audience (optional)	



1 Redirect to OpenID Connect Server

Request

```
https://sso.redbeardidentity.com/oauth2/authorize?
    client_id=646upapniu6nevr29p3cq8io2k
    &redirect_uri= https://openidconnect.net/callback
    &scope=openid profile email phone
    &response_type=code
    &state=12a8609ec2897fcafb1fa67341c5de8e862bae6e
```



Sign In

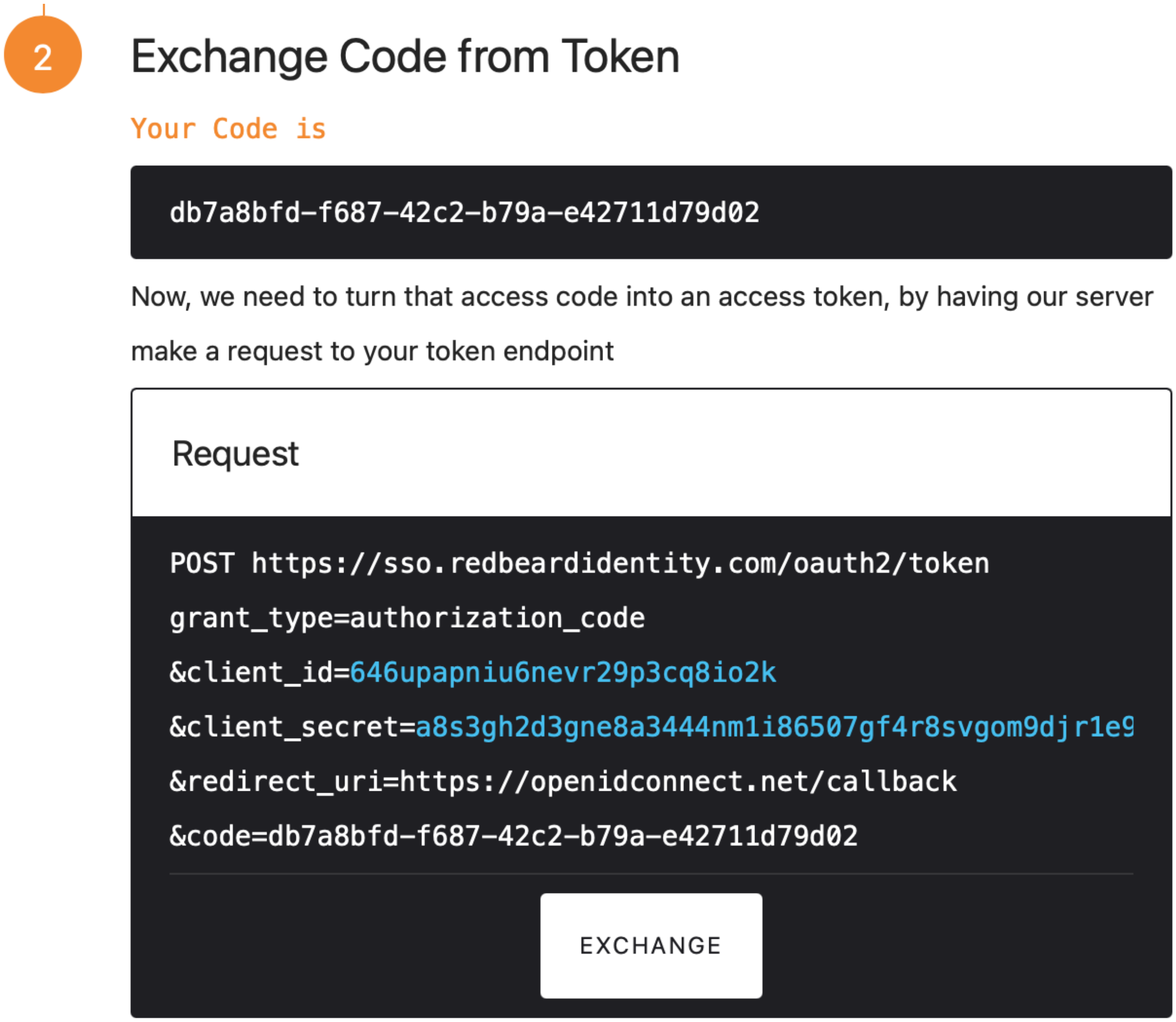
Username

redbeardidentity+iamdev@gmail.com

Password

●●●●●●●●●●●

□ Remember me



2

Exchange Code from Token

`Your Code is`

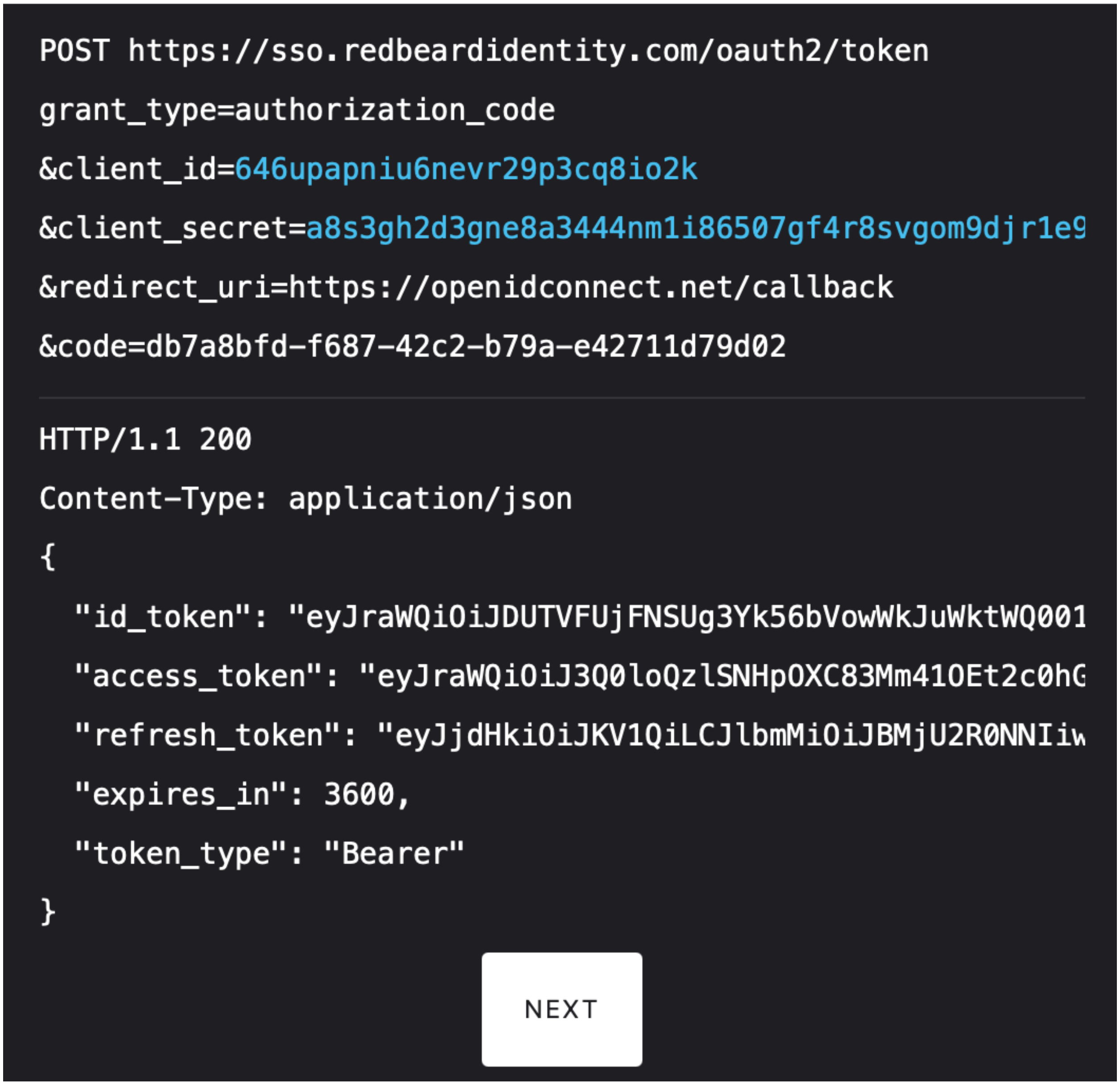
```
db7a8bfd-f687-42c2-b79a-e42711d79d02
```

Now, we need to turn that access code into an access token, by having our server make a request to your token endpoint

Request

```
POST https://sso.redbeardidentity.com/oauth2/token
grant_type=authorization_code
&client_id=646upapniu6nevr29p3cq8io2k
&client_secret=a8s3gh2d3gne8a3444nm1i86507gf4r8svgom9djr1e9
&redirect_uri=https://openidconnect.net/callback
&code=db7a8bfd-f687-42c2-b79a-e42711d79d02
```

Request



```
POST https://sso.redbeardidentity.com/oauth2/token

grant_type=authorization_code

&client_id=646upapniu6nevr29p3cq8io2k

&client_secret=a8s3gh2d3gne8a3444nm1i86507gf4r8svgom9djr1e9

&redirect_uri=https://openidconnect.net/callback

&code=db7a8bfd-f687-42c2-b79a-e42711d79d02
```

```
HTTP/1.1 200

Content-Type: application/json

{

  "id_token": "eyJraWQiOiJDUTVFUjFNSUg3Yk56bVowWkJuWktWQ001

  "access_token": "eyJraWQiOiJ3Q0loQzlSNHpOXC83Mm41OEt2c0hG

  "refresh_token": "eyJjdHkiOiJKV1QiLCJlbmMiOiJBMjU2R0NNIiw

  "expires_in": 3600,

  "token_type": "Bearer"

}
```

3

Verify User Token

Now, we need to verify that the ID Token sent was from the correct place by validating the JWT's signature

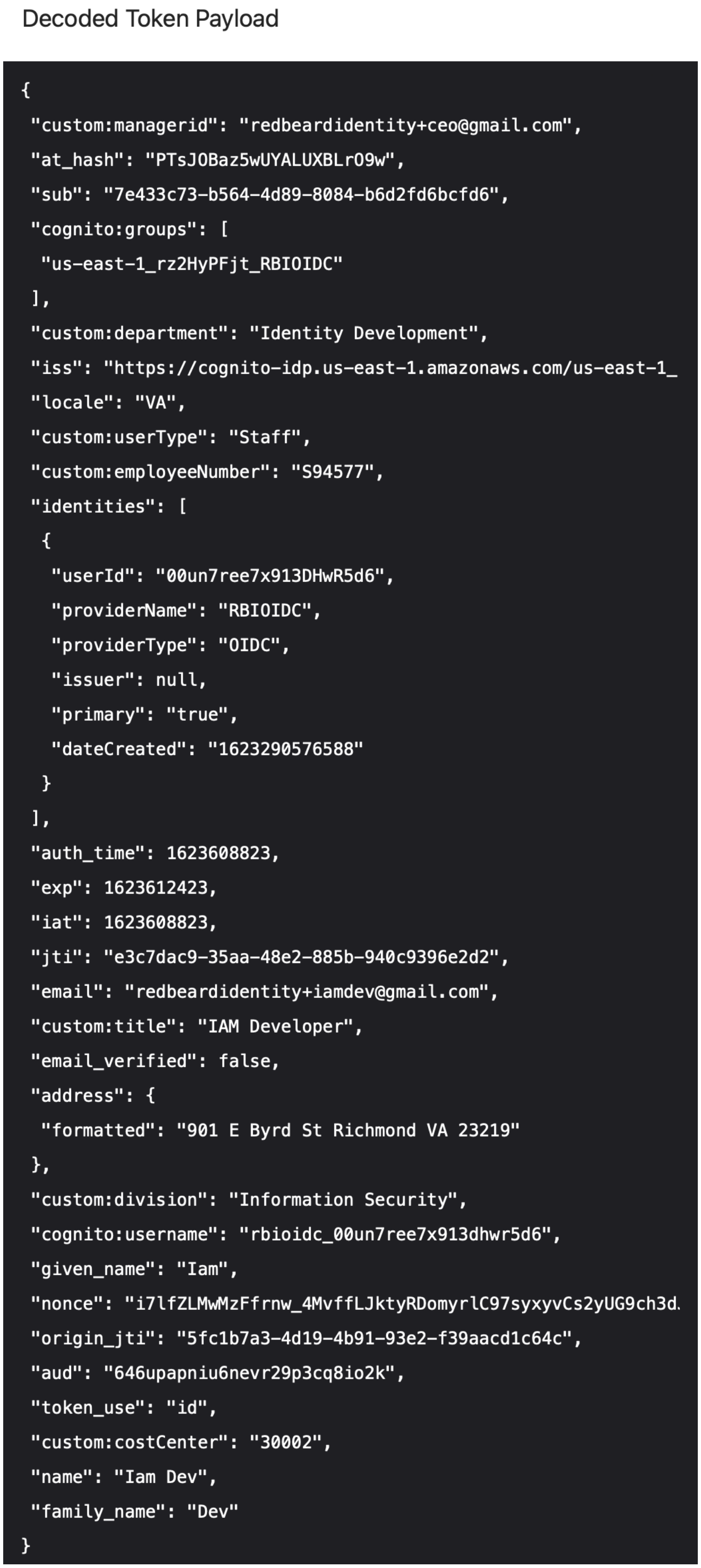
Your “id_token” is

VIEW ON JWT.IO

```
eyJraWQiOiJDUTVFUjFNSUg3Yk56bVowWkJuWktWQ001QW42ZUtmblA0ek5MS
M4IWS1JuQKVVeN5CFQEjSZGZEJSBjzKqgIqLc0B8uxgKfbjZMmoIvVcQLNF2H
Ch3fkN8DjSbBRwdHemjgxyunShiPW_2jjlWmn3-
D7Y9sNl4lqYTNTRHmWcFmo5mJOXuEXlBo9SsowmrcgtDykwVokV_VoIhl3twl
lKv0jOk199TFijf2yLVLHZBzfnVi0ivbPN2CFXIlMfm4r1naM96pCM9zQ
```

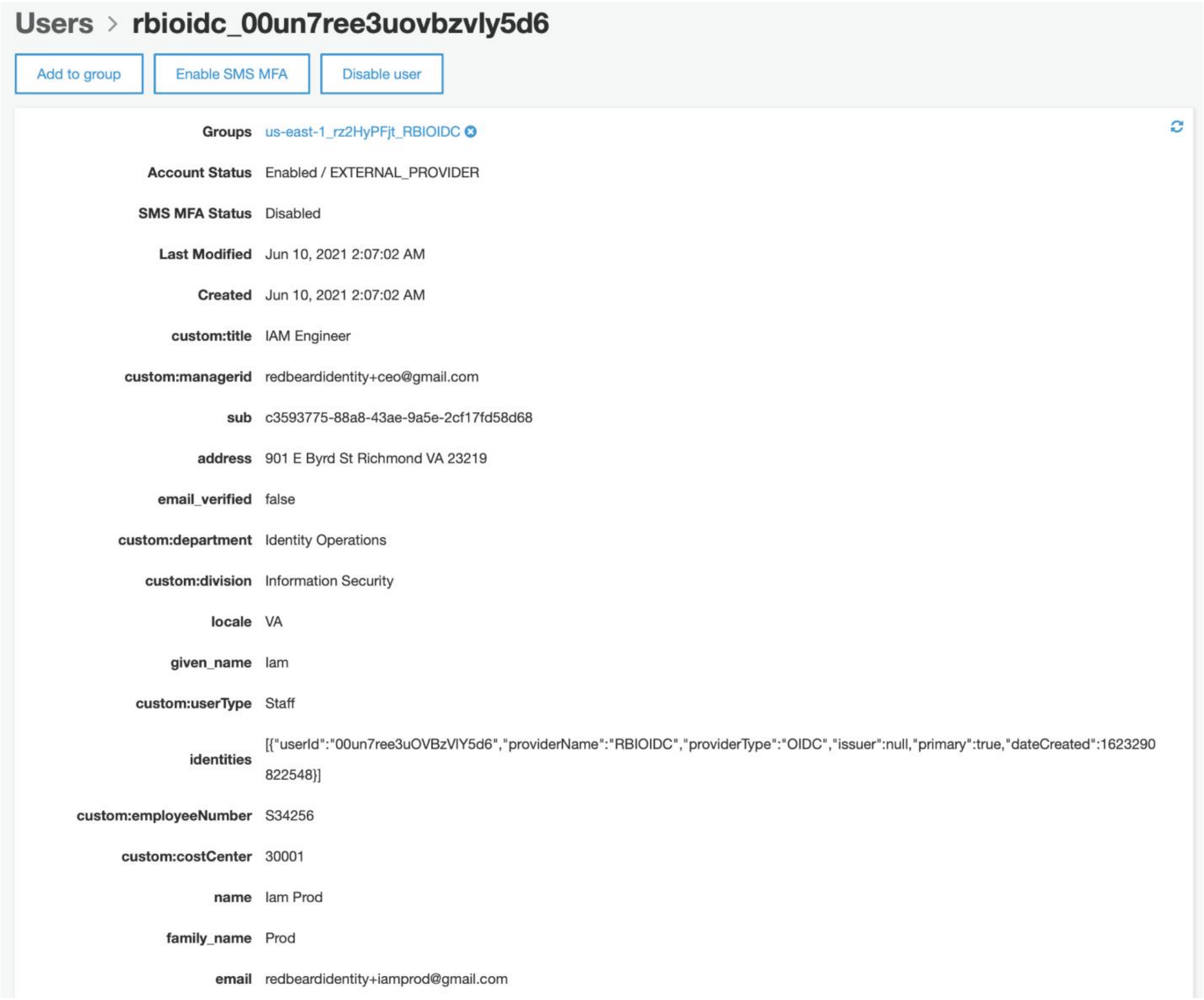
This token is cryptographically signed with the **RS256** algorithim. We'll use the public key of the OpenID Connect server to validate it. In order to do that, we'll fetch the public key from **https://cognito-idp.us-east-1.amazonaws.com/us-east-1_rz2HyPFjt/.well-known/jwks.json**, which is found in the discovery document or configuration menu options.

VERIFY



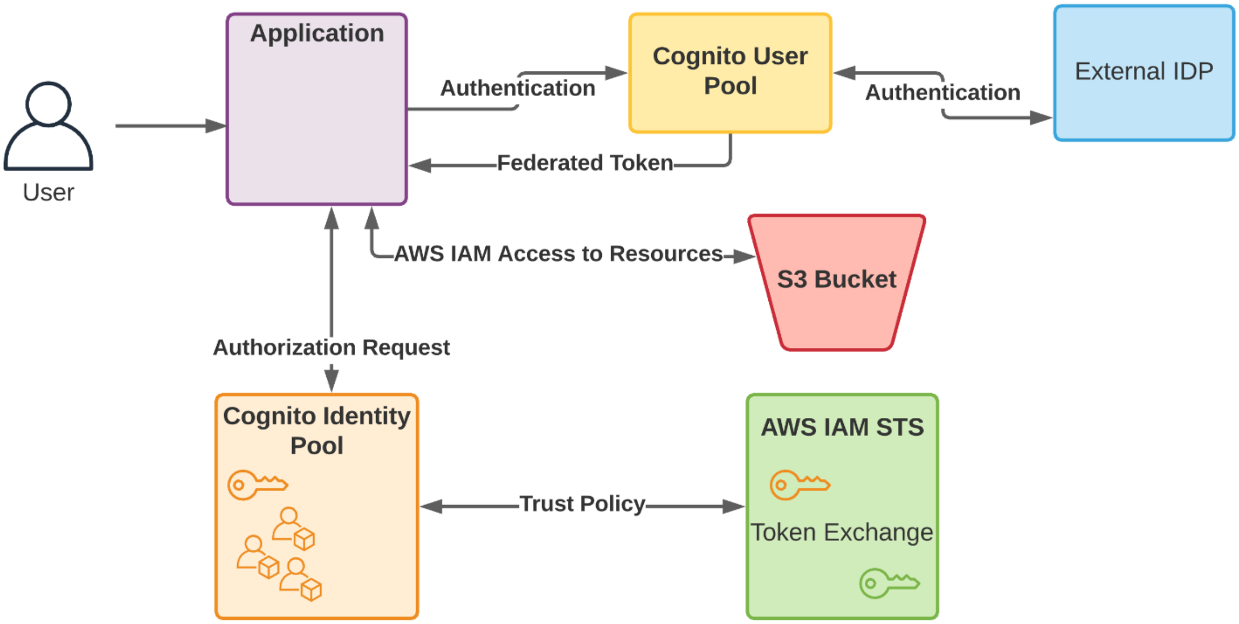
Decoded Token Payload

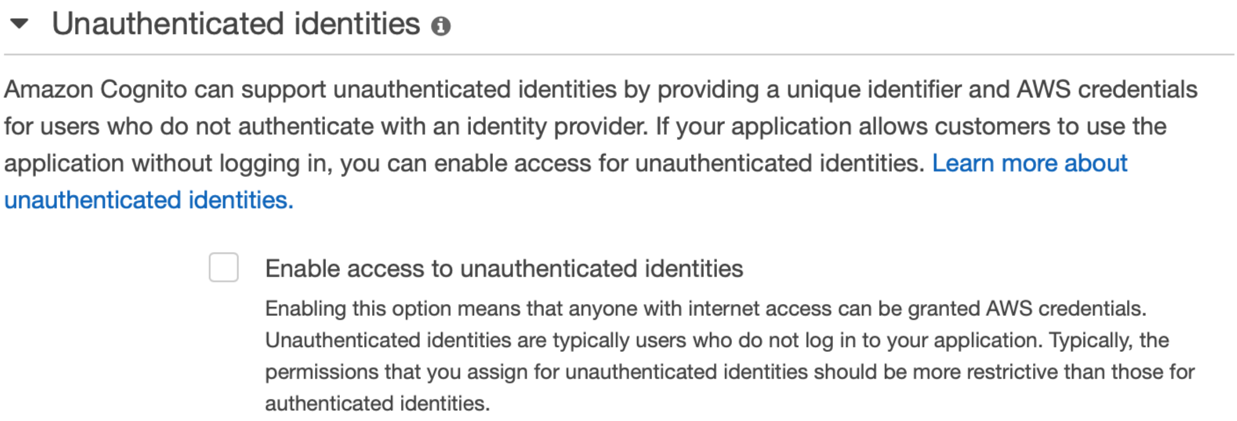
```
{
 "custom:managerid": "redbeardidentity+ceo@gmail.com",
 "at_hash": "PTsJOBaz5wUYALUXBLrO9w",
 "sub": "7e433c73-b564-4d89-8084-b6d2fd6bcfd6",
 "cognito:groups": [
  "us-east-1_rz2HyPFjt_RBIOIDC"
 ],
 "custom:department": "Identity Development",
 "iss": "https://cognito-idp.us-east-1.amazonaws.com/us-east-1_
 "locale": "VA",
 "custom:userType": "Staff",
 "custom:employeeNumber": "S94577",
 "identities": [
  {
   "userId": "00un7ree7x913DHwR5d6",
   "providerName": "RBIOIDC",
   "providerType": "OIDC",
   "issuer": null,
   "primary": "true",
   "dateCreated": "1623290576588"
  }
 ],
 "auth_time": 1623608823,
 "exp": 1623612423,
 "iat": 1623608823,
 "jti": "e3c7dac9-35aa-48e2-885b-940c9396e2d2",
 "email": "redbeardidentity+iamdev@gmail.com",
 "custom:title": "IAM Developer",
 "email_verified": false,
 "address": {
  "formatted": "901 E Byrd St Richmond VA 23219"
 },
 "custom:division": "Information Security",
 "cognito:username": "rbioidc_00un7ree7x913dhwr5d6",
 "given_name": "Iam",
 "nonce": "i7lfZLMwMzFfrnw_4MvffLJktyRDomyrlC97syxyvCs2yUG9ch3d
 "origin_jti": "5fc1b7a3-4d19-4b91-93e2-f39aacd1c64c",
 "aud": "646upapniu6nevr29p3cq8io2k",
 "token_use": "id",
 "custom:costCenter": "30002",
 "name": "Iam Dev",
 "family_name": "Dev"
}
```



Users > rbioidc_00un7ree3uovbzvly5d6

Groups	us-east-1_rz2HyPFjt_RBIOIDC
Account Status	Enabled / EXTERNAL_PROVIDER
SMS MFA Status	Disabled
Last Modified	Jun 10, 2021 2:07:02 AM
Created	Jun 10, 2021 2:07:02 AM
custom:title	IAM Engineer
custom:managerid	redbeardidentity+ceo@gmail.com
sub	c3593775-88a8-43ae-9a5e-2cf17fd58d68
address	901 E Byrd St Richmond VA 23219
email_verified	false
custom:department	Identity Operations
custom:division	Information Security
locale	VA
given_name	Iam
custom:userType	Staff
identities	[{"userId":"00un7ree3uOVBzVlY5d6","providerName":"RBIOIDC","providerType":"OIDC","issuer":null,"primary":true,"dateCreated":1623290822548}]
custom:employeeNumber	S34256
custom:costCenter	30001
name	Iam Prod
family_name	Prod
email	redbeardidentity+iamprod@gmail.com



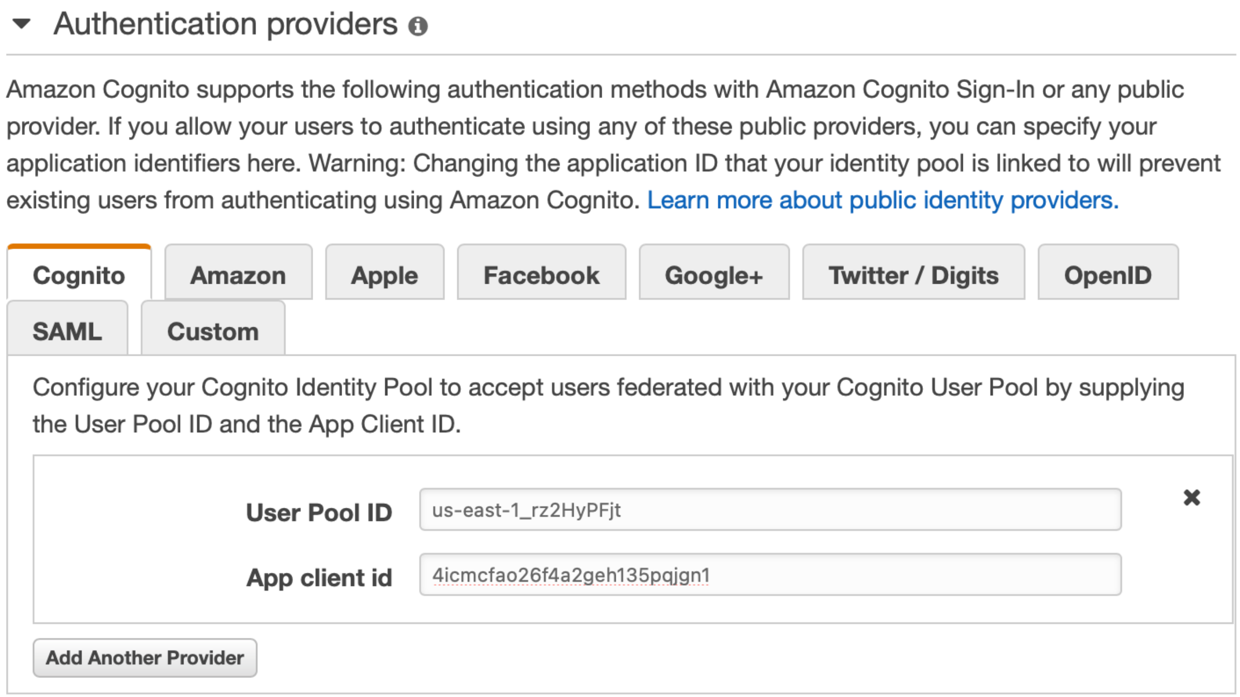


▾ Unauthenticated identities ℹ

Amazon Cognito can support unauthenticated identities by providing a unique identifier and AWS credentials for users who do not authenticate with an identity provider. If your application allows customers to use the application without logging in, you can enable access for unauthenticated identities. Learn more about unauthenticated identities.

☐ Enable access to unauthenticated identities

Enabling this option means that anyone with internet access can be granted AWS credentials. Unauthenticated identities are typically users who do not log in to your application. Typically, the permissions that you assign for unauthenticated identities should be more restrictive than those for authenticated identities.



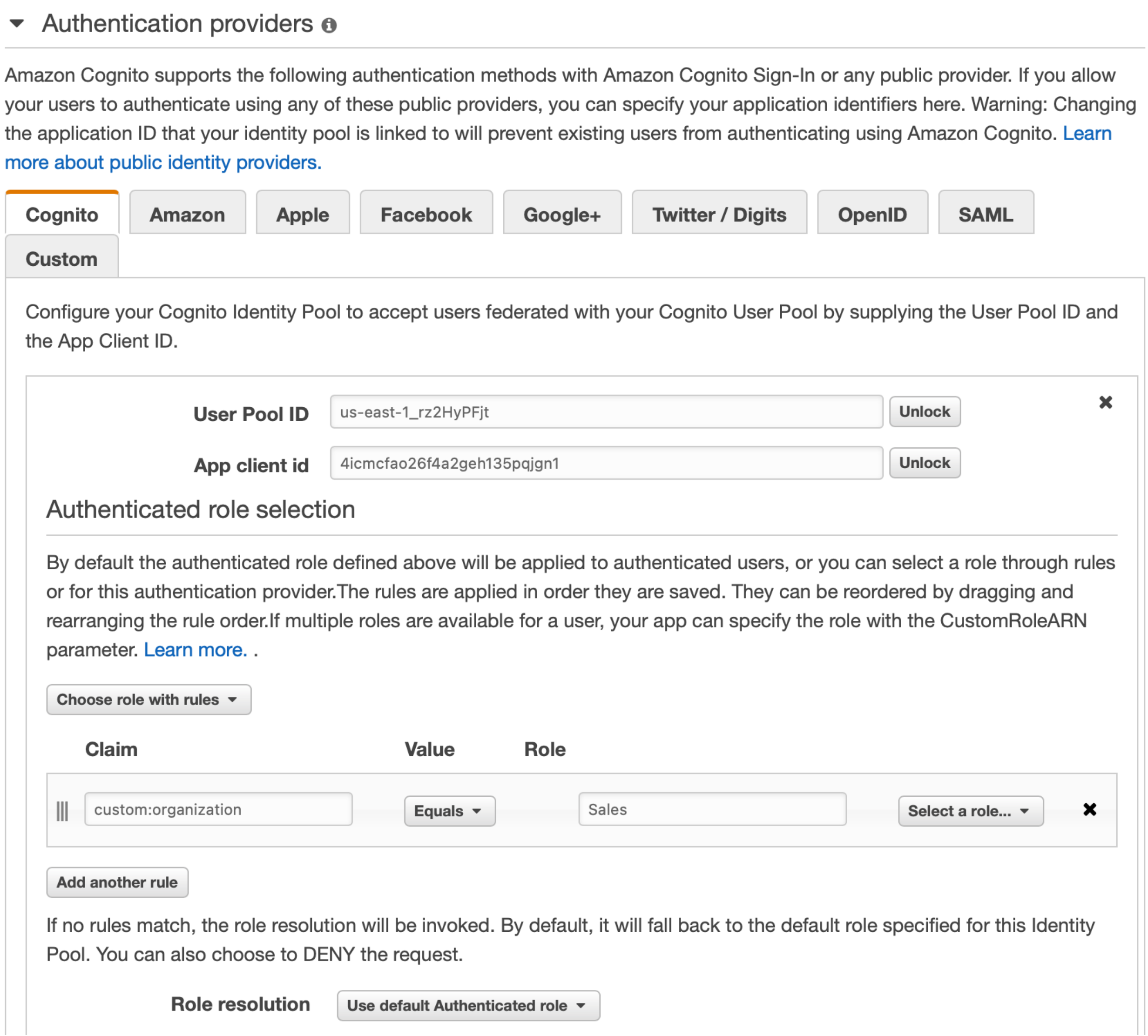
Authentication providers

Amazon Cognito supports the following authentication methods with Amazon Cognito Sign-In or any public provider. If you allow your users to authenticate using any of these public providers, you can specify your application identifiers here. Warning: Changing the application ID that your identity pool is linked to will prevent existing users from authenticating using Amazon Cognito. Learn more about public identity providers.

Configure your Cognito Identity Pool to accept users federated with your Cognito User Pool by supplying the User Pool ID and the App Client ID.

User Pool ID us-east-1_rz2HyPFjt

App client id 4icmcfao26f4a2geh135pqjgn1



Authentication providers

Amazon Cognito supports the following authentication methods with Amazon Cognito Sign-In or any public provider. If you allow your users to authenticate using any of these public providers, you can specify your application identifiers here. Warning: Changing the application ID that your identity pool is linked to will prevent existing users from authenticating using Amazon Cognito. Learn more about public identity providers.

Configure your Cognito Identity Pool to accept users federated with your Cognito User Pool by supplying the User Pool ID and the App Client ID.

User Pool ID us-east-1_rz2HyPFjt

App client id 4icmcfao26f4a2geh135pqjgn1

Authenticated role selection

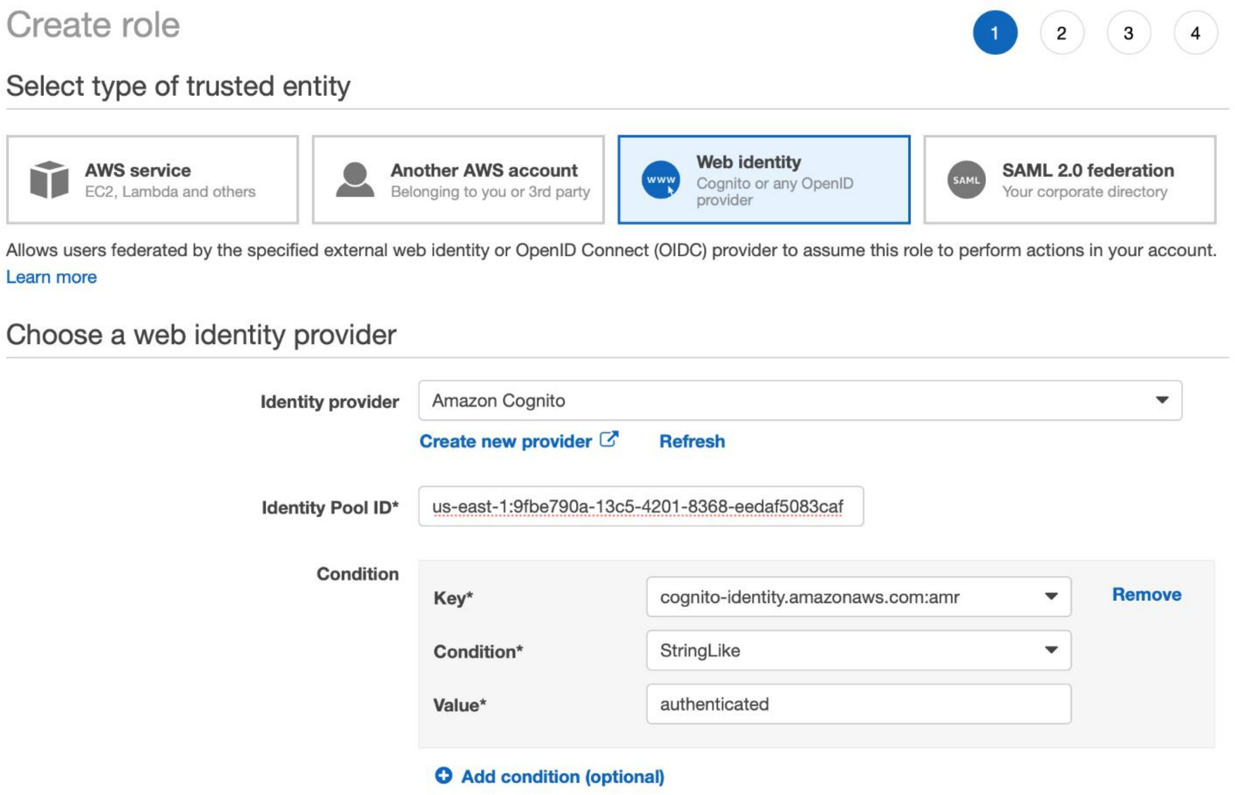
By default the authenticated role defined above will be applied to authenticated users, or you can select a role through rules or for this authentication provider.The rules are applied in order they are saved. They can be reordered by dragging and rearranging the rule order.If multiple roles are available for a user, your app can specify the role with the CustomRoleARN parameter. Learn more. .

Choose role with rules ▾

Claim	Value		Role
custom:organization	Equals ▾	Sales	Select a role... ▾

If no rules match, the role resolution will be invoked. By default, it will fall back to the default role specified for this Identity Pool. You can also choose to DENY the request.

Role resolution Use default Authenticated role ▾



Create role

1 2 3 4

Select type of trusted entity

- **AWS service** EC2, Lambda and others
- **Another AWS account** Belonging to you or 3rd party
- **Web identity** Cognito or any OpenID provider
- **SAML 2.0 federation** Your corporate directory

Allows users federated by the specified external web identity or OpenID Connect (OIDC) provider to assume this role to perform actions in your account. Learn more

Choose a web identity provider

Identity provider Amazon Cognito

Create new provider Refresh

Identity Pool ID* us-east-1:9fbe790a-13c5-4201-8368-eedaf5083caf

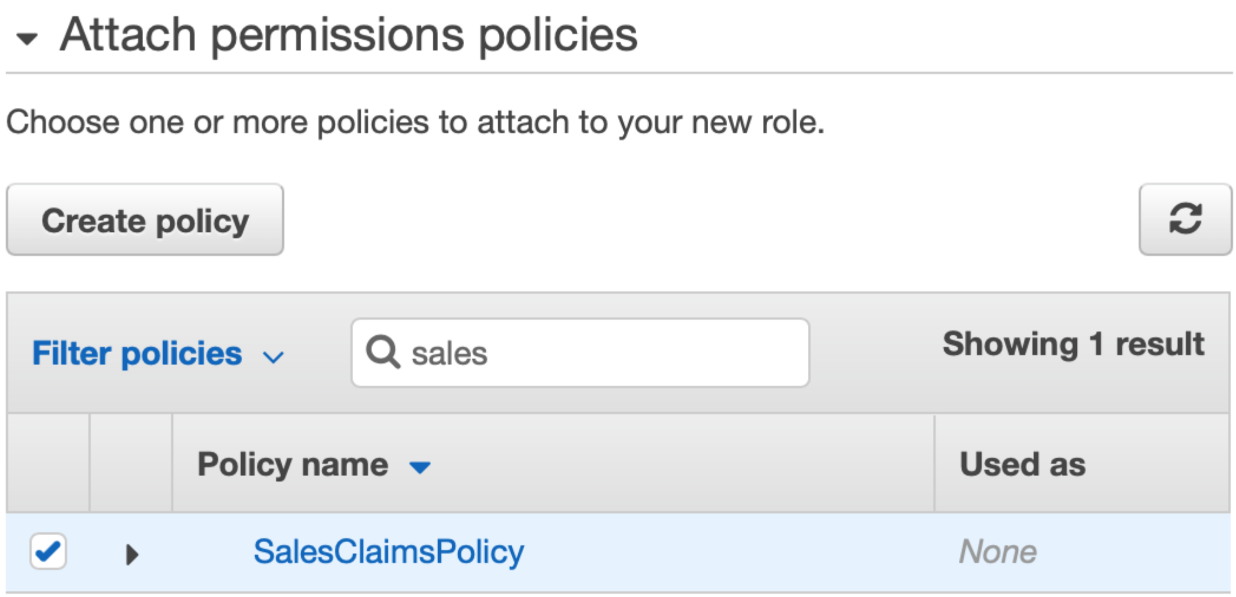
Condition

Key* cognito-identity.amazonaws.com:amr Remove

Condition* StringLike

Value* authenticated

Add condition (optional)



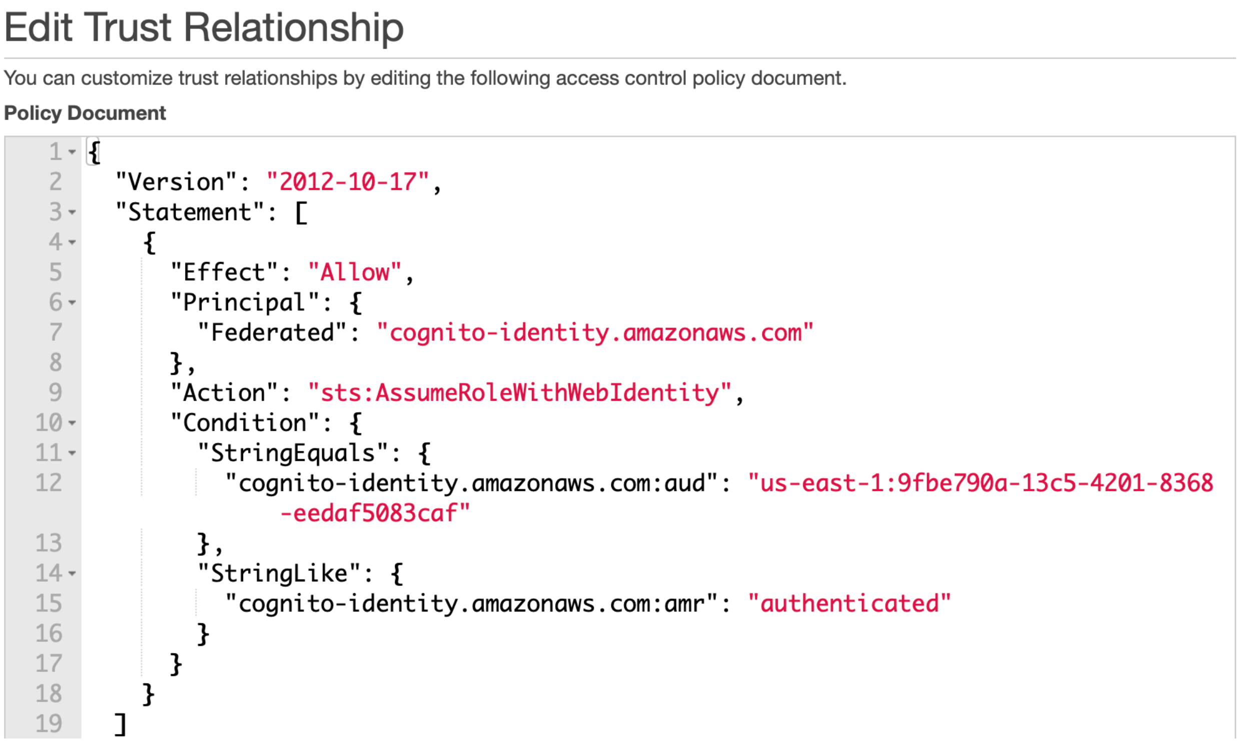
Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy

Filter policies sales Showing 1 result

		Policy name	Used as
☑	▸	SalesClaimsPolicy	*None*

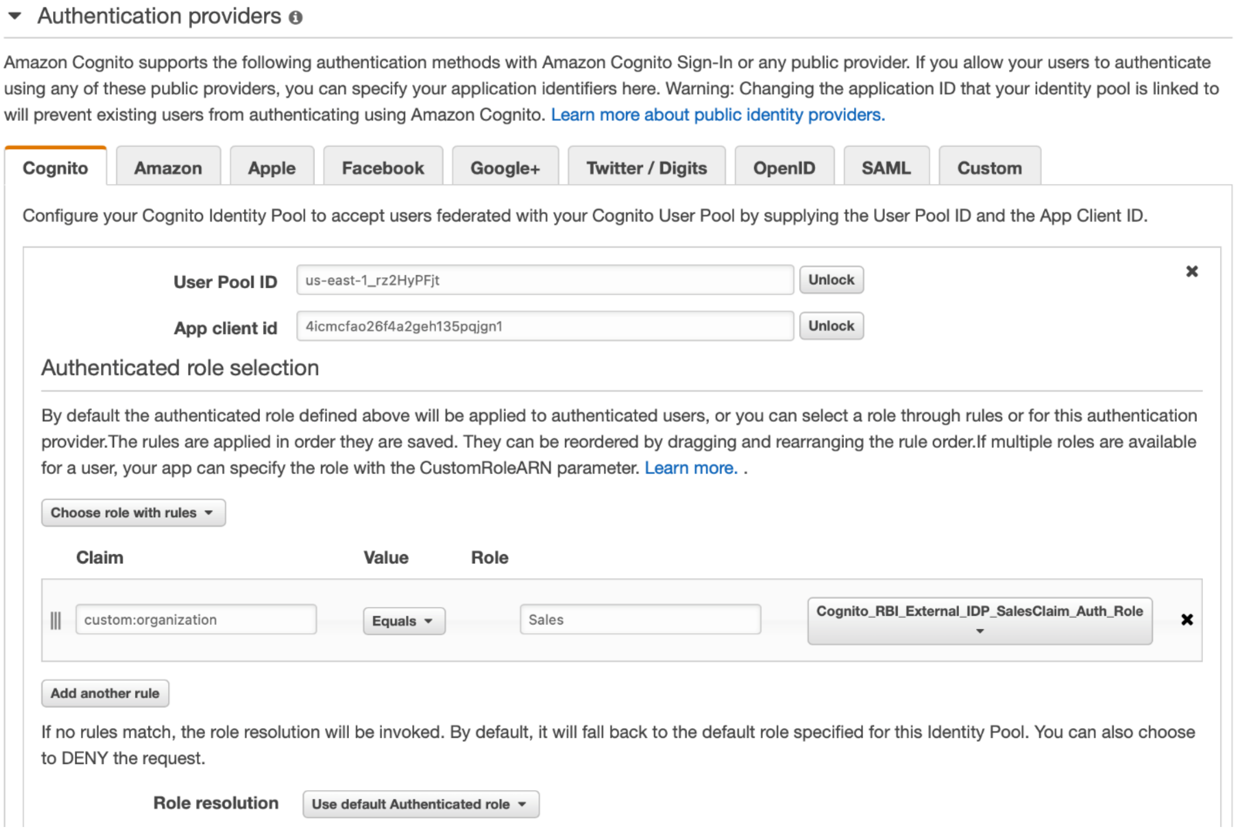


Edit Trust Relationship

You can customize trust relationships by editing the following access control policy document.

Policy Document

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "cognito-identity.amazonaws.com"
      },
      "Action": "sts:AssumeRoleWithWebIdentity",
      "Condition": {
        "StringEquals": {
          "cognito-identity.amazonaws.com:aud": "us-east-1:9fbe790a-13c5-4201-8368-eedaf5083caf"
        },
        "StringLike": {
          "cognito-identity.amazonaws.com:amr": "authenticated"
        }
      }
    }
  ]
```



Authentication providers

Amazon Cognito supports the following authentication methods with Amazon Cognito Sign-In or any public provider. If you allow your users to authenticate using any of these public providers, you can specify your application identifiers here. Warning: Changing the application ID that your identity pool is linked to will prevent existing users from authenticating using Amazon Cognito. Learn more about public identity providers.

Configure your Cognito Identity Pool to accept users federated with your Cognito User Pool by supplying the User Pool ID and the App Client ID.

User Pool ID us-east-1_rz2HyPFjt Unlock

App client id 4icmcfao26f4a2geh135pqjgn1 Unlock

Authenticated role selection

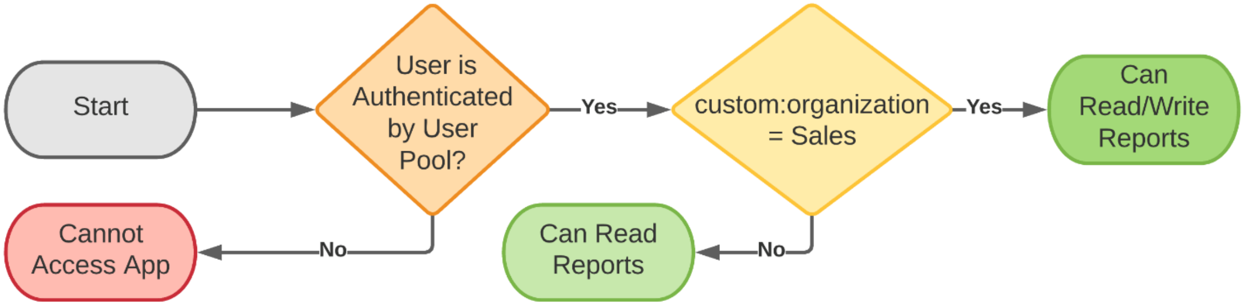
By default the authenticated role defined above will be applied to authenticated users, or you can select a role through rules or for this authentication provider.The rules are applied in order they are saved. They can be reordered by dragging and rearranging the rule order.If multiple roles are available for a user, your app can specify the role with the CustomRoleARN parameter. Learn more. .

Choose role with rules

Claim		Value	Role
custom:organization	Equals	Sales	Cognito_RBI_External_IDP_SalesClaim_Auth_Role

If no rules match, the role resolution will be invoked. By default, it will fall back to the default role specified for this Identity Pool. You can also choose to DENY the request.

Role resolution Use default Authenticated role


Start
User is Authenticated by User Pool?
Yes
custom:organization = Sales
Yes
Can Read/Write Reports
No
Cannot Access App
No
Can Read Reports