Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center
AWS Organizations

Account settings Info

Password policy Info

Configure the password requirements for the IAM users.

Edit

Edit password policy

This AWS account uses the following custom password policy:

Password minimum length
8 characters

Password strength

- Require at least one uppercase letter from the Latin alphabet (A-Z)
- Require at least one lowercase letter from the Latin alphabet (a-z)
- Require at least one number
- Require at least one non-alphanumeric character

Other requirements

- Password expires in 90 day(s)
- Allow users to change their own password
- Prevent password reuse from the past 5 changes

Centralized root access for member accounts Info

Enable

Centralized root access allows you to manage root credentials for your member accounts from the root access management page. You can launch a privileged session into your member accounts to delete root credentials and perform other privileged actions.

Status
Disabled

Security Token Service (STS) Info

STS is used to create and provide trusted users with temporary security credentials that can control access to your AWS resources.

Session Tokens from the STS endpoints

AWS recommends using regional STS endpoints to reduce latency. Session tokens from regional STS endpoints are valid in all AWS Regions. If you use regional STS endpoints, no action is required. Session tokens from the global STS endpoint (https://sts.amazonaws.com) are valid only in AWS Regions that are enabled by default. If you intend to enable a new Region for your account, you can use session tokens from regional STS endpoints or activate the global STS endpoint to issue session tokens that are valid in all AWS Regions.

Global endpoint
Valid only in AWS Regions enabled by default | Change

Regional endpoints
Valid in all AWS Regions

Endpoints (18) Info

You can enable additional endpoints from which you can request temporary credentials. Activate only endpoints you intend to use.

Edit password policy Info

Password policy

- IAM default
  Apply default password requirements.
- Custom
  Apply customized password requirements.

Password minimum length.
Enforce a minimum length of characters.

8 characters

Needs to be between 6 and 128.

Password strength

- [x] Require at least one uppercase letter from the Latin alphabet (A-Z)
- [x] Require at least one lowercase letter from the Latin alphabet (a-z)
- [x] Require at least one number
- [x] Require at least one non-alphanumeric character (! @ # $ % ^ & * ( ) _ + - = [ ] {} | ')

Other requirements

- [x] Turn on password expiration

  Expire password in 90 day(s)

  Needs to be between 1 and 1095 days.
- [ ] Password expiration requires administrator reset
- [x] Allow users to change their own password
- [x] Prevent password reuse

  Remember 5 password(s)

  Needs to be between 1 and 24.

Cancel Save changes

Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center

Password requirements for IAM users are updated.

Account settings Info

Password policy Info

Edit

Configure the password requirements for the IAM users.

This AWS account uses the following custom password policy:

Password minimum length
8 characters

Password strength

- Require at least one uppercase letter from the Latin alphabet (A-Z)
- Require at least one lowercase letter from the Latin alphabet (a-z)
- Require at least one number
- Require at least one non-alphanumeric character

Other requirements

- Password expires in 90 day(s)
- Allow users to change their own password
- Prevent password reuse from the past 5 changes

Centralized root access for member accounts Info

Enable

Centralized root access allows you to manage root credentials for your member accounts from the root access management page. You can launch a privileged session into your member accounts to delete root credentials and perform other privileged actions.

Status
Disabled

Security Token Service (STS) Info

STS is used to create and provide trusted users with temporary security credentials that can control access to your AWS resources.

Session Tokens from the STS endpoints