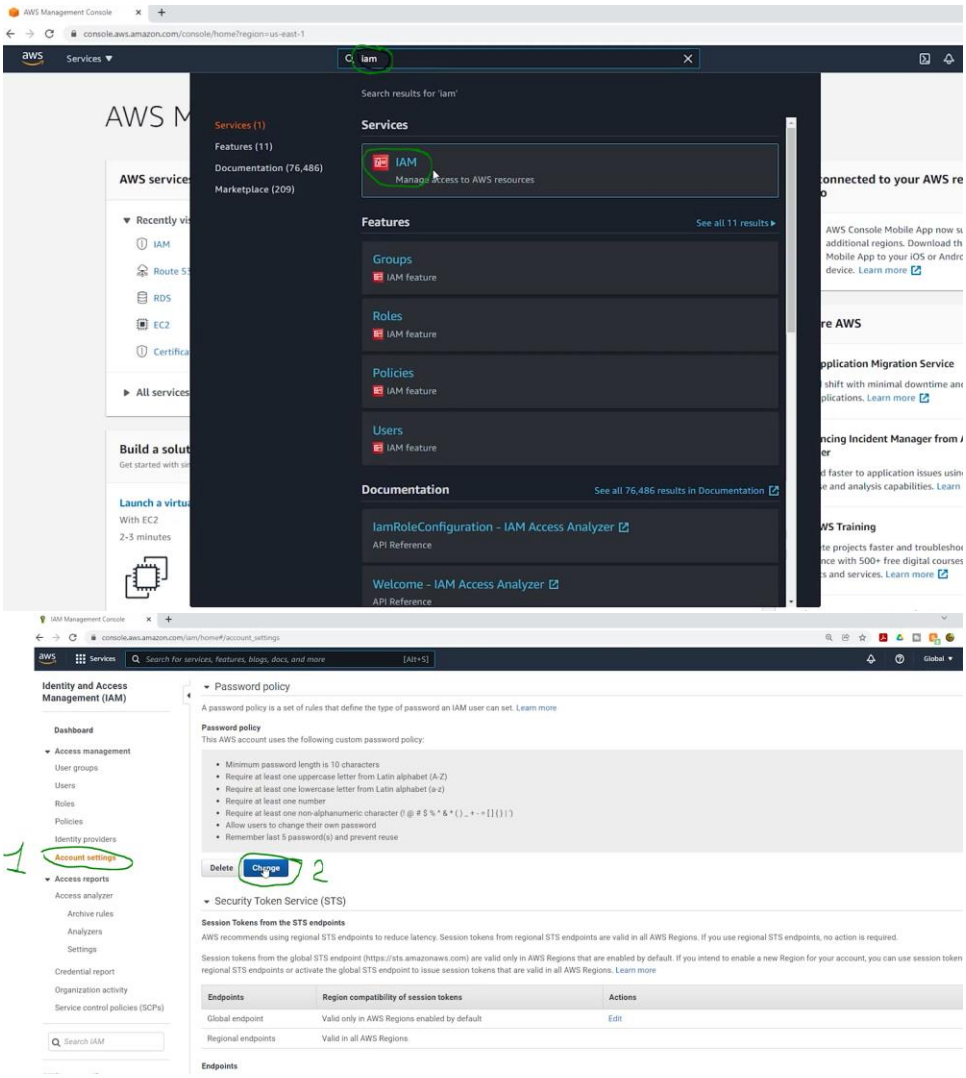
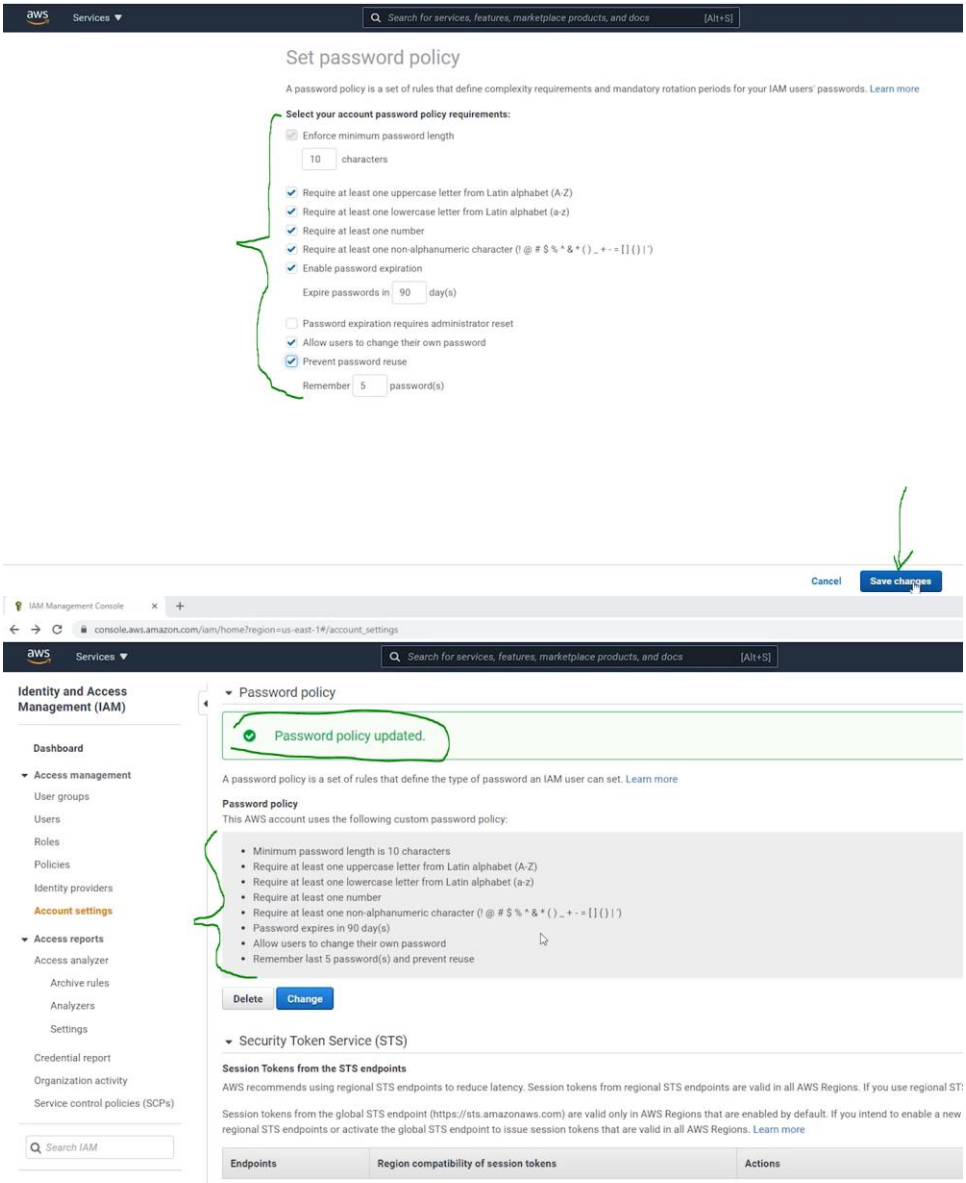

AWS Management Console
console.aws.amazon.com/console/home?region=us-east-1
Services
iam
Search results for 'iam'
Services (1)
Features (11)
Documentation (76,486)
Marketplace (209)
Services
IAM
Manage access to AWS resources
Features
See all 11 results
Groups
IAM feature
Roles
IAM feature
Policies
IAM feature
Users
IAM feature
Documentation
See all 76,486 results in Documentation
IamRoleConfiguration - IAM Access Analyzer
API Reference
Welcome - IAM Access Analyzer
API Reference
IAM Management Console
console.aws.amazon.com/iam/home#/account_settings
Identity and Access Management (IAM)
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
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 custom password policy:
Minimum password length is 10 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
Allow users to change their own password
Remember last 5 password(s) and prevent reuse
Delete
Change
1
2
Security Token Service (STS)
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.
Endpoints
Region compatibility of session tokens
Actions
Global endpoint
Valid only in AWS Regions enabled by default
Edit
Regional endpoints
Valid in all AWS Regions


Services
Search for services, features, marketplace products, and docs [Alt+S]
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
10 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)
Cancel
Save changes
IAM Management Console
console.aws.amazon.com/iam/home?region=us-east-1#/account_settings
Services
Search for services, features, marketplace products, and docs [Alt+S]
Identity and Access Management (IAM)
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Search IAM
Password policy
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 10 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)
Allow users to change their own password
Remember last 5 password(s) and prevent reuse
Delete
Change
Security Token Service (STS)
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 ST
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
regional STS endpoints or activate the global STS endpoint to issue session tokens that are valid in all AWS Regions. Learn more
Endpoints
Region compatibility of session tokens
Actions