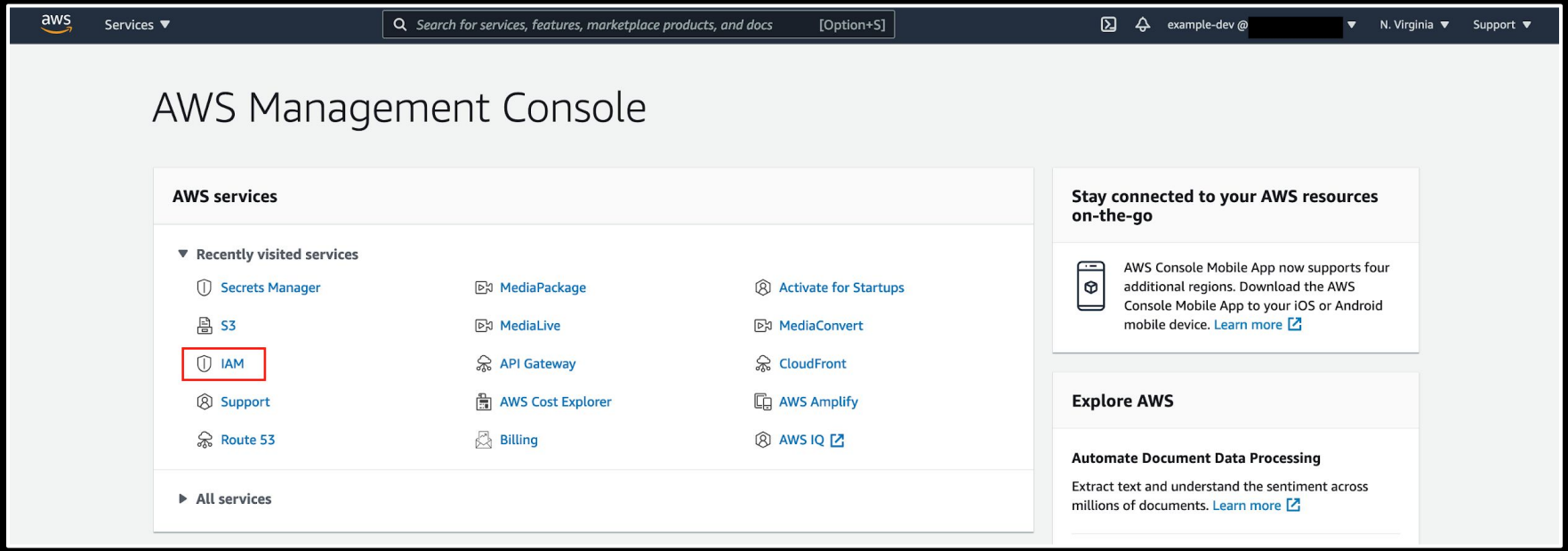
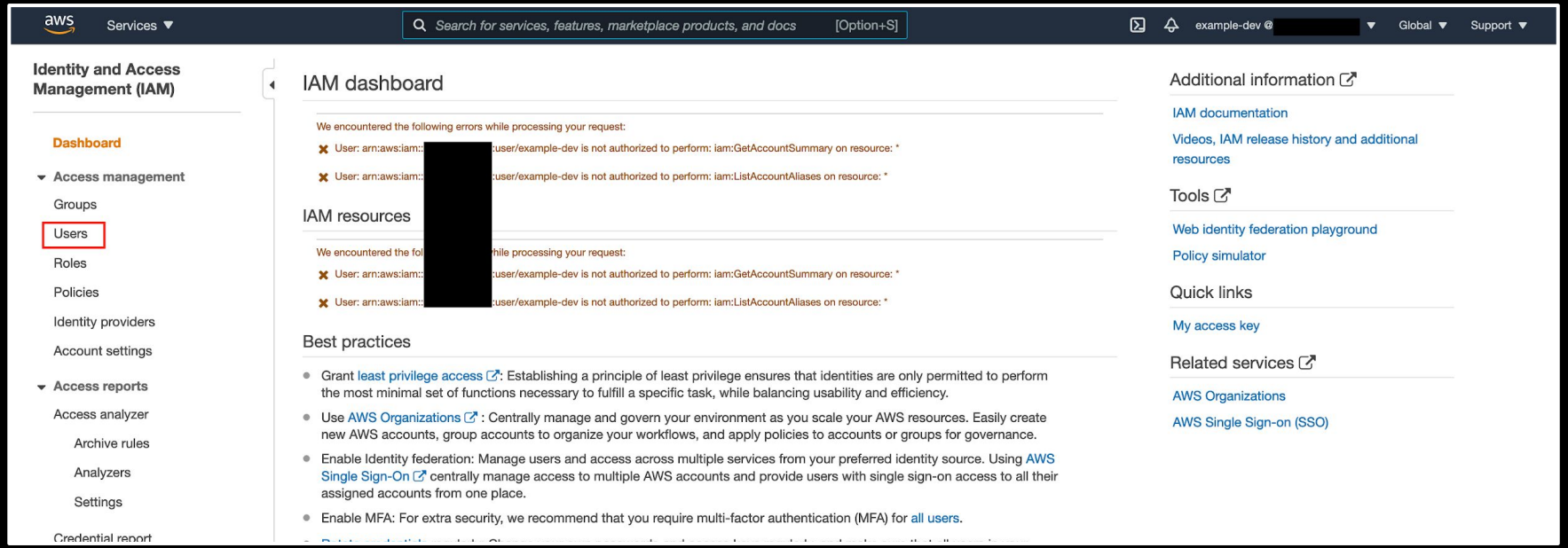
DEVELOPER ONBOARDING

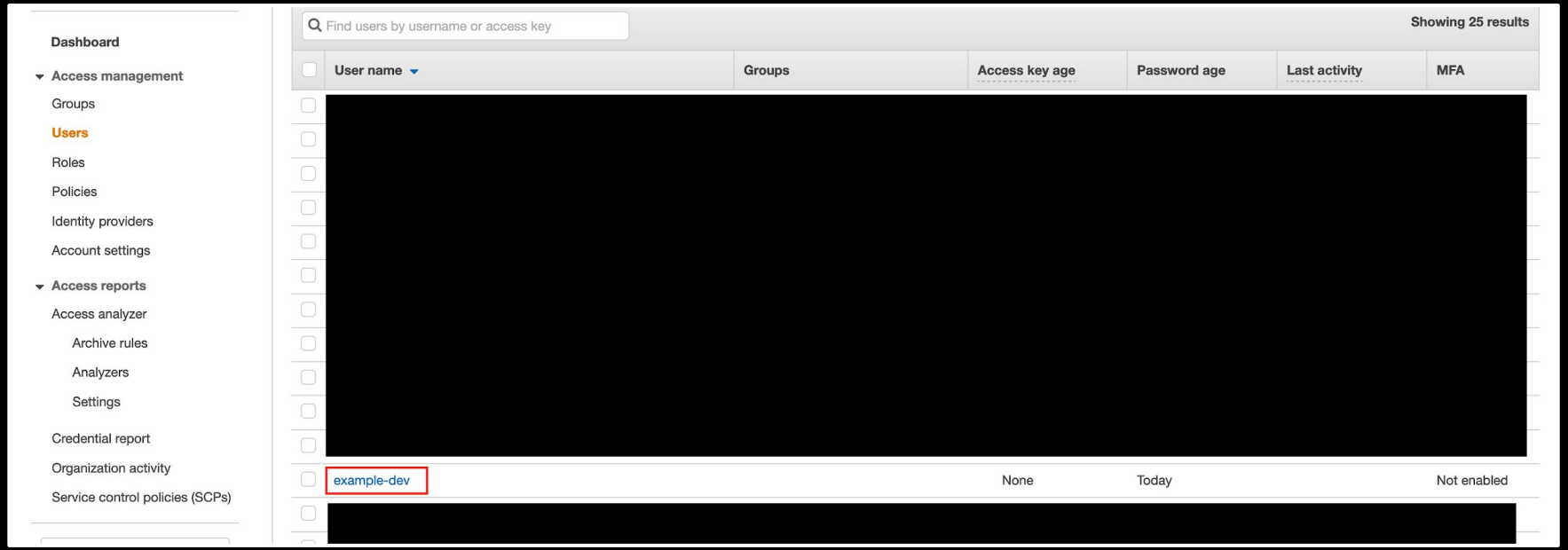
CONFIGURING AWS MFA


aws
Services
Search for services, features, marketplace products, and docs [Option+S]
example-dev @
N. Virginia
Support
AWS Management Console
AWS services
Recently visited services
Secrets Manager
MediaPackage
Activate for Startups
S3
MediaLive
MediaConvert
IAM
API Gateway
CloudFront
Support
AWS Cost Explorer
AWS Amplify
Route 53
Billing
AWS IQ
All services
Stay connected to your AWS resources on-the-go
AWS Console Mobile App now supports four additional regions. Download the AWS Console Mobile App to your iOS or Android mobile device. Learn more
Explore AWS
Automate Document Data Processing
Extract text and understand the sentiment across millions of documents. Learn more

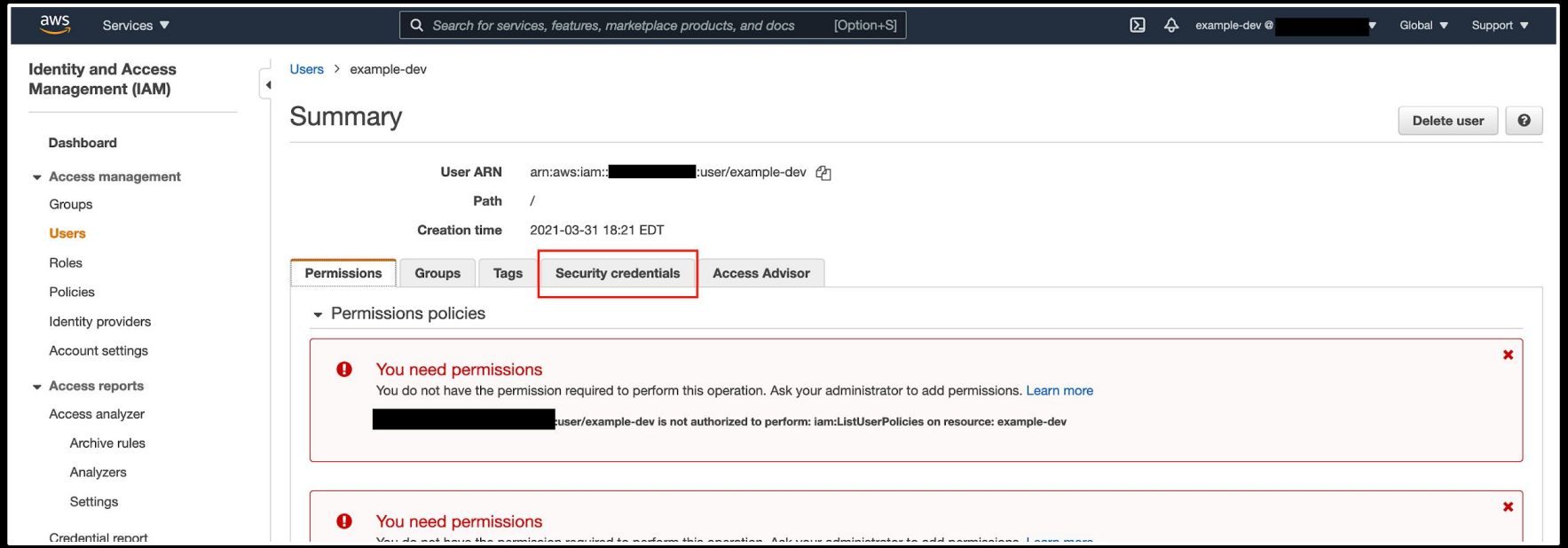
GO TO IAM


aws
Services
Search for services, features, marketplace products, and docs [Option+S]
example-dev @ [redacted]
Global
Support
Identity and Access Management (IAM)
Dashboard
Access management
Groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
IAM dashboard
We encountered the following errors while processing your request:
User: arn:aws:iam::[redacted]:user/example-dev is not authorized to perform: iam:GetAccountSummary on resource: *
User: arn:aws:iam::[redacted]:user/example-dev is not authorized to perform: iam:ListAccountAliases on resource: *
IAM resources
We encountered the following errors while processing your request:
User: arn:aws:iam::[redacted]:user/example-dev is not authorized to perform: iam:GetAccountSummary on resource: *
User: arn:aws:iam::[redacted]:user/example-dev is not authorized to perform: iam:ListAccountAliases on resource: *
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.
Use AWS Organizations : Centrally manage and govern your environment as you scale your AWS resources. Easily create new AWS accounts, group accounts to organize your workflows, and apply policies to accounts or groups for governance.
Enable Identity federation: Manage users and access across multiple services from your preferred identity source. Using AWS Single Sign-On centrally manage access to multiple AWS accounts and provide users with single sign-on access to all their assigned accounts from one place.
Enable MFA: For extra security, we recommend that you require multi-factor authentication (MFA) for all users.
Additional information
IAM documentation
Videos, IAM release history and additional resources
Tools
Web identity federation playground
Policy simulator
Quick links
My access key
Related services
AWS Organizations
AWS Single Sign-on (SSO)

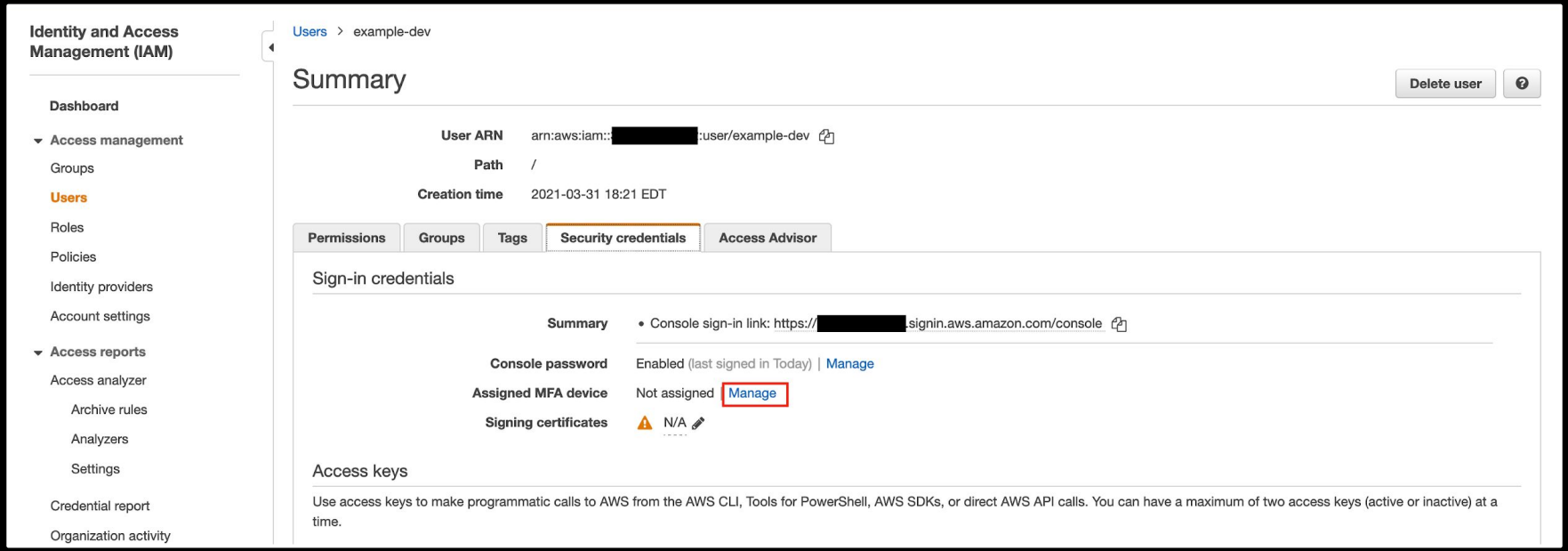
CLICK `USERS`



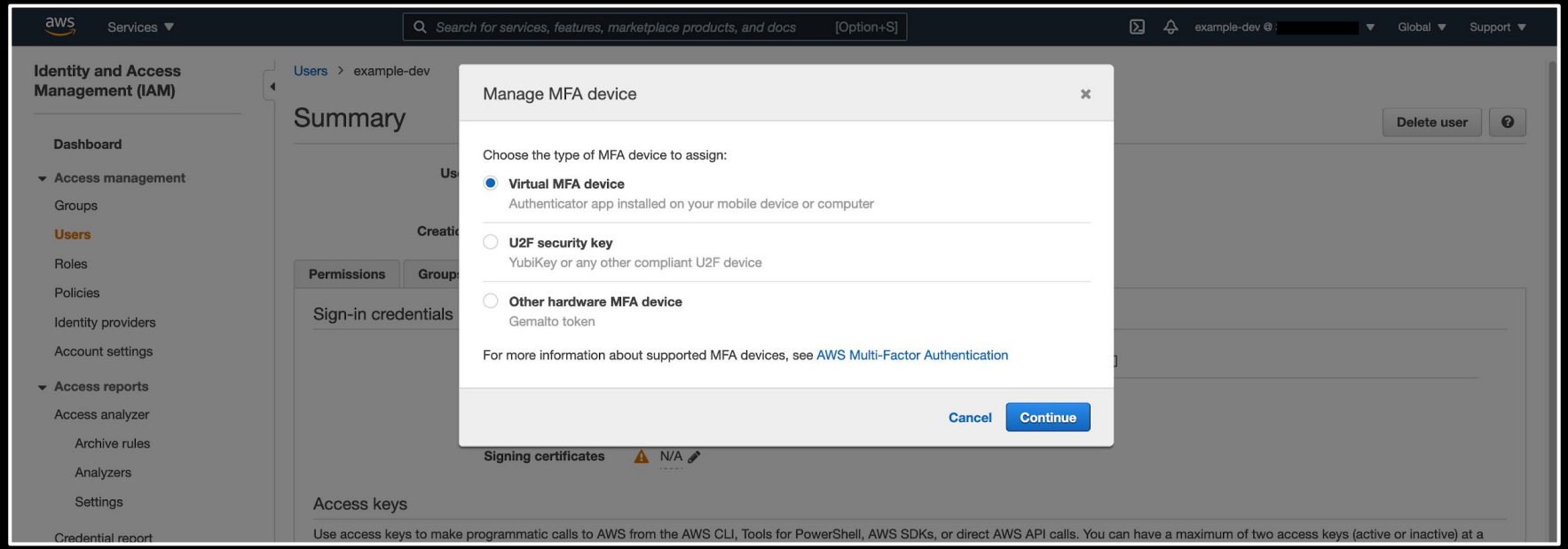
CLICK YOUR USERNAME



CLICK `SECURITY CREDENTIALS`



CLICK `MANAGE` NEXT TO “ASSIGNED MFA DEVICE”



FOLLOW ONSCREEN INSTRUCTIONS TO SETUP MFA.
UPON LOGGING IN, AWS CONSOLE SHOULD BE AVAILABLE WITH YOUR ASSIGNED PERMISSIONS.