


DEVELOPER ONBOARDING

CONFIGURING AWS MFA

 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](#) 

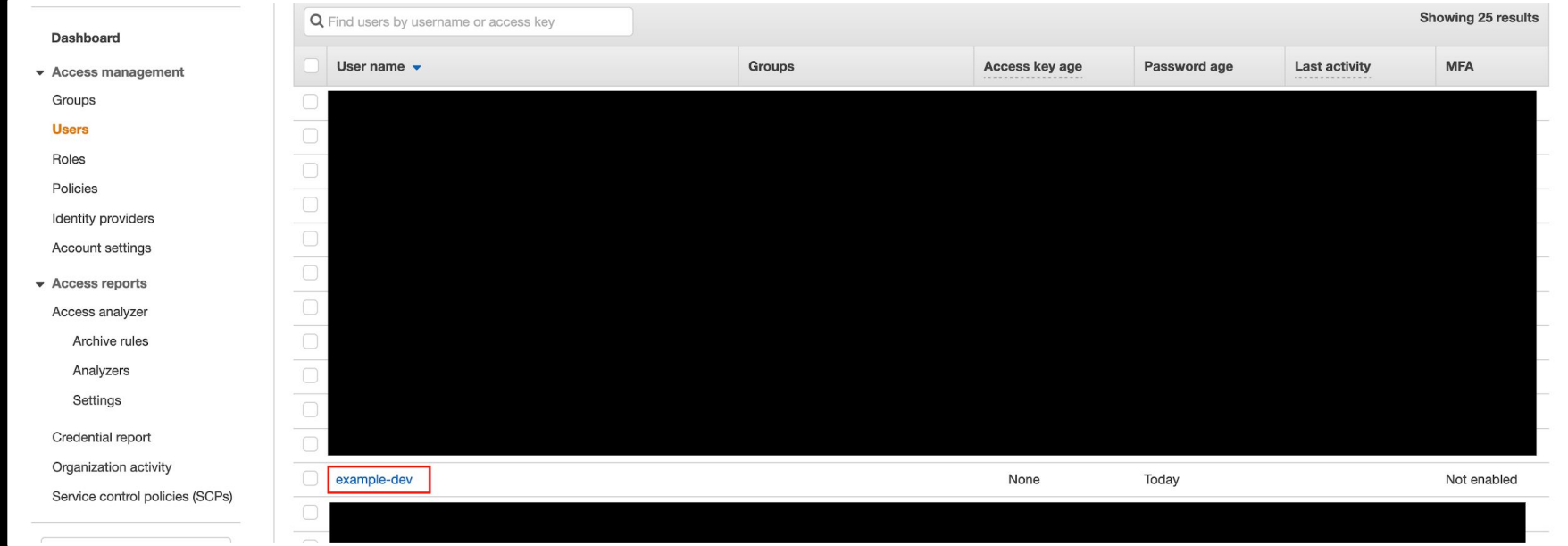
GO TO IAM

The screenshot shows the AWS IAM console interface. The top navigation bar includes the AWS logo, 'Services' dropdown, a search bar with the text 'Search for services, features, marketplace products, and docs' and a '[Option+S]' hint, a notification bell, the user profile 'example-dev @', and 'Global' and 'Support' dropdowns.

The left sidebar is titled 'Identity and Access Management (IAM)' and contains a 'Dashboard' section and two 'Access management' sections. The 'Users' link under 'Access management' is highlighted with a red rectangle.

The main content area is titled 'IAM dashboard' and displays an error message: 'We encountered the following errors while processing your request:'. The error details are partially obscured by a black redaction box. The error messages are: 'User: arn:aws:iam::[redacted]:user/example-dev is not authorized to perform: iam:GetAccountSummary on resource: *' and 'User: arn:aws:iam::[redacted]:user/example-dev is not authorized to perform: iam:ListAccountAliases on resource: *'. Below the error message, there are sections for 'IAM resources', 'Best practices', and 'Additional information'. The 'Best practices' section lists four items: 'Grant least privilege access', 'Use AWS Organizations', 'Enable Identity federation', and 'Enable MFA'. The 'Additional information' section includes links for 'IAM documentation', 'Videos, IAM release history and additional resources', 'Tools', 'Web identity federation playground', 'Policy simulator', 'Quick links', and 'Related services'.

CLICK `USERS`



CLICK YOUR USERNAME

The screenshot shows the AWS Identity and Access Management (IAM) console. The left sidebar contains the navigation menu with 'Users' highlighted. The main content area shows the 'Summary' page for the user 'example-dev'. The 'Security credentials' tab is selected and highlighted with a red box. Below the tabs, there are two error messages under the 'Permissions policies' section, both stating 'You need permissions' and indicating that the user is not authorized to perform the 'iam:ListUserPolicies' action on the resource 'example-dev'.

Identity and Access Management (IAM)

- Dashboard
- Access management
 - Groups
 - Users**
 - Roles
 - Policies
 - Identity providers
 - Account settings
- Access reports
 - Access analyzer
 - Archive rules
 - Analizers
 - Settings
 - Credential report

Users > example-dev

Summary

User ARN arn:aws:iam::[redacted]:user/example-dev

Path /

Creation time 2021-03-31 18:21 EDT

Permissions **Groups** **Tags** **Security credentials** **Access Advisor**

Permissions policies

- You need permissions**
You do not have the permission required to perform this operation. Ask your administrator to add permissions. [Learn more](#)
[redacted]:user/example-dev is not authorized to perform: iam:ListUserPolicies on resource: example-dev
- You need permissions**
You do not have the permission required to perform this operation. Ask your administrator to add permissions. [Learn more](#)

CLICK `SECURITY CREDENTIALS`

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

Organization activity

Users > example-dev

Summary

Delete user

?

User ARN

arn:aws:iam::[REDACTED]:user/example-dev

Path

/

Creation time

2021-03-31 18:21 EDT

Permissions

Groups

Tags

Security credentials

Access Advisor

Sign-in credentials

Summary

• Console sign-in link: [https://\[REDACTED\].signin.aws.amazon.com/console](https://[REDACTED].signin.aws.amazon.com/console)

Console password

Enabled (last signed in Today) | [Manage](#)

Assigned MFA device

Not assigned [Manage](#)

Signing certificates

N/A

Access keys

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

CLICK `MANAGE` NEXT TO "ASSIGNED MFA DEVICE"

The screenshot shows the AWS IAM console interface. On the left is a navigation sidebar with sections like 'Identity and Access Management (IAM)', 'Access management', 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings', 'Access reports', 'Access analyzer', 'Archive rules', 'Analyzers', 'Settings', and 'Credential report'. The main content area is titled 'Users > example-dev' and shows a 'Summary' tab. A modal dialog box titled 'Manage MFA device' is open in the center. It contains the following text: 'Choose the type of MFA device to assign:'. There are three radio button options: 'Virtual MFA device' (selected), 'U2F security key', and 'Other hardware MFA device'. Below these options is a link: 'For more information about supported MFA devices, see [AWS Multi-Factor Authentication](#)'. At the bottom right of the dialog are 'Cancel' and 'Continue' buttons. The background is dimmed, showing parts of the user's page like 'Permissions', 'Group', 'Sign-in credentials', 'Signing certificates', and 'Access keys'.

aws Services ▾

Search for services, features, marketplace products, and docs [Option+S]

example-dev @ ▾ 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

Users > example-dev

Summary

Permissions Group

Sign-in credentials

Signing certificates N/A

Access keys

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

Delete user ?

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](#)

Cancel Continue

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