

Assignment:1

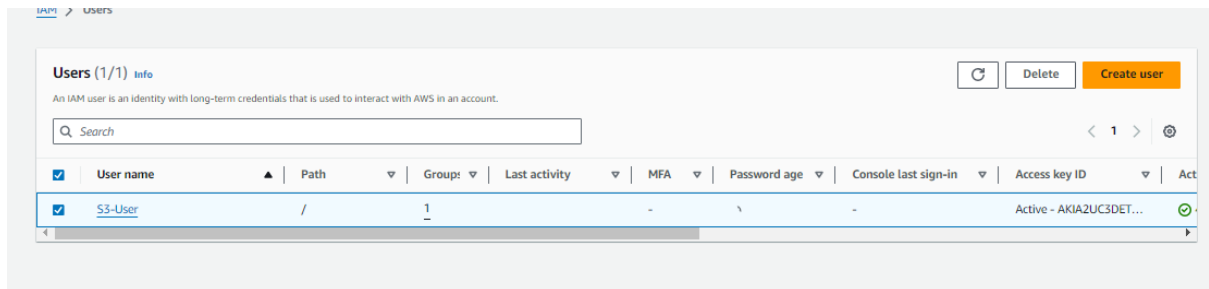
Task:4

Enable Multi-Factor Authentication (MFA) for "S3-User":

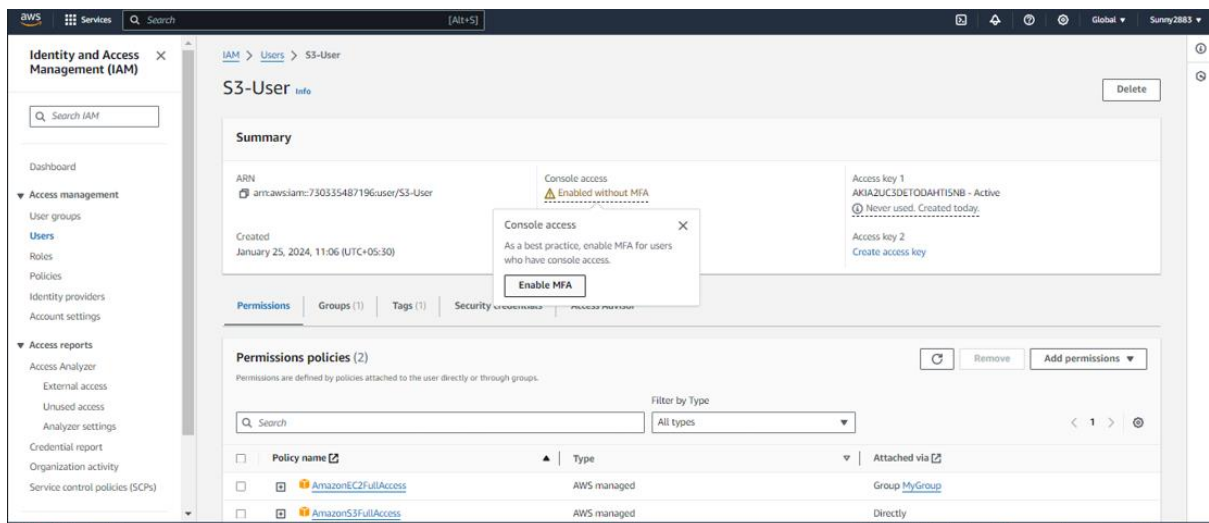
Step:1 Access AWS management console.

Step2: Navigate to IAM.

Step3: Select the user.



Step4: In console access select enable MFA.



Step5: Add MFA device.

Enter Device name and select the type of MFA device.

The screenshot shows the AWS IAM console interface. The breadcrumb trail is IAM > Users > SS-User > Assign MFA device. The left sidebar shows 'Step 1: Select MFA device' and 'Step 2: Set up device'. The main content area is titled 'Select MFA device' with an 'info' icon. It contains a form for 'MFA device name' with a text input field and a description: 'Enter a meaningful name to identify this device. Maximum 128 characters. Use alphanumeric and * , . , @ , - , _ characters.' Below this is a section titled 'MFA device' with the instruction: 'Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.' There are two radio button options: 'Authenticator app' (selected) and 'Security Key'. The 'Authenticator app' option has a description: 'Authenticate using a code generated by an app installed on your mobile device or computer.' The 'Security Key' option has a description: 'Authenticate using a code generated by touching a YubiKey or other supported FIDO security key.'

Step6: Follow the setup Wizard.

We need to scan a QR code or enter a secret key into an authenticator app.

The screenshot shows the 'Set up device' step of the MFA setup wizard. The breadcrumb trail is IAM > Users > SS-User > Assign MFA device. The left sidebar shows 'Step 2: Set up device'. The main content area is titled 'Set up device' with an 'info' icon. It contains a section titled 'Authenticator app' with the instruction: 'A virtual MFA device is an application running on your device that you can configure by scanning a QR code.' There are three numbered steps: 1. 'Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer. See a list of compatible applications.' 2. A QR code is displayed. To the right of the QR code, it says: 'Open your authenticator app, choose Show QR code on this page, then use the app to scan the code. Alternatively, you can type a secret key. Show secret key.' 3. 'Fill in two consecutive codes from your MFA device.' Below this are two input fields labeled 'MFA code 1' and 'MFA code 2'. At the bottom are three buttons: 'Cancel', 'Previous', and 'Add MFA'.

Step7: After setting up the MFA device we need to enter the code generated by the device and click on add MFA.

This screenshot is a close-up of the 'Set up device' step, focusing on the 'MFA code 1' and 'MFA code 2' input fields. The 'MFA code 1' field is currently empty. The 'MFA code 2' field is also empty. The 'Add MFA' button is highlighted in orange.

Step8: MFA device assigned successfully.

The screenshot shows the AWS IAM console interface. At the top, there's a navigation bar with the AWS logo, service name 'Services', search bar, and account information. The main header reads 'Identity and Access Management (IAM)'. A left-hand sidebar contains various navigation links like Dashboard, Access management, User groups, Users, Roles, Policies, Identity providers, Account settings, Access reports, Access Analyzer, External access, Unused access, Analyzer settings, Credential report, Organization activity, and Service control policies (SCPs). The main content area has a green banner at the top stating 'MFA device assigned' with instructions. Below this, a table lists MFA devices. In this case, one device is listed with its ARN, console access status, and two active keys. Navigation tabs below the table include Permissions, Groups (1), Tags (1), Security credentials (selected), and Access Advisor. Under 'Security credentials', the 'Console sign-in' tab is active, displaying the sign-in URL, password update info, and last sign-in status. At the bottom, there are buttons for 'Remove', 'Revoke', and 'Assign MFA device', along with a footer containing copyright and policy links.

| MFA device assigned | | |
|---|---|---|
| You can register up to 8 MFA devices of any combination of the currently supported MFA types with your AWS account root and IAM user. With multiple MFA devices, you only need one MFA device to sign in to the AWS console or create a session through the AWS CLI with that user. | | |
| Summary | | |
| ARN arn:aws:iam::730335487196:user/S3-User | Console access Enabled with MFA | Access key 1 AKIAZUCSDETOHAHTISNB - Active <small>ⓘ Never used. Created today.</small> |
| Created January 25, 2024, 11:06 (UTC+05:30) | Last console sign-in <small>ⓘ Never</small> | Access key 2 Create access key |

| Permissions | Groups (1) | Tags (1) | Security credentials | Access Advisor |
|---|------------|--|----------------------|----------------|
| Console sign-in Manage console access | | | | |
| Console sign-in link https://730335487196.signin.aws.amazon.com/console | | Console password Updated 1 hour ago (2024-01-25 11:06 GMT+5:30) Last console sign-in <small>ⓘ Never</small> | | |

Multi-factor authentication (MFA) (1)

Remove Revoke Assign MFA device

© 2024 Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences