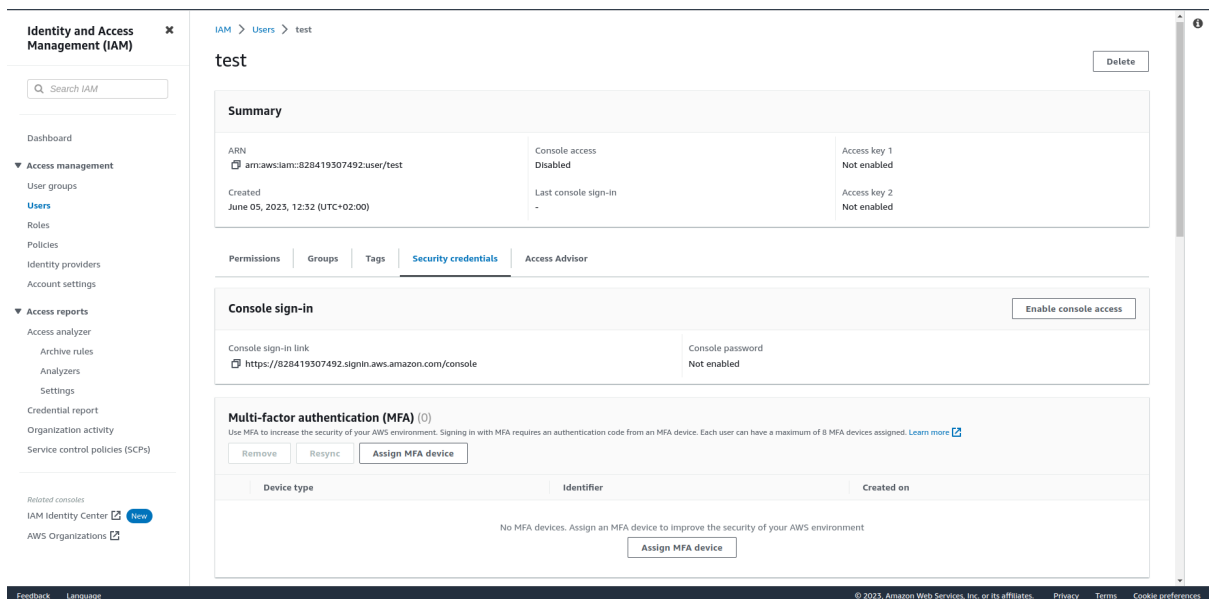


Setup MFA for human IAM users

1. Acquire a supported MFA device: You will need a supported MFA device, such as a hardware key fob or a virtual MFA app, to generate MFA codes. AWS supports a variety of MFA devices, including devices from Gemalto, Yubico, and Google Authenticator.

2. Associate the MFA device with your AWS account: You can associate the MFA device with your AWS account by logging in to the AWS Management Console, navigating to the IAM service, selecting your user, and clicking on the "Security credentials" tab. Then, click on the "Assign MFA Device" button in the "Multi-factor authentication (MFA)" section. Specify a name, choose MFA device, click next and follow further instructions.



The screenshot shows the AWS IAM console interface. On the left is the navigation menu with sections like 'Access management' (Users, Groups, Roles, Policies, Identity providers, Account settings) and 'Access reports'. The main content area is for the user 'test' under the 'Security credentials' tab. It includes a 'Summary' section with details like ARN, console access status, and creation date. Below this is the 'Console sign-in' section with a link to the console and a password status. The 'Multi-factor authentication (MFA)' section shows 0 devices and an 'Assign MFA device' button. At the bottom, there's a message: 'No MFA devices. Assign an MFA device to improve the security of your AWS environment' with an 'Assign MFA device' button.