

Scenario 2 : To ADD MFA to the user.

Get in touch with to provide user an MFA

Step 1: select the **testuser** > security credentials > scroll down to MFA , select Assign MFA device

The screenshot displays the AWS IAM console interface for the 'testuser' user. The left sidebar shows the 'Identity and Access Management (IAM)' navigation menu. The main content area is divided into two sections. The top section, 'testuser info', includes a 'Summary' card with details like ARN, console access status (Enabled without MFA), and a 'Security credentials' tab. The bottom section, 'Multi-factor authentication (MFA) (0)', provides instructions on using MFA and includes an 'Assign MFA device' button. The breadcrumb trail at the bottom indicates the current path: 'IAM > Users > testuser > Assign MFA device'.

This screenshot shows the 'Select MFA device' step in the AWS IAM console. On the left, a progress indicator shows 'Step 1: Select MFA device' as the active step, followed by 'Step 2: Set up device'. The main area is titled 'Select MFA device' and contains two selectable options. The first option is 'Passkey or security key', which involves authenticating using a fingerprint, face, or screen lock. The second option, 'Authenticator app', is selected, indicated by a blue circle and a blue border; it involves authenticating using a code generated by an app on a mobile device or computer.

Select authenticator app > next

Scan the QR from user device and ask for two codes. Once its done MFA is established.

Now whenever user logs in to aws console apart from username and password he needs to enter MFA code also.