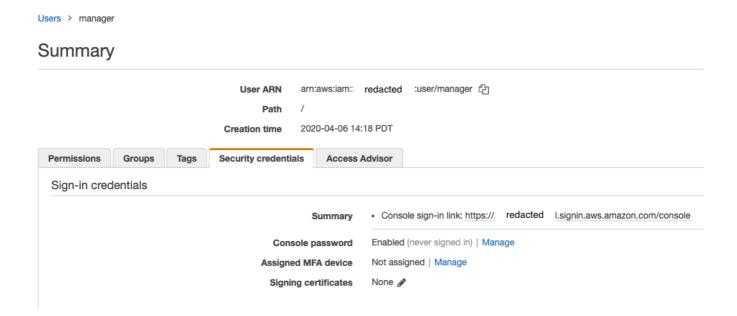
Navigate to the IAM console and select the user you want to secure with MFA (in this series of exercises this would be the manager user).

1. Click on the user account and open the Security Credentials tab



- 2. Click Manage next to the Assign MFA device
- 3. Leave the default Virtual MFA device option on and click continue
- 4. Click the **Show QR code** in the empty square

Set up virtual MFA device	×
Install a compatible app on your mobile device or computer See a list of compatible applications	
2. Use your virtual MFA app and your device's camera to scan the QR code	
Show QR code	
Alternatively, you can type the secret key. Show secret key	
3. Type two consecutive MFA codes below MFA code 1	
MFA code 2	
Cancel Previous Assign M	FA

- 5. Open the Google Authenticator app on your phone and click the Scan a barcode camera icon
- 6. Scan the barcode
- 7. Type the code you see on your phone into the MFA code 1 field
- 8. Wait for the Google Authenticator app to generate the next code
- 9. Type the next consecutive code into the MFA code 2 field and click the Assign MFA button
- 10. Using a new incognito or private browser window to login with this user and the MFA code from your phone

If you have configured MFA correctly you should be able to log in.

If not:

- 1. Log in as the root user
- 2. Proceed to the IAM service console
- 3. Click on Users
- 4. Select the **manager** user
- 5. Visit the Security credentials tab
- 6. Next to Assigned MFA device, click Manage
- 7. Remove the assigned MFA device
- 8. Log out of the root user account
- 9. Log back in with the manager account
- 10. Try again to configure MFA