Identity and Access Management (IAM): Enable Multi-Factor Authentication (MFA)

Lab 1-1 Practices

Get Started

Overview

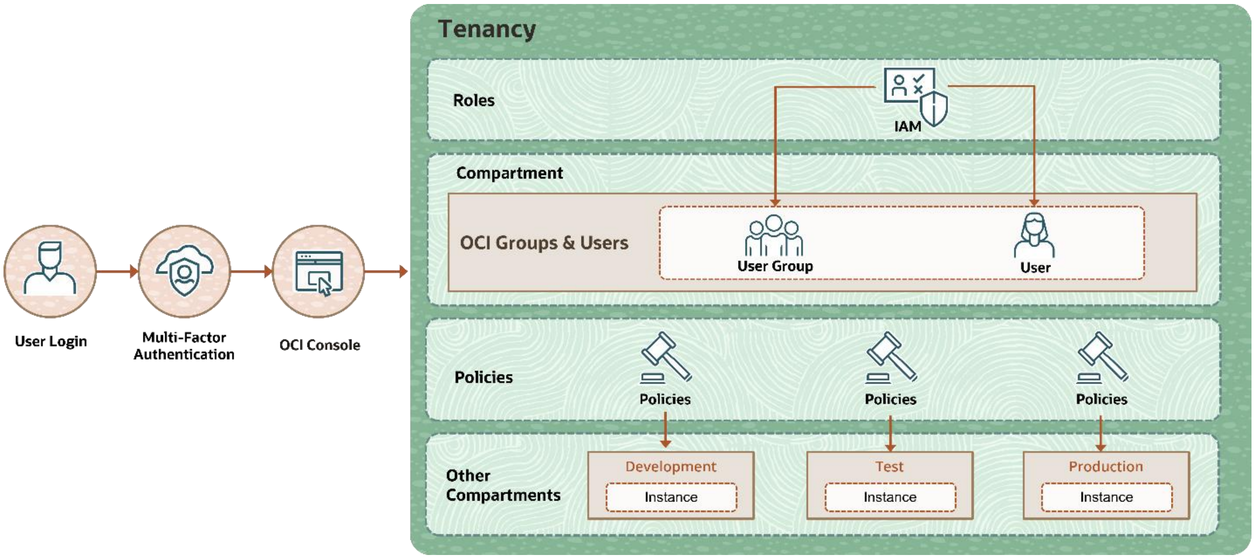
Multi-Factor Authentication (MFA) is a method of authentication that requires the use of more than one factor to verify a user’s identity.

With MFA enabled in the IAM service, a user signs in to the Oracle Cloud Infrastructure (OCI) console and is prompted to enter two factors:

- Their username and password, which are things that they *know*
- A verification code from a registered MFA device, which is something that they *have*

The two factors work together, requiring an extra layer of security to verify the user’s identity and complete the sign-in process.

In this lab, you'll enable Multi-Factor Authentication in OCI.



Note: We have instructions for accounts with and without Identity Domains enabled.

Prerequisites

- You must install a supported authenticator app (Oracle Mobile Authenticator or Google Authenticator) on the mobile device you intend to register for MFA.

Enable Multi-Factor Authentication (With Identity Domains Enabled)

You will learn how to enable Multi-Factor Authentication (MFA) for your Oracle Cloud Infrastructure (OCI) account.

In this practice, you will also learn the sign-in process after enabling MFA.

Tasks:

1. Sign in to the OCI Console.

2. Open the **Main Menu** and select **Identity & Security**. Under **Identity**, click **Domains**. A list of domains in your tenancy appears.

Note: Select the compartment that is allotted to you.

3. Select the domain that is allotted to you. Otherwise, you can click the **Default** domain.

4. In the left navigation pane, navigate to: **Identity domain** > **Security** > **MFA.**

5. Select the **Mobile app passcode** option on the Multi-factor authentication (MFA) settings details page.

6. Click **Save Changes.**

7. Click **Save Changes** on the Save MFA settings popup**.**

8. Use the breadcrumb trail to go back to the **Default Domain** page and click **Groups**.

9. Click **Create Group**.

10. Enter the following:

    a. **Name:** Enter a unique name for the group (e.g.: **MFAGroup**)

    b. **Description:** Enter a group-related description.

11. Click **Create.**

Note: Do not add any user as of now. We will create a new user in the next step.

12. Use the breadcrumb trail to go back to the **Default Domain** page and click **Users.**

13. Click **Create User.**

14. Enter the following:

    a. **First Name:** Enter the first name of the user.

    b. **Last Name:** Enter the last name of the user.

    c. **Username/Email:** Enter an email address for the user.

    d. Select **Use the same email address as the username.** Do not select the **Assign cloud account administrator role** check box.

    e. Select the group that was created in Step 10 (**MFAGroup**).

15. Click **Create**.

16. Use the breadcrumb trail to go back to the **Default Domain** page and click **Security.**

17. Under **Security,** click **Sign-on Policies.**

18. Click **Default Sign-On Policy.**

19. Click **Add Sign-on Rule.**

20. Enter the following:

    a. **Rule Name:** Enter a rule name.

    b. **Group Membership:** Select the group that was created in Step 10 (**MFAGroup**).

    c. Select **Allow Access** under **Actions** (selected by default).

        i. Select **Prompt for an additional factor**.

        ii. Select **Specified factors only**.

        iii. Select **Mobile app passcode**.

        iv. Select **Every time** under Frequency.

        v. Select **Required** under **Enrollment**.

21. Click **Add Sign-on Rule.**

22. Select the **Sign-on Rule** you created just now and click **Edit Priority.**

23. Bring the **Sign-on Rule** on top of the priority list by clicking the up arrow button and click **Save Changes**.

24. Use the breadcrumb trail to go back to the **Default Domain** page and click **Users.**

25. Click the user created in Step 14 and click **Reset Password.**

26. Click **Reset Password** when prompted. You'll receive an email on registered mail address.

27. Log in to the OCI console using credentials generated for MFA-enabled user created in Step 14.

28. The OCI Console will prompt to enable secure verification.

29. Click **Enable Secure Verification.**

30. Follow the instructions in the dialog box:

    a. Install Oracle Mobile Authenticator or a similar authenticator app on your mobile device**.**

    b. Open the app and add a new account. Scan the QR code from the dialog box when prompted.

    c. If you already have another authenticator app installed, select **Offline Mode or Use Another Authenticator App**.

    d. Enter the code displayed by the app.

31. Click **Verify**.

32. Click **Done**.

Important: The authenticator app generates a new, time-based, one-time passcode every 30 seconds. You must enter a code while the code is still valid. If you miss the time window for one passcode, you can enter the next one that is generated.

You have successfully enabled MFA in Identity Domain enabled tenancies.

Enable Multi-Factor Authentication (Without Identity Domains Enabled)

You will learn how to enable Multi-Factor Authentication (MFA) for your Oracle Cloud Infrastructure (OCI) account.

In this practice, you will also learn the sign-in process after enabling MFA.

Tasks

1. Sign in to the Oracle Cloud Infrastructure (OCI) Console by using the Direct Sign-In method.

   Note: If the **Customize your Console** pop-up window appears, select the profiles that best describe your Oracle Cloud Infrastructure work or interests.

2. In the console ribbon at the top of the screen, click the **Profile** icon and click the <*username*> with which you logged in to the OCI Console.
3. On the User Details page, click **Enable Multi-Factor Authentication** to open a dialog box.
4. Follow the instructions in the dialog box:

   a. Install Oracle Mobile Authenticator or a similar authenticator app on your mobile device**.**

   b. Open the app and add a new account. Scan the QR code from the dialog box when prompted.

   c. Enter the code displayed by the app.

5. After you've entered the code into the **Verification Code** box, click **Verify.** Multi-Factor Authentication is now enabled.

6. Click the **Profile** icon at the top right of the screen and click **Sign out.**

7. Sign in to your Oracle Cloud Infrastructure (OCI) Console by using the Direct Sign-In method:

   a. Enter your <*`username`*> in the **User Name** field.

   b. Enter your <*`password`*> in the **Password** field.

   c. Click **Sign In**.

Note: After your username and password are authenticated, you have successfully supplied the first factor for authentication. The second factor appears on an authentication page and prompts you to enter a one-time passcode.

8. Open the Oracle Mobile Authenticator app on your registered mobile device and then open the account for your Oracle Cloud Infrastructure (OCI) tenancy.

9. Enter the passcode displayed by your authenticator app and then click **Sign In**. You are now successfully signed in to the OCI Console.

   Important: The authenticator app generates a new time-based, one-time passcode every 30 seconds. You must enter a code while the code is still valid. If you miss the time window for one passcode, you can enter the next one that is generated.