Microsoft Azure Identity – Practice Exercises

Add custom domain

In this exercise you will register a new domain and then add that domain as a custom domain to Microsoft Azure.

1. Use a registrar to register a test domain for 1 year. Since this is a test, choose an inexpensive registrar and top-level domain (TLD). For example, www.namecheap.com has some domains that you can register for 1 year for $0.88 cents.
3. From the Microsoft Azure dashboard, in the left pane, click More Services.
4. Click Active Directory.
5. Click DOMAINS and then click Add a custom domain.
6. In the Domain Name textbox, type <YourDomainName> where <yourDomainName> is the name of the domain that you registered. Click add.
7. An informational message will state that the domain was successfully added.
8. In the bottom-right corner, click on the right arrow icon to proceed.
9. To verify your domain, add the appropriate TXT record to DNS then click verify.
10. An informational message will state that the domain was successfully verified.
11. Click the check mark in the bottom-right corner to complete the process.
In this exercise you will explore some user and group management tasks using the Azure Portal. You will create a new user, create a new group, and add a user to a group.

1. From the Microsoft Azure Classic Portal, click **Active Directory**.
2. Click **Default Directory**.
3. If a dialog box showcasing the features of Azure Active Directory is displayed, close the window.
4. Once the directory is ready, at the top of the page, click **USERS**.
5. On the bottom of the page, click **ADD USER**.
6. On the first page of the ADD USER wizard, use the following information to complete the form:
   a. **TYPE OF USER**: New user in your organization
   b. **USER NAME**: `<YourUserName> @ <YourDomainName>`
7. In the lower-right corner of the page, click the right arrow icon.
8. On the user profile page, use the following information to complete the form:
   a. **FIRST NAME**: `<YourFirstName>`
   b. **LAST NAME**: `<YourLastName>`
   c. **DISPLAY NAME**: `<YourDisplayName>`
   d. **ROLE**: User
9. In the lower-right corner of the page, click the right arrow icon.
10. Click **create** on the get temporary password page.
11. Note the password.
12. In the lower-right corner of the page, click the checkmark to complete the wizard.
13. Click **GROUPS** at the top of the page.
14. In the middle of the page, click **ADD A GROUP**.
15. In the Add Group wizard, use the following information to complete the form:
   a. **NAME**: `<YourGroupName>`
   b. **GROUP TYPE**: Security
   c. **Description**: `<YourDescription>`
16. In the lower-right corner of the page, click the checkmark to complete the wizard.
17. To add a user to this group, click on the group that you just created.
18. Click **ADD MEMBERS**.
19. The Azure interface will display a list of users. Click the user account that you just created.
20. In the lower-right corner of the page, click the checkmark to complete the wizard.
Enable MFA for admin accounts

In this exercise you will create a new admin account and enable MFA for the account. Note that you can enable MFA in multiple ways. This particular method shows how to do it in the process of creating a new user.

2. From the Microsoft Azure Classic Portal, click Active Directory.
3. Click Default Directory.
4. At the top of the page, click USERS.
5. On the bottom of the page, click ADD USER.
6. On the first page of the ADD USER wizard, use the following information to complete the form:
   - TYPE OF USER: New user in your organization
   - USER NAME: <YourUserName> @ <YourDomain>
7. In the lower-right corner of the page, click the right arrow icon.
8. On the user profile page, use the following information:
   - FIRST NAME: <YourFirstName>
   - LAST NAME: <YourLastName>
   - DISPLAY NAME: <YourDisplayName>
   - ROLE: Global Admin
   - ALTERNATE EMAIL ADDRESS: <YourAlternateEmailAddress>
9. Click the checkbox to enable Multi-Factor Authentication.
10. In the lower-right corner of the page, click the right arrow icon.
11. Click create on the get temporary password page.
12. Note the password.
13. In the lower-right corner of the page, click the checkmark to complete the wizard.
Add second directory

In this exercise you will add a second directory to Azure Active Directory. A second directory can be used to separate administration of directories or to segment portions of a company (such as company divisions).

2. From the Microsoft Azure Classic Portal, in the lower-left corner, click New.
4. Click Directory and then click Custom Create.
5. On the Add Directory wizard, use the following information to complete the form:
   - DIRECTORY: Create new directory
   - NAME: <YourNewDirectoryName>
   - DOMAIN NAME: <YourNewDomain Name>
   - COUNTRY OR REGION: <YourCountryOrRegion>
6. In the lower-right corner of the page, click the checkmark to complete the wizard.
Configuring Advanced Multi-Factor Authentication Settings

In this exercise you will explore multi-factor authentication settings, including advanced settings. As part of this exploration, you will create a new MFA provider and explore the dedicated multi-factor authentication configuration site.

2. From the Microsoft Azure Classic Portal, in the lower-left corner, click New.
4. Click Multi-Factor Auth Provider and then click Quick Create.
5. Create the MFA auth provider with the following information:
   - NAME: <YourAuthProviderName>
   - USAGE MODEL: Per Authentication
   - DIRECTORY: <YourDirectory>
6. Complete the quick create wizard by clicking Create in the lower-right corner of the page.
7. Now, browse to the directory that you associated the MFA Provider to and click USERS.
8. On the USERS page, click Manage Multi-Factor Auth on the bottom of the page.

   **Note:** You will be redirected to the multi-factor authentication (MFA) portal, where you have two management options: manage users and manage service settings. Please note, before enabling an account for MFA, you need to sign in once with the account to update the temporary password that was set when you first created the account. To do this, click on the Display Name of the user account and you will be taken to the Office 365 login page. After you have updated the user password, return to the MFA portal to enable and/or enforce the account for multi-factor authentication.

9. On the multi-factor authentication page, click a non-admin user account and click enable.
10. Confirm your selection and click enable multi-factor auth then click close.
11. On the multi-factor authentication page, click a non-admin user account and click enforce.
12. Confirm your selection and click enforce multi-factor auth then click close.
13. Now, click on the display name of the non-admin user account and log in to Office 365 using the password generated earlier.
14. You should see a note stating that your admin has required that you set up this account for additional security verification.
15. Click **Set it up now.**
16. Under Step 1, use the following information to complete the form:
   - Authentication phone
   - Select your country or region: `<YourCountryOrRegion>`
   - Next to the county field, enter `<YourMobilePhoneNumber>`
   - Under method, click **Send me a code by text message**
17. When your information has been input, click **Contact me.**
18. On the next page, enter the verification code that was sent to you and then click **Verify.**
19. You will see a note about creating an app password. Note this password for future use.
20. Click **Done.**
Creating App Passwords to Secure Devices And Applications

In this exercise you will complete the user setup of an account with MFA and walk through the process of creating an app password to secure an application that doesn't support MFA natively.

2. After securing an account with MFA, log into the account using the Office 365 portal.
3. Once signed in, click on the account name in the upper-right corner of the page and click View account.
4. In the middle of the page, under Security & privacy, click Manage security & privacy.
5. Click Additional security verification and then Update your phone numbers used for account security.
6. At the top of this page, click app passwords.
7. You should see your initial app password that was created when you first signed into your account after MFA was enabled and you completed the verification process for the first time.
8. Click create.
10. Click next.
11. Take note of your new app password and then click close. At this point, you can use the app password in place of your standard password to enable an application to authenticate, even though the app doesn’t support native MFA.