Lab1 Identity- Getting Started with Azure Active Directory

This lab contains four activities. These are shown below:

Pre-requisites

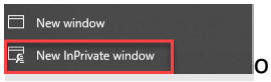
Step 1 – Create Demo Tenant

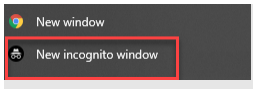
Before you start you should have completed the "Getting started with Labs". If you have not completed this you will not be able to do this lab. You can find this document which you can download from https://aka.ms/secpractice-labs. Each tenant can take up to 24 hours to provision so its important that you complete this prior to when the labs are to be run.

Step 2 – Create yourself an Admin account for your demo tenant

In this task, you will create a Microsoft 365 user account for yourself, and assign your account the Microsoft 365 Global Administrator role, which gives you the ability to perform all administrative functions within Microsoft 365.

Important: As a best practice in your real-world deployments, you should always write down the first global admin account's credentials (in this lab, the MOD Administrator) and store it away for security reasons. This account is a non-personalized identity that owns the highest privileges possible in a tenant. It is **not** MFA activated (because it is not personalized) and the password for this account is typically shared among several users. Therefore, this first global admin is a perfect target for attacks, so it is recommended to create personalized service admins and keep as few global admins as possible. For those global admins that you do create, they should each be mapped to a single identity, and they should each have MFA enforced.

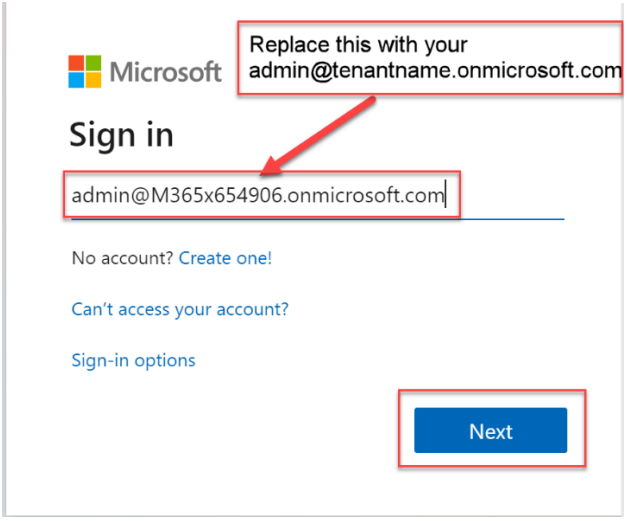
a) Open an In-private browser (Edge) 

or New in-Cognito (Chrome) 

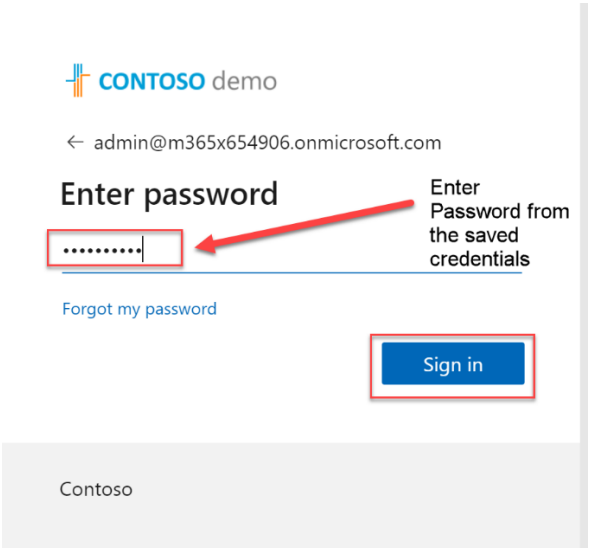
on your machine and then go to https://admin.microsoft.com/

b) Enter the admin account username that you saved in "Getting started with Microsoft Labs" to gain credentials.

c) Enter your admin credentials in the sign in as below and click NEXT



d) Enter the password and then click "Sign in"



1. In the **Microsoft 365 admin center**, in the left navigation pane, select **Users** and then select **Active users**.

2. In the **Active users** list, you will see the default **MOD Administrator** account as well as some other user accounts.

3. In the **Active Users** window, select **Add a user**.

4. In the **Set up the basics** window, enter the following information:

- First name: **Your First Name**
- Last name: **Your Last Name**
- Display name: When you tab into this field, **YOUR NAME** will appear.
- Username: When you tab into this field, **YOURFIRSTNAME-LASTNAME** may appear; if not enter this as the username

  IMPORTANT: To the right of the **Username** field is the domain field. select the **M365xZZZZZZ.onmicrosoft.com** cloud domain

  After configuring this field, **YOUR username** should appear as:

  YOURNAME@M365xZZZZZZ.onmicrosoft.com
- Password settings: select the **Let me create the password** option
- Password: **Set your own complex Password**
- Uncheck the **Require this user to change their password when they first sign in** checkbox.

5. Select **Next**.
6. In the **Assign product licenses** window, enter the following information:
   - Select location: **United States (Your Location)**
   - Licenses: Under **Assign user a product license**, select **Office 365 E5** and **Enterprise Mobility + Security E5** or if you have **Microsoft 365 E5** select this instead.

Please note – if you have no licenses available in the tenant, please free up a license by unassigning one from different user.

7. Select **Next**.
8. In the **Optional settings** window, in the Roles section select **Admin center access** By doing so, all the Microsoft 365 administrator roles are now enabled and available to be assigned.
9. Select **Global Admin** and then select **Next**.
10. On the **Review and finish** window, review your selections. If anything needs to be changed, select the appropriate **Edit** link and make the necessary changes. Otherwise, if everything is correct, select **Finish adding**.

11. Once your new username **has been added to active users** page, select **Close.**

Part 1 Deploy Azure AD Self-Service Password Reset

This section demonstrates how to deploy Self-service password reset (SSPR). SSPR is an Azure Active Directory feature that enables employees to reset their passwords without needing to contact IT staff. Employees must register for or be registered for self-service password reset before using the service. During registration, the employee chooses one or more authentication method enabled by the organization.

How SSPR Works

- When a user attempts to reset a password, they must verify their previously registered authentication method or methods to prove their identity.
- The user then enters a new password.
    - For cloud-only users, the new password is stored in Azure Active Directory.
    - For hybrid users, *with writeback enabled*, the password is written back to the on-premises Active Directory via the Azure AD Connect service.

Authentication Methods

If SSPR is enabled, you must select at least one authentication method option. You may also hear these options referred to as "gates". We highly recommend that you choose two or more authentication methods for more flexibility and a better user experience.

Note: Users can only reset their password if they have data present in the authentication methods that their administrator has enabled.

Combined Registration Experience

Before combined registration, users registered authentication methods for Azure Multi-Factor Authentication and self-service password reset (SSPR) separately. People were confused that similar methods were used for Multi-Factor Authentication and SSPR but they had to register for both features. Now, with combined registration, users can register once and get the benefits of both Multi-Factor Authentication and SSPR.

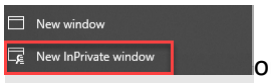
Note: Combined security information registration for Multi-Factor Authentication and Azure Active Directory (Azure AD) self-service password reset is a public preview feature of Azure AD.

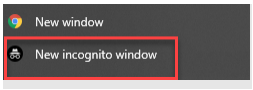
Configure Self-service password reset (SSPR) for user accounts in Azure AD

Scenario

The Help Desk has indicated that a large number of support tickets are related to password resets. You have been asked to setup a way for a group of users to reset their password on their own.

Task 1: self-service password reset

1. Open an In-private browser (Edge) 

or New in-Cognito (Chrome) 

on your machine and open Azure by going to (https:/portal.azure.com). Login as Your Admin account your created in the pre-requisites. Navigate to **Azure Active Directory**

2. In the **Manage** pane under select **Groups**.

3. Select **+NewGroup**. On the Choose a Group type - Select **Security**

4. Name the group **SSPR,** add a description **"Used to allow users access to SSPR".**

5. **Leave the other boxes as default.**

6. Under **Members –** Click on the **No Members Selected**

7. In the search box enter **Allan. Select Allan Deyoung.**

8. Also add **Bianca.**

9. Click **Create**

10. In the navigation pane under **Manage** select **Users**, then select **Password reset**.

11. In the **Password reset | Properties** window, select **Group** and choose the new group you just created **SSPR** to enable self-service password reset to all users. Select **Save**.

12. On the **Password reset | Properties** blade, select **Authentication methods**.

13. For the methods available to users, ensure that **Mobile Phone (SMS only)** and **Email** are selected, and then select **Security Questions**.

14. For the **Number of questions required to register**, select **3**.

15. For the **Number of questions required to reset**, select **3**.

16. In the **Select security questions** section, select **No security questions configured**, then select **Predefined**. Select three questions of your choice, and then select **OK** twice.

17. Select **Save**.

18. Select **Registration** Select **No** for **Require users to register when signing in**, and the select **Save**.

Task 2: Test self-service password reset

1. You will need a Test account for this section. Prior to doing this you will need to reset the password for Allan Deyoung. Go to https://portal.azure.com/. Navigate to **Azure Active Directory**
2. Select Users –from the Menu. Find Allan Deyoung and select the account by adding a tick next to his name. Select the Reset Password button in the Menu pane.
3. Select **Reset password** option. Save a copy of the password as you will need it for next steps.
4. In Microsoft Edge at the upper right of the page, select your account name, and then select **Sign in with a different account**.

5. Sign in as **AllanD@yourtenant.onmicrosoft.com** with the password that was assigned in step 3 above

6. Browse to **https://myapps.microsoft.com**.

7. On the **Microsoft** page, select on the **Allan** account in the top right corner, and then select **Profile**.

8. Select **Set up self service password reset**.

9. On the **confirm your current password** page, if it appears, select **re-enter my password**, enter the password you reset and select **Sign in**.

10. On the **don't lose access to your account** page, select **Set it up now** for the **Authentication Phone** option.

11. Choose your **country or region**, type your **mobile phone number**, and then select **text me**. *(you will need to use your own phone for this)*

12. Type the number that you receive in a text message in the text box below, and then select **verify**.

13. Select **Set it up now** for the **Authentication Email** option. Type your email address that you easily access. Select **email me**.

Note: you will need to use an e-mail address other than the tenant domain provided for this lab.

14. Sign in to your email account, read the code, type it in the verification field, and then select **Verify**.

    Note: If you don't find a message with a code in your inbox, check the junk folder.

15. On the line for **Security Questions are not setup**, select **Set it up now**. Choose the three security questions and enter in any answer. Select **Save answers**.

16. On the **don't lose access to your account!** page, select **Finish**.

17. On the **Microsoft** page, select on the **Allan** account, and then select **Profile**.

18. In the portal, select **Change password**.

19. On the **change password** page, in the **Old password** text box, type Allan's password as you entered then **Create new password** and the **Confirm new password** text boxes, type **NewPasswordofYourChoice** and then select **Submit**.

20. Wait until the Microsoft Azure profile portal appears, and then close the Microsoft Edge browser window.

Part 2 - Deploy Cloud-based Azure Multi-Factor Authentication (MFA)

This section demonstrates how to deploy Azure Multi-Factor Authentication in your environment.

How MFA Works

The security of two-step verification lies in its layered approach. Compromising multiple authentication factors presents a significant challenge for attackers. Even if an attacker manages to learn the user's password, it is useless without also having possession of the additional authentication method. It works by requiring two or more of the following authentication methods:

- Something you know (typically a password)
- Something you have (a trusted device that is not easily duplicated, like a phone)
- Something you are (biometrics)

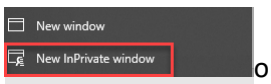
Azure Multi-Factor Authentication (MFA) helps safeguard access to data and applications while maintaining simplicity for users. It provides additional security by requiring a second form of authentication and delivers strong authentication via a range of easy to use authentication methods. Users may or may not be challenged for MFA based on configuration decisions that an administrator makes.

Azure Multi-factor Authentication is deployed by enforcing policies with Conditional Access. A Conditional Access policy can require users to perform multi-factor authentication when certain criteria are met.

Scenario

You need to enable MFA for your customers.

Task 1: Choosing Verification methods

1. Open an In-private browser (Edge) 

or New in-Cognito (Chrome) 

on your machine and open Azure by going to (https:/portal.azure.com). Login as Your Admin account your created in the pre-requisites. Navigate to **Azure Active Directory**
2. In the **Manage** pane under select **Users**
3. Select **Multi-Factor Authentication** located in the top menu. Depending on the size of your screen, this option may be located under …More. **This should launch a new multi-factor authentication | users and settings window**
4. Under Multi-Factor Authentication, select **Service Settings**

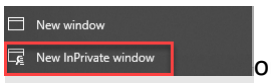
5. In the **Service Settings page**, under verification options, select
   - *Text message to phone*
   - *Notification through mobile app*
   - **Uncheck** the Verification code from mobile app or hardware token
6. Click **Save** if prompted, click **Close.** Click **x** to close the multi-factor auth settings browser tab and return to the Azure Portal.

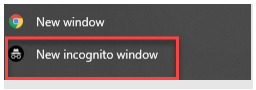
Note: You can choose the verification methods that are available for your users. When your users enroll their accounts for Azure Multi-Factor Authentication, they choose their preferred verification method from the options that you have enabled. The options we have selected are for the purpose of this lab only. For an enterprise wide deployment we recommend Notification through Mobile App (Microsoft Authenticator) and Verification code from mobile app (Microsoft Authenticator) or hardware token

Note: Before starting a deployment of Azure Multi-Factor Authentication, there are prerequisite items that should be considered Please visit aka.ms/deploymentplans for detailed deployment guidance.

Part 3- Enabling Multi-Factor Authentication with Conditional Access

To plan your Conditional Access policy strategy, which will determine when MFA and other controls are required, refer to *What is Conditional Access in Azure Active Directory*?

1. Open an In-private browser (Edge) 

or New in-Cognito (Chrome) 

on your machine and open Azure by going to (https:/portal.azure.com). Login as Your Admin account your created in the pre-requisites. Navigate to **Azure Active Directory**
2. In the **Manage** pane under select **Security**
3. On the **Security - Getting started** page, under **Protect** in the left navigation menu, click **Conditional Access**.
4. **Select + New policy**
5. In the Name textbox enter: **MFA Pilot Rollout**
6. Under Assignments, click **Users and group**s, this will expand the users and groups blade.
7. On the **Include tab**, and select the Select **users and groups** radio button
8. Select the Users and groups checkbox.
9. Click the **Select** box to expand the group search blade
10. Enter: **SSPR**
11. Select the **SSPR group** and verify that it is listed under **Selected Members**.
12. Click the **Select** button
13. Under **Assignments**, click **Cloud apps or actions** This will expand the cloud apps or actions blade.
14. Select the **All Cloud apps** radio button
15. Skip the Conditions section
16. Under **Access Controls**, click **Grant Access**, this will expand the cloud apps or actions blade.
17. Check the box for **Require multi-factor authentication** and then click Select
18. Skip the Session section
19. Set the **Enable policy toggle to On**
20. Click **Create**

You have now enabled multi-factor authentication with conditional access, congratulations!

Part 4- Validating the End-User Experience

If your organization is using Azure Active Directory Identity Protection, we recommend configuring the MFA registration policy to prompt your users to register the next time they sign in interactively.

If your organization does not have licenses that enable Identity Protection, users are prompted to register the next time that MFA is required at sign-in.
It's important to get all users registered so that bad actors cannot guess the password of a user and register for MFA on their behalf, effectively taking control of the account.

Task 1 – Reset Bianca's password

1. You will need a Test account for this section. Prior to doing this you will need to reset the password for Bianca. Go to https://portal.azure.com/. Navigate to **Azure Active Directory**
2. Select Users –from the Menu. Find **Bianca Pisani** and select the account by adding a tick next to her name. Select the Reset Password button in the Menu pane.
3. Select **Reset password** option. Save a copy of the password as you will need it for next steps.

Task 2 - Registering user MFA methods

1. Navigate to the task bar and right click the Edge icon, select **New InPrivate Window**

2. Browse to **https://myapps.microsoft.com**.

3. Sign in as Biancap@yourtenant.onmicrosoft.com with the password that was assigned in step 3 above
4. On the **More Information Required** page, click **Next**. At this point, you will be prompted to setup your multi-factor method.
5. **Enter a 10-digit phone number** you are able to receive notifications on and click **Next**.
6. Enter the 6 digit SMS code *sent to the number you entered in the previous step*, click **Next**
7. You should see a **SMS verified successfully** confirmation , Click **Next**
8. Click **Done**
9. Sign out and click the **x** to close the browser tab.

The end user has now registered his/her MFA method.

Note: This registration step is required upon the very first sign-in. Subsequent sign-ins will only require MFA based on the conditional access policy you have configured.
Note: You can choose the verification methods that are available for your users. When your users enroll their accounts for Azure Multi-Factor Authentication, they choose their preferred verification method from the options that you have enabled. The options we have selected are for the purpose of this lab only. For an enterprise wide deployment we recommend Notification through Mobile App (Microsoft Authenticator) and Verification code from mobile app (Microsoft Authenticator) or hardware token

Task 4 - User Log-in Experience

1. Navigate to the task bar and right click the **Edge** icon, select **New InPrivate Window**
2. Navigate to https://myapps.microsoft.com
3. Sign in as **BiancaP@yourtenant.onmicrosoft.com** and click **Next**,
4. Enter the 6 digit SMS code *sent to the number you entered during the registration step*, click **Verify**
5. Stay signed in? Select **No**

Your user should now be signed in to the MyApps portal and able to access their resources.

In this section, you have walked through the user registration and sign-in experience.

When your users enroll their accounts for Azure Multi-Factor Authentication, they choose their preferred verification method from the options that you have enabled.

Please note that the options we have selected are for the purpose of this lab only. For an enterprise wide deployment we recommend

- Notification through mobile app (Microsoft Authenticator) and
- Verification code from mobile app (Microsoft Authenticator) or hardware token as authentication methods.

End lab

Thank you for taking the time to complete this lab, we hope you enjoyed it.

Please visit https://aka.ms/secpractice-labs to access further labs.