

# **PROJECTS**

NAME: PIYUSH RAJ

COLLEGE: MANIPAL UNIVERSITY JAIPUR

INTERN ID: CT\_CSI\_CI\_4066

## **1)Configure & manage Azure Multifactor Authentication (MFA):-**

- **Sign in to the Azure portal:**

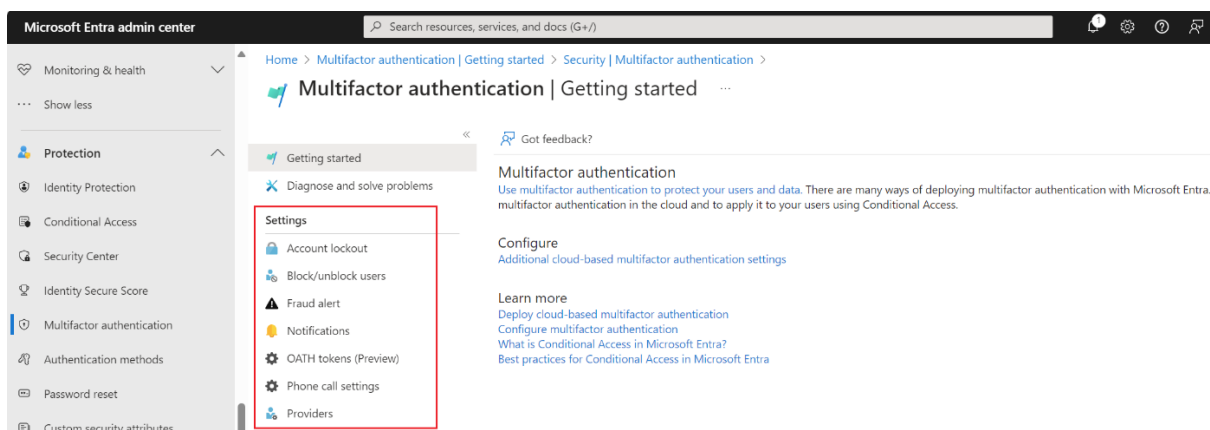
- Go to Azure portal

- **Navigate to Azure Active Directory:**

- In the left-hand navigation pane, click on "Azure Active Directory".

- **Set up MFA:**

- Select "Security" then "Multifactor authentication".
- Click on "Additional cloud-based MFA settings".
- Enable and configure the required MFA settings.



## **2) Two Factor authentication**

Two-factor authentication (2FA) requires two forms of verification: something you know (password) and something you have (phone, hardware token, etc.).

## **3)Different methods of the two factor authentication**

Azure MFA supports several methods for the second factor:

- Phone call
- SMS
- Mobile app notification
- Mobile app verification code
- Hardware token

### Phone call settings

If users receive phone calls for MFA prompts, you can configure their experience, such as caller ID or the voice greeting they hear. In the INDIA, if you haven't configured MFA caller ID, voice calls from Microsoft come from the following numbers. Users with spam filters should exclude these numbers.

Default number: +91 855-330-8653

To configure your own caller ID number, complete the following steps:

1. Go to **Protection > Multifactor authentication > Phone call settings**.
2. Set the **MFA caller ID number** to the number you want users to see on their phones. Only US-based numbers are allowed.
3. Select **Save**.

### Set up a SMS

To use your own custom messages, complete the following steps:

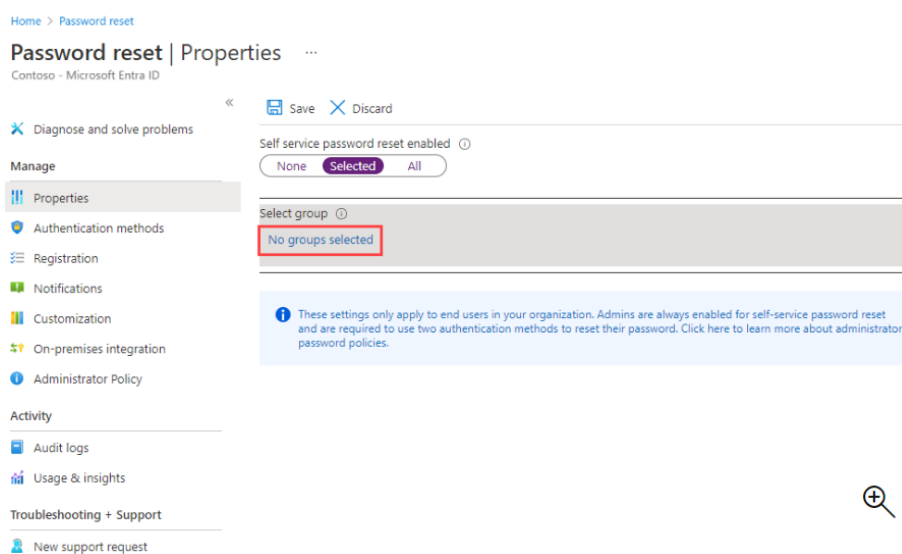
1. Go to **Protection > Multifactor authentication > Phone call settings**.
2. Select **Add greeting**.
3. Choose the **Type** of greeting, such as **Greeting (standard)** or **Authentication successful**.
4. Select the **Language**. See the previous section on custom messages.
5. Browse for and select an .mp3 or .wav sound file to upload.
6. Select **Add** and then **Save**.

## 4. Setup self-service password reset

1. Sign in to the Microsoft Entra admin center as at least an Authentication Policy Administrator.

2. Browse to **Protection > Password reset** from the menu on the left side.

3. From the **Properties** page, under the option *Self service password reset enabled*, choose **Selected**.



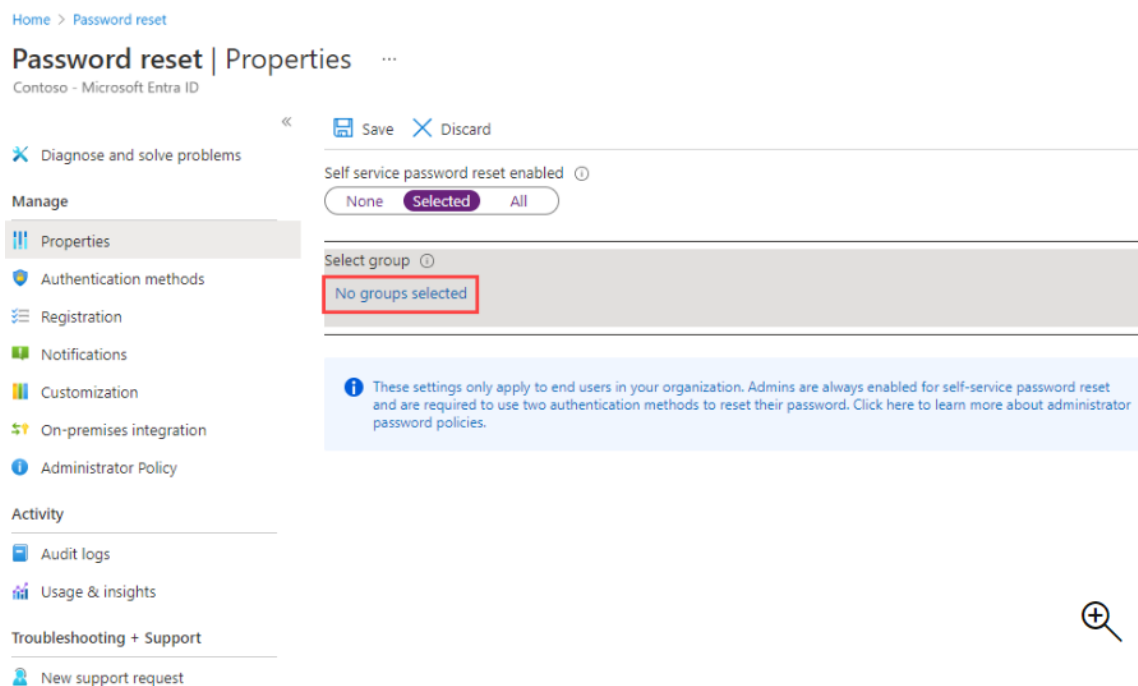
5. If your group isn't visible, choose **No groups selected**, browse for and select your Microsoft Entra group, like *SSPR-Test-Group*, and then choose *Select*.
6. To enable SSPR for the select users, select **Save**.

## 5. Configure MFA

1. Sign in to the Microsoft Entra admin center
2. Browse to **Identity > Overview > Properties**.
3. Select **Manage security defaults**.
4. Set **Security defaults** to **Enabled**.
5. Select **Save**.

Ensure that MFA is configured correctly by checking the settings in Azure Active Directory under the "Security" section.

## 6. Configure and deploy self-service password reset



## 7) Implement and manage Azure MFA settings

Go to "Azure Active Directory", then "Security", and then "Multifactor authentication". Customize settings such as:

- **Trusted IPs**
- **Fraud alerting**
- **Remember MFA on trusted devices**

### Fraud alerting

The Fraud alert feature lets users report fraudulent attempts to access their resources. When an unknown and suspicious MFA prompt is received, users can report the fraud attempt by using the Microsoft Authenticator app or through their phone.

Microsoft recommends using Report suspicious activity instead of Fraud alert due to its integration with Identity Protection for risk-driven remediation, better reporting capabilities, and least-privileged administration.

The following fraud alert configuration options are available:

- **Automatically block users who report fraud.** If a user reports fraud, the Microsoft Entra multifactor authentication attempts for the user account are blocked for 90 days or until an administrator unblocks the

account. An administrator can review sign-ins by using the sign-in report, and take appropriate action to prevent future fraud. An administrator can then unblock the user's account.

- **Code to report fraud during initial greeting.** When users receive a phone call to perform multifactor authentication, they normally press # to confirm their sign-in. To report fraud, the user enters a code before pressing #. This code is **0** by default, but you can customize it. If automatic blocking is enabled, after the user presses **0#** to report fraud, they need to press **1** to confirm the account blocking.

## Trusted IPs

Location conditions are the recommended way to configure MFA with Conditional Access because of IPv6 support and other improvements. For more information about location conditions, see [Using the location condition in a Conditional Access policy](#). For steps to define locations and create a Conditional Access policy, see [Conditional Access: Block access by location](#).

The trusted IPs feature of Microsoft Entra multifactor authentication also bypasses MFA prompts for users who sign in from a defined IP address range. You can set trusted IP ranges for your on-premises environments. When users are in one of these locations, there's no Microsoft Entra multifactor authentication prompt. The trusted IPs feature requires Microsoft Entra ID P1 edition.

## Enable remember multifactor authentication

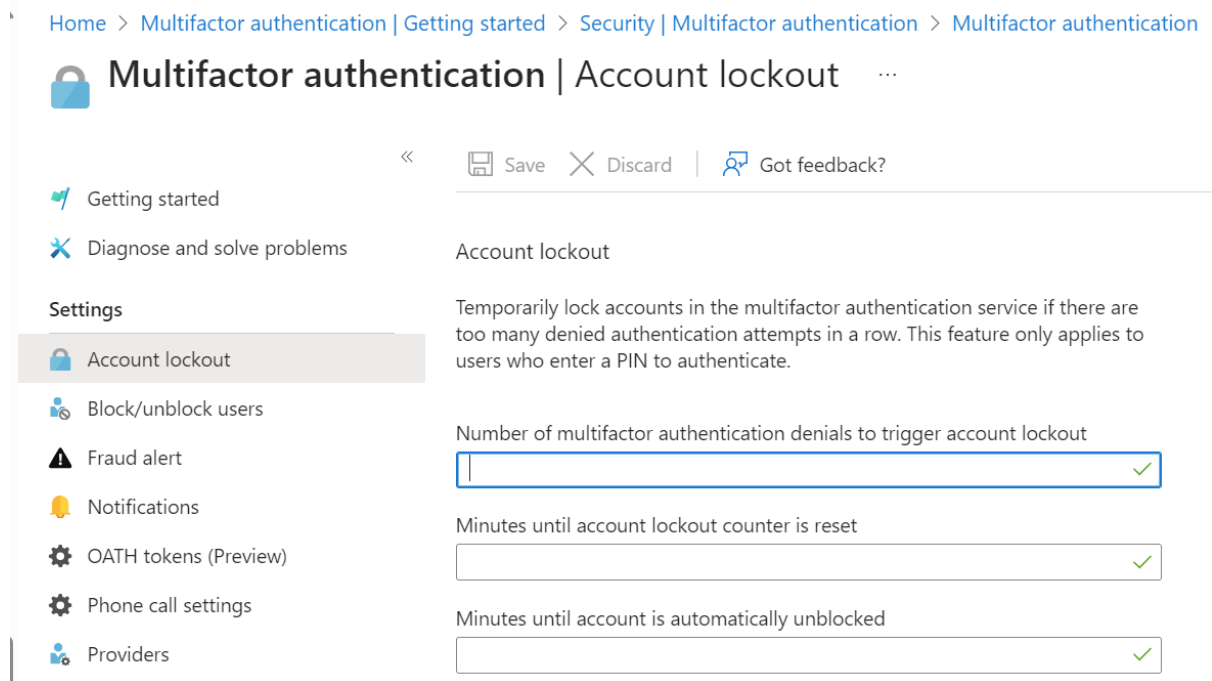
To enable and configure the option to allow users to remember their MFA status and bypass prompts, complete the following steps:

1. Sign in to the Microsoft Entra admin center as at least an Authentication Policy Administrator.
2. Browse to **Identity > Users**.
3. Select **Per-user MFA**.
4. Under **Multifactor authentication** at the top of the page, select **service settings**.
5. On the **service settings** page, under **remember multifactor authentication**, select **Allow users to remember multifactor authentication on devices they trust**.
6. Set the number of days to allow trusted devices to bypass multifactor authentications. For the optimal user experience, extend the duration to 90 or more days.
7. Select **Save**.

## Mark a device as trusted

After you enable the **remember multifactor authentication** feature, users can mark a device as trusted when they sign in by selecting **Don't ask again**.

## 8)Account Lockout



The screenshot shows the Microsoft Entra admin center interface. The breadcrumb trail is: Home > Multifactor authentication | Getting started > Security | Multifactor authentication > Multifactor authentication. The page title is "Multifactor authentication | Account lockout". On the left, the "Settings" section is expanded, showing "Account lockout" as the selected option. The main content area has a "Save" button and a "Discard" button. Below the title, there is a description: "Temporarily lock accounts in the multifactor authentication service if there are too many denied authentication attempts in a row. This feature only applies to users who enter a PIN to authenticate." There are three input fields, each with a green checkmark indicating they are valid: "Number of multifactor authentication denials to trigger account lockout" (empty), "Minutes until account lockout counter is reset" (empty), and "Minutes until account is automatically unblocked" (empty).

### To configure account lockout settings, complete these steps:

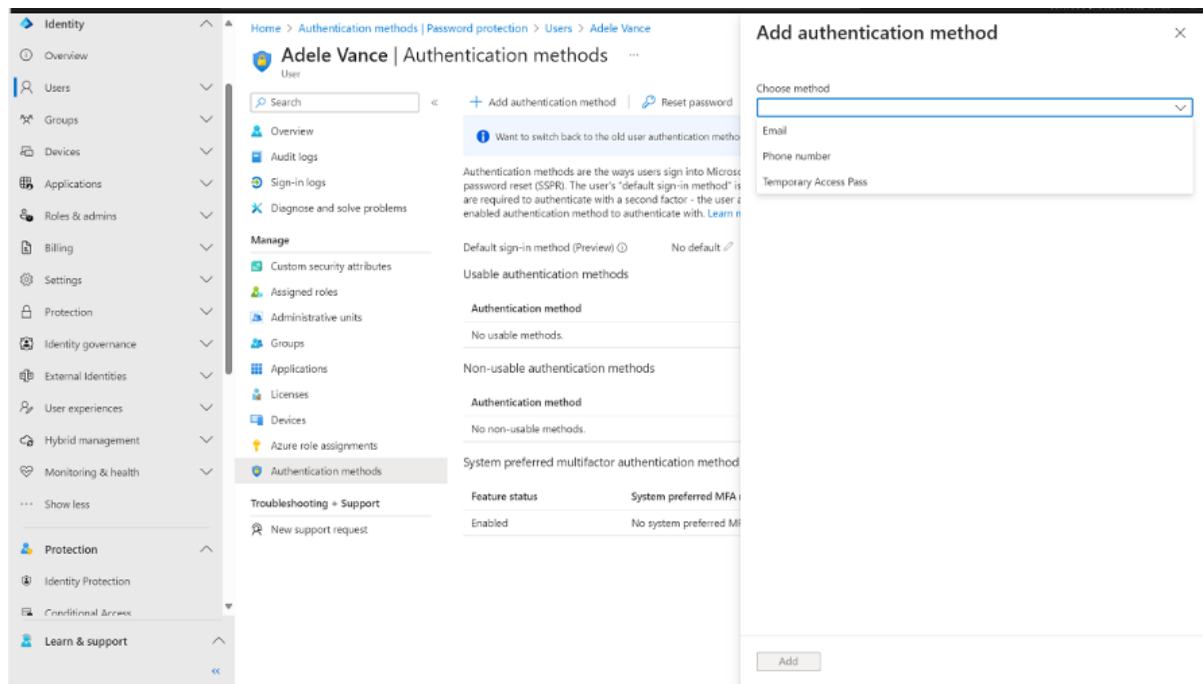
1. Sign in to the Microsoft Entra admin center as at least an Authentication Policy Administrator.
2. Browse to Protection > Multifactor authentication > Account lockout. You might need to click Show more to see Multifactor authentication.
3. Enter the values for your environment, and then select Save.

## 9)Manage MFA settings for users

To add authentication methods for a user in the Microsoft Entra admin center:

1. Sign in to the Microsoft Entra admin center as at least an Authentication Administrator.
2. Browse to **Identity > Users > All users**.
3. Choose the user for whom you wish to add an authentication method and select **Authentication methods**.
4. At the top of the window, select **+ Add authentication method**.

- Select a method (phone number or email). Email may be used for self-password reset but not authentication. When adding a phone number, select a phone type and enter phone number with valid format (such as +1 4255551234).
- Select **Add**.



## 10) Extend Azure AD MFA to third party and on-premises devices

To extend Azure AD MFA to third-party applications and on-premises devices, use Azure AD Application Proxy or integrate with an on-premises MFA server.

### • Set up Azure AD Application Proxy:

- In the Azure portal, go to "Azure Active Directory".
- Select "Application proxy", then "Enable Application Proxy". Follow the setup instructions to download and install the Application Proxy connector.

### • Publish an On-Premises Application:

- Go to "Azure Active Directory" > "Enterprise applications".
- Select "New application" > "On-premises application".
- Provide the necessary details for the application (name, internal URL, external URL).
- Configure any additional settings (authentication, SSO).

### • Enable MFA for the Application:

- Once the application is published, go to "Conditional Access" under "Azure Active Directory".
- Create a new policy and assign it to the published application.
- Under "Grant", select "Require multi-factor authentication".

## 11) Monitor Azure AD MFA activity

Request ID	Managed iden...	Managed identity name	Status	IP addr...	Resource	Resource ID	Managed Identi...
09b4f639-bf98-4383...	82a39f59-2722-4baa	AddCreatorTags	Success		Azure Key Vault	cfa8b339-82a2-471a...	
1c894355-b5c5-47d...	89949bb2-93e9-487e	storageDataScanner	Success		Azure Storage	e406a681-f3d4-42a8...	
99dee3cd-7a45-4cc4...	834af32a-539d-4c57	DesiredStateManagement	Success		Azure Key Vault	cfa8b339-82a2-471a...	
12875933-cb54-439...	834af32a-539d-4c57	DesiredStateManagement	Success		Windows Azure...	797f4846-ba00-4fd7...	

- Sign in to the Azure portal.
- In the left-hand menu, select "Azure Active Directory" and then select "Audit logs" under "Monitoring."

Sign-in events

Download Export Data Settings Troubleshoot Refresh Columns Got feedback?

Want to switch back to the default sign-ins experience? Click here to leave the preview.

Date: Last 24 hours Show dates as: Local Time aggregate: 24 hours Add filters

User sign-ins (interactive) User sign-ins (non-interactive) Service principal sign-ins **Managed identity sign-ins**

Sign-ins in the table below are grouped by application. Click on a row to see all the sign-ins for an application on that date and time.

- On the "Audit logs" page, you can use the filters to specify the time range and other parameters for the logs you want to view.
- In the "Activity" dropdown menu, select "User Management." This will show you all the user management activities, including when a user enabled MFA.
- Look for an entry with the activity "Enable MFA for a user." The "Time" column will show you the date and time when the MFA was enabled.

## 12) OAuth Tokens

Microsoft Entra ID supports the use of OATH TOTP SHA-1 tokens that refresh codes every 30 or 60 seconds. You can purchase these tokens from the vendor of your choice.

OATH TOTP hardware tokens typically come with a secret key, or seed, pre-programmed in the token. You need to input these keys into Microsoft Entra ID as



described in the following steps. Secret keys are limited to 128 characters, which might not be compatible with all tokens. The secret key can contain only the characters *a-z* or *A-Z* and digits *1-7*. It must be encoded in Base32.

Programmable OATH TOTP hardware tokens that can be reseeded can also be set up with Microsoft Entra ID in the software token setup flow.

OATH hardware tokens are supported as part of a public preview.

After you acquire tokens, you need to upload them in a comma-separated values (CSV) file format. Include the UPN, serial number, secret key, time interval, manufacturer, and model.

Name	Username	Serial Number	Model	Manufacturer	Activated
<input type="checkbox"/> ledinh04	ledinh04@wingtiptoysonlin...	123123	SafeID	DeepNet Security	<a href="#">Activate</a>

Sign in to the Microsoft Entra admin center as a Global Administrator, go to **Protection** > **Multifactor authentication** > **OATH tokens**, and upload the CSV file.

Depending on the size of the CSV file, it might take a few minutes to process. Select **Refresh** to get the status. If there are any errors in the file, you can download a CSV file that lists them. The field names in the downloaded CSV file are different from those in the uploaded version.

After any errors are addressed, the administrator can activate each key by selecting **Activate** for the token and entering the OTP displayed in the token.

Users can have a combination of up to five OATH hardware tokens or authenticator applications, such as the Microsoft Authenticator app, configured for use at any time.