

How to Setup Multi-Factor Authentication in RCMS

Background

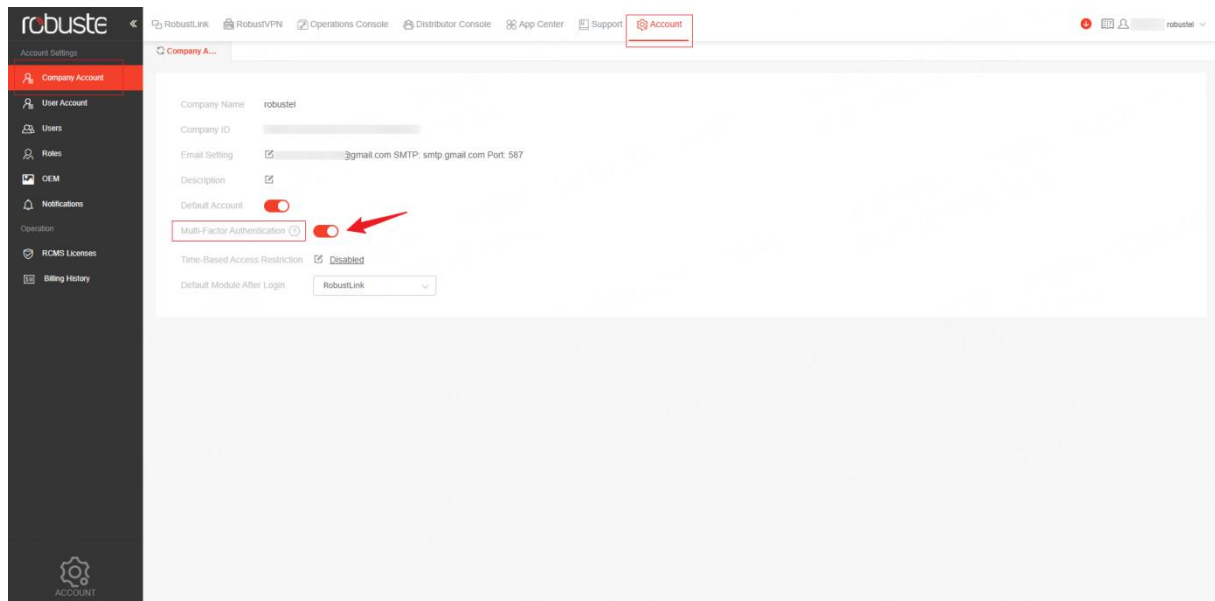
Microsoft has announced Phase 2 of its mandatory MFA (Multi-Factor Authentication) rollout for Azure beginning 1 October 2025. RCMS uses Microsoft Entra ID (formerly Azure Active Directory) for authentication. To align with best-practice security and ensure a consistent experience across Azure-integrated services, RCMS will require MFA for all user logins starting 1 October 2025.

To ensure uninterrupted access, please follow the steps below to enable and complete MFA setup.

IT Administrators: Enable MFA in RCMS

1. Log in to the RCMS.
2. Navigate to **Account** → **Company Account** → **Multi-Factor Authentication**.
3. Enable Multi-Factor Authentication (MFA), MFA will now be enforced for all users under this company.
4. Once enabled, all users will be prompted to complete MFA on their **next login**. Users who do not complete MFA will not be able to access RCMS.

Tip: Inform users before enabling MFA to avoid workflow interruptions.

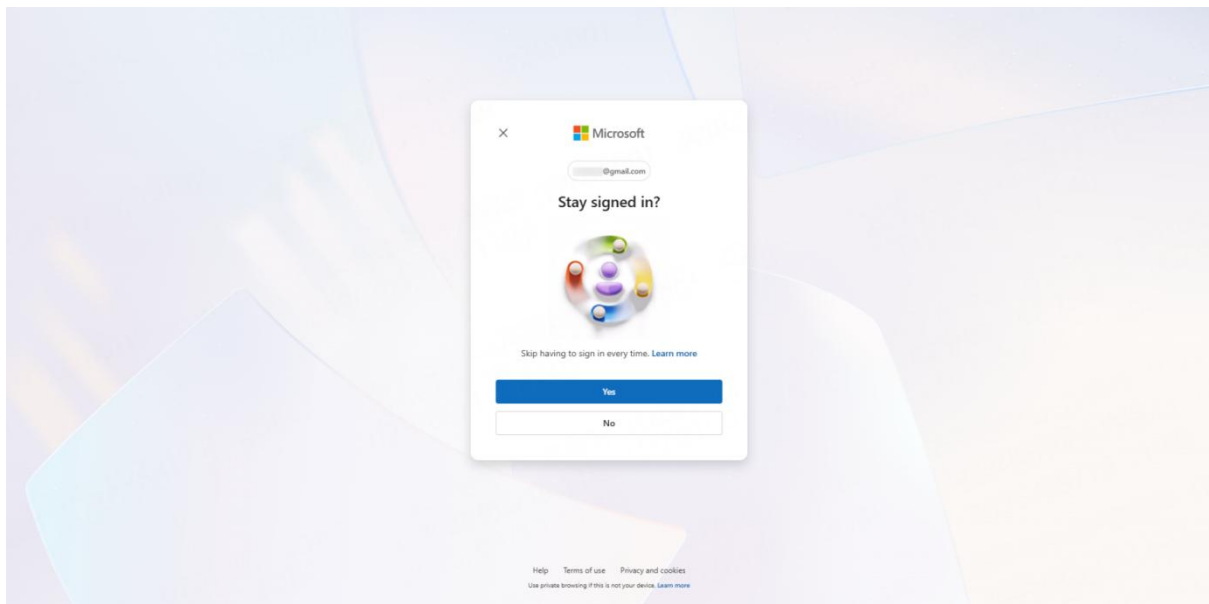


Important Notice: Starting from **October 1, 2025**, MFA will be automatically enforced for all RCMS users.

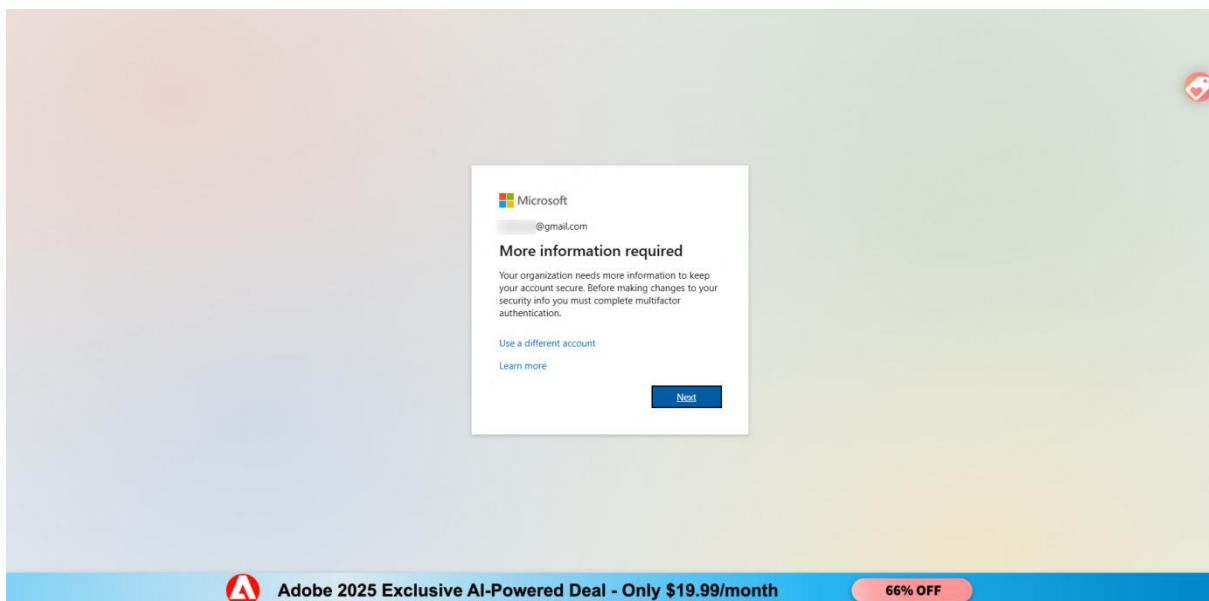
1. Users who have already set up MFA can continue logging in as usual.
2. Users who have not set up MFA before will be automatically redirected to Step 2 below (MFA setup prompt) when logging in to RCMS.

Users: Setup MFA on RCMS Login

1. Log in to RCMS with your AAD account as usual.



2. You will be automatically prompted to set up MFA. Click Next to start the setup.

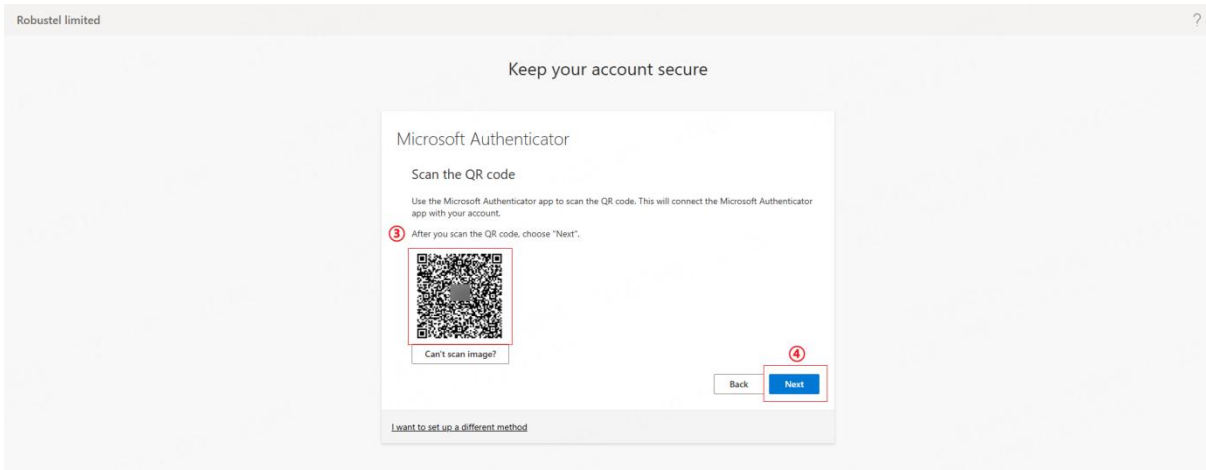
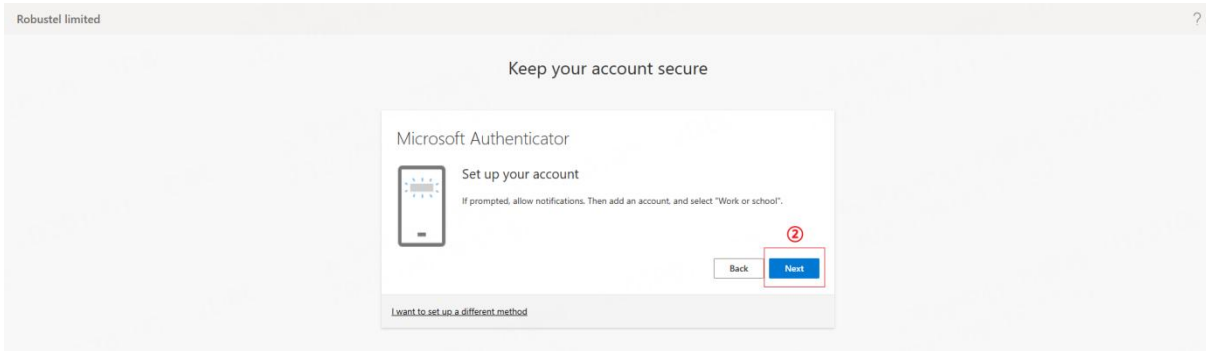
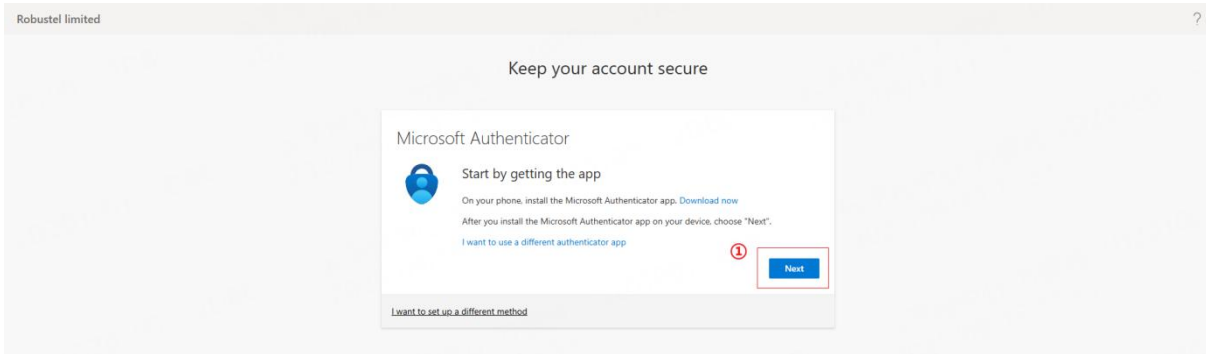


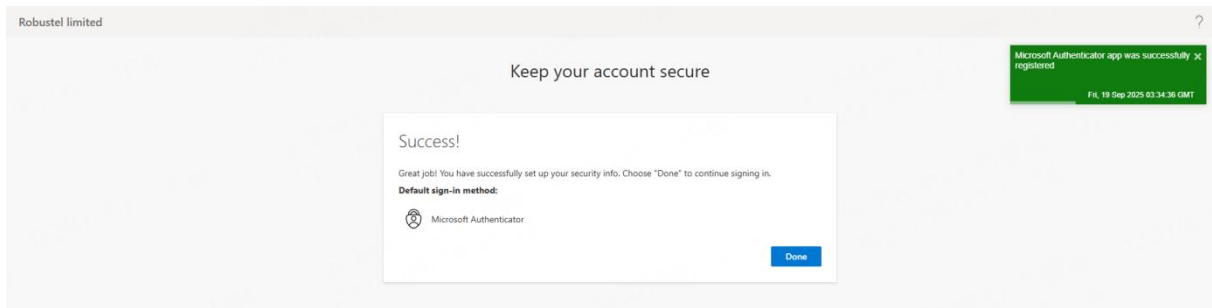
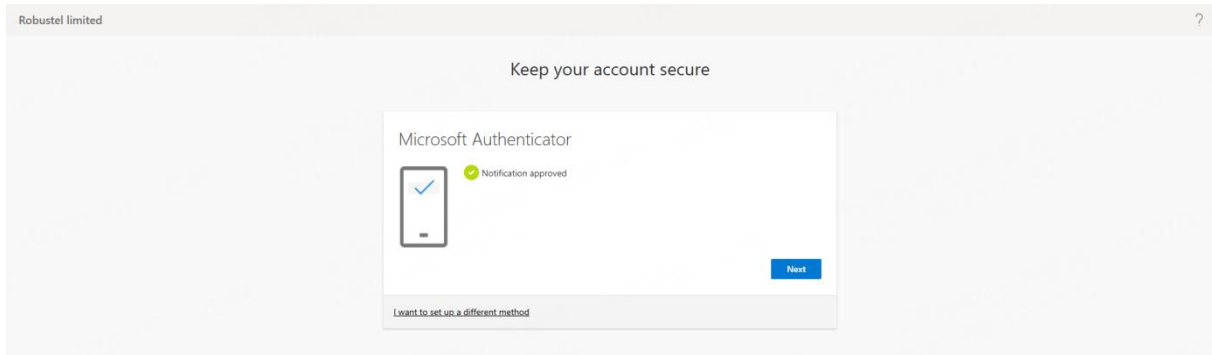
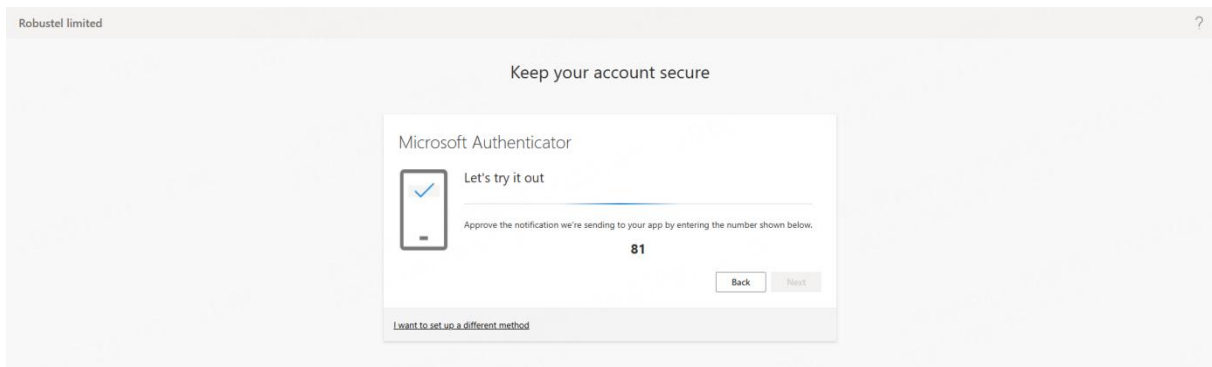
3. Follow the instructions to select a verification method. This quick guide provides step-by-step instructions for the two most commonly used methods: Authenticator App and SMS. Other methods follow a similar process and can be set up according to the on-screen

instructions.

Authenticator App (recommended)

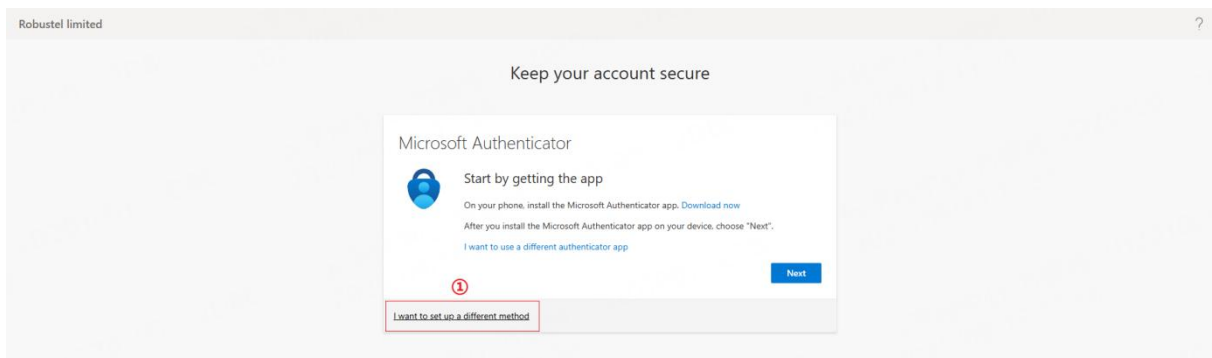
- a. Open your authenticator app (e.g., Microsoft Authenticator) on your mobile device.
- b. Scan the QR code displayed on the RCMS MFA setup screen.
- c. Enter the 2-digit code generated by the app to verify.

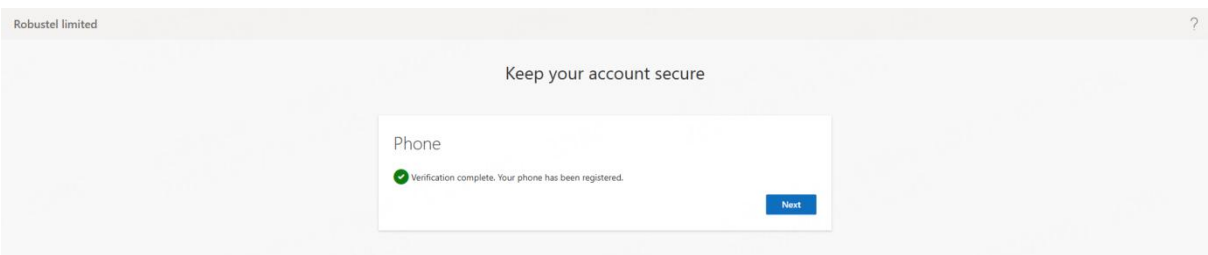
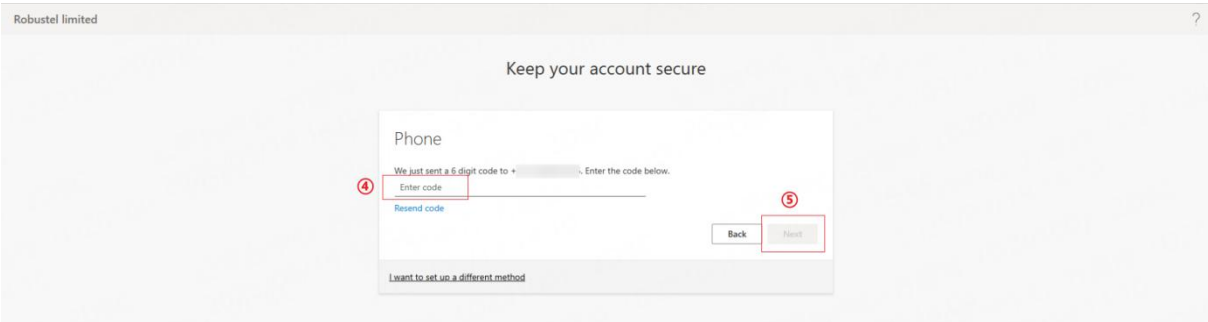
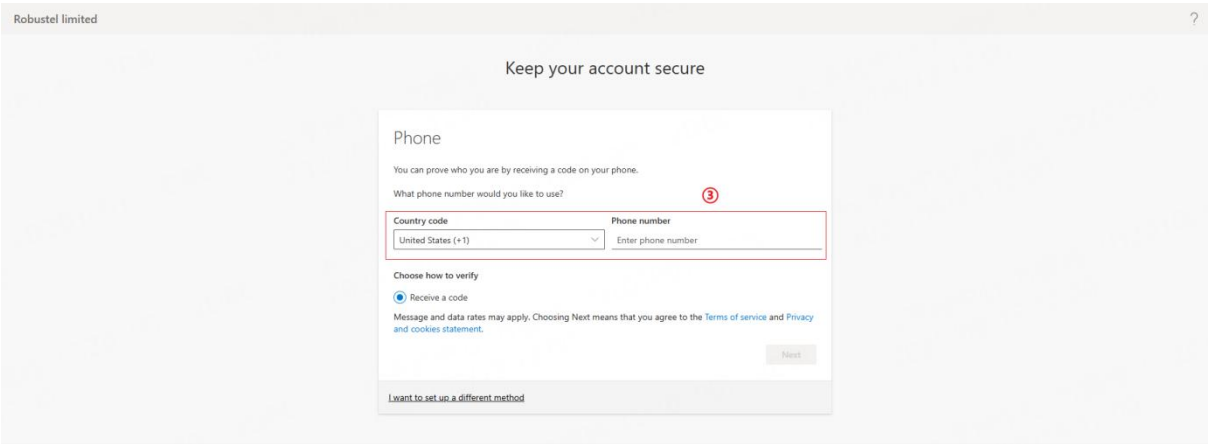
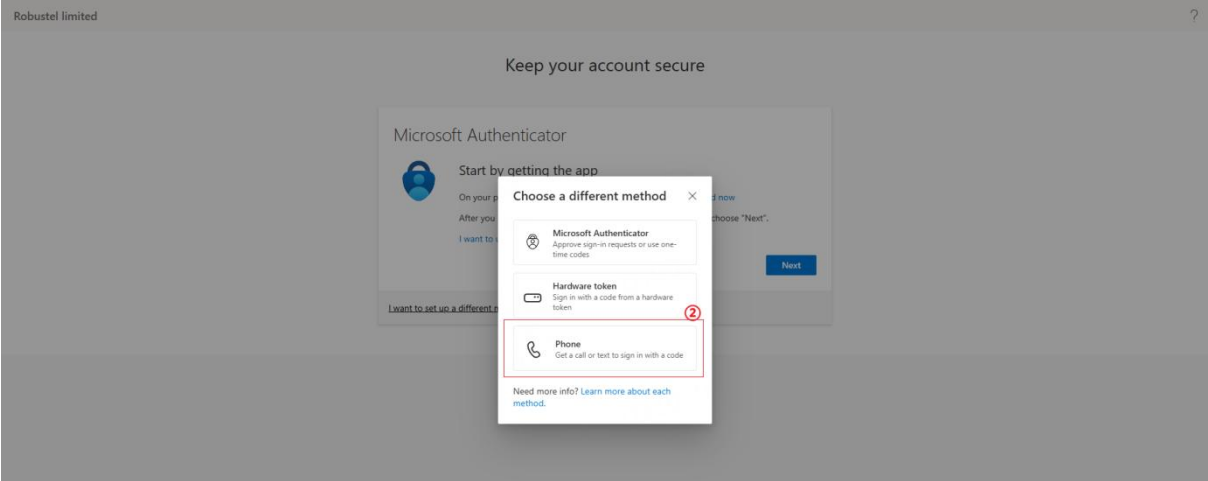


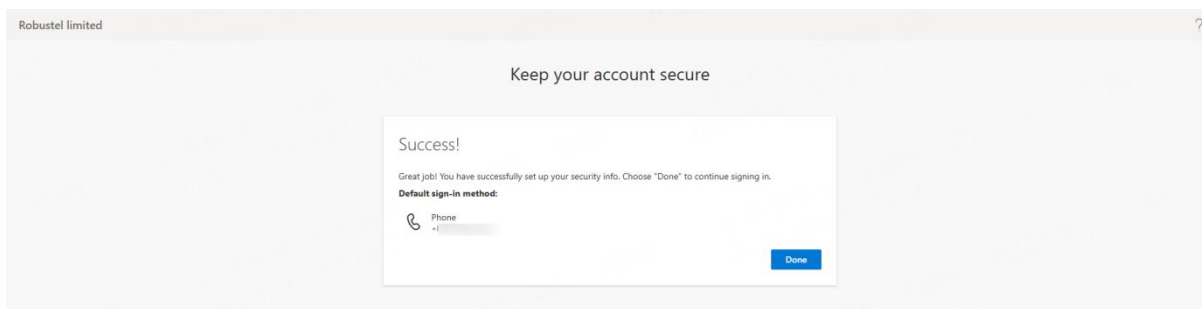


SMS

- Enter your mobile phone number.
- You will receive a text message with a verification code.
- Enter the code on the RCMS screen to verify.







4. Complete the setup to successfully log in to RCMS.
5. For subsequent logins, MFA verification will be required according to the configured settings.

Tip: Using an authenticator app (e.g., Microsoft Authenticator) is recommended for better security and convenience.

FAQ

Q1: Is this optional?

A: No. This is a Microsoft directed change and to comply RCMS will enforce MFA for all users from 1 Oct 2025.

Q2: We already have MFA in our tenant. Do we need to do anything?

A: Likely no. If users can already pass MFA in Microsoft Entra ID, they should see no change.

Q3: Which MFA methods are supported?

A: Microsoft Authenticator app, SMS, or phone call (standard Entra ID methods).

Q4: What happens if users don't set up MFA in time?

A: They'll be prompted to enroll at sign-in. Access is blocked until MFA is completed.

Q5: Is there downtime?

A: No planned downtime. This is a sign-in policy change.

Q6: Can we request an exception or a postponement?

A: No exceptions in RCMS. Enforcement is global for account security.

Q7: Who should handle this on the customer side?

A: Their IT admin/tenant admin should ensure MFA is enabled for all RCMS users.