

Multi-factor Authentication

Version 1.0.0 | Updated 2026-09-05 | 1 min read

Preparation / invited access

In this guide: [Before you start](#) | [Steps](#) | [Verify the result](#) | [Help and related information](#)

MFA adds a separate check at sign-in. The factors available depend on the product and account rollout.

Before you start

Use the access and features actually assigned to your account. Keep a rollback or recovery route before changing existing service settings.

Steps

1. Open security settings from the verified product sign-in route.
2. If authenticator enrollment is offered, add the account inside your trusted authenticator without sharing its QR image or seed.
3. Complete the verification step and save any recovery codes in protected storage separate from the device.
4. Test the new factor before removing an old one. Report unexpected prompts through support.

Verify the result

A fresh sign-in requests the configured factor. Recovery codes and authenticator seeds are never included in a support ticket.

Help and related information

Contact support, service status, and Customer Access. Never send passwords or recovery codes.