

A practical guide to setting up MFA for Microsoft 365

Breadcrumb

- 1. [Home](#) /
- 2. [Print](#) /
- 3. [Pdf](#) /
- 4. [Node](#) /
- 5. [Entity Print](#)

Insight navigation

- [Latest insights](#)
- [Latest news](#)
- [Articles](#)
- [Case studies](#)

[Download PDF](#)

Apr 2022

A practical guide to setting up MFA for Microsoft 365

Multi-factor Authentication (MFA) is an effective way of preventing hackers from accessing your accounts, even if they manage to crack your password.

Categories Future of Work, Cloud

Apr 2022

-
-
-
-

What is MFA?

It is a security measure that requires two or more methods of proof of identity to access an account.

This could be a combination of:

- 1. Something you know e.g., a password or PIN
- 2. Something you have e.g., a mobile device with an authenticator app installed
- 3. Something you are e.g., a fingerprint, iris or face scan

Proof	You	Hacker
Something you know	✓	✓
Something you have	✓	✗
Something you are	✓	✗
Login successful?	✓	✗

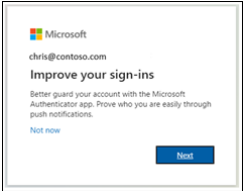
The reason MFA helps to thwart access to accounts is that it ensures that the person logging in is the owner of the account and not a hacker.

Only the owner would have each of the three forms of identification. The hacker may know the password but that's all, so their attempt to access the account will fail.

Enrolling and educating all parties is the hardest part of MFA setup, but thankfully there is a tool to help with enrolment so that you can focus on educating users on how to use MFA.

Setting up MFA

You can nudge users to set up the Microsoft Authenticator app when they next sign in, which will result in this popup encouraging them to improve their sign-in experience.



This is achieved through enabling a registration campaign to the users who are required to configure MFA by following these steps:

- 1. In the Azure AD portal (<https://portal.azure.com>), click **Security > Authentication methods > Registration campaign**
- 2. For **State**, click **Enabled**, select any users or groups to exclude from the registration campaign such as VIP users that you will personally assist.
- 3. For **Days allows to snooze** choose the number of days in which after users will be required to configure MFA, then click **Save**.

Authentication methods | Registration campaign

The Pramila - Azure AD Security

Search (Ctrl+ /)

«

Got feedback?

Manage

Policies

Password protection

Registration campaign

Monitoring

Activity

User registration details

Registration and reset events

Bulk operation results

Start a registration campaign that prompts users to set up more secure authentication methods. Exclude users and groups from the entire campaign in the Settings section or include users and groups for each authentication method (currently limited to Microsoft Authenticator).[Learn more](#)

Settings

Save Discard

State

Days allowed to snooze

Excluded users and groups

Enabled

0 days

1 Group

+ Add users and groups

Authentication method

Method	Included users and groups
Microsoft Authenticator	All users