|  |
| --- |
| Using multi-factor authentication (MFA)Microsoft |

It is recommended that you enable multi-factor authentication (MFA) in your organisation. MFA is an added step in the sign-in process which improves your security by requiring you to use a separate device to help verify your identity. This makes it almost impossible for a hacker to gain access to your account without also having your mobile phone.

## What you need to do as an organisation

To enable MFA, turn on the security defaults in Microsoft Entra ID (or confirm that they are in place):

Sign in with your admin credentials to the Microsoft Entra admin centre.

Navigate to the Overview section in the left-hand navigation and the Properties tab.

At the bottom of the page toggle the Manage Security Defaults option to Yes.

In the Enable Security Defaults pane, click Manage defaults.

Review the security defaults that will be applied and click Enable defaults.

These [preconfigured security settings](https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults#block-legacy-authentication-protocols) enable MFA and block legacy authentication (which stops 99.9% of identity-related attacks).

Legacy authentication protocols are older, less secure methods of authentication (apps using email protocols like POP, IMAP, and SMTP AUTH). These protocols were designed and implemented before modern security standards and best practices were widely adopted and responsible for most compromising sign-in attempts. Legacy authentication protocols are normally only used in old software (e.g. Office 2013 or older). If this applies to your organisation, please read this information first: [How to move away from legacy authentication](https://learn.microsoft.com/en-us/entra/identity/conditional-access/block-legacy-authentication).

## What your staff will need to do

Everyone in your organisation will need to set up Microsoft Authenticator app on their mobile phone. You can also set up additional backup options like a phone number for MFA in case you lose access to the authenticator app.

Ask your staff to follow the steps in the video below to set up MFA on their phone.

[MFA Overview Video](https://www.microsoft.com/en-us/videoplayer/embed/RE2MuO3?autoplay=false&postJsllMsg=true).

For more information, see [Use Microsoft Authenticator with Microsoft 365 – Microsoft Support](https://support.microsoft.com/en-us/topic/use-microsoft-authenticator-with-microsoft-365-1412611f-ad8d-43ab-807c-7965e5155411).

## What to expect as an administrator

You can expect some initial support inquiries from users as they start using MFA. You may need to provide guidance on setting up and using MFA methods (eg. Microsoft Authenticator app, SMS, phone calls). See “Change and adoption” below.

You can monitor MFA usage and compliance through the Entra ID admin portal under **Identity** > **Protection** > **Authentication methods** > **Activity**.

## What staff can expect

When attempting to access Microsoft 365 services or applications, they may be prompted to use MFA (e.g. enter a temporary code that is sent to their mobile phone device via SMS or authenticator app) depending on whether the systems detects this as a “risky” activity, for example where they are trying to sign in from, and/or if it is the first time they are doing so from the location.

## Change and adoption

Enabling MFA by default may initially cause some friction or disruption as users adapt to the new authentication process. However, it significantly enhances the security of your Microsoft 365 environment by requiring an additional verification factor beyond passwords. Providing clear communication and support during the rollout can help ensure a smooth transition for both administrators and users.