Set up multifactor authentication for Microsoft 365

Article • 10/02/2024

Check out all of our small business content on Small business help & learning .

Check out Microsoft 365 small business help on YouTube.

Multifactor authentication means you and your employees must provide more than one way to sign in to Microsoft 365 is one of the easiest ways to secure your business. Based on your understanding of multifactor authentication (MFA) and its support in Microsoft 365, it's time to set it up and roll it out to your organization.

Multifactor authentication (MFA) is an important first step in securing your organization. Microsoft 365 for business gives you the option to use security defaults or Conditional Access policies to turn on MFA for your admins and user accounts. For most organizations, **Security defaults** offer a good level of sign-in security. But if your organization must meet more stringent requirements, you can use Conditional Access policies .

> **Tip**
>
> If you need help with the steps in this topic, consider **working with a Microsoft small business specialist** . With Business Assist, you and your employees get around-the-clock access to small business specialists as you grow your business, from onboarding to everyday use.

Before you begin

- You must be a Global admin to manage MFA. For more information, see About admin roles.
- If you have legacy per-user MFA turned on, Turn off legacy per-user MFA.

- Advanced: If you have third-party directory services with Active Directory Federation Services (AD FS), set up the Azure MFA Server. See advanced scenarios with Microsoft Entra multifactor authentication and third-party VPN solutions for more information.

Watch: Turn on multifactor authentication

https://www.microsoft.com/en-us/videoplayer/embed/RE2MuO3?autoplay=false&postJsllMsg=true

Steps: Turn on multifactor authentication

If you purchased your subscription or trial after October 21, 2019, and you're prompted for MFA when you sign in, security defaults have been automatically enabled for your subscription. If you purchased your subscription before October 2019, follow these steps to turn on **security default MFA**.

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

For more information, see What are security defaults?

Turn off per-user MFA

If you've previously turned on per-user MFA, you must turn it off before enabling Security defaults. You should also turn off per-user MFA after you've configure your policies and settings in Conditional Access.

1. In the Microsoft 365 admin center, in the left nav choose **Users** > **Active users**.
2. On the **Active users** page, choose **multifactor authentication**.
3. On the multifactor authentication page, select each user and set their multifactor authentication status to **Disabled**.

Turn Security default MFA off

> **Important**
>
> It's not recommended to turn off MFA.

1. Sign in to the Microsoft Entra admin center as at least a security administrator or conditional access administrator.
2. Browse to **Identity** > **Overview** > **Properties**.
3. Select **Manage security defaults**.
4. Set **Security defaults** to **Disabled (not recommended)**.
5. Select **Save**.

Use Conditional Access policies

If your organization has more granular sign-in security needs, Conditional Access policies can offer you more control. Conditional Access lets you create and define policies that react to sign in events and request additional actions before a user is granted access to an application or service. You can also get started by using conditional access templates.

> **Important**

Do not forget to disable per-user MFA after you have enabled Conditional Access policies. This is important as it will result in inconsistent user experience.

Conditional Access is available for customers who bought Microsoft Entra ID P1, or licenses that include this, such as Microsoft 365 Business Premium, and Microsoft 365 E3. For more information, see create a Conditional Access policy.

Risk-based conditional access is available through Microsoft Entra ID P2 license, or licenses that include risk based conditional access, like Microsoft 365 E5. For more information, see risk-based Conditional Access.

For more information about the Microsoft Entra ID P1 and P2, see Microsoft Entra pricing .

Next steps - Send to your users

- What is multifactor authentication
- Sign-in after registration
- Change additional verification method
- Register for additional verification method

Related content

Set up multifactor authentication (video)

Turn on multifactor authentication for your phone (article)

Security defaults and multifactor authentication (article)

Feedback

Was this page helpful? Yes No

Provide product feedback