

MICROSOFT ENTRA ID

YubiKey USB Security Key User Guide

Register your security key and use it to sign in to Microsoft 365

This guide is for end users. Follow the steps below to register and use the USB YubiKey provided by your organization. The wording of options may vary slightly depending on your organization's settings and Microsoft updates.

1. Register Your YubiKey

Before you begin, have your work or school account and YubiKey ready. Make sure your computer has a working USB-A or USB-C port, and use an up-to-date browser such as Microsoft Edge or Google Chrome.

1. **Open the Security info page:** Go to <https://mysignins.microsoft.com/security-info> and sign in with your work or school account.
2. **Add a sign-in method:** Select “Add sign-in method” or “Add method.”
3. **Choose a security key:** Select “Security key” or “Passkey.” If asked to choose a device type, select “USB device.”
4. **Follow the prompts:** Select “Next” and follow the instructions in the browser or Windows security dialog. Insert the YubiKey into your computer's USB port when prompted.
5. **Create a security key PIN:** If prompted, create a PIN that you can remember and that is not easy to guess. This is your YubiKey FIDO2 PIN, not your Microsoft 365 password. Do not share it with anyone, including IT support staff.
6. **Touch the YubiKey:** When the key's sensor flashes or the screen asks you to, touch the YubiKey. If prompted, enter your FIDO2 PIN and touch the key again if requested.
7. **Finish and confirm:** Give the key a recognizable name, such as “YubiKey - Primary,” and complete setup. Return to the Security info page and confirm that the security key or passkey is listed.

Security reminder

Only touch your YubiKey when you are registering or signing in and the screen asks you to. If you receive a sign-in prompt that you did not initiate, do not touch the key.

2. Sign In to Microsoft 365 with Your YubiKey

After registration, you can use your YubiKey with supported Microsoft 365 websites and applications.

8. **Open the service:** Go to <https://www.office.com> or open the Microsoft 365 application you need.
9. **Choose a sign-in option:** Enter your work or school username if requested, then select “Sign-in options.”
10. **Select the security key option:** Choose the option related to “Security key.” The exact wording may vary.
11. **Insert and verify:** Insert the YubiKey when prompted. Enter your FIDO2 PIN if requested, then touch the key when prompted.
12. **Complete sign-in:** Confirm that the correct work or school account is shown and finish signing in.

Please note

Depending on your organization's policy and the sign-in flow, you may still be asked for your password, or the key may only be available in certain applications. Registering a YubiKey does not mean that every legacy application or every sign-in scenario supports it.

3. Troubleshooting

I cannot find “Security key” or “Passkey.”

Your organization may not have enabled this method for your account. Contact IT support; do not try to bypass your organization's settings.

My computer does not detect the YubiKey.

Try another available USB port and confirm that you are using an organization-approved YubiKey model that supports FIDO2.

My PIN is rejected or I have forgotten it.

Contact IT support for the approved recovery procedure. Do not repeatedly guess the PIN, and never send it by email or chat.

Sign-in does not complete.

Restart the sign-in process and touch the key only when prompted. If it still fails, note the error message and contact IT support.

I have lost my YubiKey.

Notify IT support promptly and follow your organization's identity-verification and recovery process. Do not use another person's security key.

4. Important Security Practices

- Never share your YubiKey PIN or write it on the key.
- Do not respond to sign-in prompts that you did not initiate. If unsure, cancel the prompt and contact IT support.
- Do not format the YubiKey or use it to store files like an ordinary USB flash drive.
- Keep your YubiKey secure. If it is lost, damaged, or you suspect unauthorized use, notify IT support promptly.

Need help? Contact your organization's IT support team.