



YubiKey resource guide for enterprises

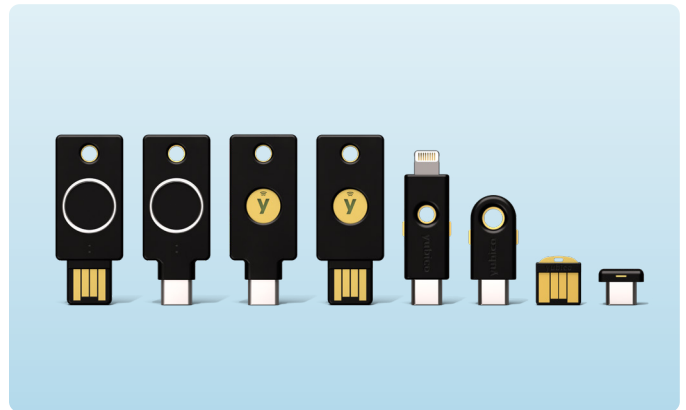
Welcome to the Yubico Family! We're excited to help you improve your online security with YubiKeys. We were founded with the mission to make the internet safer for everyone. To make that happen, we invented the YubiKey and pioneered new open authentication standards that now work seamlessly with your favorite global online services.

By purchasing a YubiKey on [Yubico.com](https://yubico.com), you are helping to secure the world at large. Through our [Secure it Forward](#) program, Yubico matches up to 5% of the number of YubiKeys purchased on [Yubico.com](https://yubico.com), donating them to non-profit organizations, election campaigns, journalists and humanitarian workers around the world.

How to get started with your YubiKey

To get started, head to yubico.com/start, select the type of YubiKey you've received, and you'll be shown a complete list of services (with instructions) that are compatible with the key. Your digital world is now secured!

Please note that if you are using an Apple device for setup, you will have to set up a FIDO2 pin beforehand through either the [Yubico Authenticator](#) or [YubiKey Manager](#).



Enable FIDO2 security key method

1. Sign in to the [Microsoft Entra admin center](#) as at least an [Authentication Policy Administrator](#).
2. Browse to Protection > Authentication methods > Authentication method policy.
3. Under the method FIDO2 Security Key, click All users, or click Add groups to select specific groups. Only security groups are supported.
4. Save the configuration.

User registration and management of FIDO2 security keys

1. Browse to <https://myprofile.microsoft.com>.
2. Sign in if not already.
3. Click Security Info.
 - a. If the user already has at least one Microsoft Entra multifactor authentication method registered, they can immediately register a FIDO2 security key.
 - b. If they don't have at least one Microsoft Entra multifactor authentication method registered, they must add one.
 - c. An Administrator can issue a [Temporary Access Pass](#) to allow the user to sign in and register a Passwordless authentication method.
4. Add a FIDO2 Security key by clicking Add method and choosing Security key.
5. Choose USB device or NFC device.
6. Have your key ready and choose Next.
7. A box will appear and ask the user to create/enter a PIN for your security key, then perform the required gesture for the key, either biometric or touch.
8. The user will be returned to the combined registration experience and asked to provide a meaningful name for the key to identify it easily. Click Next.
9. Click Done to complete the process.



Stop account takeovers in their tracks with easy-to-use authentication




Before you can login to AWS Management Console using a YubiKey, your IT Admin must enable a YubiKey for the IAM user.

1. Enter your AWS account ID or alias to sign in as an IAM user and select Next.
2. From the IAM sign-in page, re-enter your AWS account ID or alias, plus the username and password for your IAM user. Then select Sign in.
3. To authenticate with your YubiKey security key, insert your key into the USB port on your computer, wait for the key to blink, and then touch the button or gold disk on your YubiKey security key. If your key doesn't blink, please select Troubleshoot MFA to review instructions to troubleshoot the issue.
4. Your IAM user has successfully completed the MFA challenge and signed into the AWS Management console.

okta

1. [Sign in](#) to Okta.
2. On the Set up factors page of the Sign-In Widget, click Set up under YubiKey. The Set up YubiKey page appears.
3. Insert the YubiKey and tap its button when prompted.
4. Click Verify. The Set up security methods page appears.
5. Click Finish.

1Password

1. [Sign in](#) to your account on 1Password.com on your computer.
2. Click your name in the top right and choose [My Profile](#).
3. Click More Actions > Manage Two-Factor Authentication.
4. Click Add a Security Key.
5. Enter a name for your security key and click Next.
6. If 1Password asks you to [save a passkey](#), click the  button.
7. Insert your security key into the USB port on your computer.
8. If Windows Security asks you to create a PIN, enter one and click OK. Your PIN is stored locally on your security key.
9. Touch the sensor on your security key.
10. When you see "Your security key was successfully registered", click Done.



PingIdentity

1. In the admin console, go to Setup > PingID > Configuration.
2. Go to the Alternate Authentication Methods section.
3. In the Enable column, select the YubiKey check box.
4. Click Save.



1. Access the Duo enrollment page via a link emailed by your administrator, or when you log in for the first time to a Duo protected resource.
2. Select Security Key from the list of devices and then click Continue.
3. Make sure that you're not blocking pop-up windows for the enrollment site before continuing.
4. If you're using Safari 14.1 or later, click the Initiate enrollment button to proceed. Other browsers do not require this step.
5. The security key enrollment window automatically tries to locate your connected security key for approval.
6. Depending on your security key model, you'll need to tap, insert, or press a button on your device to proceed.
7. When enrolling your security key, you'll be prompted to tap to enroll your security key (possibly more than once). You may also be asked if you want to allow Duo to access information about your security key (click Allow or Proceed as applicable).
8. You'll see whether the security key identification was successful or not.

YubiKeys, the industry's #1 security keys, work with hundreds of products, services, and applications. [Browse the YubiKey compatibility list here.](#)



Questions about how to use your YubiKey? You can reach out to our support team here: yubi.co/support.