Two-factor authentication

- Configure security key authentication for two-factor Cloudflare login
  - Built-in authenticators
  - Security keys
- Configure TOTP mobile application authentication
  - Reconfigure TOTP mobile application authentication
- Configure email two factor authentication
- Regenerate backup codes
- Disable two-factor authentication for your Cloudflare account
- Use a backup code
- Related resources

import { DashButton, Render } from "~/components"

Configure security key authentication for two-factor Cloudflare login

:::caution

Security keys only work with browsers that support the WebAuthn protocol. :::

A security key provides phishing-resistant multifactor authentication to your Cloudflare account using a built-in authenticator (Apple Touch ID, Android fingerprint, or Windows Hello) or an external hardware key (like YubiKey) that connects to your computer through USB-A, USB-C, NFC, or Bluetooth.

Cloudflare recommends configuring multiple security keys. With multiple keys, you can still use 2FA if the primary key is unavailable or if you are working on a different device.

After enabling 2FA on your Cloudflare account, you can select **Manage** to configure 2FA security key authentication.

Built-in authenticators

You can configure a built-in authenticator such as Apple Touch ID, Android fingerprint, or Windows Hello.

1. In **Security Key Authentication**, select **Add**.
2. On the **Add a Security Key**, enter your Cloudflare password and select **Next**.
3. Interact with your built-in authenticator to add it to your Cloudflare account.
4. Enter a name for the built-in authenticator. If this is the initial setup, you will be prompted to generate backup codes. If not, skip to Step 8.
5. Enter your Cloudflare password.
6. Select **Next** to review your backup codes. Backup codes can be used to access your user account without your mobile device.
7. Select **Download**, **Print**, or **Copy** to save your backup codes in a secure location.
8. Select **Next** to finish the configuration.

Security keys

You can configure a security key, such as a Yubikey, to use with your account. Before you begin, ensure your hardware security key is configured and plugged in.

On a Windows device, you may need to set up Windows Hello or register your security key to your Microsoft account. Review the Windows documentation for more details.

1. Once your security key is plugged in, go to **Profile** > **Authentication**.
2. From **Two-Factor Authentication**, select **Set up**.
3. From **Security Key Authentication**, select **Add**.
4. Enter your Cloudflare password on the **Add a Security Key** screen, then select **Next**.
5. Interact with your security key to add it to your Cloudflare account. Ensure that the dialog is for the security key setup. If the Windows Hello dialog appears on a Windows device, select **Cancel**. The security key dialog box will then appear. Depending on your system, you may be required to register a PIN for the security key.
6. Enter a name for the security key. If this is the initial setup, you will be prompted to generate backup codes. If not, skip to Step 8.
7. Enter your Cloudflare password.
8. Select **Next** to review your backup codes. Backup codes can be used to access your user account without your mobile device.
9. Select **Download**, **Print**, or **Copy** to save your backup codes in a secure location.
10. Select **Next** to finish the configuration.

Configure TOTP mobile application authentication

Time-based one-time password (TOTP) authentication works by using an authenticatior app, such as Google Authenticator or Microsoft Authenticator, which generates a secret code shared between the app and a website. When you log in to the website, you enter your username, password, and the secret code generated from the authenticator app. The secret code is only valid for a short period of time, about 30 to 60 seconds, before a new code is generated.

1. Once your security key is plugged in, go to **Profile** > **Authentication**.
2. From **Two-Factor Authentication**, select **Set up**.
3. Under **Mobile App Authentication**, select **Add**.
4. Scan the QR code with your mobile device and enter the code from your authenticator application.
5. Enter your Cloudflare password, then select **Next**. If you cannot scan the QR code, select **Can't scan QR code, Follow alternative steps** to configure your authenticator application manually.

You can enable 2FA by scanning a QR code with your mobile device.

6. Enter your Cloudflare password again.
7. Select **Next** to review your backup codes. You can use backup codes to access your account without your mobile device.
8. Select **Download**, **Print**, or **Copy** to save your backup codes in a secure location.

:::note

To avoid being locked out of your account, be sure to generate and save your recovery codes. If you forget your password and cannot receive the reset code or lose access to your phone with the authenticator app, you can use the recovery codes to access your account.

You can regenerate your backup codes at any time using the Cloudflare dashboard. :::

9. Select **Next** on the backup code page to complete the recovery code setup.

Reconfigure TOTP mobile application authentication

You may need to reconfigure your mobile application authentication if you join a new organization or lose access to your mobile device. When you reconfigure your mobile application authentication, your previous TOTP codes are invalid.

:::note

Reconfiguring TOTP mobile application authentication does not turn off 2FA. :::

To reconfigure, follow Steps 1-7 as detailed above.

Configure email two factor authentication

Email 2FA works by sending you a TOTP code to your email address. This is a good option particularly if you are concerned about losing a hardware based key.

1. Navigate to **User Profile**, then **Authentication**.
2. Under **Two-Factor Authentication**, select **Set up**.
3. Under **Email Authentication**, select **Enable**.
4. You will be prompted to enter your password twice, and then be shown recovery codes. Save these somewhere safe like a password manager.

Regenerate backup codes

Each backup code is one-time use only, but you can always request a new set of backup codes using the Cloudflare dashboard. This is useful if you have lost access to or used all of your previous backup codes.

:::note

Regenerating your backup codes will invalidate your previous codes. :::

1. Log in to the Cloudflare dashboard.
2. Select **My Profile**.
3. Select **Authentication**.
4. For **Two-Factor Authentication**, select **Manage**.
5. For **Backup codes**, select **Regenerate** to generate and save a new set of two-factor backup codes.

Disable two-factor authentication for your Cloudflare account

To disable 2FA for your Cloudflare account, you must delete all security keys and TOTP authenticators from your account.

:::note

If you are not the Super Administrator of an organization with **2FA Enforcement** enabled, you may not have permission to disable 2FA. :::

1. Log in to the Cloudflare dashboard.
2. Select **Profile**.
3. Select the **Authentication**.
   - To remove your security key:
     1. Select **Edit** in the **Security Key Authentication** card. A drop-down menu shows more details about your security key.
     2. Select **Delete**.
     3. Enter your Cloudflare password, then select **Remove**.
   - To remove your TOTP mobile application authentication:
     1. Select **Delete method** in the **Mobile App Authentication** card.
     2. Enter your Cloudflare password, authenticator application code, or a recovery code, then select **Disable**.

how to disable your TOTP mobile application authentication.

Use a backup code

If you lose access to a mobile device, security key, or authentication code, you can solve these issues by using a backup code or retrieving a backup code from your preferred authentication app.

Refer to Google's documentation to transfer Google Authenticator codes from one Android device to another.

When setting up 2FA, you should have saved your backup codes in a secure location. To restore lost access using a Cloudflare backup code:

1. Retrieve the backup code from where you stored it.
2. Go to the Cloudflare login page, enter your username and password and select **Log in**.
3. You should see a page titled **Two-Factor Authentication**

- If it has a text box, enter one of your backup codes and select **Log in**.
- If instead you see "Insert your security key and touch it", cancel any prompts from your browser that appear and select **try another authentication method or backup code**. Proceed to enter one of your backup codes and select **Log in**.

:::note

Once you use a backup code, it becomes invalid. :::

Related resources

- Google Authentication documentation
- YubiKey documentation
- Set up multi-user accounts on Cloudflare
- Account recovery

□□□ #2
□ □□□ □□□ 2026-11-01 02:25:36 UTC
□ □□□ □□□ 2026-11-01 02:25:38 UTC