EXONITA DOCS · EXONITA POS

# Sign-in security guide

Exonita POS · Restaurant

Protect your login with two-step verification: a 6-digit code from an authenticator app on your phone. Set it up, sign in with it, keep your backup codes, and confirm it's you before protected actions.

Screens captured 10 November 2026
Latest version online: https://docs.exonita.com/billing/security

# Contents

1. Before you begin
2. When your role requires two-step verification
3. Set up two-step verification
4. Sign in with your code
5. See and remove trusted devices
6. Confirm it's you before a protected action

### What you can do

- Turn on two-step verification for your own login
- Sign in with a code from your authenticator app, or with a backup code
- Trust a browser you use every day, and remove it later
- Confirm it's you before protected actions such as cancelling a bill

### Ask your administrator

- Lost or changed your phone? Use one of your backup codes to sign in. If you have none left, ask your administrator to **Reset two-step verification** for you in **User Manager**; then set it up again.
- If sign-in says your set-up deadline has passed, ask your administrator to reset your two-step verification.

Your administrator can change what your login can see. If a button in this guide is missing for you, ask them.

TASK 1

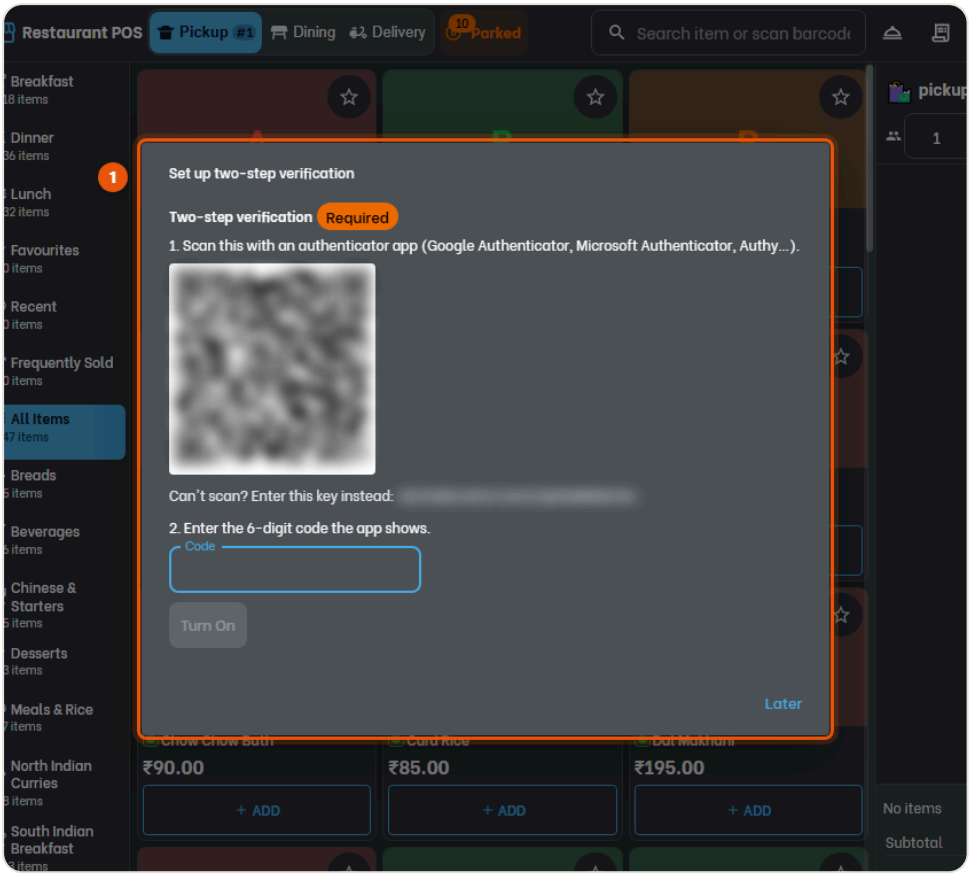
# When your role requires two-step verification

Know what the reminder after sign-in means and how long you have.

WHERE After you sign in

1. If your administrator requires two-step verification for your role, **Set up two-step verification** opens after you sign in, marked **Required**. Set it up right there (scan the QR code, enter the code, select **Turn On**, as in the next task), or select **Later** to be reminded at your next sign-in.

   **You'll see:** You can choose **Later** until the deadline your administrator set. After that, sign-in is refused until an administrator resets your two-step verification.




**IMPORTANT**

If your administrator set **0** days, there is no **Later**: you set it up the first time you sign in.

TASK 2

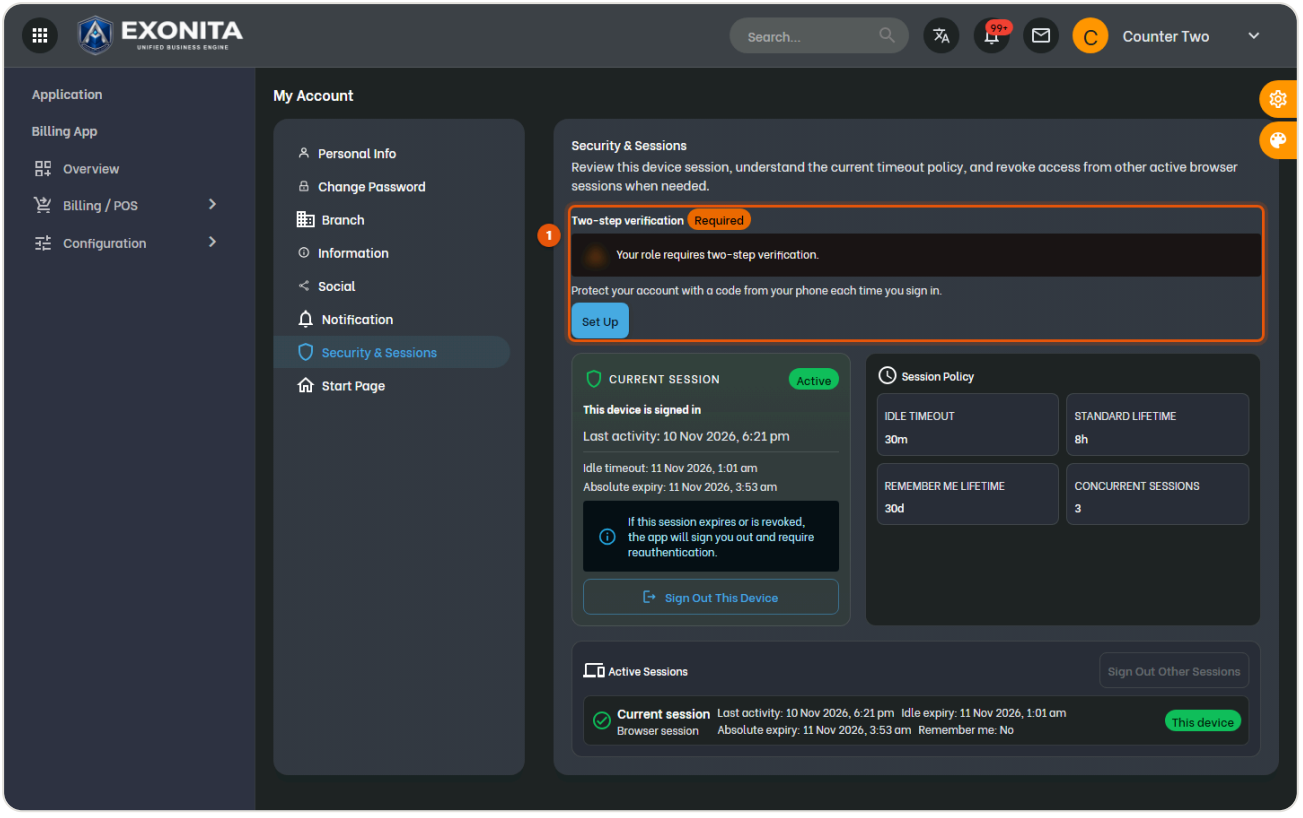
# Set up two-step verification

Link your login to an authenticator app on your phone.

WHERE Your name (top right) → My account → Security & Sessions

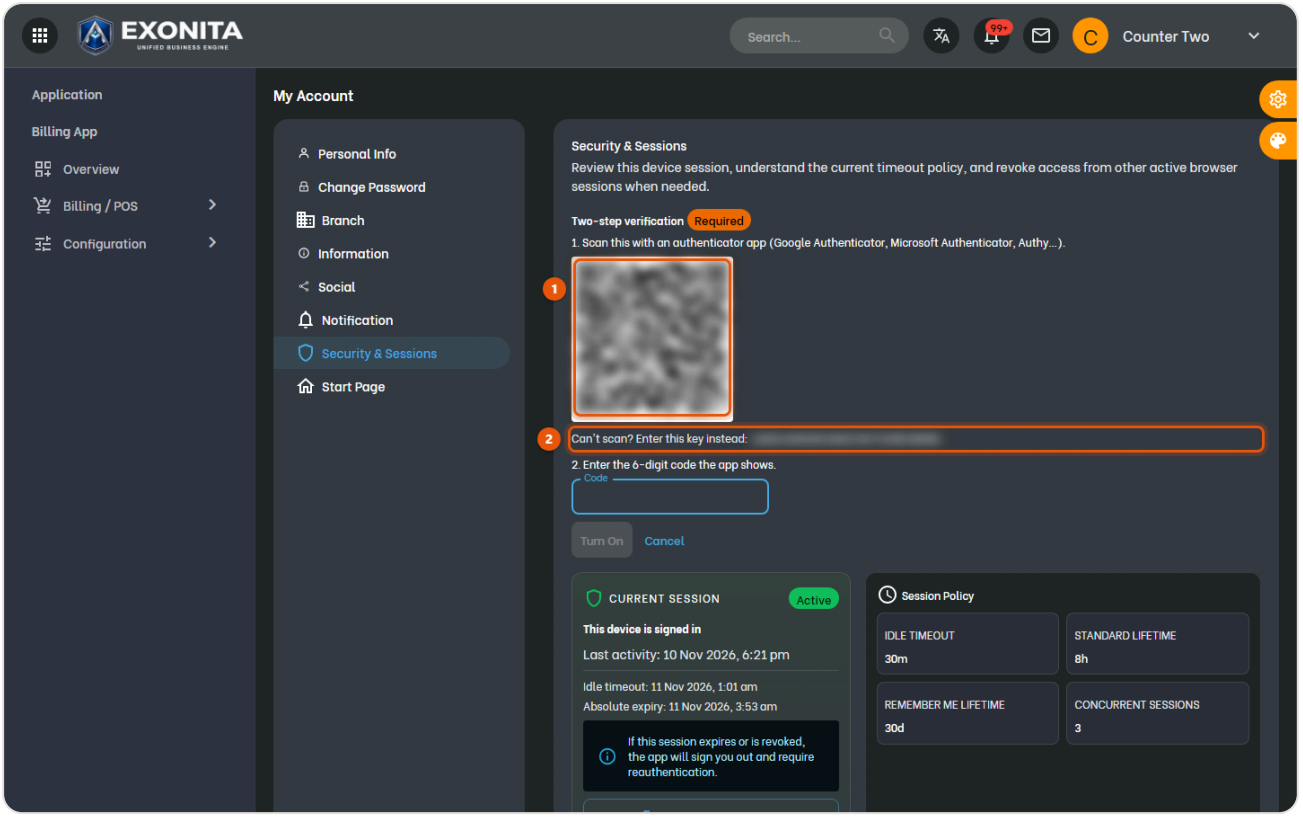
1 Install **Microsoft Authenticator** or **Google Authenticator** on your phone. Then select your name at the top right → **My account** → **Security & Sessions**. Next to **Two-step verification**, select **Set Up**.

**You'll see: Two-step verification** shows **Off** or **Required** until you finish.



2 In the authenticator app, add an account and scan the QR code. If you can't scan it, type the key shown under **Can't scan?** instead.

**You'll see:** The app shows a 6-digit code for Exonita that changes every 30 seconds.

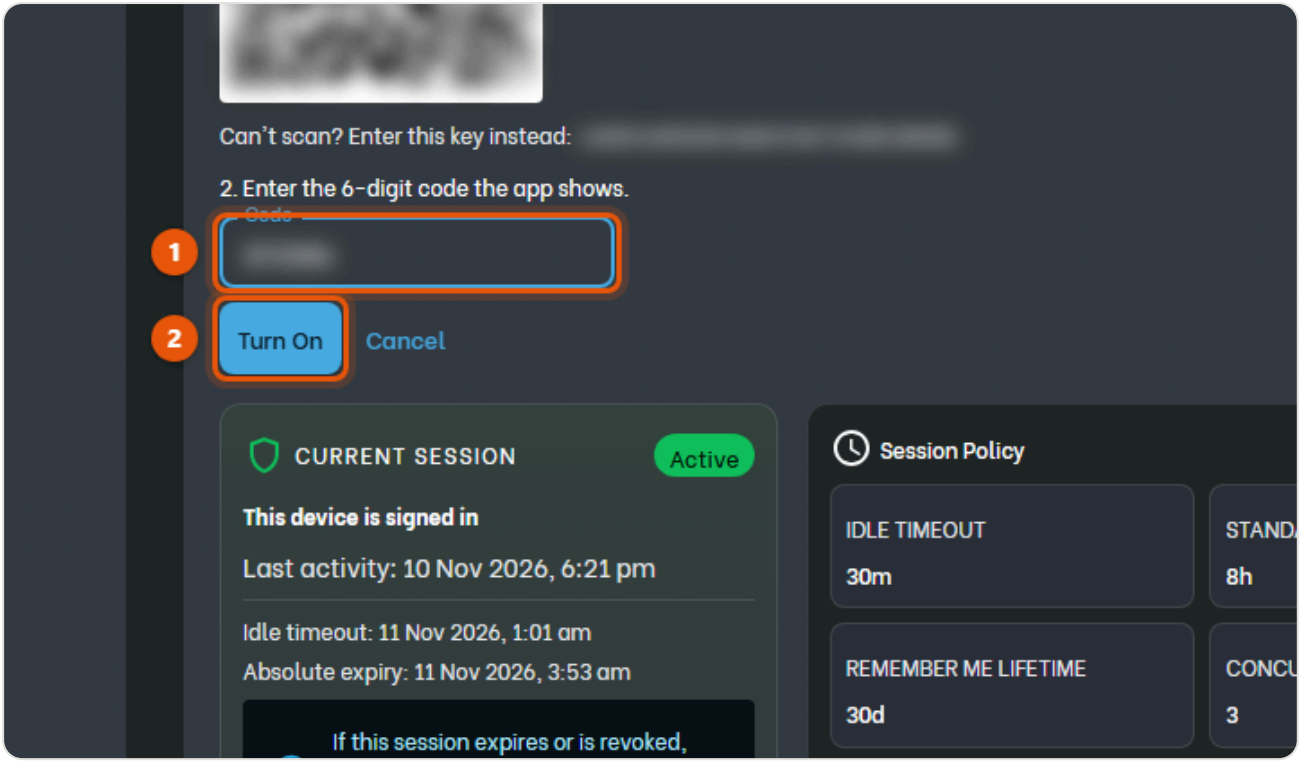



**IMPORTANT**

Never share the QR code or the key. Anyone who has them can make your codes.

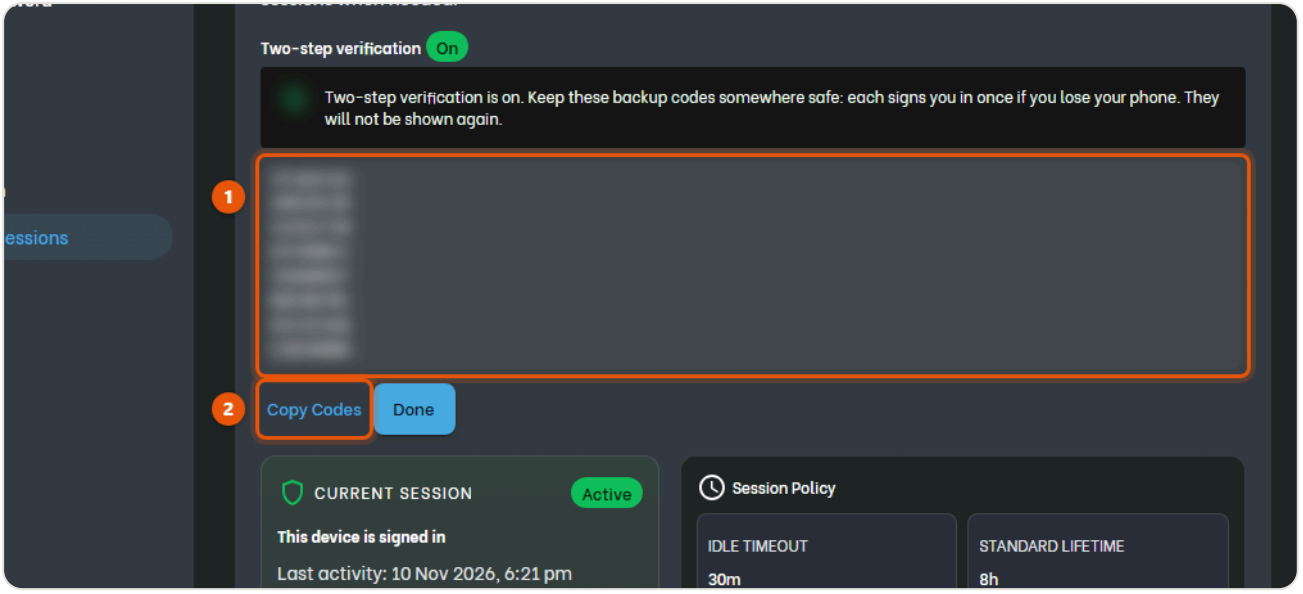
3 Type the 6-digit code from the app into **Code** and select **Turn on**.

**You'll see:** Two-step verification is on.



4 Your 8 **backup codes** appear. Select **Copy codes** and keep them somewhere safe, away from your phone, such as a password manager or a printed copy. Then select **Done**.

**You'll see:** Each backup code signs you in once if you lose your phone. They are not shown again.




**IMPORTANT**

Keep your backup codes. Without them, losing your phone means asking your administrator to reset your two-step verification.

TASK 3

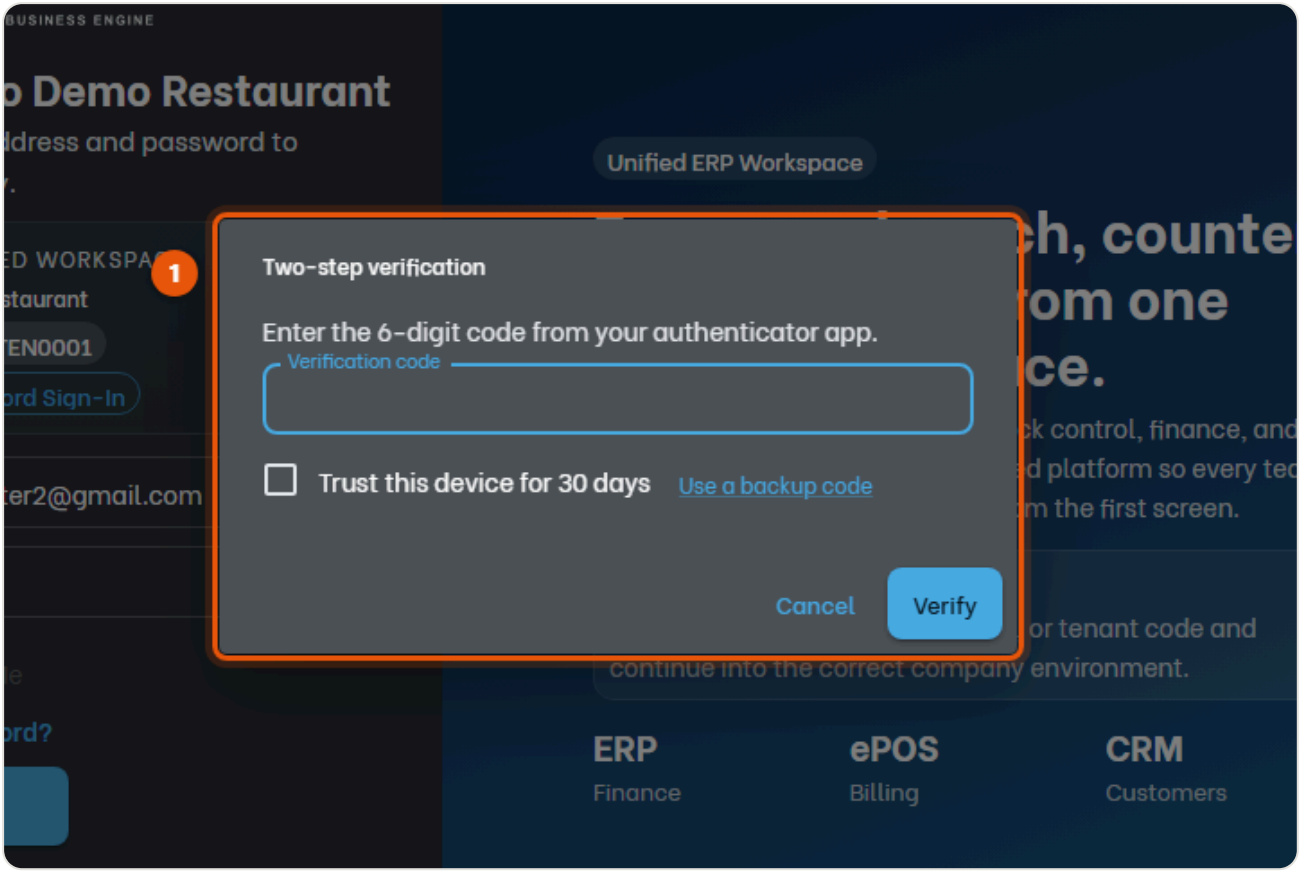
# Sign in with your code

Sign in once two-step verification is on.

WHERE Sign-in page

1. Sign in with your email and password as usual. **Two-step verification** then asks for the **Verification code**. Open the authenticator app and type the 6-digit code it shows for Exonita.

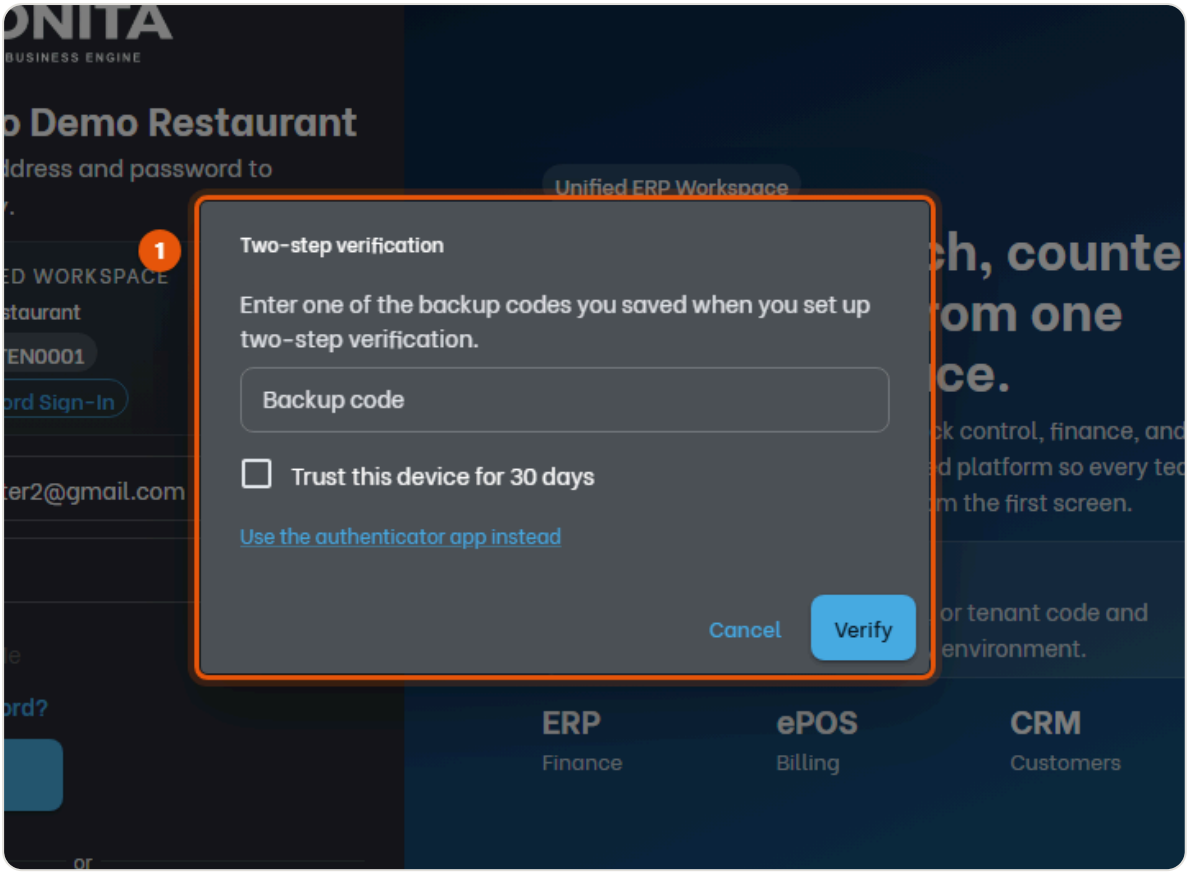
   **You'll see:** If the code is accepted, you are signed in.




> **TIP**
> A code that doesn't match usually means the phone's clock is off. Turn on automatic date and time on the phone and try the newest code.

2 No phone with you? Select **Use a backup code** and type one of your backup codes.

**You'll see:** You are signed in. That backup code can't be used again. Select **Use the authenticator app instead** to go back to the code.

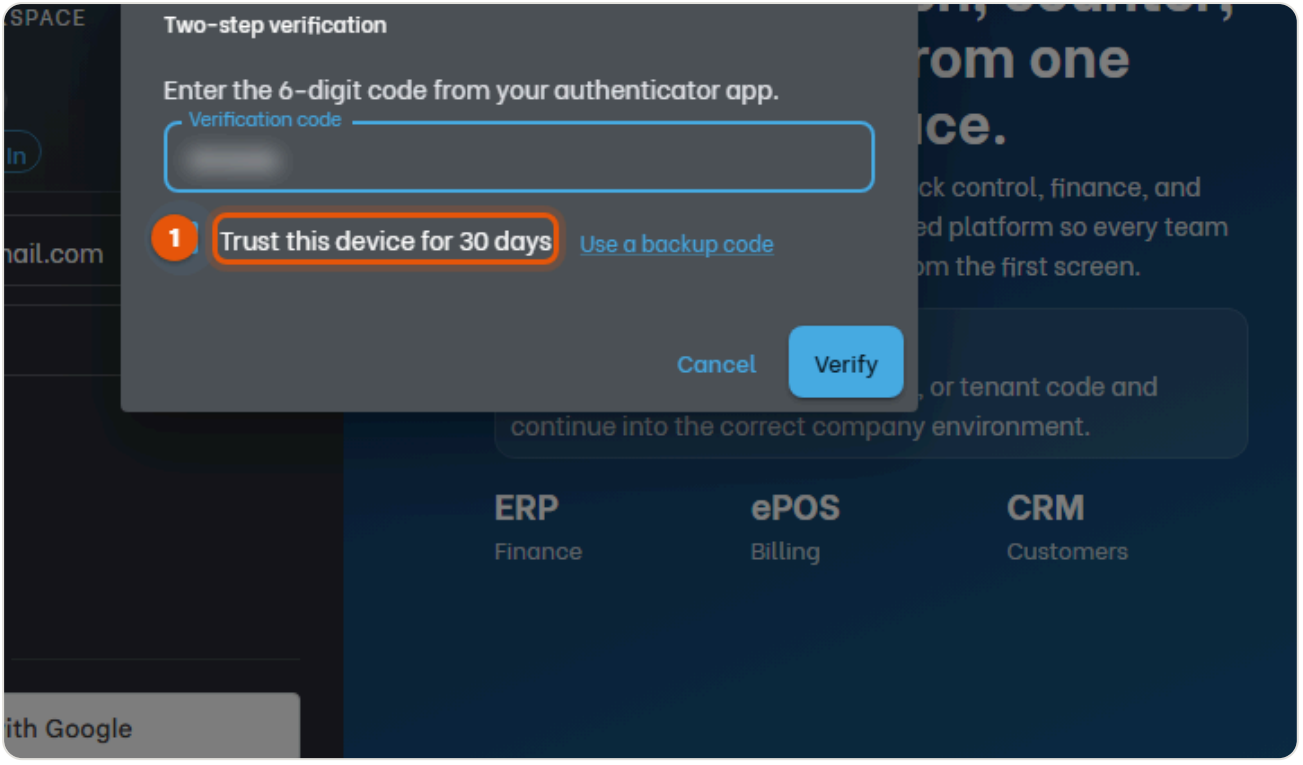



**TIP**

When you are running low on backup codes, get a fresh set: **My account** → **Security & Sessions** → **New Backup Codes**.

3 On a computer only you use, tick **Trust this device** before you enter the code.

**You'll see:** This browser won't ask for a code again for the number of days your administrator allows.




**IMPORTANT**

Never trust a shared counter PC. **Trust this device** shows only if your administrator allows it.

TASK 4

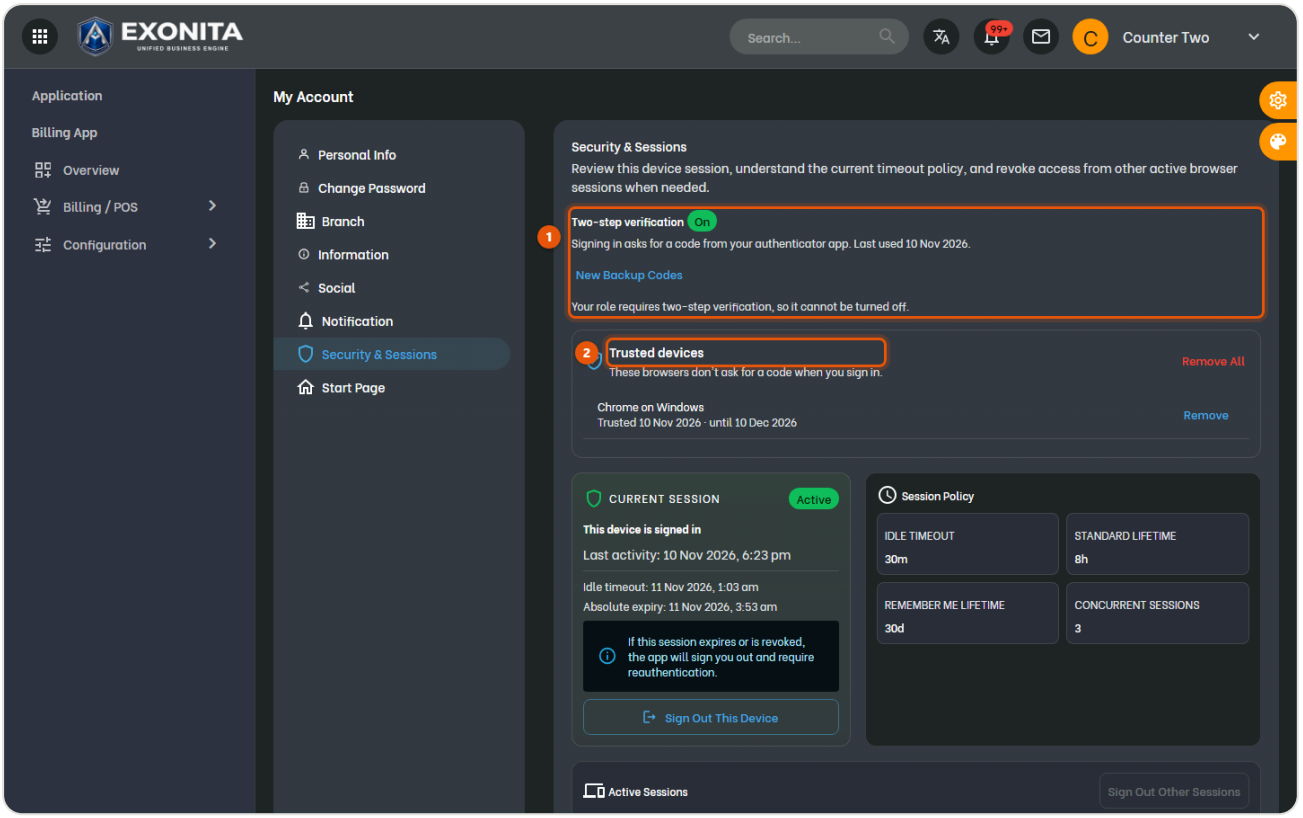
# See and remove trusted devices

Check which browsers skip the code, and stop one from skipping it.

WHERE My account → Security & Sessions

1. Open **My account → Security & Sessions**. **Two-step verification** shows **On**. Under **Trusted devices**, select **Remove** next to a browser to make it ask for a code again, or **Remove All**.

   **You'll see:** Select **New Backup Codes** if you have used most of yours: you enter a code from the app, and the new set replaces the old one.




> **TIP**
>
> Changing your password or turning two-step verification off forgets every trusted device.

TASK 5

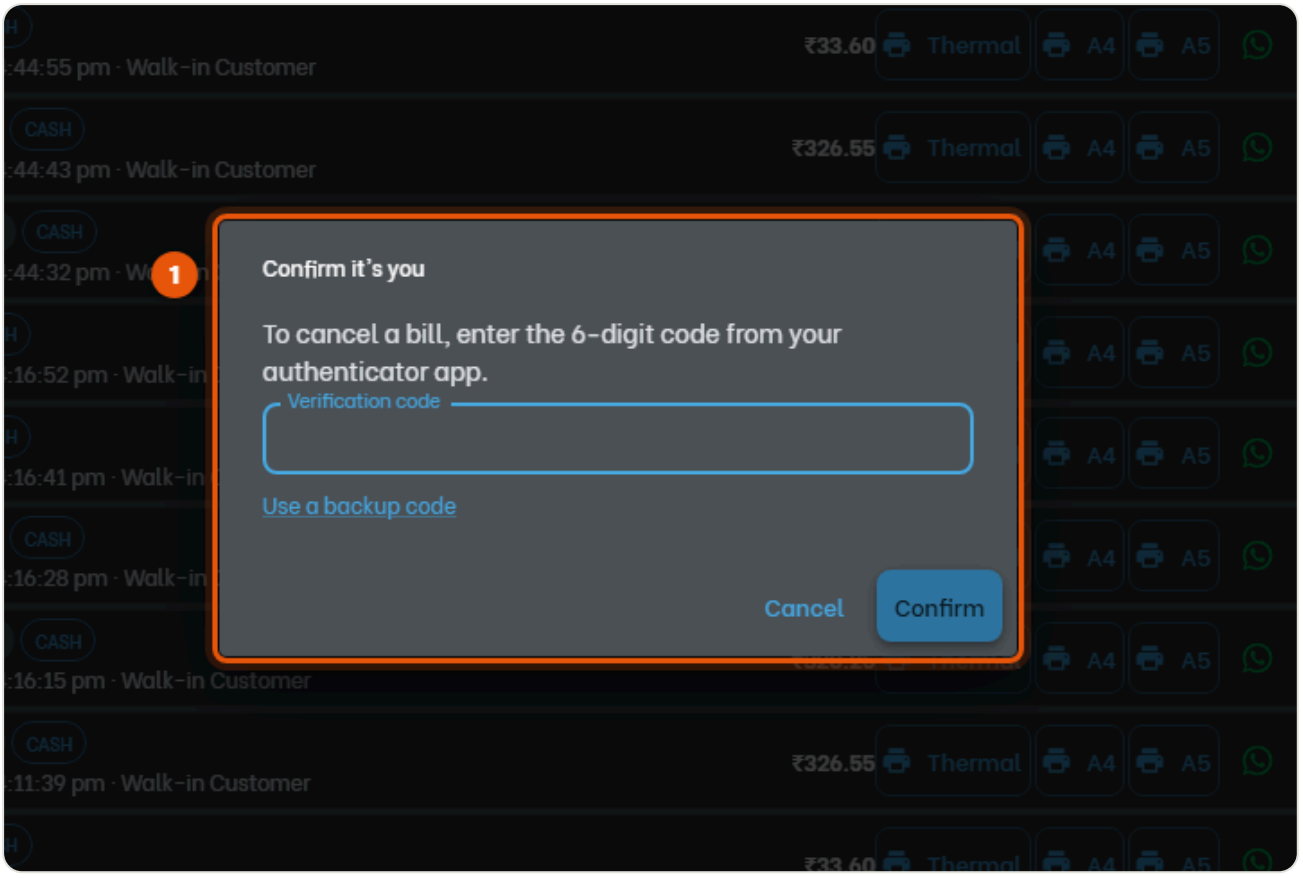
# Confirm it's you before a protected action

Know why some actions ask for your code or password again.

WHERE Any protected action, for example cancelling a bill

1. Your administrator can protect actions such as cancelling a bill, voiding a dish the kitchen already has, or changing users. When you do one, **Confirm it's you** opens: type the 6-digit code from your app (or a backup code). Staff without two-step verification type their password instead.

   **You'll see:** The action goes ahead. For about 4 minutes, repeating the same action doesn't ask again.




> **TIP**
> Select **Cancel** if you didn't mean to do it: nothing changes.