

Create google email password

1) Open google account and login:

<https://myaccount.google.com/>

2) Open **Drošība/Security**

- Home
- Personal info
- Data & privacy
- Security**
- People & sharing
- Payments & subscriptions
- About

Security

Settings and recommendations to help you keep your account secure

Your account is protected
The Security Checkup checked your account and found no recommended actions

[See details](#)

Recent security activity

New sign-in on Windows Oct 22 · Jelgava Municipality, Latvia >

[Review security activity](#)

How you sign in to Google
Make sure you can always access your Google Account by keeping this information up to date

2-Step Verification On since Mar 26 >

Passkeys and security keys Start using passkeys >

If 2-step verification is not available in the section, your company's email administrator must first enable it: [instrukction how to do it read here](#)

3) Ieslēgt "2-pakāpju verifikāciju / 2-Step verification"

← 2-Step Verification

Turn on 2-Step Verification

Prevent hackers from accessing your account with an additional layer of security.

Unless you're signing in with a passkey, you'll be asked to complete the most secure second step available on your account. You can update your second steps and sign-in options any time in your settings. [Go to Security Settings](#) ↻



[Turn on 2-Step Verification](#)

4) Create a password/key for emails

If there is no "App passwords" section in the Two-step verification / 2-step verification section, you must exit the page and re-enter it. Or use the link

<https://myaccount.google.com/apppasswords>

← 2-Step Verification

Your account is protected with 2-Step Verification

Prevent hackers from accessing your account with an additional layer of security.











Unless you're signing in with a passkey, you'll be asked to complete the most secure second step available on your account. You can update your second steps and sign-in options any time in your settings. [Go to Security Settings](#)



[Turn off 2-Step Verification](#)

Second steps

Make sure you can access your Google Account by keeping this information up to date and adding more sign-in options

 Passkeys and security keys	 Add a security key	>
 Google prompt	 2 devices	>
 Authenticator	 Add authenticator app	>
 Phone number	 29 489 925	>
 Backup codes	 Get backup codes	>

App passwords

App Passwords aren't recommended and are unnecessary in most cases. To help keep your account secure, use "Sign in with Google" to connect apps to your Google Account.

App passwords 1 App password >

5) Create password


← App passwords

App passwords help you sign into your Google Account on older apps and services that don't support modern security standards.

App passwords are less secure than using up-to-date apps and services that use modern security standards. Before you create an app password, you should check to see if your app needs this in order to sign in.


[Learn more](#)

Your app passwords

OZOLS Created on Mar 26 

To create a new app specific password, type a name for it below...

App name
CLOUDEX TMS



6) Copy new password and enter it in OZOLS or CLOUDEX TMS

Instructions for entering your email password in Ozols: <https://doc.ozols.lv/books/ozols-tms-english/page/5-e-mail-settings>

Instructions for entering your email password in CLOUDEX TMS: <https://doc.ozols.lv/books/cloudex-tms-english/page/e-mail-settings>

Generated app password

Your app password for your device

mout iekv rxib ierv

How to use it

Go to the settings for your Google Account in the application or device you are trying to set up. Replace your password with the 16-character password shown above.

Just like your normal password, this app password grants complete access to your Google Account. You won't need to remember it, so don't write it down or share it with anyone.

Done

Companies must have the option enabled that is available

[Instruktion from google](#)

The screenshot shows the Google Admin console interface. The top navigation bar includes the 'Admin' logo, a search bar for users, groups, or settings, and utility icons for notifications, a timer, help, and user profile. The left sidebar contains a navigation menu with categories like Home, Dashboard, Directory, Devices, Apps, Generative AI, and Security. The 'Security' section is expanded, showing 'Authentication' with '2-step verification' highlighted. The main content area is titled 'Security > 2-Step Verification' and displays settings for the organizational unit 'cloudex.lv'. The '2-Step Verification' settings are as follows:

- Authentication:** Locally applied. Description: Add an extra layer of security to user accounts by asking users to verify their identity when they enter a username and password. [Learn more](#)
- Allow users to turn on 2-Step Verification:** (highlighted in yellow)
- Enforcement:**
 - Off
 - On (highlighted in yellow)
 - On from:
- New user enrollment period:** Allows new users some time to enroll before enforcement is applied.
- Frequency:** Users can avoid repeated 2-Step Verification at login on their trusted devices. [Learn more](#)
 - Allow user to trust the device
- Methods:** Select the method to enforce. [Learn more](#)
 - Any
 - Any except verification codes via text, phone call
 - Only security key

Revision #4

Created Thu, Oct 23, 2025 8:35 AM by [Janis Veldre](#)

Updated Thu, Oct 23, 2025 8:56 AM by [Janis Veldre](#)