Two-step verification

Protecting your account with a second step, and setting it for your realm.

- Two-step verification
- Setting up an authenticator app
- Recovery codes
- Lost or forgotten phone
- Trusted browsers
- The email code
- Sign-in paused or blocked
- The realm's two-step verification policy (SUPERADMIN)
- Following users' two-step verification (administrators)
- When your realm requires an authenticator app
- Temporary exemption (SUPERADMIN)
- Second-step reset (SUPERADMIN)
- Desktop applications (Le Sage, Aïda, Inpro) and two-step verification

Two-step verification

Two-step verification protects your account even if someone knows your password: after your password, the platform asks for a second proof that it's really you. **It is mandatory for everyone.**

It covers every application of the Improvize platform (Studio, Karyo, Le Sage, Aïda, Inpro…): you set it up once, in your profile, and it applies everywhere you have an account.

Second steps you can use

Second step	Protection level	For whom
Email code	◫ Not recommended	Everyone: always on, nothing to set up
Authenticator app (Aegis, Google Authenticator, Microsoft Authenticator, 1Password, YubiKey…)	◫ Recommended	Anyone who wants it, and required where your realm demands it
Recovery codes	—	As a fallback, when you don't have your phone

If you set up an app, you pick between the app and the email code at each sign-in. But as long as the email code is accepted, your account is only as safe as your mailbox. Where your realm requires an app, only the app is accepted.

Where to set it up

In your profile, **Password and authentication** section, under the password. Every change asks for your password and a code, so that someone who gets hold of your open session can't weaken your protection.

At each sign-in

- After your password, you type a code: the one sent by email, or the one from your app.

  On a trusted browser, the code isn't asked again for 30 days.
- **First sign-in** and **forgotten password** also end with a code. Resetting your password never removes your authenticator app.

- In **file emails**, download links still give you the file without signing in. The button takes you to the sign-in page, then to the file.
- There is no signing in with a link sent by email.
- Opening another of your accounts from the session picker asks for nothing more.

When your realm requires an app

Your realm's SUPERADMIN can require an authenticator app for its administrators, for its other users, or for both. If you don't have one yet, your next sign-in stops, after the email code, at setting one up: see When your realm requires an authenticator app.

Learn more

- The email code
- Setting up an authenticator app
- Recovery codes
- Lost or forgotten phone
- Trusted browsers
- Sign-in paused or blocked
- For SUPERADMINs: the realm's policy

Setting up an authenticator app

An authenticator app shows a six-digit code that changes every 30 seconds. It's the safest second step: it depends neither on your mailbox nor on the network. It's optional, unless your realm requires it.

Which app?

Any TOTP-compatible app works, for example **Aegis** (Android), **Google Authenticator**, **Microsoft Authenticator** or **1Password**. A **YubiKey** works too, with the **Yubico Authenticator** app.

Setting it up

1. Open your profile, **Password and authentication** section, and choose **Set up an authenticator app**.
2. Confirm it's you: your password and a code sent by email.
3. **Scan the QR code** with your app. If you can't scan it, type the key shown under the QR code.
4. **Type the code** the app shows.
5. Save your recovery codes: they are shown only once. **Continue** becomes available only once "I have saved these codes somewhere safe" is ticked.

> **Tip: scan the QR code on two devices** (your phone and a tablet, a YubiKey, or a desktop app) before typing the code. Both will show the same codes, and losing one device won't lock you out.

When your realm requires an app and you don't have one, the same steps are shown **when you sign in**, after the email code, and you get in only once the app is set up: see When your realm requires an authenticator app.

Changing phones

Profile → **Change phone**: scan the new QR code and type a code. The old app keeps working until you confirm. You get new recovery codes, and your trusted browsers are forgotten.

Lost your old phone? See Lost or forgotten phone.

Removing the app

Profile → **Remove**: you're back to the email code alone. Not possible when one of your realms requires an app: the button is then greyed out and names the realm. You can always replace it (change phone).

Every addition, replacement or removal is confirmed by email, to all your confirmed addresses.

Recovery codes

Recovery codes let you sign in **without your phone**. You get ten of them when you set up an authenticator app.

Keeping them

- They are **shown only once**: download them (.txt), print them or copy them into your password manager.
- Keep them somewhere other than the phone that holds your app.
- Never give them to anyone: with your password, each one opens your account.

Using them

When you sign in, after your password, choose **Recovery code** and type one of them.

- **Each code works only once.**
- After a recovery code, "Trust this browser" is not offered.
- You get an email each time a code is used, with how many are left. If it wasn't you, change your password.

Getting new ones

When only two are left, the platform reminds you at sign-in. Profile → **Generate new codes**: the old ones stop working at once. You also get new ones when you change phones.

Recovery codes exist only while an authenticator app is set up.

Lost or forgotten phone

You have your recovery codes

1. Sign in with your password, then **Recovery code**.
2. In your profile, choose **Change phone** and set up your app on the new phone. A recovery code is accepted to confirm it's you.
3. Save the new recovery codes.

Also forget, in your profile, any trusted browsers you don't recognise (changing phones forgets them all).

You no longer have your recovery codes

If none of your realms requires an app, simply sign in with an **email code**, then set up a new app in your profile (or remove the old one).

Otherwise, ask your realm's SUPERADMIN for a **second-step reset**. It wipes your authenticator app, recovery codes and trusted browsers; at your next sign-in, you get in with an email code, then set up a new app before reaching your accounts.

If your accounts are spread over unrelated realms, or if you are the SUPERADMIN yourself, ask the SUPERADMIN of the parent realm or **Improvize support**.

You only forgot your phone

If your realm requires an authenticator app, its SUPERADMIN can grant you a **temporary exemption**: for 24 hours, your account accepts the email code instead of the app. It can be renewed day by day if needed. You get an email when it's granted and when it ends.

Or simply use a recovery code.

Trusted browsers

On a trusted browser, the platform doesn't ask for your second step again for **30 days**. Your password is still asked.

Trusting a browser

When typing your code, tick **Trust this browser for 30 days**. The box is never ticked for you.

- **Don't tick it on a shared computer** or one that isn't yours.
- It's not offered after a recovery code.
- A browser trusts only one account at a time, and the trust survives signing out.
- You get an email for each new trusted browser (browser, operating system, time, IP address). If it wasn't you, forget it and change your password.
- If your realm requires an authenticator app, a browser trusted with an email code doesn't count.

Forgetting them

Profile, **Password and authentication** section → **Trusted browsers**: the list shows each browser, its operating system, when it was added, which second step earned it, when it expires and which one is "This browser". **Forget** removes one, **Forget all** removes them all. No code is asked.

All your trusted browsers are also forgotten automatically when:

- you change your password;
- you add, replace or remove your authenticator app;
- an administrator resets your second step.

The email code

The email code is a six-digit code sent, at each sign-in, to the address you typed. It's everyone's second step: **it's always on**, needs no setup and can't be turned off.

- It's valid for **10 minutes** and works only once.
- A new code replaces the previous one (**Resend** becomes available after a short wait).
- After five wrong tries the code stops working: ask for a new one.
- The code is in the email's subject.
- If it's your only second step, it's sent automatically after your password. If you also have an app, choose **Email code** to receive it.

It's also used at your **first sign-in**: after choosing your password, you get a code. This checks that you can still reach that mailbox, even if the welcome email is weeks old.

Why it's not recommended

The email code is only as safe as your mailbox: someone who gets into it, and knows your password, can sign in as you. An authenticator app doesn't depend on your mailbox; that's why the platform shows the email code in orange ("Not recommended") and the app in green.

If you've set up an app, the email code is still accepted alongside it (except where your realm requires the app): your account is then only as safe as your mailbox. So protect your mailbox well (a password of its own, two-step verification on your email account).

Not receiving the code

Check your spam folder, wait a minute, then click **Resend**. The code goes to the address typed on the sign-in screen.

Sign-in paused or blocked

Every wrong code (app, email or recovery code) is counted. A wrong code after a correct password means **your password is known**: the platform protects itself.

Paused

After **10 wrong codes in a row**, sign-in is paused for **15 minutes**; each further series of 10 doubles the pause, up to 24 hours. The screen tells you when to try again. You get an alert email with the browser, operating system, time and IP address of the attempt.

If it wasn't you, change your password: someone knows it.

Blocked

After **100 wrong codes**, the second step is blocked: your password is still recognised, but no session opens. Only a **second-step reset** unblocks it: contact your realm's SUPERADMIN, or Improvize support.

Resending an email code doesn't reset the count; a correct code does.

The realm's two-step verification policy (SUPERADMIN)

For SUPERADMINs. Everyone signs in with at least an email code. A realm's two-step verification policy decides **who must also use an authenticator app**. It's set in **Edit realm → Security**, a section only SUPERADMINs see.

Settings

Two independent switches:

- **Authenticator app required for administrators**: this realm's ADMIN and SUPERADMIN accounts.
- **Authenticator app required for other users**: this realm's artist and consultant accounts.

By default, neither is on: the email code is enough.

A user concerned who doesn't have an app yet is stopped, at their next sign-in and after their email code, at setting one up: no session opens until the app is set up. No email goes out when you change the policy: **warn your users** beforehand, so they have their phone at hand.

Policies add up

A switch turned on in a realm also applies to **every realm below it**. A subrealm can turn on a switch its parent leaves off, never turn off a parent's: the section says so ("The parent realm … already requires …") and the switch is greyed out ("imposed above").

Each account is judged in its own realm: someone who is ADMIN in one realm and an artist in another falls under the first realm's administrators switch and the second realm's other-users switch. At sign-in, if any one of their accounts requires an app, the app is required.

The Improvize realm's policy applies only to its own users.

Before saving: the preview

Before you save, the section shows how many people **will have to set up an app at their next sign-in** with the new setting, in this realm and the ones below.

Who can change it

A SUPERADMIN, on their realm and the ones below (Improvize support everywhere). ADMINs don't see it. Under the policy, "Last changed by … on …" and **History** list every change (from what, to what, by whom, when).

See also

- When your realm requires an authenticator app
- Following users' two-step verification
- Temporary exemption
- Second-step reset

Following users' two-step verification (administrators)

For ADMINs and SUPERADMINs.

In the user list

One cell shows, for each account, the person's second steps: **email** or **email + app**.

- **Green**: at least what this realm and the ones above require of this account.
- **Red**: below that. A red "email" means an app is required and not set up yet: the person will have to set it up at their next sign-in.

The cell never shows trusted browsers, the number of recovery codes left, or the last method used.

In the user's sheet

The **Two-step verification** block of the sheet repeats that status and, only when true:

- **Exempted until …** — see Temporary exemption;
- **Second step blocked** — see Second-step reset.

An ADMIN sees this block read-only. A SUPERADMIN also finds the buttons for the actions they're allowed to take; a greyed-out button says why (for example "accounts outside your realms — only Improvize support can reset").

The security log

View log lists the person's security events: refused sign-ins, authenticator app added or removed, trusted browsers, administrators' actions, desktop application sign-ins. Only a SUPERADMIN who could reset this person (and the person themselves) can see it, because it may involve other realms. Entries are kept for 12 months.

When your realm requires an authenticator app

A realm's SUPERADMIN can require an authenticator app of its administrators, its other users, or both (see the realm's policy). The email code is then no longer enough for those accounts.

If you don't have an app yet

At your next sign-in:

1. Type your password, then the code sent by email: it proves it's you before an app is attached to your account.
2. The **Set up an authenticator app** screen names the realm that requires it. Scan the QR code, then type the code the app shows (details in Setting up an authenticator app).
3. Save your recovery codes and tick "I have saved these codes somewhere safe".
4. Your session opens. You can tick "Trust this browser" at step 2.

There is no "Later" button: no session opens until the app is set up. If you don't have your phone that day, ask your realm's SUPERADMIN for a temporary exemption.

Afterwards

- At each sign-in, only the app (or a recovery code) is accepted; the email code no longer is for that account.
- A trusted browser earned with an email code no longer counts.
- You can't remove the app while the realm requires it, but you can change phones.

Temporary exemption (SUPERADMIN)

For SUPERADMINs. "I forgot my phone": a temporary exemption lets a user sign in with an email code while your realm requires an authenticator app. Someone who doesn't have an app yet isn't stopped at setting one up during the exemption either.

Granting

User's sheet → **Exempt 24 h**. For 24 hours, this account accepts the email code instead of the app. The person gets an email. **Renew** extends it by 24 hours, **End now** ends it.

- The exemption lowers the requirement to the email code, never further: two-step verification stays mandatory.
- It applies only to this realm: if another of the person's realms also requires an app, that realm's exemption is needed too.
- It doesn't allow removing the app: it's for a forgotten phone, not a lost one. For a lost phone, see Second-step reset.

Who can grant it

A SUPERADMIN of the highest realm that requires the app for this account, or above, or Improvize support: only someone who could have changed the policy can exempt from it.

Second-step reset (SUPERADMIN)

For SUPERADMINs. A reset is for a user who lost both their phone and their recovery codes, or whose second step is blocked.

What it wipes

User's sheet → **Reset second step**: their authenticator app, recovery codes and trusted browsers are wiped, and the block is lifted. **The action is immediate and cannot be undone.** The person gets an email.

At their next sign-in, they get in with an email code, which is always on. If one of their realms requires an app, they will have to set up a new one before reaching their accounts. Their password doesn't change.

Who can reset

- A **SUPERADMIN**, never an ADMIN.
- Never on yourself: a SUPERADMIN who lost their phone uses their recovery codes, then asks the SUPERADMIN of the parent realm or Improvize support.
- Only if **every account** of the person is in your realms (yours and the ones below). Otherwise, only Improvize support can reset.

Second step blocked

After 100 wrong codes, a person's second step is blocked: their password is recognised but no session opens. The sheet shows **Second step blocked**. Before resetting, check with the person that the attempts were theirs; if not, also ask them to change their password. See Sign-in paused or blocked.

Desktop applications (Le Sage, Aïda, Inpro) and two-step verification

For customers who send statements to Karyo from the desktop versions of Le Sage, Aïda or Inpro.

These programs sign in to Karyo on their own, with an administrator's email and password stored in their settings: no one is there to type a code.

Two-step verification doesn't cover the desktop applications

The stored password keeps working without a code, while two-step verification is mandatory everywhere else. Nothing needs to change in the program. This way of signing in will disappear with the desktop versions.

One email per program and IP address: that's expected

Each first sign-in of a program from a new IP address sends an email: "your password opened a Le Sage session from <IP address> without a second step". So when two-step verification goes live, you'll get one per program and per office IP address: **that's expected, not an attack.**

An email from an IP address you don't know, on the other hand, means someone else is using that password: change it (then update the program's settings). An office IP address that changes regularly triggers the email again at each change.

When sending stops

Sending to Karyo is refused while that account is:

- **paused** after too many wrong codes on the web (it resumes when the pause ends);

- **second step blocked** (it resumes after a second-step reset).

See Sign-in paused or blocked.