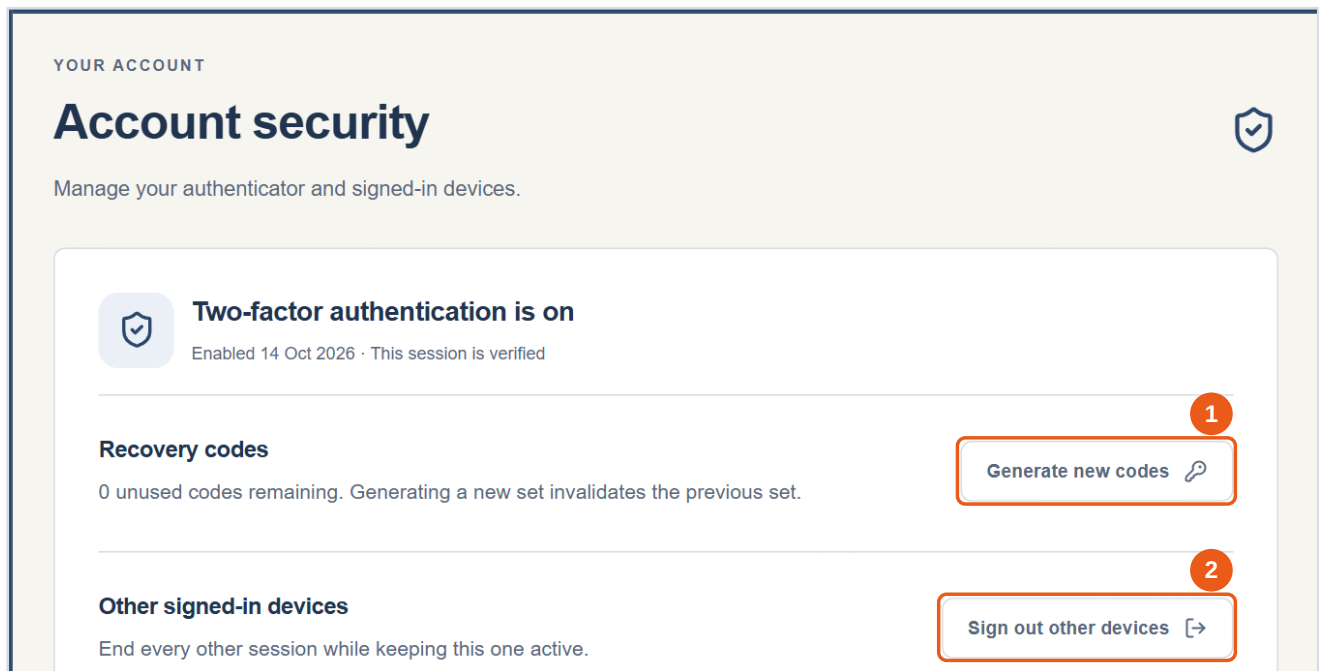


Review privileged account security

Open Account security using your own privileged account. Follow the orange numbers on the screenshot.



Actual application screen. All people, companies and training shown are fictional examples.

What to do

1. Choose Generate new codes when you need a fresh recovery set. Store it securely; the previous codes become invalid.
2. Choose Sign out other devices to end your other sessions while keeping this session active.

REMEMBER

The example contains no authenticator secret or recovery code. Keep recovery material outside ordinary case notes.

Scope and daily administration

For SUPER_ADMIN users. Read the Eurolearn administrator manual for the full company, commerce, publication, support and certificate procedures.

Use the existing platform workflows

SUPER_ADMIN shares the Eurolearn administration menus and supported business workflows. There is no separate super-administrator dashboard or general role editor in the current frontend.

Use Companies and orders, Course Studio, Certificate management, Training support, Privacy requests and Audit history as described in the administrator guide. Complete MFA; this role does not bypass authentication or immutable evidence.

Separate platform and company responsibility

Company administration is tied to an active organization administrator membership. Check the selected company and use the normal company workflow for membership, training-time review and API-key management.

A platform account and a company Primary Administrator are different responsibilities. Do not interpret broad platform access as permission to approve a crew duty interval without the responsible operator's review.

Academies add scoped training-provider roles. They are optional for organizations; refer to the Academy administrator guide for staff, client, commerce and certificate responsibilities.

Privileged-account changes

1. Verify the business need, target person and required role before requesting a privileged-account change.
2. Coordinate the change with the technical maintainer through the approved operational process. The current frontend does not provide a general global-user role-management screen.
3. Confirm that the user can complete MFA and sees only the expected workspace. Arrange removal of obsolete privilege and review existing sessions when access changes.

REMEMBER

Never use a shared demo or emergency account for routine operations. Keep credentials and recovery material out of this manual and out of ordinary support records.

Release and integration oversight

Coordinate product-owner decisions with the technical maintainer before enabling external services or operational training.

Before accepting operational users

- Confirm the deployed hostname, email delivery, account recovery and MFA workflows.
- Confirm company ownership, course review, approved certificate material and the handling of demonstration content.
- Verify that backups, restore rehearsal, monitoring and production database checks are completed by the technical owner.
- Confirm the privacy/retention procedure and the channels customers should use for support.

Payment-provider readiness

Platform Stripe requires onboarding, server keys and a verified webhook; checkout starts disabled. Qualify failed/interrupted payment and reconciliation before live use. Academy invoice sales remain a separate seller workflow and do not inherit platform Stripe checkout.

Make sure staff understand invoice issuance outside Eurolearn, exact-amount bank confirmation and the treatment of received payments awaiting access activation. Assign an owner for refund/dispute review and settlement reconciliation.

Training integrations and video

Company keys expose reviewed training records, not a complete flight-duty roster. Direct FL3XX/Leon adapters require vendor access, mapping and testing before operational use. Crew-code matches must be confirmed within the company.

Verified Vimeo completion is still pending. Do not present a saved video identifier or a draft preview as an enabled video-completion workflow.

Approve a release with evidence

Review test results and remaining limitations with the technical owner. The local SQLite/browser checks do not replace production PostgreSQL concurrency, recovery and real-provider qualification.

REMEMBER

Credentials are configured by the technical owner in the appropriate environment. They are never entered into FAQ content, user manuals or frontend source.

Start an incident evidence review

Use Audit history alongside the affected business record. Follow the orange numbers on the screenshot.

EUROLEARN ADMINISTRATION

Audit history

Review recorded actions and their changes. Showing the latest 500 matching events.

action	1	Record ID	2
from	3	to	4
dd/mm/yyyy		dd/mm/yyyy	

Actual application screen. All people, companies and training shown are fictional examples.

What to do

1. Select the relevant action type.
2. Enter the affected record identifier.
3. Set the beginning of the incident window.
4. Set its end, review the events and hand over the exact references.

REMEMBER

A broad platform role does not replace the responsible company's review of its training-time evidence.

Incidents and administrative continuity

Preserve evidence, establish the scope and assign a responsible owner before attempting recovery.

Investigate a reported incident

1. Collect the time, affected user/company and record reference, the visible error and the last successful action. Do not request passwords, card details or recovery codes.
2. Check Audit history and the relevant business record. Distinguish a pending operation from an operation that failed before saving.
3. Escalate suspected unauthorized access, payment inconsistency or service failure to the technical owner. Coordinate any containment through supported account/key controls and operational procedures.
4. After recovery, confirm the customer-visible result and document the outcome. Retain the evidence and corrections rather than deleting the incident's historical records.

Special cases

- Payment received but access missing: use provider reconciliation and the paid-activation review path; do not create a second payment.
- Incorrect certificate: use revoke/replace, preserving the original certificate and its history.
- Incorrect reviewed training interval: the company administrator creates a correction or void revision; an integration must process that revision.
- Published content error: prepare and review a successor version; do not modify the original published question bank.
- Lost privileged access: use the approved recovery process with the technical maintainer; do not reseed or reset the user database.

Keep the handover usable

Maintain a responsible owner and next action for open issues. Review administrator coverage and the ownership of payment, company and provider accounts before personnel changes.

Keep the FAQ and manuals aligned with released behavior. Route content corrections to the development team; do not document planned buttons or integrations as if they already exist.

REMEMBER

Use the Learner guide for training, Organization administrator guide for company memberships, Academy administrator guide for provider operations, and Eurolearn administrator guide for platform work.