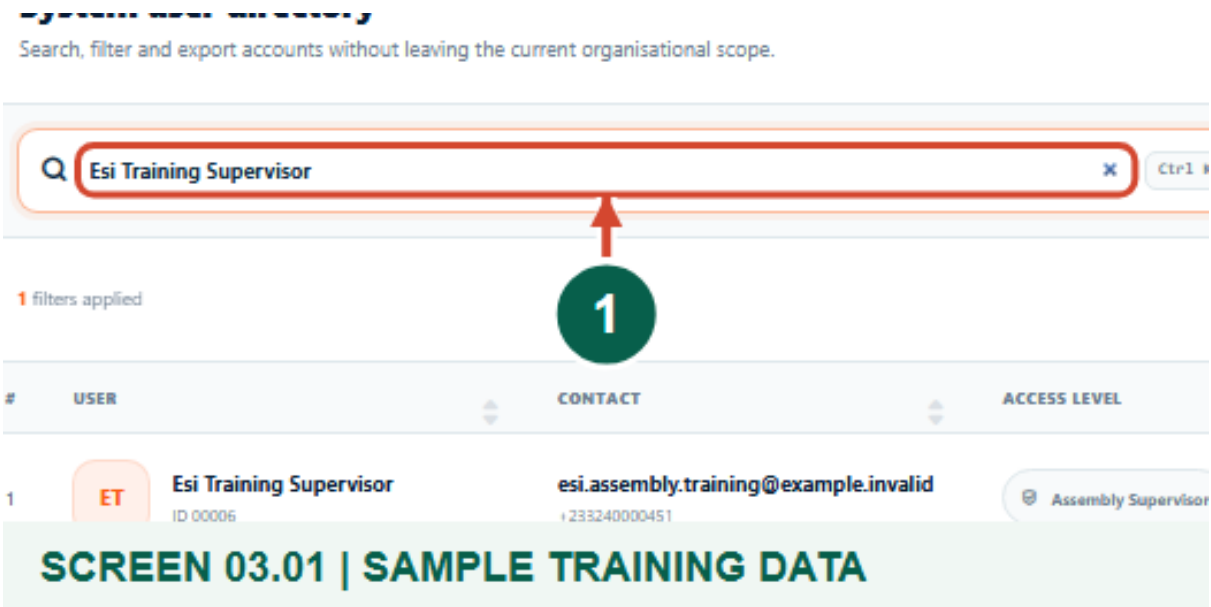


Manage assembly users

Find and review a staff account, make permitted changes within your own assembly, manage account status and start a secure password setup-link reset when justified.

WHO THIS IS FOR	ALLOW ABOUT	DOCUMENT VERSION
Assembly administrators	15-20 minutes	1.0 19 October 2026



Illustrated steps with numbered arrows and clear expected results.

About the examples

Screens show the actual application in a training environment with sample data. Use your own verified account, assigned records and contact details when following the guide.

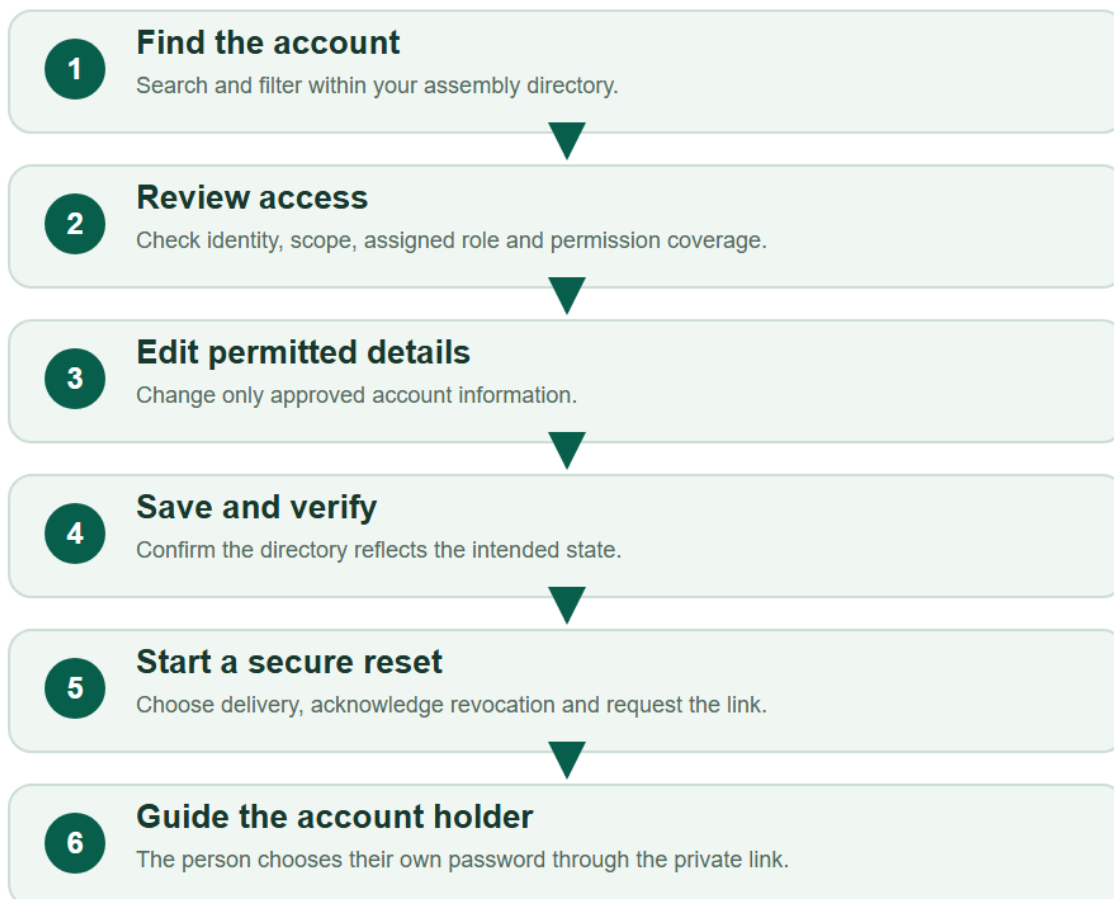
Website: assembly.gyentoboa.com

Process flow

Follow the arrows from start to finish. Optional routes are explained in the numbered steps.

Before you start

- Sign in as an Assembly Administrator with permission to view and edit users. Resetting another user also requires permission to reset passwords.
- Confirm the staff member's identity and an authorised reason for any contact, role, status or credential change.
- Check the registered contact before a reset. Resetting immediately revokes the former credential and existing sign-ins; the person must receive and use the private setup link.

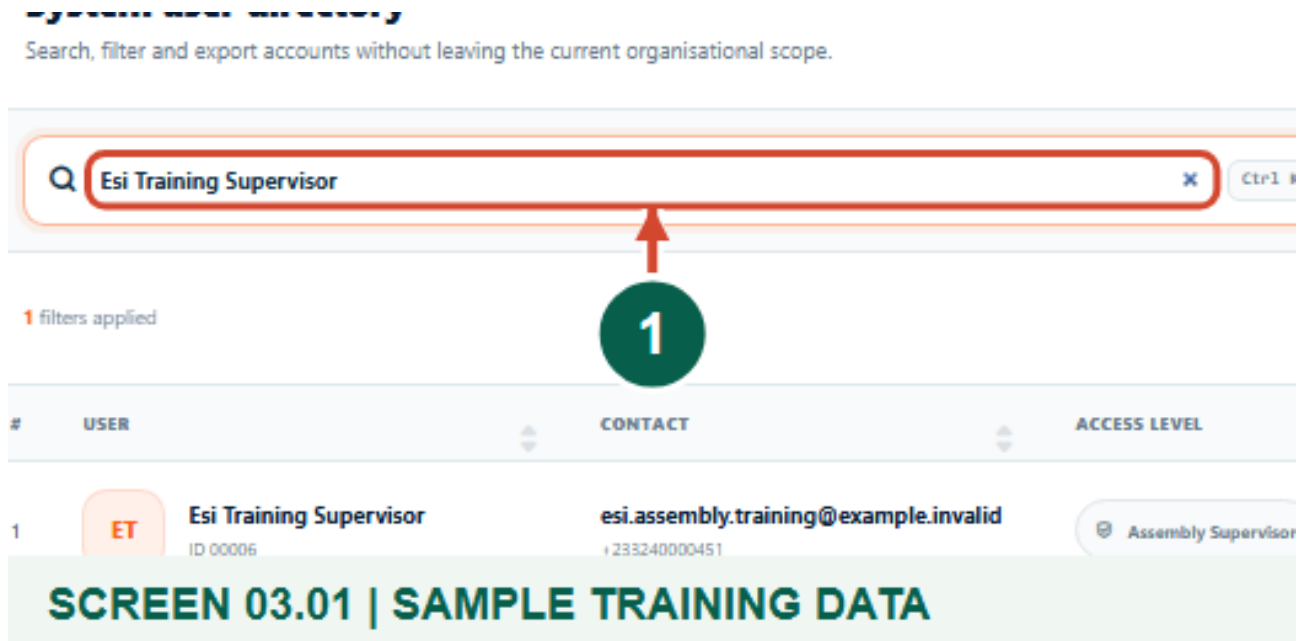


Numbered markers on screenshots identify the controls described beneath each image.

STEP 01

Find the correct staff account

1. Open Administration, then Users. Search by name, email or phone and use Status, Access or Role filters as needed.
2. Check the identity and assembly carefully before selecting a row action. Clear filters if an expected record is hidden.



Synthetic training data. Find the correct staff account.

- 1 Search staff accounts

What should happen

The intended account is visible within your permitted assembly scope.

STEP 02

Review identity, scope and effective access

1. Choose the row View action and read Account information, Assigned role and Permission coverage.
2. Confirm you have selected the right person. Choose Edit account only when the proposed change is authorised.



is currently attached to this account.

SCREEN 03.02 | SAMPLE TRAINING DATA

Synthetic training data. Review identity, scope and effective access.

1 Assigned role

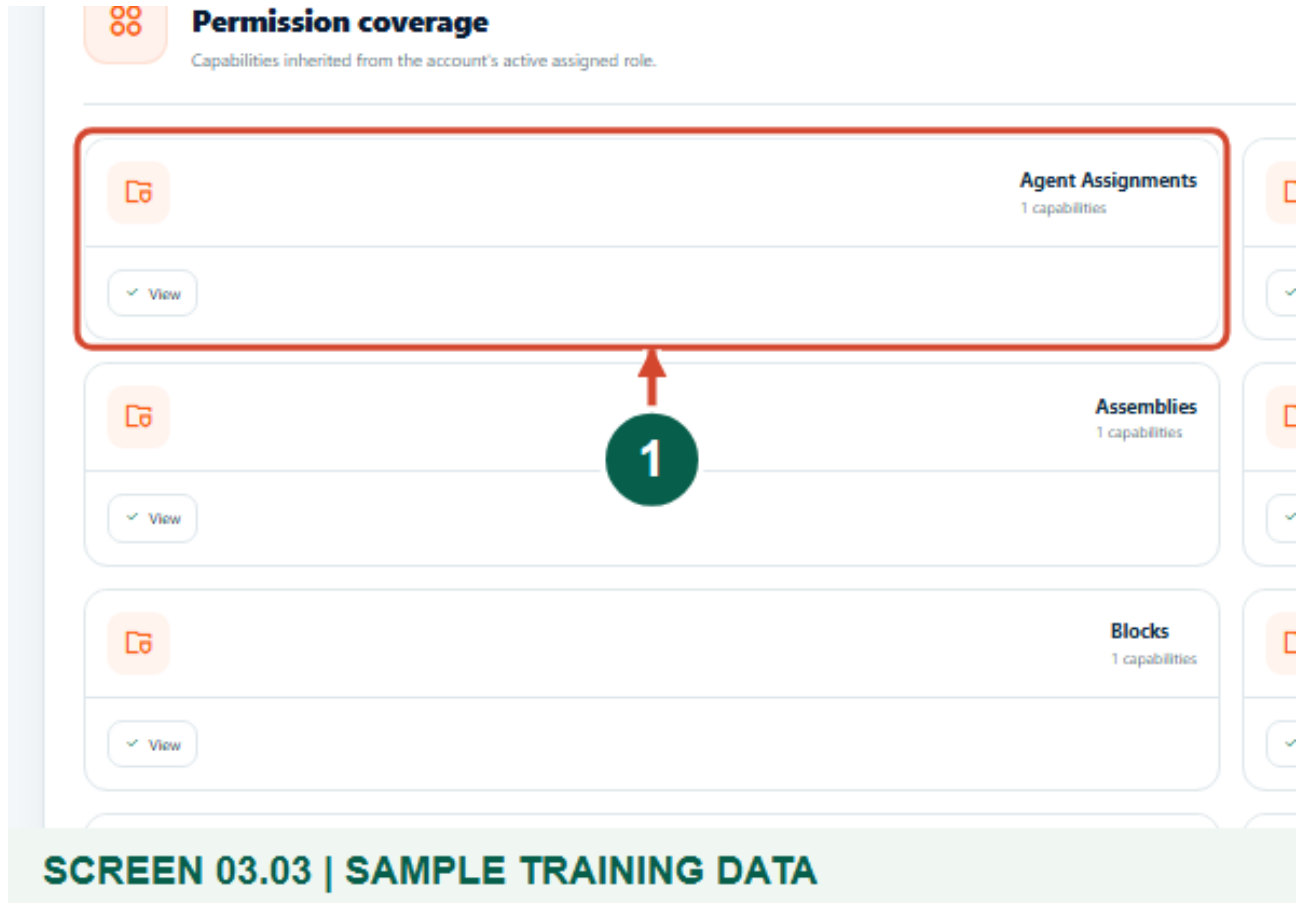
What should happen

The profile shows the saved identity, organisational scope and role-derived permissions.

STEP 03

Inspect the assigned permission coverage

1. Scroll to Permission coverage and review the capabilities inherited from the assigned role.
2. Compare these permissions with the staff member's authorised duties. Use Edit account only for approved changes to an eligible account.



Synthetic training data. Inspect the assigned permission coverage.

1 Granted capabilities

What should happen

The displayed permission groups explain what the assigned role permits.

STEP 04

Update approved contact details

1. In the edit form, correct the approved name, email, phone or other available personal details.
2. Verify the registered phone and email with the person before changing them, especially before sending a setup link.

Email address *

esi.supervisor.updated@example.invalid

Phone number

+23324000

Select a country,

SCREEN 03.04 | SAMPLE TRAINING DATA

Synthetic training data. Update approved contact details.

1 Email address

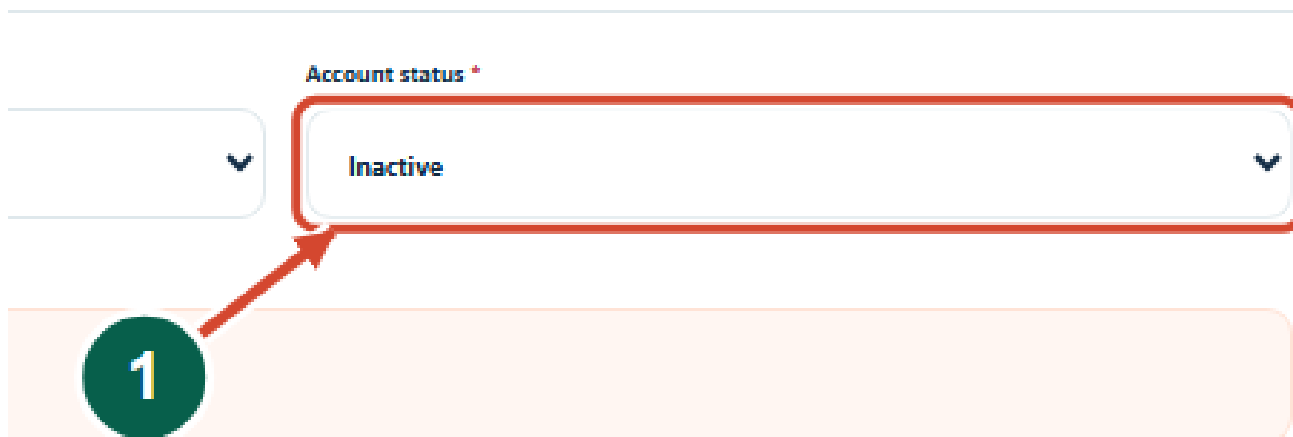
What should happen

The form contains the intended, verified account details.

STEP 05

Review role and account status deliberately

1. Keep Access level and Assigned role compatible. Use only the permissions needed for the staff member's work.
2. Choose Active or Inactive as approved. Inactive prevents a new eligible sign-in; use the secure reset workflow when immediate credential and session revocation is required.



Account status *

Inactive

1

SCREEN 03.05 | SAMPLE TRAINING DATA

Synthetic training data. Review role and account status deliberately.

1 Account status

What should happen

The intended operational role and account status are selected.

Helpful note: Changing the profile Division is not a replacement for reviewing operational supervisor coverage or existing workforce assignments.

STEP 06

Save and verify the account changes

1. Choose Save account changes and read User updated successfully.
2. Search for the account again and verify the saved contacts, role and status. This example shows an Inactive account; reactivate only when authorised.

ORGANISATION	STATUS	CREATED		
Training Municipal Assembly Greater Accra Region	Inactive	19 Oct 2026 35 seconds ago	@	

1

SCREEN 03.06 | SAMPLE TRAINING DATA

Synthetic training data. Save and verify the account changes.

1 Saved Inactive status

What should happen

The directory reflects the saved account state without creating a duplicate person.

STEP 07

Choose a secure reset-link delivery preference

1. For a justified reset of another eligible active account, choose Reset password from the directory or profile.
2. Review the displayed account and registered contacts. Choose Automatic, SMS or Email; Automatic tries SMS first and can use configured email as a fallback.

Esi Training Supervisor
A secure setup link will be sent to the registered contact.

DELIVERY PREFERENCE

☒ **Automatic** **RECOMMENDED** ☒
Try SMS first, then use configured email when SMS is unavailable.

☐ **SMS**
+***** 0451

☐ **Email**
e*****d@example.invalid

☐ I understand that this immediately revokes the user's current access

SCREEN 03.07 | SAMPLE TRAINING DATA

Synthetic training data. Choose a secure reset-link delivery preference.

- 1 Delivery preference
- 2 Access is revoked immediately

What should happen

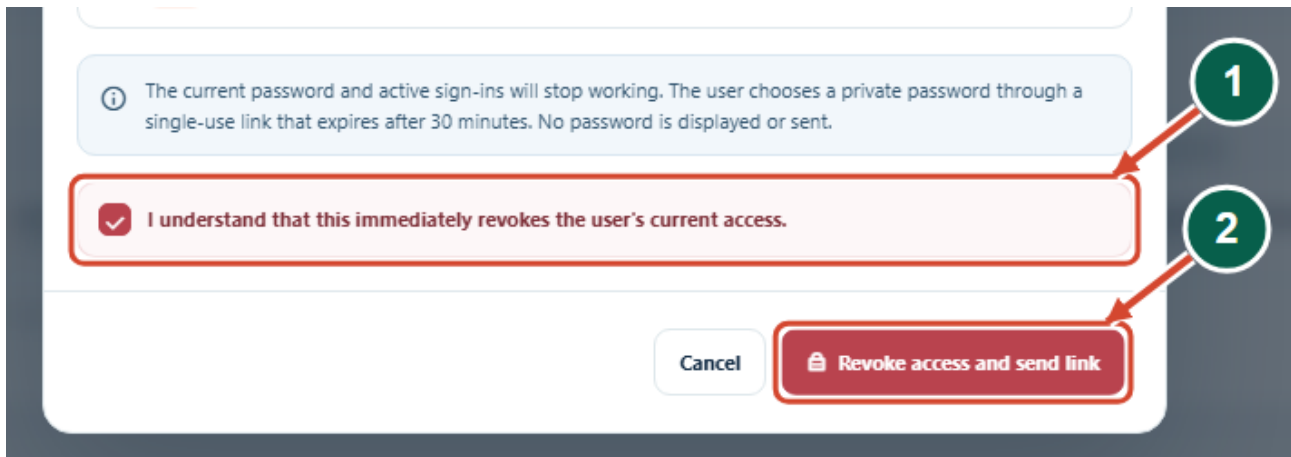
The reset dialog identifies the intended recipient and explains the access impact.

Helpful note: You cannot reset your own account through this action, and an inactive account is not eligible. Do not activate a suspended account simply to bypass that rule.

STEP 08

Acknowledge revocation before sending the link

1. Read the warning: the former password and existing sign-ins stop working, and the user must choose a private password.
2. Only when authorised, tick the acknowledgement and choose Revoke access and send link. Choose Cancel if the identity or contact is wrong.



SCREEN 03.08 | SAMPLE TRAINING DATA

Synthetic training data. Acknowledge revocation before sending the link.

- 1 Confirm access revocation
- 2 Revoke access and send link

What should happen

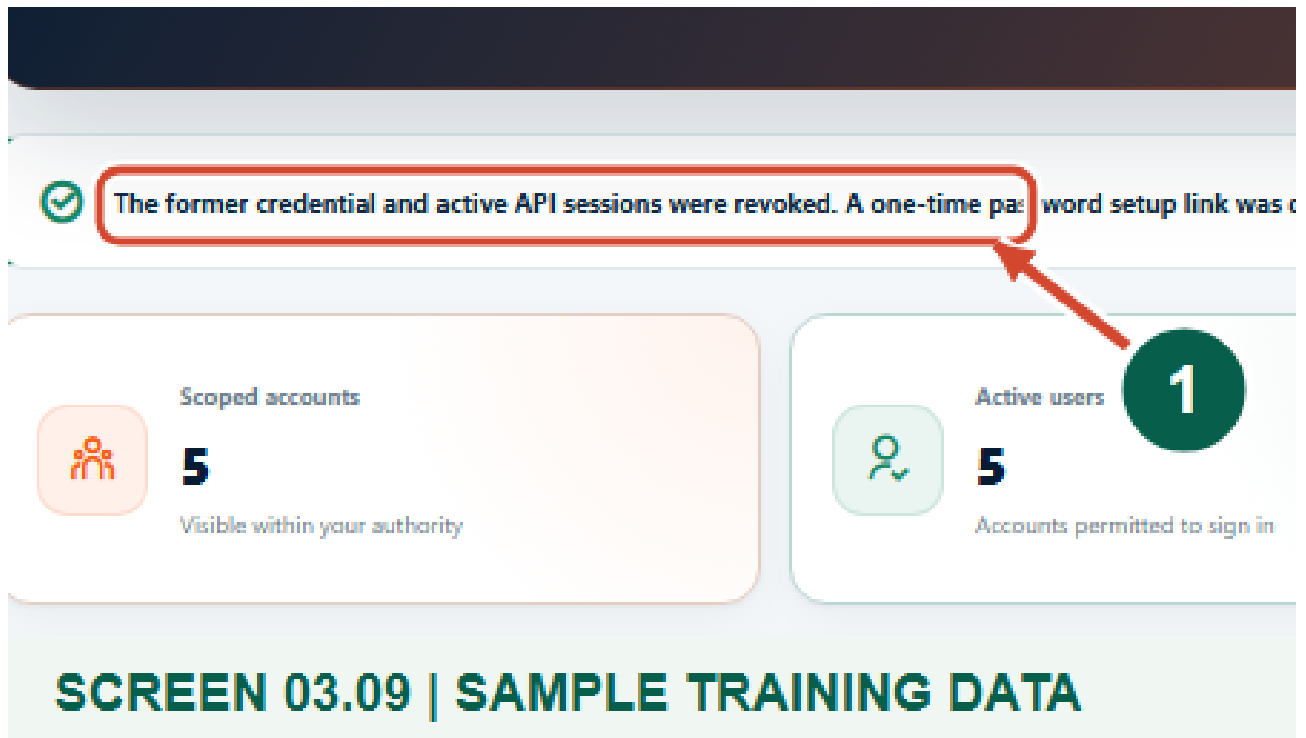
The system revokes the former credential and starts the single-use setup-link process.

Helpful note: No new password is shown to the administrator or sent in the message. A reset can interrupt active work, so coordinate with the account holder.

STEP 09

Read the queued setup-link confirmation

1. Read the directory confirmation stating that the former credential and active API sessions were revoked and a setup link was queued.
2. Ask the account holder to check the registered channel. Queued is not proof of delivery; follow up through the notification support process if the message does not arrive.



Synthetic training data. Focused view of the start of the reset confirmation; read the full message in the application.

1 Former access revoked

What should happen

The reset request is accepted and the account holder must complete private password setup.

STEP 10

Explain the account holder's next step

1. The account holder opens their own private single-use link and enters a new password and confirmation.
2. The password must have at least 12 characters, upper and lower case letters, a number and a symbol. They choose Save password and continue, then sign in at the appropriate staff portal.

Set your account password

Enter and confirm the password you will use to sign in.

1 New password

Show

Use at least 12 characters with upper and lower case letters, a number and a symbol.

2 Confirm new password

Save password and continue

SCREEN 03.10 | SAMPLE TRAINING DATA

Synthetic training data. Explain the account holder's next step.

- 1 Private new password
- 2 Save password and continue

What should happen

A valid unused link lets the person choose a private password and returns them to staff sign-in.

Helpful note: The default setup-link lifetime is 30 minutes. Never copy setup links into public manuals or support conversations; request a new authorised reset if a link expires.

Check your result

- You verified the saved account details, role and intended status within your own assembly.
- If a reset was required, the recipient knows how to use the private single-use setup link and sign in again.

If you need help

View works but Edit or Reset password is missing

The actions have different permission and target-account rules. An Assembly Administrator manages only Supervisor and Agent accounts in their own assembly; ask the appropriate higher-level administrator for other accounts.

The update is rejected

Read the validation, check unique verified email/phone, choose a compatible active role and confirm the required organisational scope.

No configured reset channel is available

Resolve the registered contact and delivery configuration through the authorised administrator. If the reset is rejected before it starts, the existing password is not replaced.

The setup link is expired, used or not received

Verify the registered contact and request a new authorised reset when needed. Treat queued delivery separately from confirmed receipt and never ask the person to share a password or code.

Useful things to know

- No account Delete action is shown in this workflow. Preserve the identity record and use the approved status/access processes.
- An account status edit is not a promise that every existing administrative browser session closes instantly. The secure reset action explicitly revokes credentials and sign-ins.
- This guide does not replace supervisor coverage, agent allocation or assignment reassignment workflows.
- The training screenshots contain only synthetic staff data; the signed setup URL and delivered codes are not published.

Continue learning

- Guide 01: Access your assembly administrator account
- Guide 02: Create assembly users

[Download all 13 guides in this collection](#)

For account or bill-record corrections, contact the relevant assembly using its verified contact details. Keep your account or bill reference available when requesting assistance.