

Part E: Administration, security and support

This part is for the people who run DFFMS day to day: the Platform Super Administrator, the Client System Administrator, and the support team. It explains how staff accounts are made, how staff sign in safely, how system settings work, and how to answer questions from outside the programme.

Names in this guide are fictional. All email addresses end in `@demo.dffms.org`.

Table of contents

1. [Staff accounts are invitation only](#)
 2. [Staff roles in plain words](#)
 3. [Inviting a staff member](#)
 4. [Accepting a staff invitation](#)
 5. [Changing a role, scope or status](#)
 6. [Revoking an invitation](#)
 7. [Signing in as staff](#)
 8. [Two-step security](#)
 9. [Password change and reset](#)
 10. [Your secure session](#)
 11. [Platform and system settings](#)
 12. [Role permission policies](#)
 13. [The audit trail](#)
 14. [Support work: contact inquiries](#)
 15. [Support work: staff messages](#)
 16. [What each role sees when it signs in](#)
 17. [Security rules everyone must follow](#)
-

1. Staff accounts are invitation only

Nobody can create a staff account by signing up on the public website. The public sign-up page only makes public accounts, for people who apply for support or invest.

Staff accounts come from one place only: an invitation sent by an administrator. This is a deliberate rule. It means every staff member has a known role, a known scope, and a known person who invited them.

Some facts to remember:

- The **Platform Super Administrator** role can never be invited. It is held by the platform owner and cannot be limited by scope.
 - The **State Coordinator Admin** role must always have a **state** scope.
 - The **Institution Admin** role must always have an **institution** scope.
 - The Client System Administrator works only inside its own tenant (the client's own space in DFFMS).
-
-

2. Staff roles in plain words

The table below lists every staff role. The short code is used in some screens and reports.

Role (code)	What it means in plain words	Can change data?
Platform Super Administrator (PSA)	Runs the whole platform. Can see everything in every tenant. Only this role can create tenants, save role policies, change the staff sign-in policy, change withholding tax, and review marketplace requests.	Yes, everything
Client System Administrator (CSA)	Runs one client's tenant. Invites and manages staff in that tenant. Changes escalation and warning settings. Acts as the top escalation level after the Programme Administrator.	Yes, inside the tenant
Programme Administrator (PA)	Manages programmes, SAPZs, institutions and reference data. Handles applications and cases. Resolves warnings and escalations at the first level.	Yes, programme work
State Coordinator Admin (SCA)	Works for one state only. Manages SAPZs, institutions, applications and state-level scheme members. Must have a state scope.	Yes, inside the state
Institution Admin (IA)	Works for one institution only. Can make transactions, disbursements and applications for that institution. Cannot see investment schemes. Must have an institution scope.	Yes, inside the institution
Finance Entry Officer (FEO)	Prepares money work. Creates transactions and disbursements, and records scheme contributions and payouts. The "maker".	Yes, prepares only
Finance Approver (FA)	Checks money work. Approves or rejects transactions and committee decisions. The "checker".	Yes, approves
Monitoring Analyst (MA)	Watches facility health. Records risk assessments, indicators, climate readings and market prices. Resolves warnings.	Yes, monitoring data
Auditor / Compliance (AUD)	Reads everything in scope to check compliance. Can generate reports.	No, read-only
Executive Donor Viewer (EXEC)	Reads dashboards, finance, schemes, monitoring, reports and exports for leadership and donors.	No, read-only
Investor Viewer (INV)	Follows its own organisation's portfolio and schemes. Receives no operational alerts.	No, read-only

Role (code)	What it means in plain words	Can change data?
Support (SUP)	Looks after system health, integrations, staff messages and help. Cannot see finance, scheme or monitoring data.	Only queues integration jobs and sends messages

Maker and checker. For money, one person prepares (the maker) and a different person approves (the checker). A maker can never approve their own transaction. The Platform Super Administrator is the only exception.

3. Inviting a staff member

Who can do it: Platform Super Administrator and Client System Administrator. A CSA can invite only into its own tenant.

Before you start

- Get the person's full name and their **official work email**. Do not use personal email addresses.
- Decide the **role**. Check section 2 above.
- Decide the **access scope**. Ask: which programme, state, SAPZ or institution should this person see?
- Make sure the organisation exists in DFFMS. If not, add it first under **Institutions** or **Stakeholders**.

Steps

1. Sign in and open **Users** from the left menu.
2. Click **Invite administrator or staff**.
3. In **Full name**, type the person's full name. Example: Hadiza Lawal .
4. In **Official work email**, type the work email. Example: hadiza.lawal@demo.dffms.org .
5. In **Tenant**, choose the client's tenant. A CSA sees only its own tenant.
6. In **Organisation**, choose the organisation the person works for.
7. In **Assigned role**, choose the role. Example: **State Coordinator Admin**.
8. In **Access scope**, choose the scope type and the matching value:
 - **Programme**: the programme the person may see.
 - **State**: the state the person may see. Required for State Coordinator Admin. Example: **Kaduna**.
 - **SAPZ**: one SAPZ zone.

- **Institution**: one institution. Required for Institution Admin.
- Leave a dimension empty if the person should be unrestricted in that dimension.

9. Check every field once more.

10. Click **Send secure invitation**.

What happens next

- The invitation appears under **Recent invitations**.
- The invitee receives a single-use invitation link by email. The link lasts **72 hours**.
- You can copy the invitation ID from the same table, or revoke the invitation (section 6).

Common problems

- **"The PSA role can never be invited."** This is correct. Only one PSA role exists, and it is not given to new staff.
 - **A State Coordinator Admin with no state scope is refused.** Pick a state.
 - **An Institution Admin with no institution scope is refused.** Pick an institution.
 - **The invitation link has expired.** Revoke the old invitation and send a new one.
 - **The person used a personal email.** Revoke the invitation and send a new one to the work email.
-
-

4. Accepting a staff invitation

Who can do it: the invited person only.

Before you start

- Open the invitation email on a device you control.
- Check the link was sent less than 72 hours ago.
- Check the email address matches the one the administrator used.

Steps

1. Click the link in the invitation email. It opens the page **Accept your staff invitation**.
2. In **Full legal name**, type your full name as it appears on official papers.
3. In **Invited work email**, check your email. Do not change it.
4. In **Password**, create a strong password.
5. In **Confirm password**, type the same password again.
6. Click **Create credentials and verify email**.

7. Open the verification email and follow the link. The link lasts **30 minutes**.
8. Return to DFFMS. Your staff access is now active.
9. If your role requires two-step security, DFFMS takes you to the **Account security** page next. Follow section 8.

What happens next

- Your membership and role become active. Your account is now a staff account.
- You receive the notice **Staff access activated**.
- The administrator who invited you receives **Staff invitation accepted**.
- An audit event **STAFF_INVITATION_ACCEPTED** is recorded.

Common problems

- **The page says "Sign in to accept this invitation"**. You already have a DFFMS account with this email. Click **Continue to staff sign in**. If you have forgotten your password, click **Reset or establish password** first.
 - **The link says it has expired**. Ask the administrator to revoke and resend the invitation.
 - **The verification email did not arrive**. Check your spam folder. Wait a few minutes. Ask the administrator if it still does not arrive.
-
-

5. Changing a role, scope or status

Who can do it: Platform Super Administrator and Client System Administrator (within their tenant).

Before you start

- Decide what must change: the role, the scope, or the account status.
- Remember that the **Platform Super Administrator** role cannot be given to anyone through this screen.
- You cannot change your own account status. Ask another administrator.

Steps

1. Open **Users**.
2. Find the person under **Activated staff accounts**. Use the columns **Staff member**, **Organisation**, **Role**, **Security** and **Status** to check.
3. Open **Manage staff** for that person.

4. To change the role or scope:
 1. Click **Change role**.
 2. Choose the new **Assigned role**.
 3. Set the **Access scope** again. Changing the role also means checking the scope.
 4. Save.
5. To change the account details:
 1. Click **Edit profile and organisation**.
 2. Update the **Name** (2 to 120 characters) and the **Organisation**.
 3. Save.
6. To **suspend** an account, click **Suspend and revoke sessions**. The person is signed out everywhere.
7. To **reactivate** a suspended account, click **Reactivate account**.
8. To **archive** an account that will not be used again, click **Archive account**.

What happens next

- The change takes effect straight away.
- Every change is recorded in the audit trail (section 13).
- A suspended person cannot sign in until the account is reactivated.
- An archived account stays in the records for audit, but cannot be used.

Common problems

- **The Change role button does not work for a PSA account.** Only the platform owner can manage a PSA account.
 - **A State Coordinator Admin changed to another role keeps the old state.** Always check the scope after a role change.
 - **The person still sees old pages.** Ask them to sign out and sign in again. For a suspended account, the sessions were already ended.
-
-

6. Revoking an invitation

Who can do it: Platform Super Administrator and Client System Administrator.

Before you start

- Check the invitation is still waiting. Accepted invitations cannot be revoked.

- Decide whether you will send a new invitation after revoking.

Steps

1. Open **Users**.
2. Scroll to **Recent invitations**.
3. Find the invitation. Check the name, email and role.
4. Click **Revoke invitation**.
5. Confirm when asked.

What happens next

- The invitation link stops working straight away.
- If the person still needs access, send a new invitation (section 3).

Common problems

- **The person says the link does not work.** It was probably revoked, or it is older than 72 hours. Send a new one.
 - **You want to copy the invitation ID for support.** Use **Copy invitation ID** from the same table. Do not paste it into public channels.
-
-

7. Signing in as staff

Who can do it: any staff member with an active account.

Before you start

- You need your work email and your password.
- If your role requires two-step security, have your authenticator app ready (section 8).
- Use a device you trust.

Steps

1. Go to the **staff sign-in page** (`/admin/sign-in`). Its title is **Staff and administrator sign in**.
2. Type your work email and password.
3. Submit the sign-in form.
4. If two-step security is switched on for you, the page **Multi-factor verification** appears.

1. Type the **Six-digit authenticator code** from your app.
2. Click **Verify and continue**.
3. If you have lost your phone, click **Use a recovery code**, type one **Single-use recovery code**, and click **Verify and continue**.
5. If your role must set up two-step security and has not yet done so, DFFMS opens **Account security**. Follow section 8.
6. When you reach the dashboard, check the footer card **Secure session**. It should say **MFA enrolled · Secure session active**.

What happens next

- You land on the **Executive dashboard**.
- Your sidebar shows only the pages your role allows.

Common problems

- **"Staff accounts are created only through a programme invitation."** You are on the staff page without an account. Use the invitation email. Do not use the public sign-up page.
 - **You are sent back to the public account page with "staff access required"**. Your account is not a staff account. Ask an administrator to check it.
 - **The code is refused five times**. The account locks for **15 minutes**. Wait, then try again with the correct code. If you cannot wait, ask an administrator.
 - **The code is always wrong**. Your phone clock may be wrong. Turn on automatic time in your phone settings, then try a new code.
 - **You used a recovery code and cannot sign in again**. Each recovery code works only once. Use another one, and then make new codes (section 8).
-
-

8. Two-step security

Two-step security adds a second check after your password: a six-digit code from an **authenticator app** on your phone. DFFMS also gives you **recovery codes** and, for some roles, **passkeys**.

Who can do it: every staff member, for their own account. The Platform Super Administrator can make two-step security mandatory for all staff (section 11).

Before you start

- Install an authenticator app on your phone. Any standard authenticator app works.
- Keep your phone with you during setup.
- Have a safe place ready for your recovery codes. Do not store them on the same phone, or in a shared document.

8.1 Set up an authenticator app

1. Sign in. If prompted, go to **Account security**. You can also open it from the profile menu (click your name, then **Account security**).
2. Read the heading **Secure your account**.
3. In **Current password**, type your password.
4. Click **Begin authenticator setup**.
5. The screen shows:
 - a **setup key** (a long text code). Click the copy button labelled **Copy authenticator setup key** to copy it.
 - a **QR code**. Use this instead of the key if you prefer.
6. In your authenticator app, choose **Add account** (or the plus sign). Then either:
 - scan the QR code on the screen, or
 - choose **Enter a setup key** and paste the key.
7. The app starts showing six-digit codes that change every 30 seconds.
8. Back in DFFMS, under **Single-use recovery codes**, copy or write down every code. Store them in an approved secure location.
9. Tick **I saved these recovery codes in an approved secure location**.
10. In **Six-digit verification code**, type the code now showing in your app.
11. Click **Verify authenticator**. The screen shows **Authenticator verified**.

8.2 Recovery codes

- Recovery codes are for when you cannot get a code from your phone.
- Each code works **only once**.
- Store them offline, in a safe place. Treat them like cash.
- If you use a code, make a fresh set as soon as you can.

Common problems

- **The setup key was pasted into a chat or email.** Treat the old authenticator setup as exposed. Tell your administrator. Set up a new authenticator from a clean start.

- **You lost your phone.** Use a recovery code to sign in. Then set up a new authenticator app from **Account security**.
- **The button is greyed out.** You must tick the box for the recovery codes first.

8.3 Passkeys

A passkey is a sign-in method stored on your device, such as a fingerprint or face unlock. It is harder to fake than a password.

- The **Platform Super Administrator** must register a **device passkey** when two-step security is mandatory. The page says: **Platform Super Administrators must also register a phishing-resistant device passkey.**
- Other staff can add a passkey from the same screen if it is offered.
- To add one, click **Register this device passkey** (or the passkey button on **Account security**) and follow your device prompts.
- Register a passkey on each device you use to sign in.

Common problems

- **The passkey prompt does not appear.** Check you are on the DFFMS address in your browser, and that your device allows passkeys.
- **You see "Setup interrupted".** Your secure session may have ended. Sign in again and start from **Account security**.

8.4 Mandatory two-step security

- By default, two-step security is **off** for general portal access.
 - The Platform Super Administrator can turn on **Require MFA before staff portal access** in the **Security centre**. Then every staff member must set up an authenticator.
 - Some actions always need two-step security, even when the policy is off. See section 10.
-

9. Password change and reset

Who can do it: every staff member, for their own password.

Before you start

- Your new password must be strong and unique. Do not reuse a password from another service.
- Check you have access to your work email.

Steps to reset a forgotten password

1. On the sign-in page, click **Forgot password?**.
2. On **Reset your password**, type your work email in **Email address**.
3. Submit the form. DFFMS sends an email. It gives the same reply whether or not the email has an account, so nobody can guess who has an account.
4. Open the email and click the reset link. The link lasts **30 minutes**.
5. Type your new password and confirm it.
6. Save. You will receive a notice that your password was changed.

What happens next

- All your other sessions are signed out. Only the new sign-in remains.
- If you have two-step security, the sign-in asks for your authenticator code.

Common problems

- **The reset link has expired.** Ask for a new one. Request it again from the sign-in page.
- **You asked for many resets.** DFFMS allows only **3 reset requests every 5 minutes**. Wait, then try again.
- **You did not ask for the reset.** Someone may be trying to get into your account. Tell your administrator at once. Change your password from the reset link, and check the audit trail (section 13).

Note on changing a password while signed in. During this review no separate "change password" page was found in the portal. Use the reset flow above. Your administrator can confirm whether a page has been added since.

10. Your secure session

Your sign-in works like this:

- A session lasts **4 hours**.
- While you are active, it is refreshed about every **15 minutes**.

- Some actions need a **fresh sign-in**. Your sign-in counts as fresh for **5 minutes**. After that, you must sign in again to approve money or make a committee decision.
- Important actions are recorded in the audit trail.

The "Secure session" card. The footer of every staff page shows one of two messages:

- **MFA enrolled · Secure session active:** two-step security is set up.
- **Authenticated session · MFA not enrolled:** you are signed in, but have not set up two-step security.

Always enforced, whatever the policy

The following actions need two-step security and a fresh sign-in, even when the staff policy is off:

- Approving, rejecting, reversing and refunding money transactions.
- Recording scheme money (contributions and payouts).
- Generating report exports.
- Opening financing cases, high-risk case changes and committee decisions.

Profile page. Open **My profile** from the profile menu. It shows **Verified staff identity** (your name, email, organisation, membership and roles), **Account security** (two-step security, passkeys, trusted devices and session), **Recent sessions**, and buttons **Notification centre** and **Review security settings**.

Common problems

- **"Session expired".** Sign in again. This is normal after four hours.
- **An action asks you to sign in again.** Your last sign-in is too old for this action. Sign in again, then repeat the action.
- **You see an unknown session in Recent sessions.** Sign out of that session from your profile, then change your password (section 9).

11. Platform and system settings

These settings control how DFFMS reacts to delays, risks and outside services. Most are on the **Configuration** page (</system/configuration>). Some are on other pages, as the table shows.

Setting	Where	What it does	Who may change it
Escalation service levels	Configuration	Sets how long a decision can wait before reminders and escalations. Default: "Approval reminder (hours)" 24; "Escalate to Programme Administrator (hours)" 48; "Escalate to Client System Administrator (hours)" 96; "Application stage limit (working days)" 5; "Repayment reminders (days overdue)" 1, 7, 30; "Escalate unpaid instalment (days overdue)" 30. Values must climb in order. Invalid values fall back to the defaults. Changes are audited.	PSA or CSA. Save with Save escalation service levels .
Scheme redemption deadline	(fixed in code)	Pay-by date plus 3 working days.	Not configurable
Early-warning thresholds	Configuration	Sets when warnings appear. Examples: receipt expiry warning 14 days; commodity price drop 1500 (15%); warehouse concentration 40%; commodity concentration 60%; delivery overdue 7 days; buyer payment delay 30 days; first-loss utilisation 75%; arrears alerts at 30 and 90 days; minimum debt-service cover 1.20x; construction delay 30 days; delayed disbursement 30 days; cost overrun 10%. Save with Save early-warning thresholds .	PSA or CSA
Staff authentication policy	Security centre	Turns on Require MFA before staff portal access . Default off. Changing it notifies the PSA who made the change.	PSA only. Others see "You have read-only access to this policy."
Withholding tax	Investment schemes, on each scheme (Withholding	Sets the tax rate on dividends and on redemptions for one scheme.	PSA only

Setting	Where	What it does	Who may change it
	tax)	Redemption rate default is 0%. You can choose whether the tax is charged on the return above cost or on the whole amount. You must give a reason (at least 5 characters). New rates apply only to new dividends and new redemption requests.	
Provider settings	Provider settings (/settings/providers)	Lists payment and messaging providers: Flutterwave, Paystack, Fincra, Squad, Termii, Twilio and a generic connector. You can enable or disable each one for new operations. Credentials are never shown on screen.	PSA can enable or disable. CSA can view.
Tenant creation	Users	Creates a new client tenant.	PSA only
Role permission policies	Roles & permissions	Narrows what each role may do (section 12).	PSA saves. CSA views.
Configuration checks	Configuration	Shows whether the database, transactional email and Google sign-in are present. These are checks only.	View only

Important notes

- Settings are changed in the portal, not in code. Ask your administrator before changing a value you do not understand.
- Warnings appear only after the daily check runs at **06:00 UTC**. A new reading does not raise a warning at once.
- The Platform Super Administrator is the only role that can change the withholding tax rate. If a CSA needs a change, it must ask the PSA.

12. Role permission policies

A role permission policy makes a role's access **narrower**. It can never make a role's access wider than its built-in rights.

Who can do it: the Platform Super Administrator saves policies. The CSA can view them.

Before you start

- Decide which role you want to narrow.
- Know the workspace names: dashboard, finance, funding, risk, programmes, reports, stakeholders, users, roles, integrations, providers, audit, security, system and marketplace.
- Know the actions: **view**, **create**, **edit**, **approve**, **export** and **manage**.
- You must have a recent sign-in. Saving a policy needs fresh authentication.

Steps

1. Open **Roles & permissions** (`/roles`).
2. In the **Role library**, choose the role you want to change.
3. Drag workspaces between **Available workspaces** and **Granted access**. You can also use **Add** or **Remove**.
4. For each granted workspace, tick only the actions the role needs: **View**, **Create**, **Edit**, **Approve**, **Export** or **Manage**.
5. Click **Save role policy**.

What happens next

- The policy applies the next time the role's users act.
- A role with no saved policy keeps its normal rights.

Common problems

- **You cannot add a right that the role does not already have.** A policy only narrows. Change the role instead, or ask for a platform change.
- **You are not sure what a right does.** Test with a demonstration account first (for example, one using `@demo.dffms.org`), not with a real staff member.

13. The audit trail

The **audit trail** (/audit) is a permanent record of important events. It is **append-only**: entries can be added, but not changed or deleted. Each entry is linked to the one before it, so tampering would show.

Who can see it: PSA, CSA and Auditor / Compliance.

What it records (examples)

- Staff invitations and invitation acceptances (STAFF_INVITATION_ACCEPTED).
- Changes to security policy, escalation service levels and early-warning thresholds.
- Withholding tax changes (INVESTMENT_SCHEME_TAXATION_UPDATED).
- Finance decisions, transactions and case changes.

Steps to look up an event

1. Open **Audit trail** from the **Administration** group.
2. Use the search box and the **Filter by status** control to narrow the list.
3. Click **Record details** to read the full entry.
4. To keep a copy, click **Export CSV**, or generate the **Audit trail** report from **Reports**. Report generation needs two-step security.

Common problems

- **You cannot edit or delete an entry.** This is by design. Explain the correction in a new record instead.
 - **An event you expected is missing.** Check the date filter and the scope of your role. Then ask an administrator.
-
-

14. Support work: contact inquiries

People outside the programme can write to DFFMS through the public **Contact** page (/contact). The page is titled **Contact DFFMS NCO**. The page says it is for questions about the Special Agro-Industrial Processing Zones (SAPZ) programme, de-risking financial products, or technical portal access.

Who can do it: Platform Super Administrator only. Other staff do not see the inbox.

How an inquiry arrives

1. The sender fills in the **Contact** form and sends it.

2. The sender receives a confirmation that the message was submitted.
3. The inquiry appears in the inbox under **Contact inquiries** with the status **PENDING**.

Before you start

- Read the whole message. Check the sender, organisation and subject.
- Check whether the question is about a finance matter that needs a specialist. Then bring in the right person through staff messaging (section 15).

Steps to answer an inquiry

1. Open **Contact inquiries** (</admin/inquiries>).
2. Check the summary tiles. They show how many inquiries are pending and how many are resolved.
3. Find the inquiry in **Inbox submissions**. The columns are **Sender**, **Organisation**, **Subject**, **Message**, **Status** and **Received**.
4. Click the row action **Reply securely**. Or open **View conversation** to read the thread first.
5. In **Send a response**, write your reply in plain words. Keep it short. Do not include passwords, codes or personal records.
6. Send it. The reply is emailed to the sender and kept on the record.
7. When the question is answered, click **Mark resolved** on the inquiry row. The status changes to **RESOLVED**.

Assigning inquiries. The inbox has no assign button. In the current version, the Platform Super Administrator handles all inquiries. If your team needs to share the work, agree who checks the inbox each day, and use staff messaging to hand over specific cases.

What happens next

- The reply stays on the record.
- The sender gets the reply by email.
- A resolved inquiry stays in the list with its history.

Common problems

- **The sender says they got no reply.** Check the reply was sent (the conversation shows it). Check the sender's spam folder. Reply again if needed.
- **The inquiry is about a case or a payment.** Do not answer with case details by email. Bring in the Programme Administrator or the relevant team through staff messaging, and ask the sender to sign in to their account for case questions.

- **You need to contact a state office.** Use the state coordinator's details from the stakeholder records, not personal contact information.
-

15. Support work: staff messages

Staff can send messages to each other inside DFFMS. A message is delivered in the app, by email, and by browser push for staff who have opted in.

Who can do it: Platform Super Administrator, Client System Administrator, Support and Programme Administrator.

Before you start

- Decide who needs the message: one person, selected people, a role, or all active staff.
- Write a clear **Subject**.
- If the message needs an action, find the page path in DFFMS (for example, the transactions page).

Steps

1. Open **Staff messaging** (`/admin/messages`).
2. Click **Compose staff message**.
3. Choose the **Audience**:
 - **One person**: pick one name.
 - **Selected people**: pick several names.
 - **A staff role**: pick a role. Example: all Finance Approvers.
 - **All active staff**: use only for important company-wide notices.
4. Type the **Subject**.
5. Type the **Message**.
6. Optionally, fill in **Optional DFFMS action path** so the reader can jump straight to the page.
7. Click **Send message**.

What happens next

- Only the chosen people receive the message.
- Recipients see it in their notification centre.
- Each recipient also gets an email. If they have opted in, they also get a browser push.

Common problems

- **Too many people received the message.** Check the audience. Do not use **All active staff** for routine messages.
 - **The link in the message does not open.** Check the action path begins with a forward slash and points to a page in DFFMS.
 - **A message needs a reply from an outside person.** Use **Contact inquiries** (section 14) instead.
-
-

16. What each role sees when it signs in

Every staff member lands on the **Executive dashboard** after signing in. What they see after that depends on their role and scope. The sidebar shows only the pages the role allows, and every list, chart and notification follows the role's scope.

Auditor / Compliance (for example, Tolulope Bakare, `tolulope.bakare@demo.dffms.org`)

- The menu covers finance, the case registers, reconciliation, the audit trail and security.
- The auditor reads everything within its scope.
- On a transaction, there are no approve or reject buttons. The auditor is read-only, but can generate reports.

Support (for example, Emeka Nwosu, `emeka.nwosu@demo.dffms.org`)

- The menu covers system health, integrations and staff messaging. It also covers the help centre.
- There is no finance, scheme or monitoring data.
- Support can queue integration jobs and send staff messages. It cannot approve anything.

Institution Admin (for example, Babatunde Adeyemi, `babatunde.adeyemi@demo.dffms.org` , for one institution)

- Access is limited to the one institution in the scope.
- The menu covers finance and monitoring for that institution, including its cases.
- Investment schemes are not in the menu.
- The institution admin can make transactions, disbursements and applications for its own institution. Approvals are done by someone else.

Investor Viewer (for example, an investor from another organisation)

- Follows only its own organisation's portfolio and the schemes.
- Read-only. No operational alerts are sent.

State Coordinator Admin (for example, Hadiza Lawal, `hadiza.lawal@demo.dffms.org` , scoped to Kaduna)

- Sees applications, financing cases and scheme members for Kaduna only.
- Every list, chart and notification respects the Kaduna scope.
- The database enforces this scope too, so a direct link to another state's record is refused.

Executive Donor Viewer

- Reads the dashboard, finance, schemes, monitoring, reports and exports. Read-only.

Platform Super Administrator and Client System Administrator

- See the most pages. The PSA sees every tenant. The CSA sees its own tenant.
-

17. Security rules everyone must follow

These rules apply to every staff member, every administrator, and every support person. Breaking them can put public money at risk.

1. **Use your own account only.** Never share your password, your authenticator, your passkey or your sign-in with anyone, including colleagues and DFFMS staff.
2. **Never send your password, verification code or recovery code to anyone.** DFFMS support will never ask for these. The security page says so directly. If someone asks you, stop and report it.
3. **Keep recovery codes safe.** Store them in an approved secure location, offline. Never store them in email, chat, a shared drive or a photo on your phone.
4. **Turn on two-step security.** Set up an authenticator app from **Account security** as soon as you can. Use a passkey on your own device if offered.
5. **Use a fresh sign-in for money.** If DFFMS asks you to sign in again before approving, decide, or pay, do it. Do not try to get around it.
6. **Keep the maker and checker apart.** Do not approve your own work, and do not ask a colleague to approve your work on your behalf.
7. **Invite only people who need access.** Give the smallest scope that does the job. Remove or suspend access as soon as a person leaves.
8. **Never forward invitation links.** Each link works once and expires after 72 hours. Send it only to the person named.

9. **Sign out on shared devices.** Use **Sign out** from the profile menu. Do not leave a session open on a public computer.
10. **Use work email only** for staff accounts. Do not use personal email addresses.
11. **Keep exports private.** Downloads are signed links that expire quickly. Do not send exports to personal email, and do not post them in public channels.
12. **Do not paste card or bank secrets into DFFMS.** Payments run through the provider's own pages. DFFMS never receives full card numbers or security codes.
13. **Report anything strange at once.** Examples: a password reset you did not ask for, an unknown session, a message asking for a code, or a record you cannot explain. Tell the Platform Super Administrator.
14. **Do not change records to hide a mistake.** Records and the audit trail cannot be edited. Record a correction instead, and explain it.
15. **Keep data inside the portal.** Do not copy personal data of beneficiaries into personal notes, chat tools or spreadsheets on your own device.