Users & Access

Creating NSCAT accounts, assigning admin roles, and controlling who can see which activity.

Registering & Managing Users

Overview — Accounts in NSCAT

Every person who works in NSCAT needs an account, and accounts are created **by an administrator** — there is no self-service sign-up. This page covers both halves of the job: creating an account with **Register a User**, and changing or disabling one afterwards with **Manage User**.

Both live under **Administration** in the left sidebar, which is visible to COG Admins and Utility Admins.

The life of an account

1. **Registered** — you create it with an email, a name, a starting password, an organization, and its roles.
2. **Active** — the person signs in and works in whatever activities they are assigned to.
3. **Adjusted** — you change their organization, add or remove an admin role, or reset a forgotten password.
4. **Disabled** — you untick **Account Enabled**. The account and its history stay, but the person can no longer sign in.

GOOD TO KNOW There is no *delete* for a user. Disabling is the intended way to remove someone's access — it keeps the audit trail on every activity, response, and observation they touched intact.

Registering a User

Open **Administration → Register a User**.

image.png

The Register a User form.

The fields

Field	What to enter
email	The person's work email. This is their username — they sign in with it, and password-reset mail goes here. It must be a valid address and must not already be in use.
First Name	Required. Shown on responses, observations, and the activity feed.
Last Name	Required.
Password	A starting password (see the policy below).
Confirm Password	Must match **Password** exactly.
Organization	The utility this person belongs to, chosen from the list of utilities. This drives what they can see.
COG Admin	Tick for cross-organization administration — ISF, utilities, activity locking.
Utility Admin	Tick for utility administration — question pool, themes, training, cross-activity reports.

The password policy

A password must have **all** of the following:

- At least **6 characters**
- At least one **uppercase** letter
- At least one **lowercase** letter
- At least one **number**
- At least one **special character** from @ $! % * ? &

HEADS UP Only the special characters @ $! % * ? & are accepted. Other symbols — #, -, _, . — will fail validation even though the field looks filled in correctly. If a password is rejected and you cannot see why, that is usually the reason.

PRO TIP Set a throwaway starting password and tell the person to change it on first sign-in from **Profile**, or to use **Forgot Password** on the login screen to set their own. You never need to know their working password.

Choosing the roles

The two role checkboxes are independent, and neither implies the other. Pick from what the person actually needs to do:

The person…	COG Admin	Utility Admin
Runs assessments; leads a team	—	—
Curates questions and themes; runs trending and CPRO reports	—	Tick
Maintains the ISF; creates utilities; locks activities	Tick	—
Is the day-to-day administrator for the whole system	Tick	Tick

HEADS UP COG Admin is **not** a superset of Utility Admin. An account with only **COG Admin** ticked has no access to Question Composer, Theme Management, Training Management, the Trending Report, the CPRO Report, the Report Builder, or Lessons Learned Review. If you are creating an account for someone who administers day to day, tick **both**.

GOOD TO KNOW Neither admin role grants access to an individual activity's contents. Activity access comes from being assigned as a **Team Lead** or **Team Member** on that activity — see **Roles & Access Control**.

When the form is valid, submit it. The account is usable immediately.

Managing an Existing User

Open **Administration → Manage User**.

Unlike the registration form, this page starts empty — you pick a person first, and the form fills in with their current details.

image.png

The Manage User form with a user selected.

Selecting the user

User Email is a searchable list of every account. Start typing a name or address to narrow it. Choosing an entry loads that person's **First Name**, **Last Name**, **Organization**, role checkboxes, and current enabled state.

PRO TIP The list searches on the whole address, so typing a domain fragment is a quick way to see everyone from one organization.

Enabling and disabling an account

The checkbox at the top of the form is the account's on/off switch, and its label reflects the current state — **Account Enabled** when ticked, **Account Disabled** when not.

Untick it and save to revoke access. The person can no longer sign in; everything they created stays where it is.

HEADS UP While the account is disabled, **every other field on the form is greyed out**. You cannot correct a name or change an organization on a disabled account. Re-enable it, make the change, save, then disable it again if that is what you want.

GOOD TO KNOW Disabling an account does **not** remove that person from the activities they are assigned to. Their name stays on the team list. If someone has genuinely left, unassign them from their activities as well — otherwise the team list keeps showing a person who cannot sign in.

Changing names, organization, and roles

With the account enabled, **First Name**, **Last Name**, **Organization**, **COG Admin**, and **Utility Admin** are all editable. Save to apply.

HEADS UP Changing **Organization** moves the person to a different utility and changes what they can see — including which activities appear on their dashboard. Confirm it is really a transfer and not a mis-click before saving.

GOOD TO KNOW A role change takes effect on the person's **next sign-in**, because the sidebar is built from the roles in their current session token. If someone says a newly granted menu is missing, have them sign out and back in.

Resetting a password

Passwords are only editable when you ask for it. Tick **Changing Password?** and the **Password** and **Confirm Password** fields become available.

The same policy applies as at registration: minimum 6 characters, with an uppercase letter, a lowercase letter, a number, and one of @ $! % * ? &.

PRO TIP For a routine forgotten password, point the person at **Forgot Password** on the login screen instead — it emails them a reset link and no one has to hand a password around. Use **Changing Password?** for accounts that cannot receive the mail.

GOOD TO KNOW Leave **Changing Password?** unticked and the existing password is untouched. Editing a name or a role never resets it.

Common Problems

What you see	What it means
Registration rejected, email flagged as invalid	The address failed format validation, or an account already exists on it. Search for it in **Manage User** before creating a new one.
Password rejected but it looks strong	Almost always an unsupported special character. Only @ $! % * ? & count.
Fields greyed out in **Manage User**	The account is disabled. Tick **Account Enabled** to edit anything.
User says a menu is missing after you granted a role	They are on an old session. Sign out and back in.
User sees **Access Restricted** on an activity	An account role is not activity access. Add them as a **Team Member** or **Team Lead** on that activity.
New admin cannot see Question Composer or Theme Management	They have **COG Admin** but not **Utility Admin**. Tick **Utility Admin** as well.

Roles & Access Control

Overview — Two Layers of Access

Access in NSCAT is decided by **two independent layers**, and most confusion about "why can't this person see that" comes from mixing them up.

1. **Account roles** — the **COG Admin** and **Utility Admin** checkboxes on a person's account. These decide which *administration menus* appear in the sidebar. Set them in **Registering & Managing Users**.

2. **Activity assignment** — whether a person is a **Team Lead** or **Team Member** on a *specific activity*, and what they may do inside it. Set these per activity in **Properties**.

An account role never grants access to an activity's contents, and an activity assignment never grants an administration menu. Someone can be a Utility Admin with no activity assignments, or a Team Member with no admin role at all.

HEADS UP The single most common support question — "*I made them an admin but they still see Access Restricted*" — is this distinction. Admin roles are not activity access. Add them to the activity's team in **Properties**.

Layer 1 — Account Roles

The two admin checkboxes are **independent**. Neither implies the other, and COG Admin is not a superset of Utility Admin.

Area	COG Admin	Utility Admin
Register a User / **Manage User**	Yes	Yes
Add Utility	Yes	—
Manage Utility	Yes	Yes
Add ISF / **Manage ISF**	Yes	—
Manage Activities (lock / unlock)	Yes	—
Activity Feed	Yes	Yes
Question Composer	—	Yes
Theme Management	—	Yes
Training Management	—	Yes
Cultural Pattern Rank Order Report	—	Yes
Trending Report	—	Yes
Report Builder	—	Yes

Lessons Learned Review	**No**	Yes

GOOD TO KNOW **Lessons Learned Review** is hidden from COG Admins by design — it is a utility-level review. A COG Admin who cannot find it in the sidebar is seeing correct behaviour.

Utility Admin is the write-access shortcut

Inside any activity, a **Utility Admin** is treated as having **write access to everything** — surveys, interviews, focus groups, observations, recommendations, lessons learned. They do not need to appear on the activity's team list at all.

HEADS UP Because of this, ticking **Utility Admin** is a broad grant. It bypasses every per-activity permission checkbox described below. Reserve it for people who genuinely administer the utility, not as a convenient way to give someone access to one activity.

A Utility Admin is still scoped to their own utility

Editing an activity's **team** — adding Team Leads or Team Members, changing their permissions — additionally requires that the admin's own utility matches the activity's utility. A Utility Admin from a different utility sees those controls **greyed out** even though the activity is visible.

GOOD TO KNOW Team editing needs all three of: the **Utility Admin** role, a **matching utility**, and the activity **unlocked**. If the fields are disabled and the activity is unlocked, check the utility match first.

Layer 2 — Activity Assignment

Open the activity's **Properties** page from its menu on the dashboard. Two separate lists control who works on it.

image.png

The Properties page, showing Team Leads and Team Members.

Team Leads

Team Leads is a simple list of user emails — no permission checkboxes. Being on it grants **write access to everything** in that activity, the same effective reach as a Utility Admin but scoped to this one activity.

Add people from the picker; remove them with the × on their chip.

PRO TIP Team Lead is the right role for the person running the assessment. It saves ticking fourteen checkboxes, and it is scoped to a single activity — much narrower than granting Utility Admin.

GOOD TO KNOW A person cannot be both a Team Lead and a Team Member on the same activity — once they are on one list, the other list's picker stops offering them.

Team Members

Team Members are added one at a time, each with their own **Read** / **Write** permissions per area of the activity:

Area	Read	Write	Controls
Interviews	Yes	Yes	Opening interviews and entering interview responses.
Focus Groups	Yes	Yes	Opening focus groups and entering focus group responses.
Survey Response	Yes	Yes	Viewing and editing survey responses and their comments.
Observations	Yes	Yes	Viewing and recording observations.
Recommendations	Yes	Yes	Viewing and writing recommendations.
Lessons Learned	Yes	Yes	Viewing and writing lessons learned.
Reports	Yes	—	Viewing the activity's reports. Read-only — there is no Write for reports.

GOOD TO KNOW **Reports** has a **Read** checkbox only. Reports are generated from the activity's data, so there is nothing to write.

Read and Write are linked

The two checkboxes in each row are not independent — NSCAT keeps them consistent for you:

- Tick **Write** and **Read** is ticked automatically. You cannot have write without read.
- Untick **Read** and **Write** is unticked automatically.

So each area has three reachable states: **no access**, **read only**, or **read and write**.

PRO TIP Four buttons at the bottom of the dialog set everything at once — **Read All**, **Write All**, **Read None**, **Write None**. Start with **Read All** and then tick the two or three areas the person needs to write, rather than working down fourteen checkboxes.

Effective access, in order

When NSCAT decides whether someone may edit something in an activity, it checks in this order and stops at the first match:

3. Is the user a **Utility Admin**? → write access.
4. Is the user's email in **Team Leads**? → write access.
5. Is the user in **Team Members**? → use that area's **Write** flag.
6. Otherwise → no access. The activity's menu shows **Access Restricted**.

HEADS UP A **COG Admin** does not appear anywhere in that list. Being a COG Admin grants no write access inside an activity — a COG Admin who needs to edit activity content must also be a Utility Admin, a Team Lead, or an assigned Team Member.

How Locking Overrides Everything

A **locked** activity is read-only for everyone, regardless of role or assignment. Save and delete buttons throughout the activity are disabled, and the activity's menu on the dashboard hides **Properties** entirely.

Only a **COG Admin** can lock or unlock, from **Manage Activities** in the sidebar. See **Manage Activities**.

HEADS UP Because locking hides **Properties**, you cannot change an activity's team while it is locked. To adjust access on a locked activity: have a COG Admin unlock it, make the change, then lock it again.

Granting Access — Which Role to Use

The person needs to…	Give them
Run one assessment end to end	**Team Lead** on that activity
Take interview notes on one activity, nothing else	**Team Member** with Interviews Read + Write
Read an activity's reports without touching data	**Team Member** with Reports Read only
Curate questions and themes for the utility	**Utility Admin** account role

Run trending and CPRO reports across activities	**Utility Admin** account role
Maintain the ISF and lock activities	**COG Admin** account role
Administer the whole system day to day	**Both** account roles

PRO TIP Work from the narrowest layer up. Try a per-area **Team Member**, then **Team Lead**, and only reach for **Utility Admin** when the person's job really is utility-wide — it silently overrides every activity-level permission.

Common Problems

What you see	What it means
Access Restricted on an activity menu	No assignment on that activity. Add them in **Properties**.
New admin menu missing after a role change	The sidebar is built from the session token. Sign out and back in.
Write won't stay ticked	**Read** is unticked for that area. Tick Read first, or tick Write and let it pull Read in.
Team Lead / Team Member fields greyed out	One of: not a Utility Admin, a different utility than the activity, or the activity is locked.
Properties missing from the activity menu	The activity is locked. A COG Admin must unlock it.
COG Admin cannot edit activity content	Expected. COG Admin grants no in-activity write access — add Utility Admin or an activity assignment.
Person cannot be added as a Team Member	They are already a Team Lead on that activity. Remove them from that list first.