

Access Reviews

Dated notes from the quarterly access reviews that the Access Management Policy requires.

- [Nextcloud access review, 29 October 2026](#)
- [ERPNext access review, 29 October 2026](#)

Nextcloud access review, 29 October 2026

Nextcloud access review, 29 October 2026

This is the first quarterly access review under the [Access Management Policy](#). Aaron Tushabe (Security DRI) reviewed and approved it on 29 October 2026. Claude ran the checks and made the approved changes. The next review is due by 31 January 2027.

Outcome

- **Public links:** Aaron had 14 public links. All of them opened for anyone, and none had a password. **13 were deleted.** The pitch deck stays public as a recorded exception.
- **Admin rights:** the MCP Server account (`mcpserver`, used by mcphub) is **no longer a Nextcloud admin**. Nextcloud's `admin` group now holds only `admin` and `fcore`.
- **Service and test accounts: Nextcloud sign-in is disabled for all 7.** Their mailboxes and SMTP logins still work. Federated Computer will delete three of them from LDAP.
- **Still open:** see the list at the end of this page.

1. Public links

Before the review, Aaron owned 14 public links. All 14 opened for anyone with the URL. None had a password, only one had an expiry date, and five let anyone with the link edit the file. Aaron's activity stream, checked back to 25 April 2026, showed downloads on only three of them.

Decision (Aaron): keep the pitch deck public and delete all other links. Deleting a link leaves the file where it is; only the URL stops working.

Share	File or folder	Result
65	NFE Business / Fundraising / NFE_Pitch_Deck_v3.pptx (read only)	Kept public, with no password or expiry: see the exception below

Share	File or folder	Result
2	NFE Business / Pearl Marina / Bellavista power-backup proposal (editable)	Deleted
3	Notes / April 2025 - Week 2 (editable)	Deleted
12	Photos / 4 phases.png	Deleted
18	Forms / Power Outages in Urban Uganda responses (anonymous)	Deleted
19	Project Spark - EU / Joint Innovation Facility application questions (editable)	Deleted
20, 31, 34	Sezibwa Rentals / September and November 2025 usage sheets	Deleted
44	OSEA Community Showcase questionnaires (editable)	Deleted
48	STI Uganda / NFE Pitch - Funders (editable)	Deleted
60	Project Spark - EU / Team CVs folder (CVs and a headshot)	Deleted
62	NFE Team / Meeting Recordings / midweek check-in, 11 June 2026	Deleted
67	Project Spark - EU / a team member's headshot	Deleted

Afterwards, Nextcloud listed only share 65. From outside, the first 10 deleted links returned "not found" (HTTP 404). Nextcloud's brute-force protection blocked the check of the last three (HTTP 429), but the sharing API and Aaron's activity stream confirm they're gone.

Exception: share 65. Approved by Aaron Tushabe on 29 October 2026. Reason: the deck is for prospective funders, who need to open it without a password. Ends: 31 January 2027. The next review decides whether to renew it.

Not changed: four email shares also have no password or expiry date, and all four let recipients edit. Two go to partners at EnAccess, one to eiot.energy, and one to a team member's personal Gmail. See the open items.

2. Admin and privileged groups

Group	Members after the review	Notes
Nextcloud <code>admin</code>	<code>admin</code> , <code>fcore</code>	<code>mcpserver</code> removed

Group	Members after the review	Notes
LDAP <code>admins</code>	aaron.tushabe, <code>admin</code> , <code>fcore</code>	No change. This LDAP group doesn't make anyone a Nextcloud admin.
NFE Leads	Aaron, Hillary, Dansturn	Matches the policy
NFE Everyone	Aaron, Dansturn, Daphine, Dismas, Esther, Hillary, Nickson, Tom	Matches the policy

- `admin` is the admin login, used only for admin work. Owner: Aaron. It was last used on 29 October 2026, for the team-folder setup and this review.
- `fcore` is Federated Computer's account (our host). Its last Nextcloud sign-in was 18 December 2025. It stays for now. Federated Computer should confirm that it's still needed and protected with 2FA.
- `mcpserver` **was removed** from `admin` for two reasons:
 - It's a local Nextcloud account, outside LDAP and Authelia, so it has no 2FA. The policy requires 2FA for admins.
 - Everyone who uses mcphub shares it. If its login leaked, someone would get full control of Nextcloud. For example, they could add the account to NFE Leads and read NFE Finance.
- Effect on mcphub:** `nextcloud_admin_list_users` now returns 403 Forbidden. The other mcphub Nextcloud tools still work (checked). To look up a username, use the `nextcloud-api` skill or the `admin` login.

3. Service and test accounts

Disabling a Nextcloud login only stops that account signing in to Nextcloud. LDAP, mail and SMTP are unchanged. To undo it, sign in as `admin` and go to Accounts → Disabled accounts, then choose Enable account from that account's menu.

Account	Purpose	Owner	Status
<code>customer.support</code> (support@)	Customer support mailbox	Aaron	Kept; Nextcloud sign-in disabled
<code>list.monk</code>	Sends mail for Listmonk	Aaron	Kept; Nextcloud sign-in disabled
<code>supabase.smtp</code> (no-reply-auth@)	Sends Supabase sign-in emails	Aaron	Kept; Nextcloud sign-in disabled
<code>nfe.team</code> (team@)	Shared team mailbox	Aaron	Kept; Nextcloud sign-in disabled (last Nextcloud sign-in 28 September 2026)
<code>nfe.accountant</code>	None (never used)	n/a	Disabled; Federated Computer to delete it

Account	Purpose	Owner	Status
derekttest1.test1	Test account (never used)	n/a	Disabled; Federated Computer to delete it
federated.test	Federated Computer test account (last used 10 October 2025)	n/a	Disabled; Federated Computer to delete it
mcpserver (Nextcloud only)	mcphub's connection to Nextcloud	Aaron	Kept; no longer an admin

4. Other findings

- **mcphub can read Aaron's whole Nextcloud.** It holds a working credential for his account and listed his home folder, NFE Finance included. This is probably the "cli" app password that an administrator created on his account on 13 October 2026. That app password is already an open item in the [2026 mailbox incident report](#). Anyone who can use mcphub's `nextcloud_user_*` tools can use this credential.
- **mcphub connects to Nextcloud over `http://`.** This showed up in one of its error messages. Unless mcphub runs inside the server's own network, its login travels unencrypted.
- **Nextcloud keeps no audit log.** The `admin_audit` app isn't enabled, although the [Audit Logging Policy](#) assumes it is.
- **Nextcloud doesn't enforce link passwords or expiry dates.** Turning both on under Administration → Sharing would make the policy's rule for links automatic.
- **Nextcloud's own 2FA enforcement is off.** Staff sign in through Authelia, which handles 2FA. Local accounts such as `mcpserver` don't go through Authelia.
- **Hillary's public link on `meter_data`** (share 55, created 24 March 2026) has no password or expiry date. Only Hillary can change it.

Open items

All are due before the next review (31 January 2027).

#	Action	Owner
1	Ask Federated Computer to delete <code>nfe.accountant</code> , <code>derekttest1.test1</code> and <code>federated.test</code> from LDAP, and to confirm <code>fcore</code> is still needed and has 2FA	Aaron

#	Action	Owner
2	List the accounts mcphub holds credentials for. Confirm or revoke the "cli" app password, and decide who may use mcphub's <code>nextcloud_user_*</code> tools	Aaron
3	Point mcphub at <code>https://</code>	Aaron
4	Enable <code>admin_audit</code>	Aaron
5	Enforce passwords and expiry dates on public links	Aaron
6	Review the four email shares: delete the one to a personal Gmail, and add expiry dates to the rest	Aaron
7	Add a password and an expiry date to share 55 on <code>meter_data</code> , or delete it	Hillary
8	Confirm that Daphine, Dismas and Tom still need their accounts. None of them has signed in to Nextcloud	Aaron
9	Do the checks this review skipped: app passwords and sessions (each person checks their own), and SSH keys	Aaron
10	Create the access register and copy the service-account table into it	Aaron

How this review was done

Notes for the next reviewer:

- **Public links:** list them through the Nextcloud sharing API (`/ocs/v2.php/apps/files_sharing/api/v1/shares` , `share_type` 3) with the `nextcloud-api` skill. When checking a link from outside, print only the HTTP code, never the link itself. After about 10 "not found" answers in 30 minutes, Nextcloud's brute-force protection starts returning 429. Wait half an hour before checking again.
- **Groups and accounts:** sign in as `admin` in a browser and use the OCS provisioning API (`/ocs/v2.php/cloud/groups/<group>/users` and `/ocs/v2.php/cloud/users/<id>`).
- **Link usage:** look for `public_links` events in the link owner's activity stream. Viewing a file in the browser may not be recorded.

ERPNext access review, 29 October 2026

ERPNext access review, 29 October 2026

This is the first review of ERPNext access under the [Access Management Policy](#), done the same day as the [Nextcloud review](#). It covers `erpnext.nearlyfreeenergy.com` (company Watt Works Foundation Limited). Aaron Tushabe (Security DRI) reviewed and approved it on 29 October 2026. Claude ran the checks and made the approved changes in the browser while signed in as `admin@nearlyfreeenergy.com`, so ERPNext's history shows that account, on 30 October between 02:50 and 02:56 Kampala time. The next review is due by 31 January 2027, together with Nextcloud.

Outcome

- **Service and test accounts:** all 7 are **disabled** in ERPNext: `list.monk`, `no-reply-auth`, `support`, `team`, `nfe.accountant`, `federated.test` and `derekttest1.test1`.
- **Staff who had never signed in:** Daphine, Dismas, Nickson and Tom are **disabled until they need ERPNext**.
- **Unused roles removed:** the four people who keep access (Aaron, Esther, Hillary and Dansturn) no longer have HR User, Manufacturing User, Projects User or Sales User.
- **Email-link sign-in is off.** The Authelia button is now the only way to sign in to ERPNext in a browser.
- **Still open:** see the list at the end of this page.

1. What the review found

- **18 accounts, all enabled.** 15 named accounts were created together when ERPNext was set up on 31 August 2026, and Esther's was added on 19 October. The other two are the built-in Administrator and Guest.
- **Everyone had the same seven roles.** Every person, mailbox and test account held Accounts User, HR User, Manufacturing User, Projects User, Purchase User, Sales User and

Stock User. Accounts User alone can create, submit and cancel journal entries, so every named account, mailboxes and test accounts included, could post to the books.

- **Only three accounts had ever signed in:** aaron.tushabe (last on 24 October), admin@ (30 October) and Esther (19 October). ERPNext keeps sign-in records for 90 days and was about 60 days old, so this history is complete.
- **ERPNext is used only for accounting:** 158 journal entries, 9 assets, 4 bills and 1 supplier. HR, sales, projects, stock and manufacturing hold no documents.
- **Email-link sign-in bypassed Authelia.** Password sign-in was already off. Next to the Authelia button, the login page offered **Login with Email Link**, which emails a one-time sign-in link to any enabled account. That skipped Authelia and its 2FA. Anyone who could read the mailbox of an enabled account, such as support@ or team@, could have signed in to the books. ERPNext's own 2FA is off.

2. Accounts and roles after the review

Account	Roles	Status	Why
aaron.tushabe	Accounts User, Purchase User, Stock User	Enabled	Bookkeeper. Has the only personal API key (see Using ERPNext with Claude)
esther.chemutai	Accounts User, Purchase User, Stock User, Spending Approver	Enabled	Accountant and approver
hillary.arinda	Accounts User, Purchase User, Stock User, Spending Approver	Enabled	Approver. Has never signed in to ERPNext
dansturn.kimbowa	Accounts User, Purchase User, Stock User, Spending Approver	Enabled	Approver. Has never signed in to ERPNext
admin@nearlyfreeenergy.com	System Manager, Accounts Manager, and the manager and user roles of each module	Enabled, unchanged	Admin login, owned by Aaron and used only for admin work. Apart from Administrator, the only System Manager: makes API keys, deletes bills, and changes roles and settings. Signs in through Authelia
Administrator	All roles	Unchanged (can't be disabled)	Built in. Its API key is mcphub's connection to ERPNext; see section 4
Guest	Guest	Unchanged	Built in, used for public pages

Account	Roles	Status	Why
daphine.nabwami, dismas.friday, nickson.kiwumulo, tom.oketch	The seven, left in place	Disabled	Staff who have never signed in. Re-enable when they need ERPNext, with the roles above
list.monk, no-reply-auth ("Supabase smtp"), support, team	The seven, left in place	Disabled	Mailboxes and mail senders, not people. Owner: Aaron
nfe.accountant, federated.test, derektest1.test1	The seven, left in place	Disabled	Never used. Federated Computer is to delete them from LDAP (Nextcloud review, open item 1)

- **Why Purchase User and Stock User stay:** the bill form needs them to look up units of measure (Stock User), price lists and purchase tax templates (Purchase User). Accounts User alone can't read those.
- **Why approvers keep Accounts User:** approving a bill submits it, and only Accounts User and Accounts Manager may submit bills.
- **Re-enabling an account:** sign in as admin@, open the user record, tick **Enabled** at the top of the User Details tab, and save. Disabled accounts still have their old seven roles, so at the same time untick HR User, Manufacturing User, Projects User and Sales User on the Roles & Permissions tab. The list view's bulk Edit doesn't offer the Enabled field.

3. Sign-in

- **Login with Email Link is off** (System Settings → Login). The login page now offers only **Login with Authelia**. Aaron, Esther and admin@ already sign in through Authelia, so no one lost access.
- **If Authelia is down, no one can sign in to ERPNext in a browser.** There are two ways back in: mcphub (Administrator's key) can turn email-link sign-in back on, or Federated Computer can do it on the server.
- **2FA for ERPNext now depends on Authelia** requiring it for erpnext.nearlyfreeenergy.com. This hasn't been checked yet (open item 2).

4. Other findings

- **mcphub's ERPNext key belongs to Administrator.** It can do anything, the no-self-approval check doesn't apply to it, and its changes show only "Administrator". The policy requires an owner and a purpose for every key, but neither is recorded for this one. The four Green Volta bills awaiting approval (ACC-PINV-2026-00001 to 00004) were prepared this way, so ERPNext shows Administrator as their preparer.

- **ERPNext doesn't log API requests** (System Settings → Log API Requests is off). Work done with an API key, through mcphub or the erpnext-api skill, leaves only each document's version history.
- **Every visitor shows the same IP address, 192.168.0.13**, which is the proxy in front of ERPNext. ERPNext's IP records therefore can't tell people apart.
- **Hillary and Dansturn have never signed in.** Only Hillary may approve Green Volta bills, and four are waiting.

Open items

All are due before the next review (31 January 2027).

#	Action	Owner
1	Give mcphub its own ERPNext user with read-only roles, and do admin work as admin@. Then generate a new Administrator key, so the old one stops working. Record who owns mcphub's key and what it's for	Aaron
2	Confirm that Authelia requires 2FA for erpnext.nearlyfreeenergy.com	Aaron
3	Decide whether to turn on Log API Requests (System Settings; requests are kept for 90 days)	Aaron
4	Ask Federated Computer to pass the visitor's real IP address through to ERPNext	Aaron
5	Sign in to ERPNext once through Authelia. Hillary then reviews the four Green Volta bills	Hillary, Dansturn
6	Confirm that Daphine, Dismas, Nickson and Tom are still at NFE. Offboard anyone who has left, in every system (Nextcloud review, open item 8)	Aaron
7	Add ERPNext accounts and roles to the access register once it exists (Nextcloud review, open item 10)	Aaron

How this review was done

Notes for the next reviewer:

- **Users and roles:** a personal key (erpnext-api skill) can list users with Enabled and last sign-in, and the Has Role table (`list "Has Role" --parent User`). It can't see user types or the Administrator account. mcphub's `frappe.client.get_list` on User and on Has Role (with `"parent": "User"`) shows everything, read-only.
- **Sign-ins:** the Activity Log (operation Login, kept for 90 days). Rows in the User Social Login table with provider `authelia` show who has signed in through Authelia.
- **Which roles a form needs:** the DocPerm rows for each role. No custom permissions existed at the time of this review.
- **Changes:** make them in the desk as admin@. Each user's version history then shows who changed what, and when.