

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 admin	admin , fcore	mcpserver 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
derektest1.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>derektest1.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.

Revision #1

Created 2026-10-29 22:18:00 UTC by aaron.tushabe

Updated 2026-10-29 22:18:00 UTC by aaron.tushabe