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 derektest1.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.

Revision #1
Created 2026-10-30 00:14:34 UTC by aaron.tushabe
Updated 2026-10-30 00:14:34 UTC by aaron.tushabe