Managing Pams Users

August 18, 2026

Understanding Pams User Accounts

A Pams user account is an internal account for a person who needs to work in Pams. Persona-admin users manage these accounts through the **Users** screen. Each user record holds the information Pams uses to identify the person, such as **First Name**, **Last Name**, **Full Name**, and **Login Email**.

Do not confuse a Pams user with an **Account**, **Client**, **Contact**, **Principal**, or **Sub-supplier** record. Those records represent companies, people, and business relationships managed in Pams. A Pams user account represents an internal person who works with those records. For example, an Account Manager may be assigned to an Account, but that Account Manager must also have an active Pams user account to sign in and work with Pams.

Managing a user account is an ongoing responsibility. The usual lifecycle is:

- Create the user record using the person’s correct identifying details.
- Activate the account when the person should be able to access Pams.
- Assign the user to the required **Branches** and **User Roles** shown on their record.
- Review and update the record when the person’s responsibilities, branch assignment, or contact details change.
- Deactivate the account when the person should no longer have access.

The **Active** status is especially important. A user record can remain in the **Users** list even when it is not active. An inactive record is useful for administration because you can still identify the person and review their existing user details, but the person cannot use that account to access Pams.

[SCREENSHOT: The Users list showing internal user records and the Active status]

Persona-admin users should keep user details, activation status, **Branches**, and **User Roles** current. This helps ensure that the people handling Sales Jobs, Projects, Invoices, Payments, Warehouse work, or Principal activities have the appropriate internal account setup for their responsibilities.

Preparing Details Before Creating a User

Before you select **Add New User**, confirm that you are signed in with persona-admin access. You need access to the **Security** area and the **Users** screen to create and maintain internal Pams user accounts. If you cannot open **Users** or cannot see **Add New User**, ask a persona-admin user to review your access.

Collect the user's details before opening the new-user form. Entering complete and accurate information at the start makes it easier to find the correct person later in the **Users** list and prevents confusion between users with similar names.

Prepare the following details from the information available for the person:

Detail	Where you use it in Pams	Why it matters
Name details	**First Name**, **Middle Name**, **Last Name**, and **Full Name**	Identifies the person in the **Users** list and on their user record.
Sign-in detail	**Login Email**	Identifies the account used for access to Pams.
Contact details	**Phone** and **Mobile**	Keeps the internal user record up to date where these fields are used.
Organizational context	**Branches** and **User Roles**	Supports the user's required responsibilities in Pams.

Decide which **Branches** and **User Roles** the person needs before creating the record. Do not assign a user to every available branch or role simply because those options are available. Start with the assignments required for the person's actual work, then update them if their responsibilities change.

Also check whether the person already has a record. Open **Security > Users** and review the existing list for the person's **Full Name** or **Login Email**. If you find an existing record, open it and update it rather than creating another user. Duplicate user records make it harder to manage activation, assignments, and account changes consistently.

[SCREENSHOT: The Users list with Full Name and Login Email visible for checking existing accounts]

Creating an Internal Pams User

Create a Pams user record when an internal person needs their own account to work in Pams. Start from the **Users** screen so the account is created in the same place where persona-admin users review, activate, and maintain all internal users.

1. Open **Security** and select **Users**.
2. Review the existing **Users** list for the person's **Full Name** and **Login Email**. If the person is already listed, open that record instead of adding a second one.
3. Select **Add New User**. Pams opens a new user record.
4. In **User Information**, enter the person's identifying details. Complete the available name fields, including **First Name**, **Middle Name** where needed, and **Last Name**. Review the resulting **Full Name** carefully so the person can be identified correctly in the **Users** list.
5. Enter the person's **Login Email**. Check the spelling and make sure it belongs to the intended internal user. Add **Phone** or **Mobile** when those details are available and should be kept on the user record.
6. Review all entered values before saving. Pay particular attention to the name and **Login Email**, because these details distinguish one internal user from another.
7. Select **Save**. If you have finished entering the initial details, you can select **Save and Close** to return to the **Users** list.
8. Confirm that the user appears in **Users** with the correct **Full Name** and **Login Email**. Open the saved record if you need to add **Branches** or **User Roles**.

[SCREENSHOT: The Add New User form showing User Information, Full Name, and Login Email]

Creating the record does not by itself mean the person can access Pams. If activation has not been completed, treat the record as an account awaiting activation. Complete the **Active** status and required assignments before relying on the account for day-to-day work.

Activating and Deactivating User Access

Use the **Active** status on a user record to control whether the internal account can access Pams. Activate a newly created account when the person is ready to use Pams. Deactivate an account when access must stop, while keeping the user record available for administrative review and future maintenance.

1. Open **Security > Users**.

2. Find the internal user in the **Users** list and open their record. Verify the **Full Name** and **Login Email** before changing the account status. This avoids activating or deactivating the wrong person when names are similar.
3. Locate the **Active** status on the user record. Review its current state before making a change.
4. To allow the person to access Pams, set the account to **Active**. Select **Save** or **Save and Close** to record the change.
5. Return to the **Users** list or reopen the user record and confirm that the account now shows as active. This confirmation is important before telling the user that their account is available.
6. To remove access, open the same user record and change the **Active** status so the account is no longer active. Select **Save** to apply the change.
7. Confirm the updated status after saving. The user record should remain in **Users**, but the account should no longer be active for access to Pams.

[SCREENSHOT: An individual user record with the Active status highlighted]

Deactivate accounts when a person leaves the business, changes to work that no longer requires Pams access, or should temporarily stop using Pams. Do not create a replacement record merely because an existing account is inactive. If the same person returns and should resume access, review their details and assignments, then reactivate the existing record when appropriate.

Before activating or reactivating an account, also review the user's **Branches** and **User Roles**. An active account should reflect the person's current responsibilities, not outdated responsibilities from an earlier position.

Assigning Users to Their Required Context

After creating the user record, review the assignment information shown on that person's record. In Pams, **Branches** and **User Roles** help record the organizational context required for the person's responsibilities. Keep these assignments limited to what the person currently needs for their work.

1. Open **Security > Users** and select the user whose assignments you need to review or change.
2. Review the existing **Branches** and **User Roles** on the user record. Do this before adding anything new so you can see what is already assigned.

3. Add the required **Branches** for the person's work. For example, use the **Branches** area when the person needs to be associated with a specific company branch shown in Pams.
4. Review **User Roles** and add the role or roles required for the user's responsibilities. Select only the roles that match the person's current work. Do not use a role simply because it is available in the list.
5. Remove any branch or role assignment that no longer applies. This is particularly important when a person changes department, branch, or job responsibilities.
6. Select **Save** to apply the updated assignments.
7. Reopen the record or review the saved user details to confirm that the required **Branches** and **User Roles** are displayed correctly.

[SCREENSHOT: A Pams user record showing the Branches and User Roles assignment areas]

Review assignments whenever a user moves between branches, takes on new responsibilities, or stops handling a workflow. For example, a person who no longer works with a particular branch should not retain an outdated **Branches** assignment. Similarly, update **User Roles** when the person's responsibilities change rather than leaving old assignments in place.

This screen records assignments for the individual user. The setup and maintenance of the available roles and teams is covered separately in Managing Roles and Teams. Use that guidance when the required role or team itself needs to be reviewed, created, or changed.

Resolving User Account Issues

When someone reports that they cannot access Pams or cannot work in an expected area, begin with their record in **Security > Users**. Check the user's **Full Name** and **Login Email** first, then review **Active**, **Branches**, and **User Roles**. These checks help you distinguish between a missing account, an inactive account, and an account with outdated assignments.

1. If the person cannot access Pams, open **Users** and check whether a record exists for their **Full Name** or **Login Email**. If no record exists, create one using **Add New User**.
2. If the record exists, open it and review the **Active** status. If the person should have access but the account is not active, update the status to **Active** and select **Save**.

3. If the user can access Pams but does not have the expected organizational context, review **Branches** and **User Roles** on the user record. Add the required current assignment, remove obsolete assignments, and save the record.

4. If you suspect a duplicate account, search the **Users** list using the person's **Full Name** and **Login Email**. Open the matching records and compare their details before creating another account. Maintain the appropriate record rather than creating a duplicate.

5. If a person no longer needs access, do not leave their account active. Open the record, update the **Active** status, and save the change. Also review **Branches** and **User Roles** so the record reflects the person's current position.

[SCREENSHOT: The Users list used to compare accounts with similar names or Login Email details]

When correcting a user record, make one clear change at a time and select **Save** before moving on. This makes it easier to confirm whether the issue was the activation state, a **Branches** assignment, or a **User Roles** assignment.

For sign-in-specific steps, refer to Signing In to Pams. If the issue relates to the person's own details rather than their internal user account setup, use Managing Your Profile.

Overview

The **Users** screen is the central place for persona-admin users to manage internal Pams accounts. Use it to create a user record, maintain the person's identifying information, control whether the account is **Active**, and review the **Branches** and **User Roles** assigned to that person.

The most important controls to review on each user record are:

- **Full Name** — identifies the internal person in the **Users** list.
- **Login Email** — identifies the account used for access to Pams.
- **Active** — shows whether the internal user account is active for access.
- **Branches** — records the branch context associated with the user.
- **User Roles** — records the roles assigned to the user.

A user record should always represent one internal person. Before selecting **Add New User**, check the existing **Users** list. Using one maintained record per person prevents confusion about which record should be active, which **Login Email** is current, and which assignments should be retained.

The user-management workflow is deliberately separate from day-to-day business records. A **Client**, **Contact**, **Account**, **Principal**, or **Sub-supplier** may be linked to sales, procurement, delivery, invoice, or payment work, but those records do not replace an internal Pams user account. Create and maintain a Pams user account only for people who need to use Pams internally.

[SCREENSHOT: The Users screen showing the user list and Add New User action]

Keep user records current as working arrangements change. Updating an existing user's **Active** status, **Branches**, or **User Roles** is preferable to creating an unnecessary new record. This gives persona-admin users a clearer, more reliable view of the internal accounts currently maintained in Pams.

Prerequisites

Before managing Pams users, make sure you have the required persona-admin access and the information needed to identify the internal person correctly. The following items help you complete user setup without creating incomplete or duplicate records:

- Access to **Security > Users**. You need to be able to open the **Users** list and select **Add New User**.
- The person's correct **First Name**, **Last Name**, and **Full Name**. Use these details to check for an existing record and to create a clear user entry.
- The person's correct **Login Email**. Review this carefully before saving because it identifies the internal account.
- Any available **Phone** or **Mobile** details that should be recorded on the user record.
- Confirmation of the user's required **Branches**.
- Confirmation of the user's required **User Roles**.
- A decision about whether the account should be **Active** immediately or remain not active until access is required.

Check the **Users** list before adding an account. Review both **Full Name** and **Login Email**, especially when the organization has people with similar names. If an account already exists, update that record rather than creating another one.

When you activate an account, make sure its **Branches** and **User Roles** are current. When you deactivate an account, review those same assignments so that the record accurately reflects the person’s current responsibilities.

The next user-security task is managing accounts for represented companies. Continue with Managing Principal Users.