Managing Principal Users

August 18, 2026

Confirming Who Needs Principal Access

Use a **Principal User** account only for a person who needs access as part of a represented **Principal** organization. This is different from access for your own agency or sales team. Before creating an account, confirm that the person needs to view or work with the Principal information made available through Pams, rather than needing a standard Pams user account.

For users who work for your own company, follow Managing Pams Users instead. Keeping Principal Users separate helps you review external access from the **Principal Users** list and avoid assigning the wrong type of access.

Before opening the new-user form, collect and confirm the details you will enter. Use the spelling and email address that the user will use for sign-in.

Detail to confirm	Where it is used	What to check
User’s name	**First Name**, **Middle Name**, and **Last Name**	Enter the name the user should see in Pams.
Sign-in email	**Email** or **Login Email**	Confirm the address is current and belongs to the intended user.
Principal assignment	**Principal** or **Is Principal**	Confirm which Principal organization the person should access.
Account availability	**Active**	Confirm whether the account should be available immediately.

You must also be able to open **Security** and select **Principal Users**. If **Principal Users** is not available in the Security area, do not create the account through another user list. Your current access may not allow you to manage Principal accounts.

Finally, check for an existing account before adding a new one. In the **Principal Users** list, search using the person’s name and their intended **Email** or **Login Email**. An existing record may need an update rather than a second account. Duplicate accounts can cause sign-in confusion and make it unclear which Principal access remains active.

[SCREENSHOT: The Security area with the Principal Users option highlighted, followed by the Principal Users list search field.]

Opening the Principal Users List

Open the **Principal Users** list before creating, updating, or removing Principal access. This list is the starting point for reviewing accounts that are intended for Principal users, checking whether a user already exists, and opening an account record for changes.

1. In Pams, open **Security** from the main navigation.
2. Select **Principal Users**.
3. Review the list before selecting any action. Check the displayed user names, email addresses, and any visible account information such as **Active** status or Principal-related details.
4. Use the list search to find a specific person. Start with the user’s name, then search again using their **Email** or **Login Email** if the name does not return a clear result.
5. If filters are available, use them to narrow the list. For example, review active accounts separately from inactive or archived records when you need to confirm whether an account is still in use.
6. Select the user’s row to open the account record. Review the **User Information** area and the Principal-related fields before making any change.

When you are checking for duplicates, do not rely only on the displayed name. Similar names can belong to different people, while a changed surname can make an existing account harder to find. The saved **Email** or **Login Email** is the most useful detail for confirming whether the account already belongs to the intended user.

If the list does not show the person you expect, clear any active filters and search again. A filter can hide a user record even when it exists. Also check whether the account may have been added as a regular Pams user rather than a Principal User; use the appropriate user-management area to review that record.

Use the list as a final review point after every change. A quick search confirms that you updated the intended person rather than another user with a similar name.

[SCREENSHOT: The Principal Users list showing the search field, user rows, and a visible account status or filter control.]

Creating a Principal User Account

Create a Principal User from the **Principal Users** list only after confirming that the email address is not already assigned to another account. Enter the user's details carefully, because the saved email address is used for the user's sign-in and any verification or activation steps shown by Pams.

1. Open **Security > Principal Users**.
2. Select **Add New User**.
3. In **User Information**, enter the person's **First Name** and **Last Name**. Complete **Middle Name** only when it is needed to identify the person correctly.
4. Enter the user's **Email** or **Login Email**. Verify the address before saving; use the address the person will actually use to sign in.
5. Select the required **Principal** assignment. If the form includes **Is Principal**, make sure it is selected for this account.
6. Review **Active** before saving. An active account should be available for the intended Principal user; do not leave an account active if it is being prepared only for later use.
7. Select **Save**. If you have finished entering the account information, use **Save and Close** where available.
8. Return to the **Principal Users** list and search for the saved email address. Confirm that the new user appears and that the displayed name and Principal assignment are correct.

After saving, Pams may show that the account is **Not activated yet** or prompt an email verification step. When Pams displays **Check your email**, **Send Verification Code to User**, or a similar email-based action, the user must use the saved **Login Email** to complete the sign-in setup. If the email address was entered incorrectly, update the account record before asking the user to continue.

Do not create a second account if the user cannot sign in immediately. First locate the saved record and confirm the email address, **Active** setting, and Principal assignment. This keeps one clear account record for each Principal user.

[SCREENSHOT: The Add New User form with User Information, Email or Login Email, Principal assignment, Is Principal, Active, and Save highlighted.]

Updating a Principal User's Details and Access

Update a Principal User record whenever the person’s displayed name, sign-in email, or Principal responsibility changes. Make changes in the existing account record rather than creating a replacement account for routine updates. This keeps the **Principal Users** list accurate and avoids leaving duplicate access records behind.

1. Open **Security > Principal Users**.
2. Search for the user by name, **Email**, or **Login Email**.
3. Select the correct user from the list to open the account record.
4. In **User Information**, update the user’s **First Name**, **Middle Name**, or **Last Name** if the displayed name has changed.
5. Review **Email** and **Login Email**. Update the saved address only when the user will sign in with a different email address.
6. Review the **Principal** assignment and **Is Principal** setting. Update these values if the user’s access should move to a different Principal organization or if the user should no longer be treated as a Principal User.
7. Check **Active** to make sure the account remains available only when the user still needs access.
8. Select **Save**, then return to the **Principal Users** list to confirm the updated information appears in the correct record.

Take extra care when changing **Login Email**. A user who continues to enter their previous email address may be unable to complete sign-in after the change. Confirm the new address with the user before saving it, and search the list for that address first to make sure it is not already assigned to another account.

If you are changing a user’s Principal responsibility, review the **Principal** field before and after the update. The user’s displayed name may remain the same, but the Principal assignment determines which Principal relationship the account is associated with.

[SCREENSHOT: An open Principal User record showing User Information, Login Email, Principal, Is Principal, Active, and Save.]

Removing Principal Access from Former Users

Remove or deactivate Principal access as soon as a person no longer needs to work with a Principal in Pams. Start from the existing account record so you can confirm that you are changing the correct person and can review the current **Principal** assignment before access is removed.

1. Open **Security > Principal Users**.
2. Search for the former user by their **Email** or **Login Email**. Searching by email is especially useful when more than one person has a similar name.
3. Open the user record and review the **User Information**, **Principal**, **Is Principal**, and **Active** fields.
4. Use the access option available on the record:
    - Clear **Is Principal** when the person should remain a Pams user but should no longer have Principal access.
    - Change **Active** when the person should no longer be able to use the account.
    - Use **Ultimate Delete** only when that action is available and the account record should be removed rather than retained.
5. Select **Save** after changing the access details.
6. Return to the **Principal Users** list, clear any filters, and search for the user again. Confirm that the record no longer appears as an active Principal User, or that the Principal setting has been removed.

Do not remove the final active Principal User responsible for a Principal organization until another appropriate person has access. First create or confirm the replacement user, then verify the replacement account in the **Principal Users** list. This prevents the Principal organization from being left without an available account.

If you are unsure whether the person may need access again later, review the options shown on the user record before using **Ultimate Delete**. Updating **Active** or **Is Principal** may preserve the record while removing the access that is no longer required.

[SCREENSHOT: A Principal User record showing Is Principal and Active settings, with the Principal Users list used to verify the result.]

Resolving Principal User Account Issues

Most Principal User issues can be resolved by checking the user's existing record in **Security > Principal Users** before creating or changing another account. Use the saved **Email** or **Login Email** as the main reference, because it identifies the account used for sign-in.

1. If Pams does not allow an email address to be saved, return to **Principal Users** and search for that exact **Email** or **Login Email**. Open the existing record and update it if it belongs to the intended person. Do not create another account with a variation of the same address.
2. If a user seems to be missing from the list, clear the current search and filters. Search once by the person's name and again by their **Login Email**. Check whether the account is inactive or no longer marked with **Is Principal**.
3. If the user cannot sign in or cannot complete activation, open the account record and compare the saved **Email** or **Login Email** with the address the user is using. Correct the saved address if needed, then use any visible email action such as **Send Verification Code to User**.
4. If Pams shows **Not activated yet**, review the saved email address first. When Pams displays **Check your email**, the user must use the inbox for the exact address saved on the record.
5. If the user has unexpected Principal access, open their record and review **Principal**, **Is Principal**, and **Active**. Correct the Principal assignment, clear **Is Principal**, or deactivate the account as required, then select **Save**.
6. Search for the user again in the list to confirm the correction is visible.

When an account problem affects a user who recently changed email address or Principal responsibility, review both items together. An updated email with an outdated **Principal** assignment can still leave the wrong access in place, while a correct Principal assignment with the wrong **Login Email** can prevent the intended user from signing in.

[SCREENSHOT: A Principal User record with Login Email, Principal, Is Principal, Active, and an email verification action highlighted.]

Overview

The **Principal Users** area in **Security** is used to maintain accounts for people who need access as part of a represented Principal organization. It gives you one list where you can search for Principal accounts, open their records, check their saved sign-in details, and review whether they are still active.

Use the **Principal Users** list for these account-management tasks:

- Check whether a Principal User already exists before selecting **Add New User**.
- Create a new record with **User Information**, **Email** or **Login Email**, and the required **Principal** assignment.

- Confirm that **Is Principal** is selected for accounts that should have Principal access.
- Use **Active** to review whether an account remains available.
- Update a person's name, sign-in email, or **Principal** assignment when responsibilities change.
- Remove Principal access by changing **Is Principal**, updating **Active**, or using the available record-removal action.
- Check email-related account status, including **Not activated yet**, and use a visible action such as **Send Verification Code to User** when Pams provides it.

A Principal User record is not only a name in a list. The combination of **Login Email**, **Principal**, **Is Principal**, and **Active** determines whether the account is set up for the right person and the right Principal relationship. Review all four items whenever you create or update access.

Use the **Principal Users** list as the verification point after every change. Search for the person by email, open the record if needed, and confirm that the displayed values match the access you intended to provide or remove. This is particularly important when a Principal has several users with similar names or when a user changes organizations.

[SCREENSHOT: Principal Users list with a selected record, showing how the list and account details work together.]

Prerequisites

Before managing accounts in **Security > Principal Users**, make sure you have the information and access needed to complete the change accurately. Preparing these details before selecting **Add New User** reduces duplicate accounts and avoids activation problems caused by an incorrect sign-in email.

Confirm the following before you create, update, or remove a Principal User:

- You can open **Security** and select **Principal Users**.
- You know whether the person needs a **Principal User** account rather than a regular Pams user account. For regular internal users, see Managing Pams Users.
- You have the person's correct **First Name** and **Last Name** for the **User Information** section.
- You have confirmed the email address that should be entered as **Email** or **Login Email**.

- You know the correct **Principal** assignment for the account.
- You have searched the **Principal Users** list by name and email to check for an existing record.
- You know whether the account should be available immediately through the **Active** setting.
- Before removing access, you have confirmed that another appropriate Principal User remains available for the Principal organization.

When changing an existing record, open the user's account first and note the currently saved **Login Email**, **Principal**, **Is Principal**, and **Active** values. This makes it easier to confirm exactly what changed after you select **Save**.

After Principal User accounts are in place, continue with Managing Roles and Teams to organize the roles and teams that support the right access across Pams.