Managing Roles And Teams

August 18, 2026

Reviewing Roles and Their Assigned Permissions

Use the **Roles** list to understand the access levels that are already available in Pams before changing any user assignments. A role groups the permissions needed for a particular responsibility. Teams, team members, and team leaders are separate assignments: a user can belong to a team without receiving the permissions required to manage that team.

1. Open **Security** and select **Roles**.
2. Review the **Roles** list. Use the **Role Name** to identify the intended responsibility of each role.
3. Open a role to view its details. In the role record, review the **Permissions** area and the users assigned to that role.
4. Check whether the role includes permissions for the administrative action the user needs, such as managing roles, managing teams, or maintaining team membership.
5. Compare the user assignments shown for the role with the user's team assignments. A user may be a team leader, a team member, or neither, regardless of the role assigned to them.
6. Return to the **Roles** list when you have finished reviewing the role.

[SCREENSHOT: The Roles list in Security, showing Role Name entries and a selected role record with its Permissions area.]

When reviewing a role, focus on what every assigned user needs to do in Pams. A change to one role affects all users who hold that role. For example, adding a permission that allows team management gives that ability to every user assigned to the role, not only one person.

Use an existing role when its access level already matches the responsibility you need to support. Create a separate role when a group of users needs a clearly different level of access. This keeps roles meaningful and prevents a single broad role from being used for unrelated responsibilities.

User accounts and their role assignments are covered in Managing Pams Users. If you are working with access for a principal's users, use Managing Principal Users rather than changing internal team assignments.

Creating and Updating Roles

Create a role when users need a distinct set of permissions that is not covered by the roles already listed in **Security > Roles**. Choose a name that makes the responsibility clear to other administrators. A clear **Role Name** helps you identify the correct role later when assigning users or reviewing access.

1. Open **Security** and select **Roles**.
2. Start a new role record.
3. Enter a descriptive value in **Role Name**. Use a name that reflects the work the role is intended to perform, such as a responsibility for team administration or membership maintenance.
4. In the **Permissions** area, select only the permissions this role requires. Add the permissions before assigning the role to users.
5. Click **Save**. If you are finished, use **Save and Close** where available.
6. Return to the **Roles** list and confirm that the new **Role Name** appears.
7. Open the saved role again and review the **Permissions** area to make sure the selected permissions are displayed.

To update a role, open its record from the **Roles** list, change the **Role Name** or the entries in **Permissions**, and click **Save**. Renaming a role changes the label used throughout Pams; it does not create a separate access level. Changing the permissions changes what all current role holders can do.

[SCREENSHOT: A role form showing the Role Name field, the Permissions area, and the Save button.]

After saving the role, assign it to the appropriate users through their user records. Do not assume that creating a role automatically assigns it to anyone. Review Managing Pams Users for the user-assignment process.

Before editing a role that is already in use, check the users assigned to it. If the requested access is needed by only a small group, create a separate role instead of expanding an existing role that may be used more widely.

Configuring Permission Access for Each Role

The **Permissions** area in a role record determines which administrative actions users with that role can carry out. Configure permissions around actual responsibilities: give users the ability to manage the records they are responsible for, without automatically giving them access to manage every security-related area.

1. Open **Security > Roles** and select the role you want to configure.
2. In the **Permissions** area, review the permissions already assigned to the role.
3. Identify the tasks role holders must perform in Pams. For example, decide whether they need to maintain roles, manage teams, or add and remove team members.
4. Add the permissions required for those specific responsibilities.
5. Keep role and permission administration separate from team administration. A user who needs to maintain a team may not need permission to change roles or alter the permissions assigned to a role.
6. Remove permissions that no longer match the role's responsibility.
7. Click **Save**, then reopen the role and review the **Permissions** area again.

[SCREENSHOT: The Permissions area of a role record, with permissions selected for role administration, team management, and team membership management.]

Consider the effect on all assigned users before saving. A permission added to a role is available to each user with that role, including users in different teams. Similarly, removing a permission can prevent every role holder from completing an action they previously performed.

Use separate roles when responsibilities differ. For example, one role can support people who maintain team membership, while another can support people who also manage roles and permissions. This separation makes it easier to review access when staff responsibilities change.

If a user cannot complete an expected action after you update permissions, first confirm that the user has the correct role assigned. The role's permission configuration and the user's assigned role must both match the responsibility you are trying to support.

Creating Teams and Assigning Team Leaders

Teams let you group users around shared sales, operational, or administrative responsibilities. A team record identifies the group, while team leader assignments identify the users responsible for leading it. A team leader still needs the appropriate role permissions to manage team records and memberships.

1. Open **Security** and select **Teams**.
2. Start a new team record.
3. Enter the team name in the available **Name** field. Choose a name that clearly identifies the group’s responsibility.
4. Complete any other available team details that are relevant to identifying the team.
5. Click **Save**.
6. Return to the **Teams** list and open the new team to confirm that its record was created.
7. Use the team’s leader assignment control to select one or more team leaders.
8. Save the team again and reopen it to verify that the selected leaders remain listed.

[SCREENSHOT: The Teams list and a team record showing the team name, leader assignment area, and member list.]

Choose leaders based on the responsibilities they need to carry out. A leadership assignment identifies the user as a leader for that team; it does not replace the user’s role. Before selecting a leader, open the user’s assigned role and confirm that the **Permissions** area includes the permissions required to manage teams or team membership, where that work is expected.

You can assign more than one team leader when responsibility is shared. Review the team name and leader list whenever the team’s coverage changes, such as when sales responsibilities move between groups or an operational Inquiry changes.

Creating a team does not automatically add users as members. Add the team’s members after the team and its leaders are saved.

Adding Members and Maintaining Team Membership

Use the team record to maintain the people who belong to each team. Team membership identifies who is included in that group. It is separate from a user’s role and separate from a team leader assignment, so changing membership does not automatically change a user’s permissions.

1. Open **Security > Teams**.
2. Select the team you want to maintain.
3. Use the member assignment control in the team record to add the required users.
4. Save the team and review the member list.
5. Check the leader assignment area separately to confirm which members are designated as team leaders.

6. To remove a user, open the same team record, remove that user from the member list, and click **Save**.
7. Reopen the team to verify that the member and leader lists show the intended assignments.

[SCREENSHOT: A team record showing separate areas for team leaders and team members.]

Keep the distinctions clear when making changes:

Assignment	What it identifies
Role	The permissions available to the user in Pams
Team member	The user’s membership in a specific team
Team leader	The user’s leadership responsibility for a specific team

Remove users from a team when they no longer work with that group. This change does not remove their user account and does not change their assigned role. If their responsibilities have changed more broadly, review their role assignment separately through the user record.

Review team membership when responsibilities move between sales teams, project groups, or operational teams. Keeping the member list current helps ensure that team leaders are managing the right group and that team assignments reflect current ownership. If you need to revise a user’s role as well as their team membership, follow the user process in Managing Pams Users.

Verifying Role, Team, and Leadership Assignments

When a user cannot manage roles, teams, or team membership as expected, check each assignment separately. The issue may be caused by the user’s assigned role, the permissions within that role, their absence from a team, or a missing team leader assignment.

1. Open the relevant user record and check the user’s assigned role.
2. If the user does not have the intended role, update the user assignment as described in Managing Pams Users.
3. Open **Security > Roles**, select that role, and review the **Permissions** area.
4. Confirm that the role includes the permission needed for the action the user is trying to perform, such as maintaining teams or managing team members.
5. Open **Security > Teams** and select the relevant team.

6. Review the team's member list to confirm that the user belongs to the team.
7. Review the leader assignment area to confirm that the user is listed as a team leader when leadership responsibility is required.
8. After making a change, click **Save** and reopen the role, user, or team record to verify that the assignment remains displayed.

[SCREENSHOT: A verification view showing a user's assigned role alongside the selected team's leader and member lists.]

Use this order because each item answers a different question. The role identifies the user's available permissions. The **Permissions** area identifies what that role allows. The team member list identifies whether the user belongs to the group. The leader assignment identifies whether the user is responsible for leading that team.

When reviewing a saved role, confirm both the **Role Name** and the selected permissions. When reviewing a saved team, confirm the team name, member list, and leader list. This final check is particularly important after moving responsibilities between teams or changing administrative access for several users.

Overview

Roles and teams work together in Pams to organize responsibilities and control access to administrative work. Use **Roles** to define what users can do. Use **Teams** to group users who work together. Use team leader assignments to identify who Inquiry a particular team.

The three assignments are related but independent:

- A user's role controls the permissions available to them.
- Team membership places a user in a specific group.
- A team leader assignment identifies leadership responsibility within that group.
- A user can belong to more than one team when their responsibilities span multiple groups.
- A team leader must also have a role that includes the permissions needed to manage the team or its membership.

For example, a user can be listed as a team member without being able to change the team's member list. Another user can be a team leader, but may still be unable to maintain team information if their assigned role does not include the required permissions. Review both the **Permissions** area of the role and the team record whenever access or leadership responsibility is unclear.

[SCREENSHOT: A simple Pams security workflow showing Roles, Users, Teams, Team Leaders, and Team Members as separate assignments.]

Use roles to avoid assigning broad administrative access to every user who needs to work with a team. Use teams to reflect current working responsibilities without changing permissions unnecessarily. This separation is useful when sales, purchasing, project, or operational responsibilities change while a user's general access level remains the same.

For principal-side access, maintain principal users separately through Managing Principal Users]. Principal user access should not be managed by adding those users to internal teams unless their user records and responsibilities specifically require it.

Prerequisites

Before creating or changing roles and teams, make sure you can access **Security**, **Roles**, **Teams**, and the relevant user records in Pams. You need sufficient administrative access to save role, permission, team, leader, or member changes.

Prepare the following information before you begin:

- The responsibility that the role or team should support.
- A clear **Role Name** for any new role.
- A clear team **Name** for any new team.
- The users who need to be assigned to the role.
- The users who should be added as team members.
- The users who should be assigned as team leaders.
- The specific administrative actions each role holder must be able to perform.
- Confirmation of whether a requested change applies to every user with an existing role or only to a smaller group.

Review existing entries in **Roles** and **Teams** before creating new ones. Reusing a suitable existing role or team can prevent duplicate entries with similar names. However, do not change an existing role simply because its name is similar; first check which users already hold it and what permissions it currently includes.

For changes to user access, first review Managing Pams Users. For changes affecting principal users, review Managing Principal Users. These records determine which role is assigned to each user, while the **Roles** and **Teams** screens determine the permissions and group responsibilities behind those assignments.

After setting up roles, teams, leaders, and members, continue with Configuring Two Factor Authentication to configure the next security setting in Pams.