PAMS (V2 PIPELINE RUN)

Configuring Company Settings

August 18, 2026

Accessing Settings as an Administrator

Company configuration affects the information and controls that people use throughout Pams. Before opening **Settings**, make sure you are signed in with administrator access. Administrators can review and change the available **Account**, **Company**, **Branch**, **Data Management**, and **Security** categories. If you cannot see one of these categories, or Pams does not allow you to save a change, stop and confirm your access with an administrator who manages user permissions.

1. Open the **Settings** area in Pams.
2. Review the available settings categories: **Account**, **Company**, **Branch**, **Data Management**, and **Security**.
3. Open the category that matches the change you need to make. For example, use **Company** for information shared across the company and **Branch** for information belonging to one branch.
4. Before editing, read the values currently shown in the form. This helps you avoid replacing information that is already correct.
5. Confirm whether the change should affect your administrator account, the whole company, or only one branch before selecting **Save**.

[SCREENSHOT: The Pams Settings area showing the Account, Company, Branch, Data Management, and Security categories.]

Use the categories for their intended scope:

Settings category	Use it for
Account	Preferences and information that apply to the administrator account
Company	Information used throughout the company in Pams
Branch	Information associated with one individual branch
Data Management	Controls for maintaining company and branch records
Security	Controls related to access and sign-in protection

Review the current **Company** and **Branch** configuration before making any change. Company information can be used across sales, purchasing, delivery, invoicing, and reporting workflows. Branch information can affect how branch-level operations are organized. Changes in **Data Management** may affect existing records, while changes in **Security** may change how users access Pams. Make changes deliberately and save only the settings that you have checked.

Maintaining Account Settings

Use **Account** settings when you need to maintain information or preferences that belong to your administrator account rather than the company or a branch. Do not use this category to update company-wide details or branch information; those belong in **Company** and **Branch** settings.

1. In the Pams **Settings** area, select **Account**.
2. Review the information and preferences displayed in the **Account** settings form before changing anything.
3. Identify the value you need to update and make the required change directly in the form.
4. Recheck the remaining values on the form so that an account-level update does not unintentionally alter another displayed setting.
5. Select **Save**.
6. Allow the page to refresh, then reopen or review **Account** settings to confirm that the updated value is still visible.

[SCREENSHOT: The Account settings form in Pams, with the Save button visible.]

Keep account settings separate from operational company configuration. For example, a change made in **Account** is intended for the administrator account currently being maintained. It should not be used to replace details that are shared by all users, all company records, or all branches.

If the value does not remain after you select **Save**, first confirm that you are still signed in with administrator access. Then return to **Account** and compare the displayed value with the value you entered. Avoid repeatedly changing the form without checking the saved result, especially if other administrators also maintain company configuration.

When several administrators use Pams, let the relevant administrator know when you make a meaningful account-related change. This reduces the chance that someone else later interprets an account preference as a company-wide or branch-wide setting. For related user access tasks, use the separate Pams guidance for Managing Pams Users and Managing Roles and Teams.

Updating Company and Branch Details

Pams separates information that applies to the entire company from information that belongs to an individual branch. Use **Company** settings for organization-wide configuration and **Branch** settings for branch-level configuration. Keeping these two areas separate prevents a branch update from replacing information that should remain shared across the company.

1. Open **Settings** and select **Company**.
2. Review the current company details shown in the **Company** settings form.
3. Update the company detail that needs to change, checking the existing values before replacing them.
4. Select **Save** and confirm that the revised company information remains displayed.
5. Return to the **Settings** categories and select **Branch**.
6. Review the branch-level information separately from the **Company** settings form.
7. Confirm that you are maintaining the correct branch before changing any branch value.
8. Update the applicable branch details and select **Save**.
9. Reopen **Branch** settings to verify the saved branch configuration.

[SCREENSHOT: Company and Branch settings categories shown side by side in the Pams Settings area.]

Company details can be used across records and workflows in Pams, including sales activity, purchasing activity, delivery documentation, invoices, and reports. For that reason, confirm that a change is appropriate for the whole organization before saving it in **Company** settings.

Branch settings should be reviewed with equal care. A branch may need its own configuration, but that configuration should remain limited to the applicable branch. Do not use **Branch** settings to overwrite information intended for the whole company. If the company works with more than one branch, agree internally on which administrators maintain each branch before making changes. Continue with Managing Company Branches for guidance focused on maintaining branch records.

Changing Company-Level Information

Use the **Company** settings page only for information that should be shared throughout the organization in Pams. Company-level configuration can be reflected across business records and documents, so review the existing form carefully before replacing a value.

1. Open **Settings** and select **Company**.
2. Read the existing company values in the **Company** settings form.
3. Determine whether the change is intended to apply across the company, rather than to one branch or to your own administrator account.
4. Edit only the company value that requires an update.
5. Review the form again before selecting **Save**.
6. Select **Save**.
7. Confirm that the saved value remains visible in **Company** settings after the page refreshes.

[SCREENSHOT: The Pams Company settings form, showing the company-level configuration and Save button.]

Use particular care when an existing value is already in use across Pams. Company information can be relevant to records created by sales, purchasing, finance, and operational teams. Replacing it without reviewing the current configuration can create inconsistency between current work and the information displayed on future records.

If you are uncertain whether a value is company-wide, do not save it in **Company** settings until you have checked with the administrator responsible for company configuration. The **Account** category is for the administrator account, while **Branch** is for a specific branch. Keeping this distinction clear makes it easier for teams to understand where maintained information belongs.

After saving, do not assume the change is complete until you reopen **Company** settings and check the displayed value. If the previous value remains, confirm your administrator access and review whether the value was entered in the correct settings category. Avoid making the same edit across both **Company** and **Branch** settings unless the information is intentionally required in both places.

Maintaining Branch-Level Information

Use the **Branch** settings page for information associated with one individual branch. Branch-level configuration must remain separate from the information maintained in **Company** settings. Before editing, confirm that the branch currently shown is the branch whose details you intend to maintain.

1. Open **Settings** and select **Branch**.
2. Review the current branch configuration displayed in the **Branch** settings form.
3. Confirm the active branch before changing any value.
4. Update the branch-specific detail that requires maintenance.
5. Check that the change belongs to this branch and does not belong in **Company** settings.
6. Select **Save**.
7. Reopen or refresh **Branch** settings and verify that the updated value remains visible.

[SCREENSHOT: The Pams Branch settings form, with the active branch configuration visible.]

Maintain only the information that is applicable to the selected branch. Do not use the **Branch** form to replace company-wide information simply because a branch needs to view or use it. If the same type of detail appears in both **Company** and **Branch** settings, use the scope of the setting to decide where to make the change: shared organization information belongs in **Company**, while information specific to one branch belongs in **Branch**.

When more than one administrator works with branch configuration, coordinate changes before saving them. This is especially important when a branch has active sales, purchasing, warehouse, delivery, or finance work in Pams. A branch-level change should be checked by the person responsible for that branch when possible.

After confirming the saved value, compare it with the **Company** settings only when you need to ensure that branch information has not been entered as company information. For broader branch maintenance and sharing choices, continue with Managing Company Branches.

Controlling Data Management Settings

Use **Data Management** settings to review and maintain the controls available for application data in Pams. Because these settings can affect existing company or branch records, treat them differently from ordinary personal preferences. Read each displayed option before changing it and confirm the intended effect with other administrators when the setting affects shared data.

1. Open the Pams **Settings** area and select **Data Management**.

2. Review the data-management options displayed in the form before making changes.
3. Identify whether the option relates to company records, branch records, or data maintained by multiple users.
4. Check the current selection and decide whether changing it could affect existing records.
5. Update only the option you have reviewed and agreed to change.
6. Select **Save** to apply the selected configuration.
7. Reopen **Data Management** settings after saving and confirm that the chosen option remains displayed.

[SCREENSHOT: The Data Management settings form in Pams, showing the available data-maintenance controls and Save button.]

Coordinate before saving a change when the displayed option can influence shared company or branch records. This is particularly important if other administrators maintain accounts, contacts, projects, products, sales jobs, purchasing records, or finance records. A data-management choice made for one team can have consequences for records used by another team.

Keep a clear internal record of the configuration you selected, including the date of the change and the reason it was needed. This makes it easier to review a recent change if someone later notices unexpected behavior in company or branch records. Do not make several unrelated changes at once. Save and verify one reviewed change before moving on to another setting.

If you cannot determine how an option affects existing records from the **Data Management** form, pause before selecting **Save** and coordinate with the other administrator responsible for the affected area. For example, a change connected to shared branch information should be discussed with the administrator who maintains **Branch** settings. After saving, review the displayed configuration again rather than relying on the values you entered.

Strengthening Security Settings

Use **Security** settings to review controls that govern access and sign-in protection in Pams. Security configuration can affect how users access Pams, so inspect the current values before making any change. Do not alter an access-related or sign-in-related setting unless you understand which users may be affected.

1. Open the Pams **Settings** area and select **Security**.
2. Review the security controls currently displayed in the **Security** settings form.
3. Identify the setting that needs to be updated and consider whether it changes access or sign-in requirements for other users.
4. Make the approved change in the form.
5. Review the selected value one more time before saving.
6. Select **Save**.
7. Return to **Security** settings after the page refreshes and confirm that the updated value is displayed.

[SCREENSHOT: The Security settings form in Pams, showing security controls and the Save button.]

Communicate a security change to affected users when it changes how they access Pams. Users need advance notice if the updated configuration changes the sign-in process or an access-related requirement. Keep the communication focused on the change users will experience and when it takes effect.

Separate security configuration from day-to-day user maintenance. Use **Security** settings for the security controls available in that category. Use the Pams guidance for Managing Pams Users, Managing Roles and Teams, and Configuring Two Factor Authentication when your task concerns users, roles, teams, or two-factor authentication.

If a security value cannot be saved, first confirm that you have administrator access. Do not repeatedly attempt unrelated changes in the same form. Reopen **Security**, compare the displayed value with the intended value, and review any recent settings changes with the relevant administrator. This controlled approach helps prevent one security adjustment from creating avoidable access issues for the wider team.

Verifying Your Settings Configuration

After changing any setting, verify the result in the same category where you saved it. Pams separates **Account**, **Company**, **Branch**, **Data Management**, and **Security** settings, so confirmation must include checking that information was saved in the correct place as well as checking that the displayed value is correct.

1. Return to **Account** settings and confirm that account-level changes are still displayed.

2. Open **Company** settings and verify that company-wide values appear in the **Company** settings form.
3. Open **Branch** settings and confirm that branch-specific values appear there without replacing company-level information.
4. Open **Data Management** settings and review the selected data-management configuration.
5. Open **Security** settings and check the saved security configuration.
6. If a value is missing or unchanged, confirm that you selected **Save** and that you were signed in with administrator access.
7. If a change has unexpected effects, review the most recent setting changes before editing additional values.

[SCREENSHOT: The Settings categories in Pams, used to verify Account, Company, Branch, Data Management, and Security configuration.]

Use the scope of each category as a verification check. A value meant for the company should be visible in **Company** settings. A value meant for one branch should be visible in **Branch** settings. A value intended only for the administrator account should remain in **Account** settings. If information appears in the wrong category, correct it carefully rather than duplicating it across categories without a clear reason.

For unexpected results after a **Data Management** or **Security** change, avoid making several corrective edits at once. First identify the most recent configuration change, review the value currently displayed, and coordinate with other administrators if shared records or user access may be affected. If saving is unavailable, check administrator permissions before attempting the change again.

Verification is especially important before users rely on revised company or branch information in active sales, purchasing, delivery, invoice, payment, or reporting work. Checking the saved settings immediately makes it easier to correct an incorrect entry before it affects wider operations.

Overview

Pams settings are organized by the scope of the information or control you are maintaining. Use the category that matches the intended outcome rather than placing the same information in several locations. This keeps company configuration clear for administrators and helps teams rely on consistent information during sales, purchasing, finance, warehouse, delivery, and reporting work.

- **Account** contains information and preferences for the administrator account being maintained.
- **Company** contains details that should apply throughout the organization.
- **Branch** contains configuration associated with an individual branch.
- **Data Management** contains controls for maintaining data that may affect existing company or branch records.
- **Security** contains controls related to access and sign-in protection.

The most important decision before selecting **Save** is the scope of the change. Ask whether the value applies only to the current administrator account, to the whole company, or to one branch. Then open **Account**, **Company**, or **Branch** accordingly. For controls affecting shared records or user access, use **Data Management** or **Security** and coordinate with other administrators where necessary.

[SCREENSHOT: A simple Pams Settings category view showing the five configuration areas.]

The settings categories support connected B2B operations in Pams. Company information can be used across sales jobs, purchasing work, delivery documentation, invoices, and reports. Branch configuration supports branch-level operations without overwriting organization-wide information. Data-management choices can affect records that teams use across Pams, while security choices can change the way users access Pams.

This document focuses on maintaining the settings categories themselves. It does not replace guidance for related configuration tasks such as users, roles, teams, document templates, dashboards, reports, or custom fields. Use the relevant Pams documentation when your work concerns those specific areas. For branch-specific administration, the next document, Managing Company Branches, explains how to maintain branch records and related branch configuration.

Prerequisites

Before changing **Account**, **Company**, **Branch**, **Data Management**, or **Security** settings in Pams, make sure you have the information and authority needed for the change. Settings can affect shared records, branch operations, and user access, so preparation reduces the risk of entering a correct value in the wrong category or applying an unapproved change.

- You are signed in to Pams with administrator access.

- You can open the **Settings** area and see the category relevant to your task: **Account**, **Company**, **Branch**, **Data Management**, or **Security**.
- You know whether the required change is for your administrator account, the whole company, or a specific branch.
- You have reviewed the current value in the applicable settings form before replacing it.
- You have confirmed the active branch before editing anything in **Branch** settings.
- You have coordinated with other administrators if the change may affect shared company records, branch records, or user access.
- You are ready to select **Save** and return to the same settings category to verify the displayed result.

Do not begin in **Company** or **Branch** settings until you can clearly identify the intended scope. Company-wide information belongs in **Company** settings. Information for one individual branch belongs in **Branch** settings. Information for the administrator account belongs in **Account** settings. This distinction is essential when multiple branches and multiple administrators use Pams.

For **Data Management** and **Security**, review the existing configuration and the likely effect on other users before saving. If the change relates to users, roles, or access controls, use the relevant Pams guidance alongside the **Security** settings form. If the change relates to branch records or branch-level operations, continue with Managing Company Branches.