

Understanding Role Visibility and Access Restrictions

August 25, 2026

Understanding What Users See After Signing In

In **Sherkety ERP & Website Platform**, the admin portal does not look the same for every signed-in user. What appears in the left navigation, which admin pages open successfully, and which buttons are available all depend on the user's assigned role. A content-focused user may see areas such as **Dashboard**, **Content**, **Services**, **Pricing**, **SEO**, and **Settings**, while a user without broader administrative access may not see every item in that list.

When a user reports that "a page is missing," start by checking whether the item is truly unavailable or simply hidden for that role. In daily use, **hidden navigation items usually mean the role was not given access to that portal area**. For example, if **Users** does not appear in the admin menu, that normally points to a role restriction rather than a page error.

It is also important to separate **menu visibility** from **actual page access**. A user might not see a menu item but still try to open a saved browser bookmark or direct link. In that case, Sherkety ERP & Website Platform can still block the page and show an access restriction message. In other words:

- **Visible in the menu** means the page is intended to be discoverable for that role.
- **Able to open the page** means the role is allowed to enter that screen.
- **Able to use buttons on the page** means the role has permission for specific actions inside that screen.

Before investigating a complaint, verify the user's assigned role in the **Users** area of the admin portal. If you already reviewed account details in [Viewing and Maintaining User Accounts](#), use that same user record to confirm whether the role matches the access the person expects to have.

[SCREENSHOT: User account screen showing the assigned role field and admin navigation]

Reviewing Which Portal Areas Each Role Can Access

In **Sherkety ERP & Website Platform**, access is usually divided by admin area first, then by what the user can do inside that area. The most common portal sections you may review are:

- **Dashboard** for the main admin landing page
- **Content** for website content editing
- **Users** for user account management
- **Settings** for site-wide configuration
- **SEO** for search-facing page information
- **Services** for service listings and related content
- **Pricing** for pricing tiers and package details

A role may be allowed into one area but blocked from another. For example, a content editor may be able to open **Dashboard**, **Content**, **Services**, **Pricing**, **SEO**, and **Settings**, while access to **Users** may be limited to a smaller group. That means two people can both sign in successfully but see different admin menus.

Visibility can also change within the same area. A user may be able to:

- Open a list page but not open certain records
- Open a record but not change any fields
- View page details but not use **Save**, **Delete**, or other action buttons
- See a page header but find row-level menus missing options

This is why you should not assume that “page opens” means “full access.” In practice, the differences administrators notice most often are:

- **View only** access: the user can read information but cannot update it
- **Limited action** access: the user can edit but not delete, approve, or publish
- **Section-only** access: the user can work in one admin area but not others

Restricted users usually experience one of three patterns:

- The navigation link is **missing**
- The page opens to an **access denied** or blocked state
- The page opens, but key actions are **not shown**

[SCREENSHOT: Admin sidebar with some sections visible and others absent for a restricted role]

Interpreting Hidden Buttons, Disabled Actions, and Access Denied Messages

When you review a user's complaint, the screen state itself often tells you what kind of restriction is in place. In **Sherkety ERP & Website Platform**, restrictions usually appear in three ways: **hidden controls**, **disabled controls**, or **blocked page access**.

A **hidden** control means the user is not meant to use that action at all. Common examples include:

- No **Create** button at the top of a list
- No **Edit** option on a page
- No **Delete** choice in a row menu
- No **Users** or **Settings** item in the navigation

A **disabled** control means the action is visible, but the user cannot complete it in the current permission state. You may see a **Save** or **Submit** button that remains unavailable, or fields that appear on screen but cannot be changed. This usually means the user can view the page but does not have permission to finish the action.

A **blocked page load** is different again. If a direct link opens an **access denied** message, the user is being stopped at the page level before they can work with the content at all. This often happens when someone receives a shared link to an admin page that their role does not include.

If a user can open a detail page but cannot change values or save updates, treat that as **view access without edit access** unless you find another explanation. Look closely at:

- Whether fields are editable or read-only
- Whether **Save** appears and can be used
- Whether page header actions are present
- Whether row-level menus show fewer options than expected

Read restriction messages in context. A missing menu item usually points to **section access**, a blocked page points to **page access**, and a missing or unavailable button points to **action access**.

Checking Access for a Specific User or Role

To verify access properly in **Sherkety ERP & Website Platform**, start in the **Users** area and open the affected person's account. Confirm the assigned role before

looking anywhere else. Many visibility issues come from the user expecting one level of access while the account is assigned another.

Once you have the user record open, review the role connected to that account and compare it with the reported problem. Focus on the exact area the user mentioned, such as **Content**, **SEO**, **Pricing**, **Services**, **Settings**, or **Users**. Then compare what the role should allow with what the person actually sees.

A practical review should include these checks:

- **Left navigation:** Is the expected section visible in the sidebar?
- **Page access:** Can the user open the target page at all?
- **Page tabs or sections:** Are all expected parts of the page available?
- **Toolbar actions:** Are buttons like **Save**, **Edit**, or other page actions present?
- **Row-level menus:** Do record menus show the expected options?

If your team uses a test account for each role, sign in with that account and reproduce the issue directly. That is often the fastest way to confirm whether the behavior is correct for the role. If your admin process includes an impersonation-style review, use that same approach to see the portal exactly as the affected user sees it. The goal is to compare the real interface, not just the intended setup.

As you review, keep your findings specific. Instead of noting “user has no access,” record the exact result, such as:

- **Users** is missing from the sidebar
- **SEO** opens, but **Save** is unavailable
- **Pricing** opens, but row actions are missing
- Direct access to **Settings** shows an access denied message

[SCREENSHOT: Admin user record with role details and a comparison against visible admin sections]

Managing Daily Administration When Access Is Restricted

Access complaints are part of normal admin work in **Sherkety ERP & Website Platform**, especially when different teams handle content, pricing, SEO, and user administration. The key is to decide whether the restriction is **expected by role design** or whether it points to an incorrect account setup.

When a user reports a missing page, missing button, or blocked action, avoid changing access immediately. First confirm what the role is supposed to allow. A

restriction is usually expected when the user is intentionally limited to a smaller set of tasks. For example, someone who updates content may not need access to **Users**, and someone who can review records may not be allowed to delete them.

A simple review flow works well for daily administration:

- Confirm the user's assigned role in the **Users** area
- Identify the exact page, menu item, or button involved
- Reproduce the issue with the same role, if possible
- Decide whether the current restriction matches the person's job
- Change access only if the role assignment or permission setup is wrong

This matters because broader access affects more than visibility. Granting additional rights can allow a user to:

- Change live website content
- Update pricing information
- Modify SEO details
- Adjust site-wide settings
- Manage user accounts
- Perform edit or delete actions that were previously restricted

Be especially careful when enabling actions tied to **editing, deleting, approval-style decisions, export-related tasks, or settings changes**. Those actions have a wider impact than simple page visibility.

If the issue turns out to be expected behavior, explain it clearly in user-facing terms: "Your role can open **Content**, but it does not include **Settings**," or "You can view this page, but your role does not include editing on this screen." That keeps the conversation focused on the visible interface instead of internal permission language.

Resolving Common Visibility and Access Problems

Most access issues in **Sherkety ERP & Website Platform** fall into a few repeat patterns. When you troubleshoot them consistently, you can usually tell whether the problem is caused by role setup, a saved session, or a misunderstanding about what the role includes.

If a user **cannot find a menu item in the sidebar**, first verify that the assigned role includes that admin section. In many cases, the item is intentionally hidden. Check

whether the missing item is one of the restricted areas such as **Users** or **Settings**, then compare the user's role with another account that should see it.

If a user **can open a page but cannot use key actions**, look beyond page access. This often means the role has permission to view the page without matching permission to act on it. Common signs include:

- No **Edit** button
- No **Delete** option in row menus
- A visible but unavailable **Save** button
- Read-only fields on a detail screen

If an administrator **changed a role but the user still sees the old behavior**, confirm three things:

- The role change was actually saved
- The correct role is assigned to the correct account
- The user refreshed the session by signing out and back in, or by reloading the portal

If a **direct link opens an access denied page**, treat that separately from menu visibility. A hidden sidebar item and a blocked page load are related, but they are not the same check. The user may have received a bookmark or shared link to a page that their role cannot open directly.

When the cause is unclear, compare the affected user with a known-good account that has the expected role. Look at the same sidebar, the same page header, and the same row menus. That side-by-side review usually reveals whether the issue is missing section access, missing action rights, or simply the wrong role on the account.

Overview

Role visibility in **Sherkety ERP & Website Platform** controls what each signed-in user can see and do inside the admin portal. This affects more than the sidebar. It also changes which admin pages open, which buttons appear in page headers, and which actions are available inside lists and detail screens.

The most important idea is that access works at more than one level:

- **Section visibility** controls whether areas like **Dashboard**, **Content**, **Users**, **SEO**, **Services**, **Pricing**, and **Settings** appear in navigation
- **Page access** controls whether a user can open a screen directly

- **Action access** controls whether buttons such as **Save**, **Edit**, or **Delete** are available once the page is open

As an administrator, you will usually notice restrictions in one of these ways:

- A menu item is completely **missing**
- A page opens with an **access denied** message
- A page opens, but important controls are **hidden** or **unavailable**

This document focuses on how to read those signs correctly and how to verify whether the user's current role matches the experience they are reporting. If you need help with the user list, account details, or where to find user records, return to [Viewing and Maintaining User Accounts](#) before continuing your review.

Use this guide when you need to answer questions such as:

- Why can one admin see **Users** but another cannot?
- Why does a user have access to **SEO** but not **Settings**?
- Why can someone open a page but not save changes?
- Why does a direct link fail even though the user is signed in?

[SCREENSHOT: Admin portal showing sidebar, page header actions, and an example restricted state]

Prerequisites

Before you review role visibility in **Sherkety ERP & Website Platform**, make sure you can already access the admin portal and open user records. You do not need to know every role rule in advance, but you do need enough access to inspect user accounts and compare what different users can see.

You should already be comfortable with:

- Signing in to the admin portal
- Opening the **Dashboard**
- Navigating to the **Users** area
- Opening an individual user account
- Recognizing common admin sections such as **Content**, **Services**, **Pricing**, **SEO**, and **Settings**

If you have not done that yet, use [Viewing and Maintaining User Accounts](#) first. That guide covers how to locate users and review their account details, which you will need

before you can investigate access complaints.

It also helps to have the following ready before you start checking a reported issue:

- The affected user's name or account
- The exact page or menu item they expected to see
- The specific action they could not use, such as **Save**, **Edit**, or **Delete**
- A second account or known role example for comparison, if your team uses one

During your review, pay attention to visible interface clues rather than assumptions.

Compare:

- Sidebar items
- Page tabs
- Header buttons
- Row action menus
- Access denied messages

That comparison is often enough to tell whether the issue is caused by the assigned role or by a mismatch between the user's expectations and their current access. From here, the next document is [Managing User Lifecycle in the Admin Portal](#), which continues with the day-to-day handling of user accounts after access has been reviewed.