

Assigning Roles and Understanding Visibility Rules

August 25, 2026

Reviewing how roles control what appears in the admin portal

In Sherkety ERP & Website Platform, a user's assigned role controls much more than whether they can sign in. It changes what appears in the admin navigation, which admin pages open successfully, which records appear inside lists, and which action buttons are available on each screen. A content-focused user may see areas such as **Dashboard**, **Content**, **Services**, **Pricing**, **SEO**, and **Settings**, while someone without the right access may not see those menu items at all.

Visibility usually changes in three clear ways in the interface:

- **Hidden navigation items:** a page such as **Users** or **Settings** may not appear in the admin menu
- **Blocked pages:** a user may open a saved link or bookmarked page and be stopped from entering it
- **Missing action buttons:** the page opens, but buttons such as **Add**, **Edit**, **Delete**, or other management actions are not available

This distinction matters because viewing access and action access are not always the same. A user might be able to open the **Users** list and read account details, but still be unable to change a role or update a profile. Another user might see the **Content** area and edit page text, but not access **SEO** or **Settings**.

Role changes can also affect what appears inside a page after it opens. For example, a list may show fewer records, search results may be limited, or details inside a record may be reduced based on the user's access level. If a user reports that "the page is there, but I can't see everything," the issue may be record visibility rather than menu visibility.

[SCREENSHOT: Admin menu showing one user with more sections visible than another]

For a deeper explanation of how these restrictions work before you make changes, see [Understanding Role Visibility and Access Restrictions](#).

Checking the roles and permissions available before assigning access

Before you assign access, review the role options already available in Sherkety ERP & Website Platform. Start by signing in to the admin portal and opening the **Users** area from the admin navigation. From there, look for the part of the user profile or administration area where access is managed. Depending on your screen layout, this may appear as a **Roles**, **Permissions**, or **Access** section when you open a user account.

As you review the available choices, focus on what each role allows the person to do in the admin portal. In this product, the most important distinction is whether the role gives access to protected admin pages such as:

- **Dashboard**
- **Content**
- **Users**
- **Settings**
- **SEO**
- **Services**
- **Pricing**

Some roles are broad and open several sections at once. Others are narrower and are intended for a specific kind of work, such as content editing. If your organization uses more than one role on the same account, review the full combination before saving changes. A user with overlapping roles may receive more access than expected.

Use this quick review approach before assigning anything:

What to check	What to look for in the interface
Role name	Whether it clearly matches the person's job
Admin sections opened by the role	Which menu items become available
Allowed actions	Whether the user can only view, or also add, edit, and remove
Combined access	Whether multiple assigned roles expand visibility

You should also confirm that you personally have permission to manage user access. If you can open the **Users** page but cannot change role-related fields or save updates, your own account may not have enough administrative access.

If you need a refresher on finding and opening user records first, see [Viewing and Maintaining User Accounts](#).

Assigning roles to a user account

Use the **Users** page in Sherkety ERP & Website Platform to assign or change access for an administrator.

1. Open the admin portal and select **Users** from the navigation.
2. In the user list, find the person you want to update and open their profile.
3. Locate the **Roles**, **Permissions**, or **Access** area on that user's screen.
4. Select the role or roles that match the work this person should perform.
5. Click **Save** to apply the change.

[SCREENSHOT: User profile with Roles or Access section highlighted]

After saving, pay attention to the feedback message on screen. Sherkety ERP & Website Platform may show a confirmation message that the update was saved. In many cases, access changes take effect right away, but the user may need to sign out and sign back in before the menu and page visibility fully refresh in their session. If the user is already signed in when you make the change, ask them to refresh their session before you test the result.

To remove access, return to the same user profile, open the **Roles** or **Access** area, and clear the role you no longer want assigned. Then click **Save** again. If someone has been given a role that is too broad, replace it with a narrower role instead of simply adding another one on top. Stacking roles can unintentionally expand access.

If you make a change by mistake, reopen the user profile immediately and restore the previous role selection before leaving the page. It is helpful to review the user's current access before editing so you know exactly what changed.

If the account itself needs to be activated, deactivated, or otherwise maintained before role assignment, use the steps in [Managing User Lifecycle in the Admin Portal](#).

Matching roles to the work each administrator needs to perform

The safest way to assign access in Sherkety ERP & Website Platform is to match each role to the person's actual day-to-day work. Start with the smallest amount of access needed, then add only what is required. This keeps the admin portal easier to use and reduces the chance that someone edits content, settings, or user accounts they were only meant to review.

A practical way to think about role assignment is by job responsibility:

Administrator responsibility	Access usually needed
Website content updates	Content access, and possibly Services or Pricing if they maintain public offerings
Search and page metadata updates	SEO access
Site-wide configuration changes	Settings access
User account administration	Users access
General monitoring	Dashboard access, often without broad editing rights

Broad administrative roles are useful for a small number of trusted administrators who manage several areas. For most users, narrower access is better. For example, someone who updates multilingual website copy may need **Content** but not **Users** or **Settings**. A person reviewing page search snippets may need **SEO** without being able to edit service packages or pricing.

Combine roles only when the work truly crosses areas. A user who manages both website copy and service listings may need access to **Content** and **Services** together. Keep user management separate whenever possible, since that area affects who can enter the admin portal and what they can see.

Be especially careful with full-access assignments. A role that opens many admin pages may also expose records, controls, and settings that are unrelated to the person's job. If the user only needs to read information, avoid assigning a role that also enables **Edit**, **Delete**, or other management actions.

For more background on user lists and account maintenance, refer to [Viewing and Maintaining User Accounts](#).

Verifying what the user can see after changing permissions

After you save a role change, verify the result from the user's point of view. This is the fastest way to confirm that the assigned access matches the intended job. In Sherkey ERP & Website Platform, do not stop at checking the user profile alone—open the admin portal as that user if possible, or ask the user to sign in and confirm what appears on screen.

1. Sign in with the affected account, or have the user sign in after refreshing their session.
2. Check the admin navigation and confirm the expected menu items are visible, such as **Dashboard**, **Content**, **Users**, **SEO**, **Services**, **Pricing**, or **Settings**.
3. Open each relevant page and confirm it loads normally.
4. Test the actions the user is supposed to perform, such as opening records, changing fields, or saving updates.
5. Confirm restricted areas remain unavailable.

[SCREENSHOT: Admin navigation and page actions being checked after a role update]

When you test, look at both page access and action access. A user may be able to open **Content** but still be missing edit controls. Another user may reach **Users** but be unable to change roles. Also check whether lists and records show the expected information. If a page opens but appears incomplete, the issue may be limited visibility inside that page rather than a missing role.

Use this checklist while verifying:

- The correct admin menu items are visible
- Allowed pages open without restriction
- Expected records appear in lists and search results
- Buttons such as **Save**, **Edit**, or other management actions appear where needed
- Restricted pages stay hidden or blocked

If the user cannot reach a page they should have, or can reach one they should not, continue with the troubleshooting steps in the next section.

Fixing common visibility problems after assigning roles

Most access problems in Sherkey ERP & Website Platform come from one of four situations: the role change was not saved as expected, the user session has not refreshed, the user has overlapping access from more than one role, or the page is visible but action-level access is still missing.

If the user still cannot see a page after you assign a role, start with the basics:

- Reopen the user's profile in **Users**
- Confirm the role is assigned to the correct account
- Click **Save** again if you are unsure the change was stored
- Ask the user to sign out and sign back in
- Check whether the missing page should appear in the admin menu or only through a direct page link

If the user can open a section but cannot find certain records, the issue may be inside the list rather than in the role assignment itself. Review whether the user's access limits which entries appear in lists, search results, or detail pages. This often shows up as "I can open the page, but my items are missing."

If the user sees too much information, inspect the full set of assigned roles. Multiple roles can combine and widen access. Remove any extra role that is no longer needed, then save and test again. This is especially important when someone temporarily received broader access and it was never fully removed.

If buttons are missing even though the page is visible, compare what the user can do against what they need to do:

Problem	What to check
Page opens, but no edit option	The role may allow viewing only
User can view records, but not add new ones	Create access may be missing
User can edit, but not remove items	Delete access may be restricted
User can open admin pages, but not manage users	Their role may not include user administration rights

For broader troubleshooting patterns, continue with [Reviewing User Access and Resolving Common Admin Issues](#).

Overview

This guide focuses on one specific task in Sherkety ERP & Website Platform: assigning roles and confirming that those roles change visibility in the admin portal the way you expect. You use the **Users** area to open a person's account, update the **Roles**, **Permissions**, or **Access** section, save the change, and then verify the result by checking the admin navigation, page access, and available action buttons.

The most important idea in this guide is that access is layered. A role can affect:

- Which admin menu items appear
- Which pages open successfully
- Which records appear in lists and searches
- Which actions, such as editing or deleting, are available on a page

That means a successful role assignment is not just about seeing the right page name in the menu. You also need to confirm the user can do the work they were given access for—and cannot do work outside that scope.

This guide does not repeat the basics of finding user accounts or handling account status changes. If you need those steps, use [Viewing and Maintaining User Accounts](#) and [Managing User Lifecycle in the Admin Portal](#). It also builds on the visibility concepts explained in [Understanding Role Visibility and Access Restrictions](#).

Use this guide when you are granting access to a new administrator, narrowing access for an existing one, or checking why a user sees too much or too little in the admin portal. The final section points you to the next document for deeper troubleshooting when the visible results still do not match the assigned role.

Prerequisites

Before you assign or change roles in Sherkety ERP & Website Platform, make sure these conditions are in place:

- You can sign in to the admin portal successfully
- Your own account has access to the **Users** area
- You can open a user profile and save changes to that profile
- The user account you want to update already exists in the **Users** list
- You know which admin areas the person should access, such as **Content**, **Users**, **SEO**, **Services**, **Pricing**, or **Settings**

It also helps to prepare a clear access decision before opening the user record. Decide whether the person needs:

- View-only access
- Access to edit existing records
- Access to create new entries
- Access to remove items
- Access to sensitive areas such as user administration or site-wide settings

If you are unsure which account to edit, first review [Viewing and Maintaining User Accounts](#). If the account is inactive or needs status changes before role assignment, use [Managing User Lifecycle in the Admin Portal](#).

For the smoothest testing process after you save changes, arrange one of these options in advance:

- Access to sign in with the affected user account for verification
- Coordination with the user so they can sign out, sign back in, and confirm the result
- A clear list of pages and actions you expect them to see after the update

Once you have those pieces ready, move on to role assignment and then verify the visible changes carefully. The next document, [Reviewing User Access and Resolving Common Admin Issues](#), picks up from there when assigned access still does not behave as expected.