SHERKETY BYTES ALIGN

Managing Users and Role Based Access

August 25, 2026

Opening the Users area in the admin portal

To manage accounts in **Sherkety ERP & Website Platform**, start by signing in to the admin portal and opening the main admin navigation. From there, select **Users** to open the user management screen. This area is part of the protected admin workspace, so only people whose own account includes the right level of access will be able to open it. If you do not see **Users** in the admin navigation, your current role does not allow user maintenance.

When the **Users** screen opens, you will work from a list view that helps you review accounts at a glance. Look for the user directory table and scan the visible details for each person, such as their name, email address, current status, and assigned role. These columns help you quickly tell who can access the portal and what level of responsibility they have.

Common actions are usually available directly from this screen:

1. Click **Add User** to create a new admin portal account.
2. Click a user row or open action to view that person’s full record.
3. Review the **Role** or access setting to confirm what that user can manage.
4. Save any updates so the list reflects the latest account details.

[SCREENSHOT: Users screen showing the user list, Add User button, and role/status columns]

If you need a refresher on reaching admin areas and moving between sections, use Using the Admin Dashboard for Navigation. If you recently updated search-facing page details, that work remains separate from user access and is covered in Maintaining SEO and Search Facing Page Information.

Reviewing who can see and access the portal

The **Users** list is the fastest place to review who is currently available in the admin portal and what kind of access each person has. Start by scanning the **Status** and

Role information for each account. This helps you separate people who can actively use the portal from people whose access is disabled or limited.

An account can exist in the user directory without giving that person full working access. For example, someone may appear in the list with a role that allows content work but not settings changes. Another person may be listed but marked in a way that prevents normal access or removes them from regular visibility. When you are checking access issues, always review both the user's visibility in the list and the permissions attached to their role.

To inspect one account more closely:

1. Open the **Users** screen.
2. Select the person you want to review.
3. Check the main profile details, including **Name**, **Email Address**, **Status**, and **Role**.
4. Confirm whether the account should be active and whether the assigned role matches that person's responsibilities.

A useful way to think about this screen is:

What you review	What it tells you
Name	Who the account belongs to
Email Address	Which sign-in identity is tied to the account
Status	Whether the account is active, disabled, or otherwise limited
Role	Which admin areas and actions are available to that user

Being listed in **Users** does not automatically mean the person can edit content or manage settings. Those abilities come from the assigned role. To understand how content and configuration areas differ, you can also compare this guide with Managing Services Pricing and Site Settings.

Adding a user and maintaining account details

When a new team member needs access to the admin portal, open **Users** and click **Add User**. This opens the account form where you enter the person's basic details. Focus on the visible profile fields first, then review status and role before saving.

Use the form to enter the user's identity details exactly as you want them to appear in the portal. The most important fields to review are the person's display name and email address. After entering those details, choose the appropriate account status and role, then save the record. Once saved, return to the user list and confirm the new account appears with the expected information.

A typical setup flow looks like this:

1. In **Users**, click **Add User**.
2. Enter the user’s **Display Name**.
3. Enter the user’s **Email Address**.
4. Set the account **Status**.
5. Choose the correct **Role**.
6. Click **Save**.
7. Confirm the new account appears in the user list.

[SCREENSHOT: Add User form with name, email, status, role, and Save button]

You can also open an existing user record to update profile information later. This is useful when a person changes their display name or when you need to correct an email address. If you only need to update identity details, edit those fields and save the record without changing the role.

Status changes are helpful when responsibilities change or access should be paused. For example, you may need to disable a user temporarily, reactivate a returning user, or hide an account from normal admin use. After saving, go back to the list and verify the updated status appears correctly. If you are working across several admin areas, toast messages and confirmation prompts may also appear; those patterns are explained in Understanding Toast Messages and Action Feedback.

Assigning roles that control content and settings access

The **Role** field on each user record determines which parts of **Sherkety ERP & Website Platform** that person can use inside the admin portal. To review or change access, open the user’s record and locate the **Role** or **Access** setting. This is where you decide whether the person can work with content only or also manage higher-level administrative areas.

In practical terms, role-based access affects what the user sees after signing in. A content-focused role can allow access to editing areas such as website content and other publishing tasks, while a higher-level administrative role can also unlock settings-related sections. If a user should not manage configuration, do not assign a role that exposes settings screens.

Use this approach when reviewing role choices:

1. Open the user's profile from **Users**.
2. Find the **Role** field.
3. Review the available role options.
4. Choose the role that matches the person's real responsibilities.
5. Click **Save** so the change is stored.

Here is the key distinction to keep in mind:

Role type	What the user can usually access
Content-focused role	Content editing areas, page updates, and publishing-related tasks
Administrator-level role	Content areas plus settings and other restricted admin controls

A user with a limited role may notice fewer navigation items, fewer action buttons, or missing settings pages. That is expected behavior and helps protect important configuration areas from accidental changes. If you need more detail on how restricted pages behave when access is limited, see Understanding Admin Page Access and Protected Navigation.

After you save a role change, the new permissions are intended for future sessions. If the user is already signed in, have them sign out and sign back in so the updated navigation and page access appear correctly.

Controlling who can manage content and configuration

Good user management is not just about creating accounts. It is also about matching each person's access to the work they actually do. In **Sherkety ERP & Website Platform**, the safest approach is to give content access only to people who maintain website pages, service details, pricing content, or other published information, while reserving settings access for a smaller group of trusted administrators.

Start by reviewing the user's day-to-day tasks. If the person only updates public-facing content, assign a role that allows content editing without exposing settings screens. This keeps the admin navigation simpler for that user and reduces the chance of accidental changes in configuration areas. If the person is responsible for broader administration, use a higher-level role that includes settings access.

To check whether a role is appropriate:

1. Open the user's record in **Users**.

2. Review the assigned **Role**.
3. Compare that role with the admin areas the person should be able to open.
4. Save any role change.
5. Ask the user to start a new session and confirm the visible menu items match expectations.

You can also verify effective access by comparing what the user sees in the admin portal:

- If they can open content areas but not settings, they likely have an editor-style role.
- If they can open both content and settings sections, they likely have administrator-level access.
- If important menu items are missing, the assigned role may be too limited.

This is especially useful when responsibilities change. A user may begin with content maintenance only, then later take on broader administrative work. In that case, update the role rather than creating a second account. For related guidance on content areas and settings areas themselves, refer to Managing Services Pricing and Site Settings and Viewing and Maintaining User Accounts.

Fixing common user access and visibility problems

Most user access problems can be solved from the **Users** screen by checking three things: whether the account exists, whether the account is active and visible, and whether the assigned role matches the work the person needs to do.

If a person does not appear in the admin portal user directory, first search the **Users** list and confirm the account was created. Then open the record and check the account **Status**. If the account is disabled or hidden, update the status and save. After that, return to the list and confirm the person now appears as expected.

If a user can sign in but cannot manage content, the most likely cause is the assigned **Role**. Open the user record and verify that the role includes content management access. Save the record after any change, then ask the user to sign in again.

If a user can manage content but cannot open settings, this usually means the current role is limited to editor-level work. That is normal if you want to protect configuration screens. If the person should be allowed to manage settings, update the role to an administrator-level option and save.

Use this quick troubleshooting table:

Problem	What to check
User does not appear in **Users**	Confirm the account was created and is not hidden
User appears but cannot sign in normally	Review **Status** and make sure the account is active
User can sign in but cannot edit content	Check whether the **Role** includes content access
User can edit content but not settings	Confirm whether the role includes settings access
Role change seems ignored	Save the record and have the user start a new session

[SCREENSHOT: User record showing status and role fields used during troubleshooting]

If the page itself is slow to appear, shows a loading message, or displays an error, compare what you see with Understanding Loading Placeholders Empty States and Errors and Responding to Missing Content and Retry Messages.

Overview

Managing users in **Sherkety ERP & Website Platform** centers on one admin destination: the **Users** screen. From there, administrators review the user list, open individual records, update account details, and assign the right role for each person. The most important idea in this workflow is that account visibility and account permission are not the same thing. A person may appear in the directory but still have limited access, depending on the role shown on their record.

The user list gives you a quick operational view of the admin team. By checking **Name**, **Email Address**, **Status**, and **Role**, you can quickly answer common questions such as who still has access, who is hidden or inactive, and who can manage content versus settings. Opening a user record lets you make targeted changes without affecting unrelated areas of the portal.

This guide fits alongside earlier admin tasks you may already be doing:

- If you are updating page search details, continue using Maintaining SEO and Search Facing Page Information for that work.
- If you need help moving around the admin area, use Using the Admin Dashboard for Navigation.
- If you are comparing content work with configuration work, see Managing Services Pricing and Site Settings.

The main outcomes of user management are straightforward:

- The right people appear in the admin directory
- Active users can sign in and reach the correct areas
- Content editors do not receive settings access by mistake
- Administrator-level access is reserved for approved users

After your user list and role assignments are in order, the next related task is ending sessions correctly in Signing Out and Ending Admin Sessions Safely.

Prerequisites

Before you start managing users in **Sherkety ERP & Website Platform**, make sure you have the correct level of access yourself. The **Users** area is not available to every signed-in person. If you cannot see **Users** in the admin navigation, your current role does not include user maintenance.

You should have the following in place before making changes:

- A working admin sign-in for **Sherkety ERP & Website Platform**
- Permission to open the **Users** screen
- A clear decision about whether the person needs content access, settings access, or both
- The user's correct **Display Name** and **Email Address**
- Agreement on whether the account should be active, disabled, or hidden

It also helps to know which admin areas the person is expected to use after signing in. For example:

- Someone updating website copy, service details, or page content usually needs content-related access
- Someone maintaining configuration and admin controls may need administrator-level access
- Someone who should no longer use the portal may need their status changed instead of their profile edited

If you are new to the admin portal, review these guides first:

- Signing In and Accessing the Admin Portal
- Using the Admin Dashboard for Navigation
- Understanding Role Visibility and Access Restrictions

When you are ready, open **Users**, review the current list, and make changes one account at a time so each **Status** and **Role** update is easy to verify. After finishing your user changes, continue with Signing Out and Ending Admin Sessions Safely.