SHERKETY BYTES ALIGN

Managing User Accounts and Role Assignments

August 25, 2026

Opening the user management area and finding an account

In Sherkety ERP & Website Platform, start by signing in to the admin portal and opening the **Users** area from the admin navigation. If you need help reaching the admin area or understanding protected pages, see Signing In and Accessing the Admin Portal and Understanding Admin Page Access and Protected Navigation.

The **Users** screen is where you review existing accounts and open each person's record for changes. At the top of the page, look for the account list and the controls that help you narrow it down. In most cases, you will use:

- a **search box** to find a person by name or email address
- list controls such as filters or role-based views, if shown
- the account table or grid that displays matching users

[SCREENSHOT: Users page showing the search box, filters, and account list]

The account list is your quickest way to confirm you have the correct person before editing anything. Review the visible columns carefully. The list typically shows key details such as:

What to check	Why it matters
User name	Confirms the account owner
Email address	Helps distinguish similar names
Current role assignments	Shows the user's present level of access
Access visibility status	Indicates whether the user can see only selected records or a broader set

To open a user, click the row or the action that opens the account details. Once inside, some information may be displayed for reference only, while administration sections such as **Roles** or **Visible Access Assignments** are the parts you update.

Use search when the person already has an account and only needs maintenance. If the person does not appear in the list at all, do not guess by editing another account. Follow your organization's separate onboarding process or account creation process instead. For broader user list maintenance, see Viewing and Maintaining User Accounts.

Reviewing account details before making changes

Before changing roles or visibility, pause on the user's detail page and review what is already assigned. This is the easiest way to avoid removing access the person still needs or adding duplicate permissions.

Start with the identifying details at the top of the record. Confirm you are editing the correct person by checking the visible profile information, such as the user's name and email address. If the page shows a current account status, review that too before making changes. A user who appears inactive, restricted, or otherwise not in normal use may need a different action than a role update.

Next, move to the **Roles** or **Role Assignments** section. This area shows which roles the user already has. Read the full list before entering edit mode. If the page separates assignments into different groups, pay attention to whether a role appears as something directly assigned on this user record or shown as inherited from another rule. That distinction matters when you later remove access, because deleting one visible assignment may not remove all access if another assignment still grants it. For more detail on visibility rules, refer back to Reviewing Access Restrictions and Common User Issues.

Then open or review the **Visible Access Assignments** area. This section shows which organizations, sites, customers, or other scoped records the user is allowed to see. Compare this list with the user's job need. A person may have the right role but still be unable to view the correct records if this section is too limited.

If the page includes a **last updated** note, change history, or similar indicator, check it before editing. Recent updates can signal that another administrator is already adjusting the same account. When that happens, confirm the intended setup first so you do not overwrite a change that was just made.

Updating a user's role assignments

Use the role area only after you have confirmed the correct account and reviewed the current setup. In Sherkety ERP & Website Platform, role changes control what parts of the admin portal a user can open and what actions they can perform there.

1. Open the user's record and go to the **Roles** or **Role Assignments** section.
2. Click the edit control for that section. Depending on the page layout, this may appear as **Edit**, a pencil icon, or an assignment action beside the role list.
3. In the role selector, choose the roles the user should have. The page may show these as checkboxes, a multi-select list, or an add/remove assignment control.
4. Remove any roles the user should no longer keep. Review the full list before saving so you do not leave behind an outdated assignment.
5. Click **Save** to apply the changes.

[SCREENSHOT: User detail page with the Role Assignments section in edit mode]

As you work, focus on the role names shown on the page rather than trying to infer access from memory. If your organization uses similar role names, double-check the selected entries before saving. This is especially important when a user needs content editing access, dashboard access, or user administration access.

After saving, wait for the page to refresh and confirm that the assigned roles list now shows the new selection. In some admin workflows, the change takes effect as soon as the save completes. In others, the user may need to sign out and sign back in before the updated permissions appear in their session. If the user reports no change after a successful save, review Managing Users and Role Based Access together with Reviewing User Access and Resolving Common Admin Issues.

If the save completes but the list still shows the old role set, refresh the page and reopen the record before trying again. That helps you confirm whether the update was stored or whether the change needs to be re-entered.

Managing visible access assignments

Roles decide what a user is allowed to do. **Visible Access Assignments** decide what records they can actually see. In Sherkety ERP & Website Platform, both parts must be correct for the user to work normally.

1. Open the selected user's detail page and find the **Visible Access Assignments** section.
2. Click the edit control for that section to start updating the list.
3. Use the assignment picker to add the records the user should be able to view. Depending on how your organization uses Sherkety ERP & Website Platform,

these may be organizations, sites, customers, or another scoped list shown in the picker.
4. Review the current entries and remove any items the user should no longer access.
5. Click **Save** and wait for the updated list to appear on the user record.

[SCREENSHOT: Visible Access Assignments section showing add and remove controls]

When you add visibility, choose the exact entry that matches the user's work area. If two items have similar names, confirm the right one before saving. A small mistake here can leave the user looking at the wrong records while still appearing correctly configured at first glance.

When you remove visibility, watch how the page separates assigned items from available but unassigned items. Active entries usually remain listed in the user's current assignments until you remove them. Once removed and saved, they should no longer appear in the active list.

After saving, read the updated visibility list from top to bottom. Make sure every required organization, site, customer, or scoped record is present and that outdated entries are gone. If the user still cannot see expected data after this step, the issue is often not the role itself but a missing visibility assignment. For a deeper explanation of how role scope affects what appears on screen, see Understanding Role Visibility and Access Restrictions.

Confirming the user's effective access after updates

Once you save role and visibility changes, verify the result before telling the user the account is ready. A quick confirmation step prevents repeat support requests and helps you catch mismatched assignments immediately.

1. Refresh the user detail page or reopen the user record from the **Users** list.
2. Confirm that the **Roles** section shows the updated role assignments you intended to save.
3. Confirm that the **Visible Access Assignments** section shows the correct organizations, sites, customers, or other scoped records.
4. Compare both sections together rather than reviewing them separately.
5. If your admin portal includes an effective access view, preview mode, or another way to inspect what the user can actually reach, use it to confirm the final result.

The key check is the combination of permission and scope. A user may have a role that allows access to a feature area, but if the visibility list does not include the required organization or site, the expected records may still not appear. The opposite can also happen: a user may have visibility entries listed correctly but still be blocked because the needed role was never assigned.

[SCREENSHOT: User record after saving, showing updated Roles and Visible Access Assignments]

When validating access, think in terms of the user’s real task. For example:

- Can they open the admin area they need?
- Can they see the expected records inside that area?
- Are they limited to only the correct scoped entries?

If Sherkety ERP & Website Platform offers a preview of effective permissions, use that as your final check. If it does not, the safest approach is to reopen the account and compare the saved role list with the saved visibility list line by line. If a user should see a record type but still cannot, the most common cause is missing scope in **Visible Access Assignments**, not a failed save.

Fixing common problems with role and access changes

Most issues after a role update come from one of four places: the wrong role was assigned, the visibility list is incomplete, the save did not complete, or another assignment is still granting access.

If the role update saved but permissions did not seem to change, start by reopening the user record and checking the **Roles** section again. Make sure the exact intended role appears in the saved list. If it does, ask the user to sign out and sign back in before testing again. A user can sometimes continue seeing their old session until they log in again.

If the user still cannot see expected records, go straight to **Visible Access Assignments**. Confirm that the needed organization, site, customer, or other scoped record is actually listed there. A correct role without the right visibility scope will still leave lists empty or incomplete.

If the **Save** action is unavailable, or the page rejects your changes, check for these conditions:

- a required field elsewhere on the record still needs attention

- your own admin account does not have permission to change that user
- the selected combination of assignments conflicts with the current setup
- another recent change may already be affecting the same account

If unexpected access remains after cleanup, do not assume the removal failed. Review the user's full setup again. Access may still come from:

- another role that is still assigned
- another visibility entry you did not remove
- an inherited assignment shown separately from direct assignments

For repeated problems, compare the current account with a working account that should have similar access. That often reveals a missing role or missing visibility item faster than editing blindly. If you need a refresher on troubleshooting patterns, return to Reviewing Access Restrictions and Common User Issues.

Overview

This guide focuses on the day-to-day admin work of maintaining existing user access in Sherkety ERP & Website Platform. The main tasks are finding the correct account, reviewing the current setup, updating **Role Assignments**, and adjusting **Visible Access Assignments** so the user can reach the right areas and see the right records.

Use this guide when:

- a user needs access to a new admin area
- a user should stop seeing a specific organization, site, customer, or other scoped record
- a role needs to be corrected after a job change
- a user reports that expected records are missing even though they can sign in

This guide does not repeat the full background on role visibility logic or general troubleshooting theory. Those topics are already covered in:

- Viewing and Maintaining User Accounts
- Understanding Role Visibility and Access Restrictions
- Reviewing Access Restrictions and Common User Issues

What matters here is the practical workflow on the **Users** page: locate the account, open the detail view, update the role list, update the visibility list, save, and verify the result. In Sherkety ERP & Website Platform, role changes and visibility changes work together. If only one side is updated, the user experience can still be wrong.

Keep that pairing in mind throughout the process:

- **Roles** control what the user is allowed to access.
- **Visible Access Assignments** control which records appear within that allowed area.

That combination is the core of successful user maintenance in the admin portal.

Prerequisites

Before you change any user account in Sherkety ERP & Website Platform, make sure these conditions are met:

- You can sign in to the admin portal successfully.
- Your own account has permission to open the **Users** area and edit user records.
- You know which user account needs to be updated.
- You know which role or roles the user should have after the change.
- You know which organizations, sites, customers, or other scoped records the user should be able to see.
- The account already exists if you are following this guide for maintenance rather than onboarding.

It also helps to gather the user's current access request before you begin. For example, confirm whether they need:

- access to a new admin section
- removal of an outdated role
- visibility into an additional business area
- cleanup of old visibility entries

If you are unsure whether the problem is caused by role restrictions or visibility scope, review these documents first:

- Managing Users and Role Based Access
- Understanding Role Visibility and Access Restrictions
- Reviewing User Access and Resolving Common Admin Issues

You should also be ready to verify the result after saving. That means reopening the user record, checking the saved role list, and checking the saved visibility list. If your team expects the user to test the change immediately, plan for the possibility that they may need to sign out and sign back in before the update is reflected in their session.

This is the last document in the User Administration set, so you can use it as the practical reference point alongside the earlier role and visibility guides when handling real account updates.