5. How to Edit an Employee

Editing an employee lets you keep your team’s access, credentials, and schedules up to date as roles evolve or people move between teams. Use this guide whenever you need to:

1. Promote or demote someone (change their Role or Type)
2. Correct a misspelled name
3. Rotate or reset a user’s password
4. Scope their data access to new Projects or Desks
5. Deactivate an account when someone leaves
6. Schedule shifts or meetings on their Calendar

1. Open the Employees List
In the left-hand navigation panel, click **Employees** to load the full roster.

> **Tip:** Use the **Filter** button or **Search…** box to quickly locate the person you need. You can also click any column header (Name, Role, Created, Last login) to sort the list.

2. Enter Edit Mode
In the desired user’s row, click the ✏ **Edit** icon in the **Actions** column.
The **Edit Employee** form appears, pre-filled with their current details.

3. Modify General Details
Under the **General** header on the left, adjust any of these fields:

Name:
Update their display name as it appears on dashboards, records, and notifications.
Example: Change “Jon Smith” → “Jonathan Smith” if they prefer their full legal name.

Role:
Select a new system role (Admin, Viewer, ProjectAdmin, etc.) to grant or revoke high-level permissions.
Roles are defined in the **Roles** module and take effect immediately.

Email (Editable – Sensitive Field):
The Email field defines the employee’s login identity and is used across authentication, analytics, audit logs, and system notifications.

This field is editable, but it is considered **sensitive**.

When changing an employee’s email:

1. The new email must be unique.
2. The email must follow valid format rules.
3. The change is logged for audit purposes.
4. Authentication behavior may be affected (see Email Change Impact section below).

> Changing an email does not create a new employee.
> It updates the existing employee identity.

Use this feature carefully and only when required (e.g., corporate domain migration, role handover, typo correction).

Password:
Enter a new password (≥8 chars, uppercase, lowercase, digit, special).
Generate icon: auto-create a secure password.
Toggle icon: show/hide entry for verification.

Type:
Choose a business category (Manager, Sales, Support, Analytics) used for reporting and default workflows.

Active:
Toggle on () to enable or off () to disable logins without losing audit history.

4. (Optional) Update Additional
In the **Additional** panel, use the tree picker to apply custom tags—such as Region, Business Unit, or Skill Set.
These tags power advanced filtering, permission scopes, and automation rules across WBCS.

5. Assign Projects & Desks
An employee’s data access is controlled by Project → Desk assignments in the right-hand panel:
Edit an existing Project assignment:

1. Locate the Project card.
2. Click its ✏ **Edit** icon to open the drawer.
3. Check or uncheck specific Desks to fine-tune access.
4. Click **Save** in the drawer.

Remove a Project entirely: Click the **Delete** icon on the Project card to revoke all access to that Project and its Desks.

Add a new Project:

1. Click **+ Add project** at the top of the panel.
2. Select one or more Projects from the dropdown.

3. *(Optional)* Restrict to specific Desks if the user's Role is "View Own."
4. Click **Save** in the drawer to confirm.

> **Example:**
>
> Assign Alice to "Acme USA" (Sales, Support Desks) and to "Acme Canada" (Sales only) by adding each Project and selecting the appropriate Desks.
>
> Bob, with a "GlobalViewer" Role, automatically sees all Projects and needs no explicit assignments.

6. Save Your Changes
After updating any General fields, Metadata, or Project assignments, click **Save** at the bottom-left of the form. All edits apply immediately.

> **Note:** You cannot remove projects to which an employee has already been assigned. Instead, go to the **Projects** tab and remove specific members from the project.

7. Email Change – Impact & Behavior
Changing an employee's email address affects multiple system domains. This feature was introduced only after full impact review and approval.

Identity & Authentication
Email serves as the employee's login identifier.

After email change:

1. The employee must log in using the new email.
2. Old email can no longer be used for authentication.
3. Active sessions behavior depends on system configuration:
    1. Either preserved until expiration
    2. Or invalidated immediately (implementation-defined)

Password reset links will be sent only to the updated email address.

Analytics
Employee email may be stored in analytics as an attribution dimension.

After email change:

1. Historical analytics data remains associated with the old email value.
2. New activity will be recorded under the updated email.

This reflects identity change over time and is considered acceptable.

No historical analytics rewriting is performed.

Permissions & Access
Changing email:

1. Does NOT change employee role.
2. Does NOT change project or desk assignments.
3. Does NOT create a new permission scope.

The employee remains the same system entity (same ID).

Audit & Logging
Email changes are logged with:

1. Who performed the change
2. Previous email value
3. New email value
4. Timestamp

This ensures traceability and prevents silent identity modification.

Notifications & Integrations
All system notifications are redirected to the updated email.

If external integrations rely on email as an identifier:

1. They may treat the updated email as a new identity.
2. Historical external mappings are not automatically migrated.

Review external integrations before performing bulk email changes.

Risk Considerations
Before changing email, verify:

1. The employee is not being replaced by a different person.
2. Analytics interpretation remains acceptable.
3. No external system depends strictly on the previous email.

If the change represents a new person taking over the account, consider creating a new employee instead.

> Email is a primary identity attribute. Changing it may impact login behavior, analytics attribution, and integrations. Proceed carefully.

Revision #17
Created 3 September 2024 15:22:31
Updated 6 March 2026 15:00:53