1. Roles: Overview

The **Roles** module is the heart of your access-control framework in Wifox Business Core Solution. It defines *who* can do *what*—from viewing sensitive client data to performing high-impact administrative tasks. By grouping discrete system capabilities (like “view client profiles,” “edit KYC information,” or “export transaction logs”) into named Roles, you create reusable permission sets that can be assigned to any number of employees. This approach ensures consistency, enforces the principle of least privilege, and dramatically simplifies onboarding, auditing, and ongoing security management.

Core Concepts

1) Role Definition

Name & Description: Each Role carries a clear, descriptive name and summary so that even non-technical stakeholders immediately understand its purpose (e.g., “Support Agent,” “Compliance Reviewer,” or “System Administrator”).

Permission Toggles: Inside the Role editor, every discrete action or data-view permission is surfaced as an on/off switch. Permissions are grouped by feature area (Clients, Requests, Transactions, Logs, Settings, etc.), making it easy to see at a glance which modules a Role can touch.

2) Assignment to Users

Employee Profiles: Roles are granted on each Employee’s record. You can assign multiple Roles to a single person, allowing their effective permissions to be the union of all their Roles.

Dynamic Updates: When you edit a Role’s permissions, those changes immediately cascade down to every assigned user—no need to manually reconfigure each individual.

3) Hierarchy & Inheritance

While Wifox doesn’t enforce a strict parent/child Role hierarchy, you can achieve the same effect by cloning an existing Role (via the “duplicate” action) and then adding or removing specific permissions. This makes it easy to build “junior” and “senior” versions of any Role without starting from scratch each time.

4) Audit & Compliance

Built-in Reporting: You can export your entire Role list—complete with names, descriptions, and permission flags—to maintain an external audit record or to cross-check against organizational policies.

Change History: Every time a Role is edited, Wifox logs the timestamp and the user who made the change. This immutable audit trail ensures you can track how permissions have evolved over time.

Typical Workflow

Onboarding a New Team:
Review your organizational chart and identify distinct functional groups (e.g., Support, Finance, Compliance).
For each group, decide which modules and actions they need. Create a new Role (or clone a similar one), toggle the appropriate permissions, and save.
Assign the Role to all relevant employees in bulk via the Employee directory.

Responding to a Security Incident:
If you discover that a Role grants excessive access, simply open the Role editor, turn off the problematic permissions, and publish. Changes take effect immediately, locking down vulnerable areas without touching individual employee settings.

Regular Access Reviews:
Quarterly or semi-annually, export your Roles and compare them against your company’s security policies.
Identify any unused or overly permissive Roles, and either retire them or tighten their scope.

The following actions are available in the **Roles** module:

1. Creation
2. Viewing assigned users
3. Searching
4. Editing
5. Deletion

Revision #28
Created 4 September 2024 10:05:05
Updated 20 May 2026 13:12:53 by Anastasiia Rudaya