

User permissions

The **Security Role** assigned to a user determines their **level of access** within the platform. There are **three levels of access**, each designed to meet the needs of different types of users.

1. Default

- **Access Level:** Read-only
 - **Pages Accessible:**
 - [Tasks & Costs](#)
 - **Cash & Contributions** ([Cashflow](#), [Contributions](#))
 - **Typical Users:** Standard body corporate members (unit owners)
 - **Purpose:** Allows owners to view their contributions and the maintenance plan without making changes.
-

2. Admin

- **Access Level:** Full access
 - **Pages Accessible:** All pages, including:
 - Tasks & Costs
 - Cash & Contributions
 - Approvals
 - Building
 - Units
 - People
 - Documents
 - Settings
 - **Typical Users:** Building managers or committee members responsible for updating the plan and managing settings
 - **Purpose:** Allows users to **create, edit, and delete** data, as well as manage other users and system settings.
-

3. Viewer

- **Access Level:** View-only
 - **Pages Accessible:** All pages
 - **Typical Users:** External consultants, surveyors, or service providers
 - **Purpose:** Allows users to **monitor and review** all information without the ability to make any changes.
-

Key points

- Security roles ensure that users have **access appropriate to their responsibilities**.
 - Roles can be assigned when creating a user or updated later via the [Edit User](#) side panel.
 - Using these roles helps maintain **data integrity** while allowing transparency for all stakeholders.
-

Revision #4

Created 15 October 2025 05:42:04 by Laurent Hautefeuille

Updated 5 February 2026 08:08:58 by Laurent Hautefeuille