



KYC Protect

Release Notes

JUNE 2026

User Configuration (Roles & Permissions)

We're introducing a new role-based access control system in KYC Protect to help organisations manage user access more securely and efficiently. This enhancement ensures that users only have access to the features and data relevant to their responsibilities, improving operational control, reducing risk, and maintaining clear accountability across all actions performed in the system.

Each user is assigned a predefined role that determines their level of access across modules such as Profiles, Screening, Monitoring, Alerts, and Settings.

Role Types

KYC Protect provides predefined roles designed to support different user responsibilities:

- **Viewer:** View-only access across all modules. Users can review profiles, screening results, alerts, and reports, but cannot make changes.
- **Analyst:** Enables operational activities such as initiating AML screening, generating reports, and managing profiles within permitted areas.
- **Manager:** Full access across all modules, including managing users, assigning roles, and configuring permissions.
- **Admin:** Complete system control with full access across all modules, including user and permission management.

Assigning Roles to Users

Roles can be assigned or updated within the User Configuration section. Admins and users with permission to configure roles for others can update roles at any time to meet organisational needs.

Managing Permissions

Each role comes with a predefined set of permissions governing access and actions within the platform.

- Default permissions are pre-configured to provide a consistent starting point
- Permissions ensure users can only access relevant data and functionality

Role-Based Access Behaviour

KYC Protect dynamically adjusts functionality based on each user's assigned role:

- Users can only perform actions permitted by their role
- Restricted features are automatically hidden or disabled within the application

Audit and Traceability

All role-related changes are fully tracked for audit and compliance purposes:

- Any updates to roles or permissions are logged in the Change Log
- This ensures complete transparency and accountability across user activity

Notifications

To ensure visibility and avoid workflow disruptions, users receive notifications for key changes:

- Role updates trigger email notifications to both the affected user and the acting user
- Permission updates trigger notifications to users with Admin or Manager roles
- Overrides of screening or monitoring preferences trigger notifications to the acting user and users with Manager roles