SETTING UP A NEW USER & PERMISSIONS | User Guide

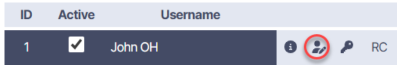
2026

The process for adding a new user to RiskClear depends on whether your organisation uses Microsoft Single Sign On (SSO) or not.

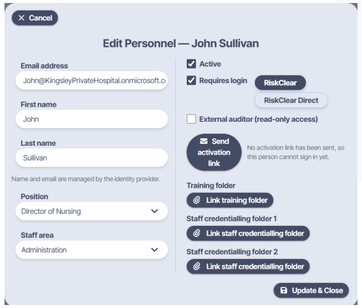
Healthcare Organisations using Microsoft Single Sign On (SSO)

When SSO is configured, staff are automatically synchronised with Microsoft. An Administrator then determines which staff require access to RiskClear and their login type.

1. Go to **Settings > Logins & SSO**.
2. Locate the staff member and select the **Update** icon.



The following appears>



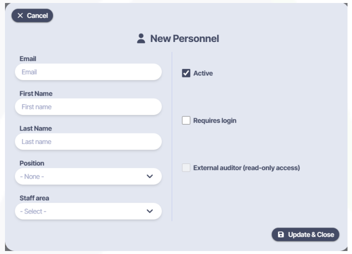
3. Select the appropriate login type – **RiskClear** or **RiskClear Direct**.
4. Complete any additional details as required, such as **Position**, **Staff Area**, or links to **Training** and **Staff Credentialling** folders.
5. Select **Send Activation Link**.

The staff member will receive a welcome email containing a link to RiskClear. When they select the link, they will sign in using their Microsoft credentials and RiskClear will open.

Organisations not using Microsoft Single Sign On (SSO)

Where SSO is not enabled, new users are created manually by an Administrator.

1. Go to **Permissions** > **Personnel Update**.
2. Select **+ New Personnel**.



3. **Complete** the staff member's details.
4. Select **Requires Login**.
5. Select the **appropriate login** type - **RiskClear** or **RiskClear Direct**.
6. Select **Send Activation Link**.

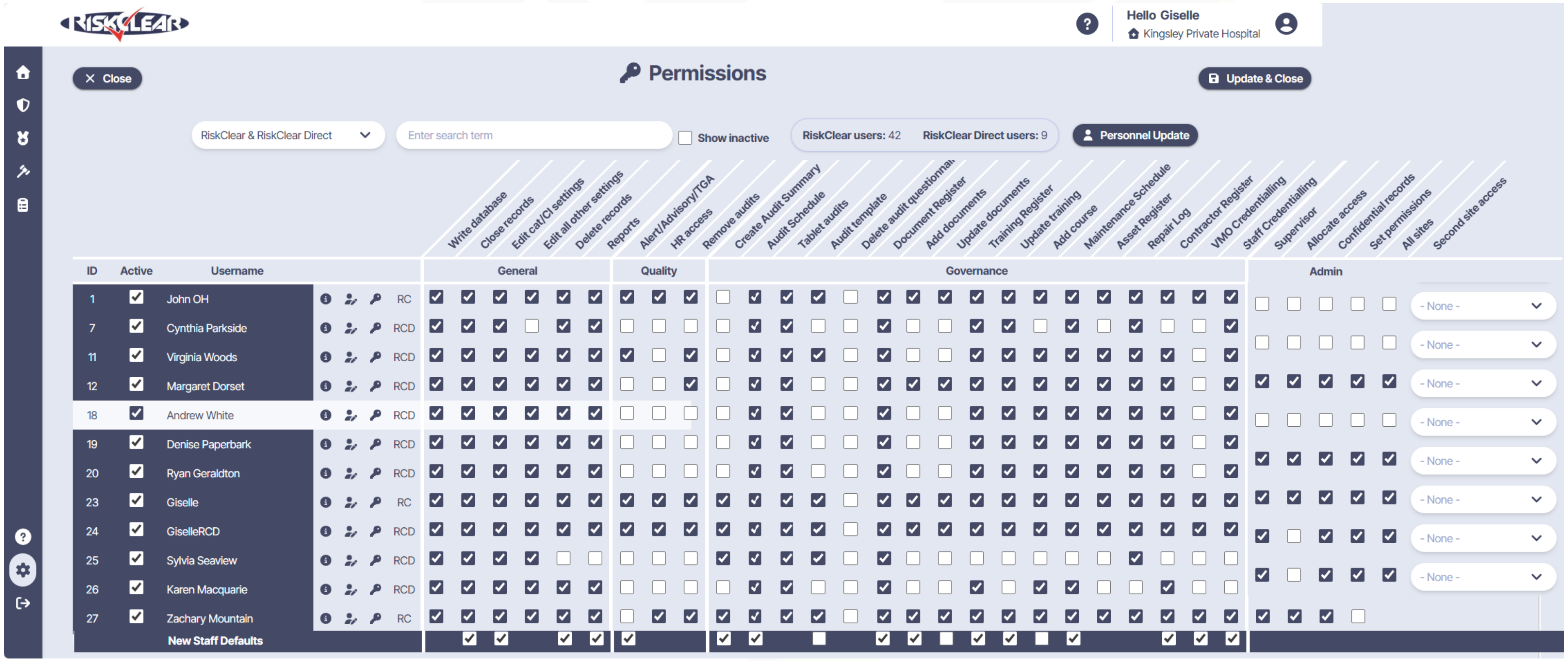
The staff member will receive a welcome email containing a link to RiskClear. When they first access RiskClear, they will be prompted to create their password before signing in.

Assigning Permissions

User Permissions can be configured or updated by an Administrator at anytime after the staff member has been synchronized through SSO or manually created in RiskClear. Refer to **Pages 2-5** of this guide for detailed information on Permissions. Refer to **Page 6** of this guide to deactivate and reactivate existing users.

To access **Permissions** go to the **Side Navigation Panel** > ⚙ > **Advanced Settings** > **Permissions**

This is where you you can assign permissions based on an individuals role and responsibilities within your Healthcare Organisation. **Pages 4 & 5** of this guide provide detail of each "tick box" and the permission or access you are granting. The permissions are grouped under **General, Quality, Governance and Admin.** There are also **New Staff Defaults** (bottom of page) assigned to every new user which you can adjust accordingly**.** Along the top of the page you can **filter by RiskClear or RiskClear Direct** users, **search** for an individual user, tick **show inactive** and also see the **number of RiskClear and RiskClear Direct users** listed also. Clicking **Personnel Update** allows you to update/edit existing personnel details.



Permissions Screen example is a Multi-site RiskClear

PERMISSION TYPES

GENERAL	
WRITE D'BASE	All new users receive this by default. If this is removed, the user will open RiskClear in "Read-only" mode. This means that existing records can be updated however new records cannot be created
CLOSE RECORDS	Tick to allow access to close risk, incident, and complaint records
EDIT CATs & CIs	Tick to allow users to update risk, incident and complaint categories/subcategories, clinical indicators and clinical indicator groups
EDIT ALL OTHERS	Tick to allow users to update remaining setup fields such as Standards, locations, areas etc
DELETE RECS	Tick to allow the user to delete records
REPORTS	Tick to allow access to the reports section
QUALITY	
ALERTS	Tick to allow access to Alerts
HR ACCESS	Tick to allow access to HR details
REMOVE AUDITS	This will give the staff member the ability to remove audits from the audit schedule. It is not possible to remove an audit that has a completed locked audit attached
GOVERNANCE	
CREATE AUDIT SUMMARY	Tick to allow creation of Audit Summary
AUDIT SCHED	Tick to allow access to the Audit Schedule
TABLET AUDITS	Tick to allow access to the Tablet Audit function
AUDIT TEMPL	Tick to allow add/change audit template
DELETE AUDIT QUESTIONNAIRE	Tick to allow user to delete Audit questionnaire
DOCUMENT REGISTER	Tick to allow access to the Document Register
ADD DOCUMENTS	Tick to allow staff to add new documents to the Document Register

UPDATE DOCUMENTS	Tick to allow staff to update documents
TRAINING REGISTER	Tick to allow access to the Training Register
UPDATE TRAINING	Tick to allow user to update training
ADD COURSE	Tick to allow staff to add new courses to the training register
MAINTENANCE SCHEDULE	Tick to allow access to the Maintenance Register
ASSET REGISTER	Tick to allow access to the Asset Register
REPAIR LOG	Tick to allow access to the Repair Log
CONTRACTOR REGISTER	Tick to allow access to the Contractor Register
VMO CREDENTIALLING	Tick to allow access to the VMO Credentialing Register (NA in Aged Care)
STAFF CREDENTIALLING	Tick to allow access to the Staff Credentialing Register
SUPERVISOR	This gives permission to all tabs in Setup except the Auditor Login and Permissions tabs
ALLOCATE ACCESS	Tick to allow user to allocate access to others
CONFIDENTIAL RECORDS	Tick to allow user access to confidential records (Safety modules & Document Register)
SET PERMISS'NS	This gives access to this Permissions and Auditor Login tabs
ALL SITES	This applies where multiple hospitals are connected to the single RiskClear database. Allows the user to view, create, update and report on records for any/all sites

EXAMPLES (ONLY) OF PERMISSION SETTINGS BASED ON ROLE:
Depending on the size and scope of your hospital/site and the governance/role structure, permissions will vary.
Director of Nursing: all permissions > tick every box (except *all sites unless applicable)
Senior Management: >tick every box except Add Course, Remove Audits, Supervisor, All Sites
Quality Coordinator: all permissions > tick every box (except *all sites unless applicable)
General Staff: > tick every box except Add Docs, Add Course, Remove Audits, Supervisor, Set Permissions, All sites

DEACTIVATING OR REACTIVATING USER ACCESS TO RISKCLEAR OR RISKCLEAR DIRECT

For those **clients with Microsoft SSO** personnel data automatically updates every 24 hours, so if a staff member has left (resigned, parental leave, long service leave) they will no longer appear on Permissions and their access is removed.

For **clients not using Microsoft SSO** personnel can be manually updated in Permissions by unticking (deactivating) the active box alongside their name. You can also reactivate a staff member that has had prior access by following the 4 steps below:

STEP ONE: Go to Settings > Advanced Settings > **Permissions**
STEP TWO: Tick the **Show Inactive** box
STEP THREE: Type the staff members name into the **search** field
STEP FOUR: If the staff members name appears, tick the **Active** box

Permissions Screen shown is a Single Site RiskClear