ICT PROTEGE GX

PRINT-READY DESK CARDS

Protege GX Quick Cards

One-page checklists for the most common operator and access-control tasks.

USE WITH THE FULL GUIDES

These cards summarize steps; they do not replace authorization, local SOP, or site-specific validation.

CURRENTNESS BASIS

Public GX release 4.3.402 (May 2026) • Setup Guide (July 2026) • Operator Reference Manual (December 2025)

Before use, enter your actual installed build here: ______________________ Interface: Desktop / Web App / Web Client

Prepared 27 July 2026 • Toronto

QUICK CARD 01

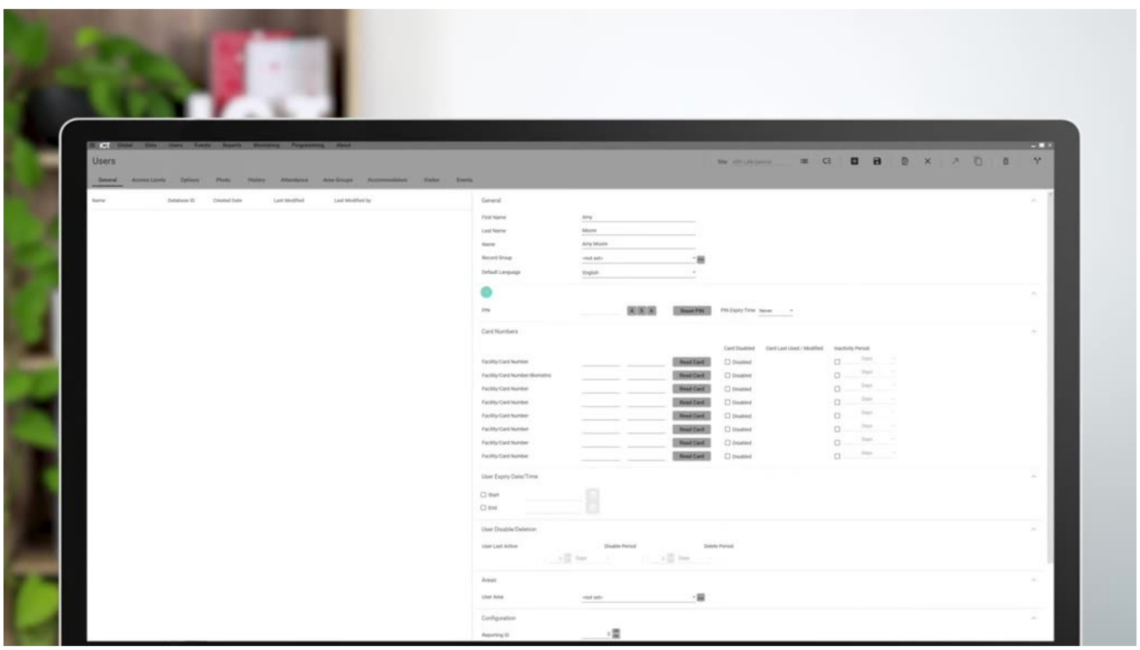
Add a user and fob

AMBER · REVERSIBLE CHANGE

MENU PATH	**Users ⟶ Users ⟶ Add**

Do this

1. Confirm Site, person, fob Facility/Card numbers, dates, and approved access level.
2. Click Add; enter first/last name.
3. Enter Facility and Card number in one credential row.
4. Set approved start/end date for temporary access.
5. Open Access levels → Add; choose the approved level.
6. Recheck every digit and click Save.
7. Test one allowed and one denied door; check Events.



Official ICT video capture — user General tab.

VERIFY

Reopen the user; identity, credential, dates, and access level are correct. Events names the expected access level.

STOP AND ESCALATE IF

The access level is unclear, another user has the credential, the controller is offline, or the selected Site is wrong.

QUICK CARD 02

Lost fob: stop one credential

AMBER · REVERSIBLE CHANGE

MENU PATH	**Users ⟶ Users ⟶ user ⟶ General ⟶ credential row**

Do this

1. Confirm the user with two identifiers.
2. Confirm which credential is lost.
3. Enable Card disabled on that credential row.
4. Do not delete the user or clear other credential rows.
5. Click Save and wait for synchronization.
6. Verify the lost credential is denied.
7. Record authorization, time, and replacement-fob process.

VERIFY

The lost credential is still recorded but disabled; other approved credentials behave as intended.

STOP AND ESCALATE IF

You cannot identify the exact credential, the user has duplicate/unknown credentials, or the request is to stop all access.

QUICK CARD 03

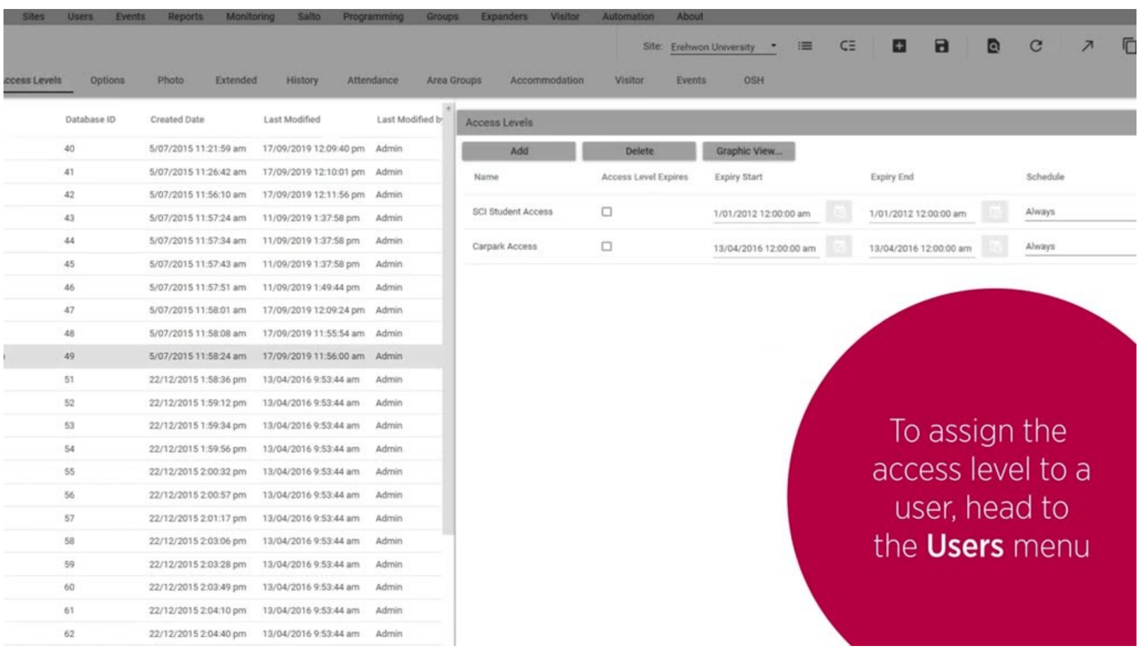
Change a user’s access

AMBER · REVERSIBLE CHANGE

MENU PATH	Users ⟶ Users ⟶ user ⟶ Access levels

Do this

1. Confirm the new approved level and read every existing level.
2. Click Add and select the new approved level.
3. Save; test new access.
4. Return to the user’s Access levels.
5. Select the old row and click Remove—not Delete.
6. Save.
7. Test one allowed and one now-denied door/floor.



Official ICT video capture — the user’s Access Levels tab.

VERIFY

Only approved levels remain; Events confirms the new grant and the revoked location is denied.

STOP AND ESCALATE IF

Another level still grants the same location, the access-level name is ambiguous, or you would need to edit a shared level.

QUICK CARD 04

Temporarily unlock, then secure a door

AMBER · REVERSIBLE CHANGE

MENU PATH	**Monitoring → Status Page/Floor Plan → right-click door**

Do this

1. Confirm the exact door and authorization.
2. Right-click the door.
3. Choose Unlock—not Unlock latched.
4. Supervise the entry and watch live status.
5. Confirm the door closes and returns to secure state.
6. If it remains unlocked, choose Lock.
7. Check Events for unlock and restore.

VERIFY
Live status, physical latch, and Events agree that the intended door returned to secure state.

STOP AND ESCALATE IF
The only visible choice is Unlock latched, a lockdown is active, the door is held/forced, or a schedule immediately unlocks it again.

QUICK CARD 05

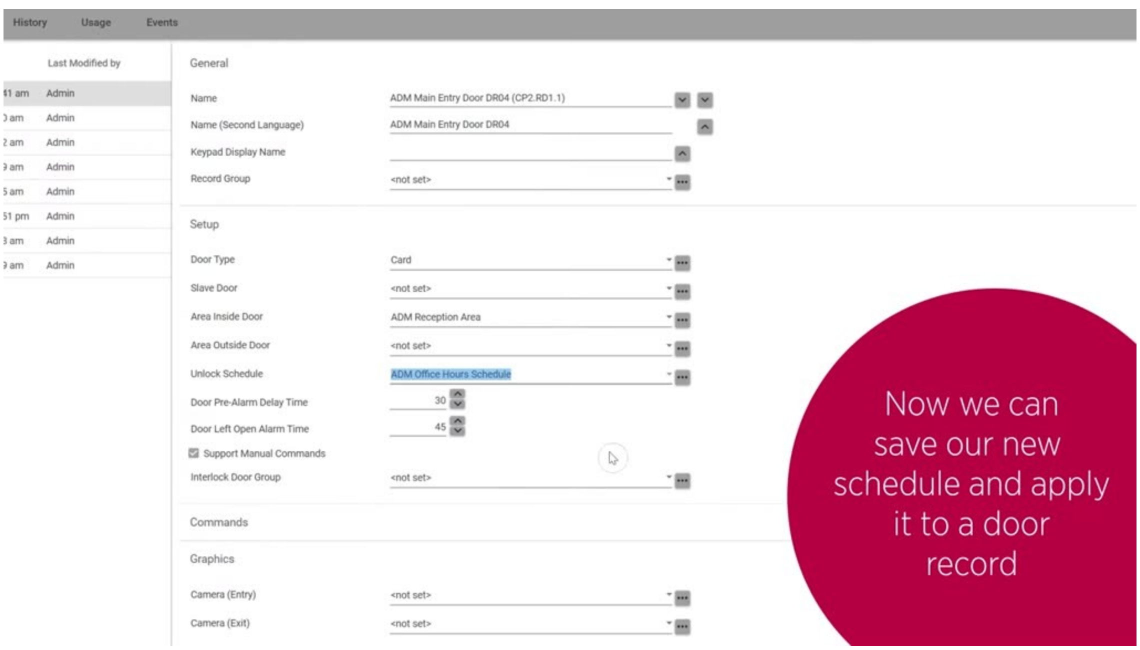
Door: free by day, fob-only by night

RED · SHARED OR HIGH IMPACT

MENU PATH	**Sites ⟶ Schedules ✦ Programming ⟶ Doors ✦ Users ⟶ Access levels**

Do this

1. Create/verify the approved free-access schedule and holiday behavior.
2. Assign it to the door’s Unlock schedule.
3. Confirm approved user access levels include the door after hours.
4. Test before opening: locked; approved fob works.
5. Test opening transition: door becomes free.
6. Test closing transition: door locks.
7. Test approved and denied credentials after hours; check Events.



Official ICT video capture — assign the door’s Unlock schedule.

VERIFY

Valid door schedule = free. Invalid door schedule + valid user level = fob-only. Invalid both = no access.

STOP AND ESCALATE IF

The same office-hours schedule is also limiting the users, holidays are unclear, or the door has late-open/area/enforcement options you have not assessed.

QUICK CARD 06

Put elevator floors on a fob

RED · SHARED OR HIGH IMPACT

MENU PATH	**Users → Users → Access levels OR Users → Access levels**

Do this

1. Identify the elevator integration and approved access level.
2. Prefer assigning that existing level to the user.
3. If building a level, add the approved Floor/Floor group.
4. Add the approved Elevator/Elevator group or vendor-specific interface points.
5. Apply approved schedules.
6. Save and synchronize.
7. Test an allowed floor and a denied floor from the correct car; check Events.

VERIFY

The user has both required halves—floor and car/interface—and no broader floor access.

STOP AND ESCALATE IF

The integration type is unknown, only one half is configured, Include all is enabled without approval, or an HLI vendor note requires a different path.

QUICK CARD 07

Temporarily unlock one elevator floor

RED · SHARED OR HIGH IMPACT

MENU PATH	**Monitoring → Status Page/Floor Plan → exact elevator car → right-click floor**

Do this

1. Confirm low-level/supported integration, exact car, exact floor, and authorization.
2. Check the floor schedule and Schedule verify.
3. Choose Activate timed for a defined window when possible.
4. Use Activate only for an approved latch-unlock.
5. Watch Events and live floor state.
6. At the end, choose Deactivate.
7. Verify this car—and other cars if required—are secure.

VERIFY

Only the intended floor through the intended car changed, and it returned to secure state.

STOP AND ESCALATE IF

The command menu differs, Schedule verify reverses the command, the system is HLI/vendor-controlled, or another car remains free.

QUICK CARD 08

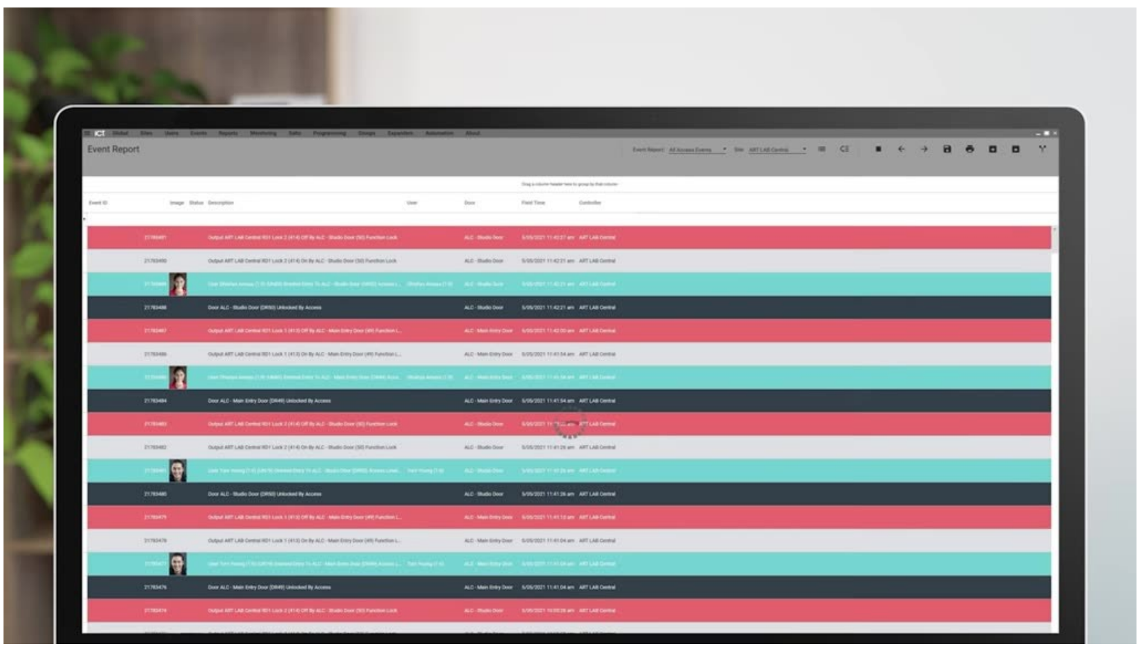
Verify any change

GREEN · READ / ROUTINE

MENU PATH	Refresh record ✦ Monitoring/Status Page ✦ Reports → Events

Do this

1. Refresh and reopen the saved record.
2. Confirm normal controller/integration download.
3. Test one expected allowed action.
4. Test one expected denied action.
5. Confirm the door/floor returns to secure state.
6. Run/filter Events for the exact user, door/floor, and time.
7. Check History; capture evidence and monitor the next schedule transition.



Official ICT video capture — event report verification.

VERIFY

Record, live state, physical result, Events, and History all agree.

STOP AND ESCALATE IF

Any result differs from the approved plan. Roll back once and escalate; do not stack speculative changes.