

ICT PROTEGE GX

LEVEL 3

Advanced Admin & Elevator Guide

Elevator/floor access, manual floor commands, advanced door behavior, bulk operations, roles, controller health, backup, compatibility, and change control.

ADVANCED • ADMINISTRATOR / INTEGRATOR

For supervised administrators and qualified access-control/elevator integrators.

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

Your Level 3 roadmap

Use the modules in order. If a menu or field is missing, stop: your operator role, license, selected site, or interface may be different.

MODULE	YOU WILL LEARN
01	Identify the elevator integration before using any procedure.
02	Grant a fob both the required elevator car and floor permissions.
03	Remove floor/elevator access without accidentally leaving another grant active.
04	Schedule free elevator-floor access and understand Schedule verify.
05	Manually Activate, Deactivate, or Activate timed for one floor/car.
06	Separate operator-safe work from reader, relay, output, HLI, and vendor engineering.
07	Review advanced door, interlock, antipassback, authentication, and lockdown risks.
08	Import users in bulk with a controlled staging and rollback process.
09	Build least-privilege operator roles and audit every change.
10	Check controller/download health without disruptive recovery actions.
11	Protect backups, compatibility, and upgrade/rollback readiness.

Advanced means change control first

DO NOT USE THIS AS PERMISSION

This guide explains the architecture and verified menu paths. It does not replace your integrator's design, elevator-vendor approval, fire/life-safety review, or written site authorization.

- Use a maintenance window, test credential, test door/floor, witness, event window, and written rollback.
- Capture every current field before editing a shared record.
- Check Usage before changing schedules, groups, access levels, doors, floors, elevators, outputs, or areas.
- Never paste values into a Commands field unless an exact current ICT document or support case directs it.
- Never use Update module or Force Download merely because a normal saved change is not instantly visible.

1. Identify the elevator type

THERE IS NO SINGLE UNIVERSAL ELEVATOR PROCEDURE

Protege GX can control floor relays directly (low-level control) or exchange permissions with a vendor high-level interface (HLI). KONE, Otis, Schindler, MCE, TKE/ThyssenKrupp, destination dispatch, and other integrations can behave differently.

TYPE	HOW IT WORKS	PRIMARY AUTHORITY	GUIDE RULE
Low-level relay control	GX activates physical outputs for permitted floor buttons.	AN-248 plus Operator Manual	Floor/car commands in this guide apply most directly.
Vendor HLI / destination dispatch	GX sends access/destination data to an elevator vendor system.	Exact ICT application note for the manufacturer	Door/COP/DOP/kiosk records and home-floor rules may also be required.
Unknown	The site has not confirmed integration type or vendor mapping.	Integrator and elevator vendor	Stop after read-only inspection; do not edit floor, output, reader, or HLI programming.

COMPATIBILITY IS COMPONENT-SPECIFIC

The GX server can be current while the controller, Web App, wireless-lock, biometric, or elevator integration requires a particular supported build. Check the July 2026 compatibility matrix and the vendor-specific application note.

Source: [ICT Protege GX Compatibility Matrix \(24 Jul 2026\)](#) • [ICT AN-248: Low Level Elevator Control \(2 Oct 2024\)](#), pp. 5–17 • [ICT AN-241: Protege GX MCE Elevator Integration](#)

The elevator permission model

A FOB NEEDS BOTH HALVES

Floor/floor group answers ‘which floors?’ Elevator/elevator group answers ‘through which cars or interface points?’ A low-level elevator access level normally needs both.

FLOOR / FLOOR GROUP	+	ELEVATOR / ELEVATOR GROUP
Which controlled floors	+	Which elevator cars can deliver the permission
Optional per-floor schedule	+	Correct vendor/reader/COP/DOP scope

2. Put approved elevator floors on a fob

RED • SHARED OR HIGH IMPACT

WHAT THIS DOES

Adds an existing approved elevator/floor access level to one user—or builds that shared level under change control.

Use this when: A resident or employee must use specified elevator cars to reach specified controlled floors.

Before you click

- Identify the elevator integration and the site’s approved floor/elevator access level.
- Prefer assigning an existing approved level to the user.
- If building a level, list exact floors, cars/interface points, and per-item schedules.
- Check every existing level on the user; another level may already grant broader elevator access.

MENU PATH **Users → Users → Access levels OR Users → Access levels → Floors/Floor groups + Elevator groups**

Exact steps

1. For an existing approved level: open Users → Users, confirm the person, open Access levels, click Add, select the level, and Save.
2. For a new shared level: open Users → Access levels and click Add.
3. Enter a descriptive name and approved overall Operating schedule.
4. Open Floors or Floor groups; Add only the approved floor records/groups.
5. Set any approved per-floor schedule.
6. Open Elevator groups; Add only the approved elevator group. Use direct elevator records only if your site design requires them.
7. Do not enable Include all floors/elevators unless the approved design explicitly includes future records.
8. Save the level.
9. Assign it to one test user, wait for normal synchronization, and test from the correct elevator car.
10. Check Events for the user, elevator, granted floor, and access level.

6. Set the following options for Floor 1:
 - **Schedule:** The unlock schedule for the floor. Set to Office Hours.
 - **Schedule verify / Verify** (depending on your system): Enable this option to allow the floor to unlock and relock on schedule. If the floor is locked while the schedule is valid or latch unlocked while the schedule is invalid, it will be returned to the correct state within one minute.
 - **Output:** Elevator Floor 1 Relay
7. For the other three floors, set the corresponding **Output** as programmed above.
8. Click **Save**.

Configuring the Reader Expander

The reader expander port must be configured to provide elevator control instead of door control.

1. Navigate to **Expanders | Reader expanders** and select the reader expander that is being used for access in the elevator car.
2. Open the **Reader 1** or **Reader 2** tab, depending on the reader port that is being used for access.
3. Ensure that the **Reader 1/2 door** is not set.
4. Set the **Reader 1/2 mode** to Elevator.
5. Set the **Reader 1/2 elevator** to the Elevator 1 record created above.
6. Click **Save**.
7. Wait for the changes to be downloaded to the controller, then right click on the expander record and click **Update module**.

Assigning Access to Users

To gain access to a floor, a user must have both the elevator car and the floor assigned in their access level. You will need to create any elevator groups and floor groups that are necessary to grant the required access.

For this scenario, we will grant access to two users: Mike Tory (manager), who has access to all floors at all times, and Kevin Simon (employee), who only has access to Floor 2.

1. Navigate to **Groups | Elevator groups** and add a new elevator group called Building 1 elevator group.
2. Add Elevator 1 to the group, and click **Save**.
3. Navigate to **Groups | Floor groups** and create the Managers floor group.
4. Add Floors 1-4 to the group, and click **Save**.

It is possible to set a **Schedule** on each individual floor to limit access to particular times.

5. Navigate to **Users | Access levels** and create the Managers access level.
6. In the **Floor groups** tab, add the Managers floor group.
7. In the **Elevator groups** tab, add the Building 1 elevator group. Click **Save**.

The **Include all floors** and **Include all elevators** options should be used with caution, as these will automatically grant users access to any new floors or elevators created in the site.

8. Create the Floor 2 Employees access level.
9. In the **Floors** tab, add Floor 2.
10. In the **Elevator groups** tab, add the Building 1 elevator group. Click **Save**.
11. In **Users | Users**, create the users Mike Tory (with the Managers access level) and Kevin Simon (with the Floor 2 Employees access level). Assign each user a credential for use in testing.

Figure 1 — ICT AN-248 p. 20: a user needs both the floor/floor group and elevator/elevator group in the access level.

VERIFY	The user can select only approved floors through approved cars during approved times; at least one denied floor remains denied.
UNDO	Remove the new level from the user or restore the captured shared-level rows; Save and retest. Do not delete the shared record.
WATCH FOR	Adding only floors or only elevator groups, wrong car, broad Include all options, missing schedule, or using low-level steps on an HLI system.

Source: [ICT Protege GX Operator Reference Manual \(18 Dec 2025\)](#), pp. 128–132, 248–251, and 289–290 • [ICT AN-248: Low Level Elevator Control \(2 Oct 2024\)](#), pp. 19–21

3. Remove floor or elevator access from a fob

RED • SHARED OR HIGH IMPACT

WHAT THIS DOES

Removes the permission path while keeping the user and unrelated credentials/access intact.

Use this when: A person changes floor, loses garage/elevator privileges, or no longer needs a particular car.

Before you click

- Decide whether to remove one shared level from one user or edit the shared level for everyone.
- Read all user access levels; another level may grant the same floor/elevator.
- Capture the intended allowed and denied test matrix.

MENU PATH **Users → Users → Access levels; then inspect Users → Access levels as required**

Exact steps

1. Open the user and list every access level.
2. If one assigned level alone provides the unwanted elevator access, select that row and click Remove.
3. Save, synchronize, and test.
4. If the requirement is to remove a floor from a shared role, stop and check Usage on that access level.
5. With approval, open Users → Access levels and remove the exact Floor/Floor group or Elevator group row—not the record itself.
6. Save and test every affected user category.
7. Check Events for the expected denial and ensure unrelated floors still work.

VERIFY	The target floor/car is denied, an approved remaining floor works, and no other user population was unintentionally affected.
UNDO	Re-add the captured row or access level under authorization, Save, and repeat allowed/denied tests.
WATCH FOR	Removing only the elevator group while another level grants it, editing a shared level without Usage review, or deleting the floor/group record.

Source: [ICT Protege GX Operator Reference Manual \(18 Dec 2025\)](#), pp. 118, 128–132, 248–251, and 289–290 • [ICT AN-248: Low Level Elevator Control \(2 Oct 2024\)](#), pp. 19–21

4. Schedule a floor for free access versus fob access

RED • INSTALLER / INTEGRATOR ONLY

WHAT THIS DOES

Uses the elevator car's per-floor Schedule as an unlock schedule: valid means free access; invalid means a credential is required.

Use this when: A shared lobby floor should be freely selectable during office hours but controlled after hours.

Before you click

- Confirm this is low-level or a supported integration with the same semantics.
- Confirm exact car, floor output/mapping, schedule, holidays, and desired fail-safe/fail-secure behavior.
- Check whether Schedule verify, Late to open, Follow area status, input/output, or area control is enabled.

MENU PATH

Programming → Elevator cars → select car → Schedules and areas

Exact steps

1. Open Programming → Elevator cars and select the exact car.
2. Open Schedules and areas.
3. Find or add the exact floor row.
4. Set Schedule to the approved free-access schedule.
5. Enable Schedule verify only if the approved design requires continuous one-minute enforcement.
6. Review Output and any Area/Input mapping; do not change them as a routine schedule task.
7. Save and test the next valid transition.
8. When valid, confirm the floor is free without a credential.
9. When invalid, confirm the floor is secure but an approved credential can enable it.
10. Test a denied credential and check Events.

Testing the Elevator

Finally, we can use our two users to test the programming.

In Protege GX, it is recommended that you set up a status page or floor plan that includes the Elevator 1 record, as well as an event window. This will allow you to view and control the status of each individual floor that can be accessed from the elevator.

Events in Protege WX can be viewed on the **Monitoring | All Events** page. You can view and control floor status on the **Monitoring | Elevators** page.

1. To test the unlock schedule, set the controller time to 8:59:00 AM:
 - **Protege GX:** Navigate to **Sites | Controllers** and right click on the controller. Enter the new time and select **Set controller date time**.
 - **Protege WX:** Navigate to **Scheduling | Time**. Enter the new **Time** and click **Save**, then press F5 to refresh the page.

Elevator 1, Floor 1 should be secured.

2. Wait until the controller field time reaches 9:00 AM. Floor 1 should unlock within 1 minute of the schedule becoming valid.

```
Schedule Office Hours Is Valid
Elevator Elevator 1 Floor Floor 1 Unlocked By Schedule Office Hours
Output Elevator Floor 1 Relay On By Floor Floor 1
```

3. Badge the card belonging to Kevin Simon. Access should be granted and Floor 2 unlocked for 5 seconds.


```
User Kevin Simon Granted Access To Elevator 1 Using Access Level Floor 2
Employees
Output Elevator Floor 2 Relay On By Floor Floor 2
...
Output Elevator Floor 2 Relay Off By Floor Floor 2
```

4. Badge the card belonging to Mike Tory. Access should be granted and all floors unlocked for 5 seconds (except for Floor 1, which is already unlocked).

```
User Mike Tory Granted Access To Elevator 1 Using Access Level Managers
Output Floor 2 Relay On By Floor Floor 2
Output Floor 3 Relay On By Floor Floor 3
Output Floor 4 Relay On By Floor Floor 4
...
Output Floor 2 Relay Off By Floor Floor 2
Output Floor 3 Relay Off By Floor Floor 3
Output Floor 4 Relay Off By Floor Floor 4
```

5. Right click on Floor 1 and click **Deactivate** to lock the floor. The floor should unlock again within 1 minute.

```
Operator Admin Locked Floor Floor 1 On Elevator 1
Output Elevator Floor 1 Relay Off By Floor Floor 1
...
Elevator Elevator 1 Floor Floor 1 Unlocked By Schedule Office Hours
Output Elevator Floor 1 Relay On By Floor Floor 1
```

6. Set the controller time to 4:59:00 PM.
 - **Protege GX:** Navigate to **Sites | Controllers** and right click on the controller. Enter the new time and select **Set controller date time**.
 - **Protege WX:** Navigate to **Scheduling | Time**. Enter the new **Time** and click **Save**, then press F5 to refresh the page.

7. Wait until the controller field time reaches 5:00 PM. Floor 1 should be locked within 1 minute of the schedule becoming invalid.

```
Schedule Office Hours Is Invalid
Elevator Elevator 1 Floor Floor 1 Locked By Schedule Office Hours
Output Elevator Floor 1 Relay Off By Floor Floor 1
```

Figure 2 — ICT AN-248 p. 21: schedule transition and credential tests for a low-level elevator.

VERIFY	Valid schedule = free floor through this car; invalid schedule = credential required; Schedule verify behaves as documented.
UNDO	Restore the captured floor-row settings and retest both transitions under integrator supervision.
WATCH FOR	Treating a valid floor schedule as a user-access window, changing the wrong car, or enabling Schedule verify and then expecting a manual override to persist.

Source: [ICT Protege GX Operator Reference Manual \(18 Dec 2025\), pp. 248–250](#) • [ICT AN-248: Low Level Elevator Control \(2 Oct 2024\), pp. 19–22](#)

SCHEDULE VERIFY CHANGES MANUAL-CONTROL BEHAVIOR

When enabled, GX checks the floor state every minute. A manual Deactivate during a valid schedule can be unlocked again within one minute; a manual Activate during an invalid schedule can be relocked within one minute.

5. Manually unlock or lock one elevator floor

RED • SHARED OR HIGH IMPACT

WHAT THIS DOES

Controls one floor through one selected elevator car from an approved status page or floor plan.

Use this when: An authorized event or service task requires a temporary or latched floor unlock on a supported low-level configuration.

Before you click

- Confirm integration supports GX manual floor commands.
- Confirm exact elevator car and floor; another car may remain controlled differently.
- Check the floor's schedule and Schedule verify.
- Prefer Activate timed. Use Activate (latched) only with a named person responsible for Deactivate.

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

Exact steps

1. Open the approved status page or floor plan containing the elevator car.
2. Locate the exact car and floor icon.
3. Right-click the floor.
4. Choose Activate timed for a defined temporary unlock and enter the approved time, or Activate for a latch unlock.
5. Watch live status and the output/floor Events.
6. When the approved period ends, choose Deactivate to lock the floor.
7. Verify the floor returns to secure state through this car.
8. Check another car if the design requires consistent building-wide state.

Manual Elevator Car (Floor) Commands

When an elevator car has been added to a status page or floor plan the floors that can be accessed from that elevator car are displayed. Right clicking on a floor icon opens a menu with manual commands for that floor.

Control

- **Activate** (latch unlock the floor until it is locked again)
- **Deactivate** (lock the floor)
- **Activate timed** (unlock the floor for the time set in the field below)

Manual commands only affect access to the floor via that specific elevator car. For example, if you unlock the floor with a command it may be freely accessible from one elevator car, but not from others.

Figure 3 — Official Operator Reference Manual p. 250: Activate, Deactivate, and Activate timed. Command scope is one floor through one car.

VERIFY	Only the intended floor/car changes, the timed/latched behavior matches the command, and the floor is secure afterward.
UNDO	Choose Deactivate for that floor/car, verify physical/system state, and escalate if Schedule verify or vendor HLI reapplies another state.
WATCH FOR	Assuming the command affects every car, choosing Activate instead of Activate timed, or fighting Schedule verify with repeated commands.

Source: [ICT Protege GX Operator Reference Manual \(18 Dec 2025\), p. 250](#) • [ICT AN-248: Low Level Elevator Control \(2 Oct 2024\), pp. 20–22](#)

6. Elevator engineering: installer-only sequence

RED • INSTALLER / INTEGRATOR ONLY

OPERATOR BOUNDARY

The following is an architecture checklist, not a live-system shortcut. Reader ports, floor relays, outputs, fail-safe behavior, destination inputs, HLI credentials, and Update module belong to a qualified integrator and elevator vendor.

LAYER	DESIGN RESPONSIBILITY	PATH
Outputs and fail behavior	Map each physical floor relay, inversion, module-offline state, and fire/life-safety behavior.	Programming → Outputs
Floor records	Create unique floor relay numbers in physical order.	Programming → Floors
Elevator car	Set reader expander/port, unlock access time, authentication, destination reporting, and floor rows.	Programming → Elevator cars
Reader port	Ensure no door is assigned; set mode to Elevator and link the elevator record.	Expanders → Reader expanders → Reader 1/2
Groups and access	Build floor/elevator groups and access levels with controlled schedules.	Groups + Users → Access levels
Download and test	Wait for normal download; only then use the documented Update module step in a maintenance window.	Controller/expander diagnostics + physical test

6. Set the following options for Floor 1:
 - **Schedule:** The unlock schedule for the floor. Set to Office Hours.
 - **Schedule verify / Verify** (depending on your system): Enable this option to allow the floor to unlock and relock on schedule. If the floor is locked while the schedule is valid or latch unlocked while the schedule is invalid, it will be returned to the correct state within one minute.
 - **Output:** Elevator Floor 1 Relay
7. For the other three floors, set the corresponding **Output** as programmed above.
8. Click **Save**.

Configuring the Reader Expander

The reader expander port must be configured to provide elevator control instead of door control.

1. Navigate to **Expanders | Reader expanders** and select the reader expander that is being used for access in the elevator car.
2. Open the **Reader 1** or **Reader 2** tab, depending on the reader port that is being used for access.
3. Ensure that the **Reader 1/2 door** is not set.
4. Set the **Reader 1/2 mode** to Elevator.
5. Set the **Reader 1/2 elevator** to the Elevator 1 record created above.
6. Click **Save**.
7. Wait for the changes to be downloaded to the controller, then right click on the expander record and click **Update module**.

Assigning Access to Users

To gain access to a floor, a user must have both the elevator car and the floor assigned in their access level. You will need to create any elevator groups and floor groups that are necessary to grant the required access.

For this scenario, we will grant access to two users: Mike Tory (manager), who has access to all floors at all times, and Kevin Simon (employee), who only has access to Floor 2.

1. Navigate to **Groups | Elevator groups** and add a new elevator group called Building 1 elevator group.
2. Add Elevator 1 to the group, and click **Save**.
3. Navigate to **Groups | Floor groups** and create the Managers floor group.
4. Add Floors 1-4 to the group, and click **Save**.

It is possible to set a **Schedule** on each individual floor to limit access to particular times.

5. Navigate to **Users | Access levels** and create the Managers access level.
6. In the **Floor groups** tab, add the Managers floor group.
7. In the **Elevator groups** tab, add the Building 1 elevator group. Click **Save**.

The **Include all floors** and **Include all elevators** options should be used with caution, as these will automatically grant users access to any new floors or elevators created in the site.

8. Create the Floor 2 Employees access level.
9. In the **Floors** tab, add Floor 2.
10. In the **Elevator groups** tab, add the Building 1 elevator group. Click **Save**.
11. In **Users | Users**, create the users Mike Tory (with the Managers access level) and Kevin Simon (with the Floor 2 Employees access level). Assign each user a credential for use in testing.

Figure 4 — AN-248 p. 20 includes reader-expander configuration and access-level assignment. Use only in the approved integration design.

Source: [ICT AN-248: Low Level Elevator Control \(2 Oct 2024\)](#), pp. 18–30 • [ICT Protege GX Operator Reference Manual \(18 Dec 2025\)](#), pp. 248–251

7. Vendor HLI differences you must not flatten

- Some HLI systems use door/door-group records for COPs, DOPs, kiosks, or readers as well as floor/elevator permissions.
- All relevant schedules on the HLI permission path must be valid.
- Home/default destination floors may be set on the access level for supported integrations.
- KONE Office Flow and other destination systems can have integration-specific defaults and broad-grant failure modes.
- Use the current ICT application note for the exact vendor and version; do not adapt a Protege WX or another vendor's screenshot.

MCE EXAMPLE

ICT AN-241 documents floor/floor-group permission plus the door/door-group records representing COP/DOP/kiosk/reader points, with all relevant schedules valid. This is why a low-level 'floors + elevator group' recipe is not universal.

Source: [ICT AN-241: Protege GX MCE Elevator Integration](#) • [ICT Protege GX Compatibility Matrix \(24 Jul 2026\)](#)

8. Advanced door architecture and red lines

FEATURE	WHY IT MATTERS	OWNER
Door type	Inherited hardware/behavior template. Affects multiple doors.	Integrator only
Lock output / activation	Physical lock output and pulse/toggle behavior.	Integrator only
REX / REN	Egress/entry request inputs and release behavior.	Life-safety/integrator
Inside/outside area	Alarm-area state and access interactions.	Admin/integrator
Antipassback	Stops invalid entry/exit sequences.	Designed rollout + reset SOP
Dual authentication	Requires multiple credentials or PIN/card logic.	Security-design approval
Door interlock	Prevents simultaneous unlock of related doors.	Integrator + egress review
Lockdown	Overrides ordinary unlock behavior.	Emergency SOP only
Always check unlock schedule	Continuously enforces scheduled state.	Admin with transition test
Commands field	Low-level documented configuration commands.	ICT support/document only

Source: [ICT Protege GX Operator Reference Manual \(18 Dec 2025\)](#), pp. 198–211

9. Import users from CSV safely

RED • SHARED OR HIGH IMPACT

WHAT THIS DOES

Creates or updates many user records by mapping spreadsheet columns into Protege GX fields.

Use this when: A controlled onboarding project has a reviewed CSV, naming convention, access matrix, test batch, and rollback.

Before you click

- Back up/export according to policy and work from a reviewed copy of the CSV.
- Remove blank rows, duplicate credentials, formulas, and unnecessary personal data.
- Decide whether the first line contains headers and confirm the delimiter.
- Test with 1–3 records in a non-production or isolated test scope.
- Do not use a default access level or generated PIN broadly without written approval.

MENU PATH **Sites → Import users**

Exact steps

1. Open Sites → Import users.

- 2. Choose the reviewed CSV file.
- 3. Set the first-line/header and delimiter options.
- 4. Map every source column deliberately to the correct GX field.
- 5. Review any facility number, first-card, access-level, record-group, and PIN-generation options.
- 6. Preview the records and correct every warning before import.
- 7. Run the smallest approved test batch.
- 8. Verify names, credentials, dates, access levels, and duplicate handling.
- 9. Only then run the approved production batch.
- 10. Monitor downloads and test a sample of allowed and denied access.

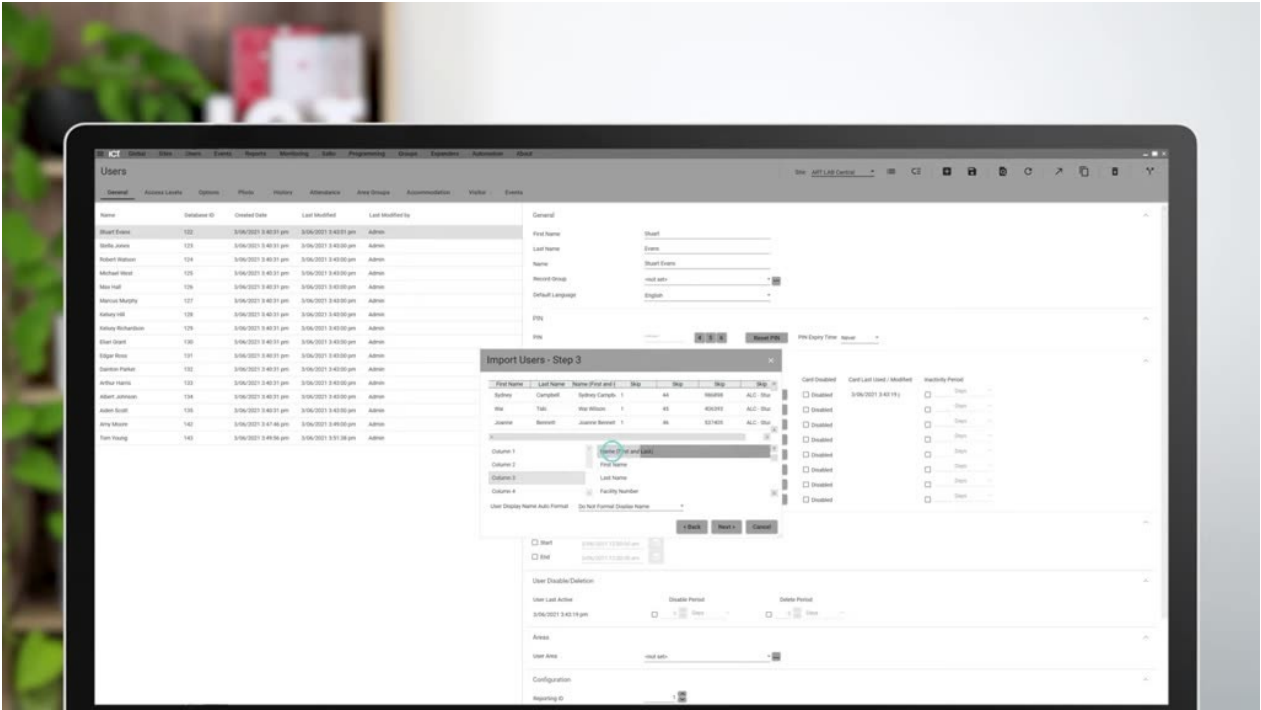


Figure 5 — Official ICT user-import wizard. Validate every mapped column before Finish.

VERIFY	Imported row count matches approval; no duplicate credentials/users; sample access behaves exactly as the matrix.
UNDO	Disable the test/imported population using the captured batch identifier and follow the authorized restore/removal plan. Avoid broad multiselect deletion.
WATCH FOR	Wrong delimiter, shifted columns, facility/card fields reversed, broad default access, generated duplicate PINs, or importing into the wrong Site.

Source: [ICT Protege GX Operator Reference Manual \(18 Dec 2025\), pp. 112–114](#) • [Official ICT video: Adding a User in Protege GX, 3:34–4:57](#)

10. Operator roles and least privilege

USER ≠ OPERATOR

A User holds physical credentials. An Operator logs into GX. Keep routine user/fob work separate from shared scheduling, door, elevator, backup, and integration administration.

ROLE	NORMAL AUTHORITY
Routine operator	Find/read users; add approved level; disable credential/user; temporary Unlock/Lock; view approved events.
Access administrator	Create/edit shared access levels and schedules with Usage review and change control.
System administrator	Operators, roles, sites, record groups, backups, SQL/service configuration, upgrade coordination.
Integrator	Doors, readers, outputs, REX/REN, areas, controller/expander, elevator relays/HLI, firmware, Commands.
Emergency authority	Lockdown/fire/life-safety activation and reset under a separate tested SOP.

HIGH-RISK RIGHTS

Super rights, lockdown, Include all records, operator administration, backups, Commands, Update module, and multi-record changes must not be bundled into a routine front-desk role.

Source: [ICT Protege GX Operator Reference Manual \(18 Dec 2025\), pp. 62–65](#)

11. Controller and download health

SAVED ON THE SERVER IS NOT THE SAME AS ACTIVE IN THE FIELD

GX changes must reach the relevant controller/integration. Check health and download status before assuming a field device received the change.

1. Confirm the correct Site and controller.
2. Read controller online/offline state and Last downloaded time.
3. Use the standard download diagnostics or Enterprise Global → Diagnostics → Downloads when available.
4. Use Get health status only when permitted by your SOP.
5. Review Events/diagnostics for the exact record or controller.
6. If normal synchronization stalls, capture the state and escalate.
7. Use Force Download only as an approved diagnostic/recovery step.
8. Use Update module only in a maintenance window under integrator direction; it restarts the controller and connected modules and temporarily takes them offline.

DO NOT MASK THE ROOT CAUSE

Repeated Force Download or Update module can interrupt access control without fixing role, schedule, version, network, database, or integration errors.

Source: [ICT Protege GX Operator Reference Manual \(18 Dec 2025\)](#), pp. 83–92

12. Backup, rollback, and version control

- Maintain approved backups of both the Main and Events databases; test restore procedures.
- Export/capture shared records before high-impact edits.
- Record GX server, client, Web App/Web Client, controller firmware, elevator interface, SQL Server, and integration versions.
- Check release notes, AN-366, and the current compatibility matrix before upgrading.
- Do not assume 'latest GX' means every controller, elevator vendor, wireless lock, or biometric component should immediately run its newest build.
- Rollback of a database, controller, firmware, or vendor integration is a coordinated administrator/integrator operation.

Source: [ICT Protege GX 4.3.402 Release Notes \(8 May 2026\)](#) • [ICT Protege GX Compatibility Matrix \(24 Jul 2026\)](#) • [ICT Protege GX Operator Reference Manual \(18 Dec 2025\)](#), pp. 29–30

13. Advanced troubleshooting decision flow

1 • Scope	One credential, one user, one door/floor, one controller, or whole site?
2 • Server record	Correct Site, record, dates, disabled state, access levels, schedules, areas, groups?
3 • Download	Did the relevant controller/integration receive the saved record?
4 • Event reason	Granted/denied by which access level, schedule, area, antipassback, authentication, or integration response?
5 • Physical path	Reader read, input/output state, lock/relay, door contact, elevator vendor response?
6 • Compatibility	Supported GX/controller/integration/SQL/OS combination?
7 • Rollback/escalate	Restore the one approved change; attach evidence; stop speculative edits.

Final change-control checklist

STOP RULE

If the saved result differs from the approved plan, roll back once and escalate. Do not make repeated speculative changes on a live access-control system.

Before

- Confirm written authorization, current Site, exact person/door/floor, and intended start/end time.
- Confirm the controller is online and there is no active lockdown, fire response, or unresolved alarm.
- Capture the current values; check History and Usage before changing any shared record.
- Choose the most reversible method and identify a test credential, witness, and rollback.

During

- Change one thing at a time and avoid multiselect unless specifically approved.
- Reconfirm the selected record immediately before Save or Delete.
- Wait for normal download/synchronization. Do not use Force Download or Update module as a first reaction.

After

- Refresh and reread the record; verify controller download/health.
- Test one expected allowed action and one expected denied action.
- Confirm the door/floor returns to the secure state; check Events and History.
- Record evidence and monitor the next scheduled transition, especially holidays and overnight periods.

Official source set

- [ICT Protege GX 4.3.402 Release Notes \(8 May 2026\)](#)
- [ICT Protege GX Setup Guide \(15 Jul 2026\)](#)
- [ICT Protege GX Operator Reference Manual \(18 Dec 2025\)](#)
- [ICT Protege GX End User Guide \(30 Jul 2025\)](#)
- [ICT Protege GX Compatibility Matrix \(24 Jul 2026\)](#)
- [ICT AN-248: Low Level Elevator Control \(2 Oct 2024\)](#)
- [ICT AN-241: Protege GX MCE Elevator Integration](#)

COPYRIGHT AND PRIVACY

The screenshots in this guide are limited training excerpts from official public ICT videos/manuals. For your final internal edition, replace them with redacted captures from your own licensed installation. Remove names, PINs, facility/card numbers, IP addresses, controller serials, floor-plan security details, and operator credentials.