

ICT PROTEGE GX

LEVEL 1

Basic Operator Guide

Daily user, fob, access-level, door-control, and verification tasks—written one click at a time.

BASIC • START HERE

For front desk, security, concierge, and other operators using approved records.

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 1 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	Recognize users, operators, credentials, access levels, and the current Site.
02	Find the correct person and read the record before editing.
03	Add a user and assign one approved access level.
04	Change access without leaving an old access level active.
05	Disable one lost fob, disable a whole user, expire access, or delete only when authorized.
06	Temporarily unlock a door and lock it again.
07	Verify the result in live status, Events, and History.
08	Troubleshoot the common 'saved but still not working' cases safely.

Start with the right interface

THIS GUIDE IS FOR THE WINDOWS DESKTOP CLIENT

Protege GX has a Windows desktop client, a modern Web App, and a legacy Web Client. They do not use identical menus. This guide uses desktop paths such as Users → Users and Sites → Schedules. Do not follow a Web App or Protege WX screenshot as though it were the same screen.

1. In the desktop client, open About → Version.
2. Write the complete installed build on the cover of this guide.
3. Open About → Help when a field differs; built-in Help best matches the installed build.
4. Confirm the Site selector shows the building you intend to change.

Source: [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 \(18 Dec 2025\), pp. 348–349](#)

Five words that prevent most mistakes

TERM	PLAIN ENGLISH
User	The person whose fob, card, PIN, mobile credential, or remote opens controlled items.
Operator	The person logged into Protege GX. An operator is not the same thing as a user.
Credential	The fob/card/PIN. The desktop form still labels these as Facility/Card number.
Access level	A reusable permission package: where the user may go, when, and sometimes in which direction.
Unlock schedule	When a door or floor is free without a fob. This is different from a user's access schedule.

THE SAFEST DEFAULT

If access must stop, disable the specific credential or disable the user. Deletion is permanent and should be the last step, not the first.

1. Find and confirm the correct user

GREEN • READ / ROUTINE

WHAT THIS DOES

Opens the person's existing record without changing anything.

Use this when: A resident, employee, contractor, or visitor asks you to check or change access.

Before you click

- Ask for two identifiers, such as full name plus suite/company/employee number.
- Confirm the current Site. Similar names can exist in more than one site.
- Never identify a person only by the visible card number on an event.

MENU PATH **Users → Users**

Exact steps

- 1. Open Users, then choose Users.
- 2. Use the Find/search field and enter the person’s name.
- 3. Select the result once. Do not Shift-click or Ctrl-click other rows.
- 4. Read the General tab: first name, last name, facility/card number, start/end date, and disabled state.
- 5. Open Access levels and read every assigned level.
- 6. If available, open Events for recent credential activity and History for prior record changes.
- 7. Confirm the second identifier before you edit anything.

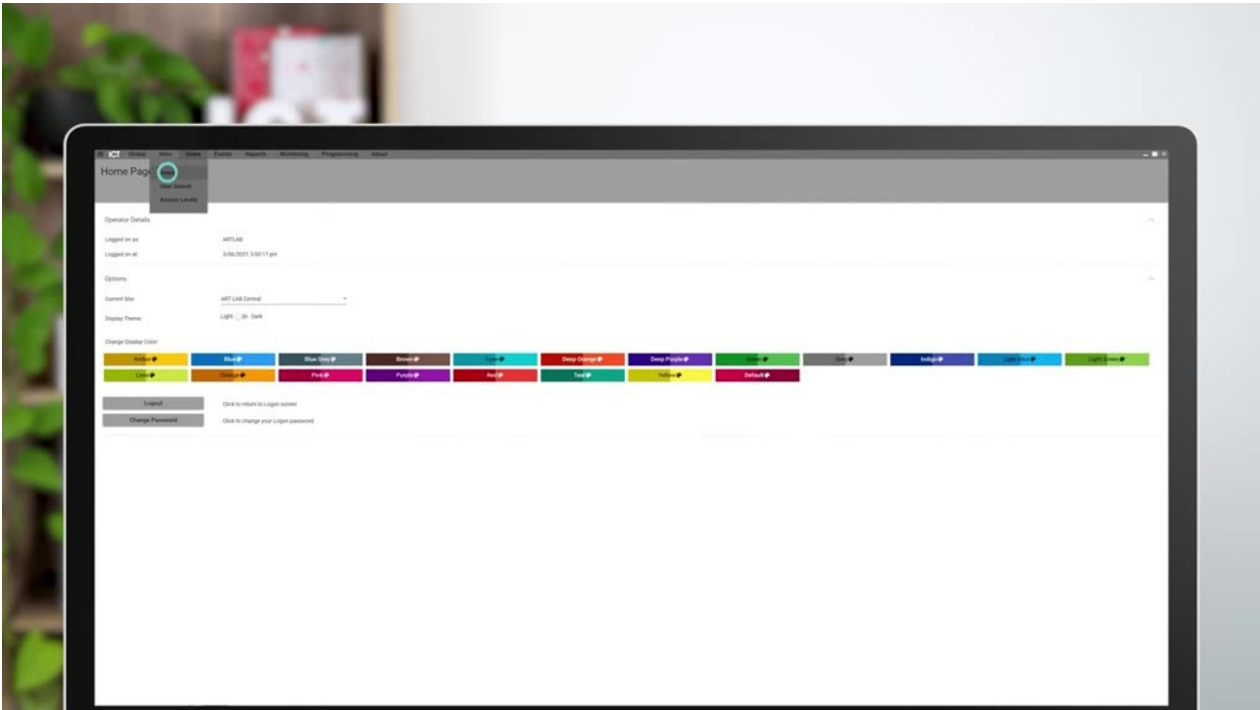


Figure 1 — Users menu in an official ICT video. The exact icon layout may differ on GX 4.3.402.

VERIFY	The name, second identifier, credential, and assigned access levels all match the intended person.
UNDO	No undo is needed; this procedure is read-only.
WATCH FOR	A duplicate name, wrong Site, hidden additional access level, expired credential, or disabled user.

Source: [ICT Protege GX Operator Reference Manual \(18 Dec 2025\), pp. 20–22 and 114–120](#) • [ICT Protege GX End User Guide \(30 Jul 2025\), pp. 11–14](#)

2. Add a new user with one fob

AMBER • REVERSIBLE CHANGE

WHAT THIS DOES

Creates a person, records the fob number, and gives the person an already-approved access level.

Use this when: A new resident or employee has an approved fob and an approved access package.

Before you click

- Have the person's exact name and the printed Facility/Card numbers—or your approved enrollment method.
- Know the single approved access level. Do not guess from a similar person.
- Know whether start/end dates are required for temporary access.
- Use a training/test user first if this is your first live entry.

MENU PATH

Users → Users → Add

Exact steps

1. Open Users → Users.
2. Click Add once.
3. Enter First name and Last name. Complete Display name if your site uses it.
4. Enter a PIN only if the approved access method requires one.
5. Enter the credential's Facility number and Card number in one available credential row.
6. For temporary access, set an approved start and end date/time. Otherwise leave dates according to site policy.
7. Open the Access levels tab.
8. Click Add, select the approved access level, and click OK.
9. Recheck name, credential digits, dates, and access level.
10. Click Save once and allow the normal controller download/synchronization to complete.

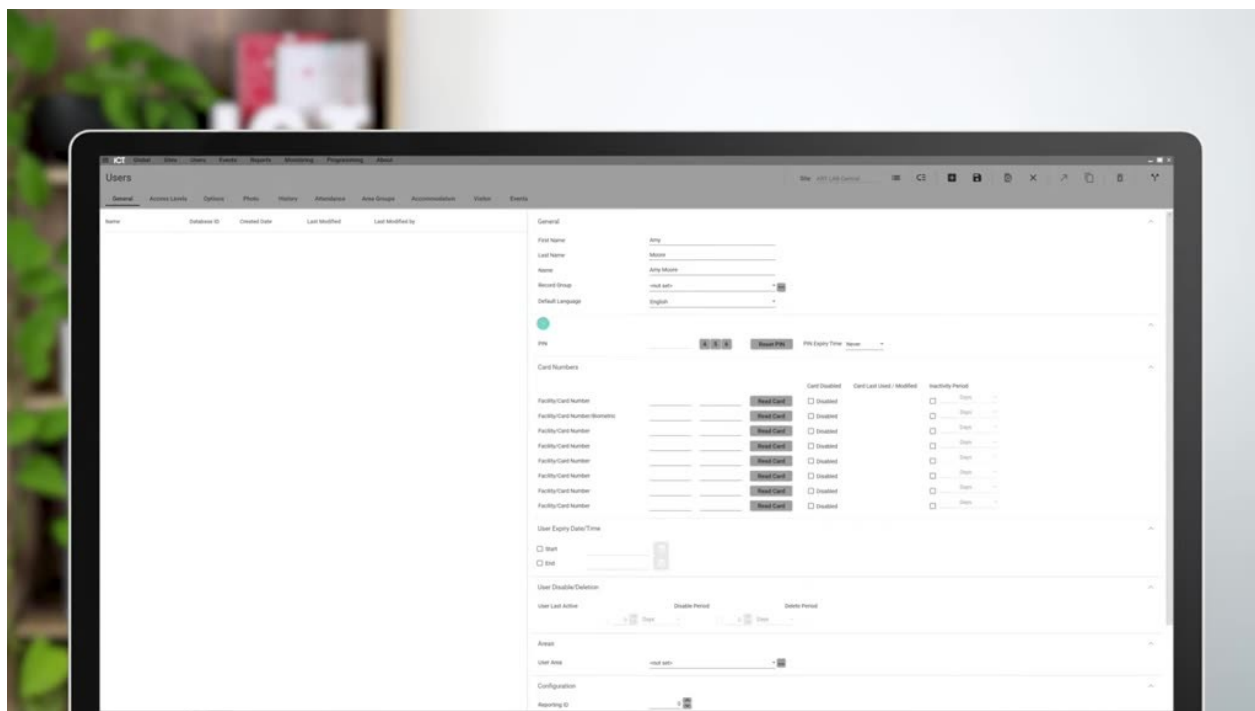


Figure 2 — General tab with identity and credential fields. Official ICT video capture.

VERIFY	Refresh and reopen the user. Test one allowed door and one door that should remain denied. Confirm the access result in Events.
UNDO	If the wrong fob was entered, immediately mark that credential Card disabled, save, then correct it. If the wrong access level was added, add the correct one first, test, then remove the wrong one.
WATCH FOR	Transposed facility/card digits, a duplicate user record, no access level, wrong Site, no end date for a contractor, or an access level that contains broader doors/floors than its name suggests.

Source: [ICT Protege GX Setup Guide \(15 Jul 2026\), pp. 23–24](#) • [ICT Protege GX Operator Reference Manual \(18 Dec 2025\), pp. 114–120](#) • [Official ICT video: Adding a User in Protege GX, 0:48–1:52](#)

The screenshot displays the ICT Protege GX desktop client interface. The top navigation bar includes tabs for Sites, Users, Events, Reports, Monitoring, Salto, Programming, Groups, Expanders, Visitor, Automation, and About. The 'Users' tab is selected, and the 'Access Levels' sub-tab is active. The main window shows a list of access levels for a user named 'Admin'. The list includes columns for Database ID, Created Date, Last Modified, and Last Modified by. The 'Access Levels' panel on the right shows a table with columns for Name, Access Level Expires, Expiry Start, Expiry End, and Schedule. Two access levels are listed: 'SCI Student Access' and 'Carpark Access'. A red circular callout on the right side of the screen contains the text: 'To assign the access level to a user, head to the **Users** menu'.

Database ID	Created Date	Last Modified	Last Modified by
40	5/07/2015 11:21:59 am	17/09/2019 12:09:40 pm	Admin
41	5/07/2015 11:26:42 am	17/09/2019 12:10:01 pm	Admin
42	5/07/2015 11:56:10 am	17/09/2019 12:11:56 pm	Admin
43	5/07/2015 11:57:24 am	11/09/2019 1:37:58 pm	Admin
44	5/07/2015 11:57:34 am	11/09/2019 1:37:58 pm	Admin
45	5/07/2015 11:57:43 am	11/09/2019 1:37:58 pm	Admin
46	5/07/2015 11:57:51 am	11/09/2019 1:49:44 pm	Admin
47	5/07/2015 11:58:01 am	17/09/2019 12:09:24 pm	Admin
48	5/07/2015 11:58:08 am	17/09/2019 11:55:54 am	Admin
49	5/07/2015 11:58:24 am	17/09/2019 11:56:00 am	Admin
51	22/12/2015 1:58:36 pm	13/04/2016 9:53:44 am	Admin
52	22/12/2015 1:59:12 pm	13/04/2016 9:53:44 am	Admin
53	22/12/2015 1:59:34 pm	13/04/2016 9:53:44 am	Admin
54	22/12/2015 1:59:56 pm	13/04/2016 9:53:44 am	Admin
55	22/12/2015 2:00:32 pm	13/04/2016 9:53:44 am	Admin
56	22/12/2015 2:00:57 pm	13/04/2016 9:53:44 am	Admin
57	22/12/2015 2:01:17 pm	13/04/2016 9:53:44 am	Admin
58	22/12/2015 2:03:06 pm	13/04/2016 9:53:44 am	Admin
59	22/12/2015 2:03:28 pm	13/04/2016 9:53:44 am	Admin
60	22/12/2015 2:03:49 pm	13/04/2016 9:53:44 am	Admin
61	22/12/2015 2:04:10 pm	13/04/2016 9:53:44 am	Admin
62	22/12/2015 2:04:40 pm	13/04/2016 9:53:44 am	Admin

Name	Access Level Expires	Expiry Start	Expiry End	Schedule
SCI Student Access	☐	1/01/2012 12:00:00 am	1/01/2012 12:00:00 am	Always
Carpark Access	☐	13/04/2016 12:00:00 am	13/04/2016 12:00:00 am	Always

To assign the access level to a user, head to the **Users** menu

Figure 3 — Open the user's Access Levels tab, then Add an approved level.

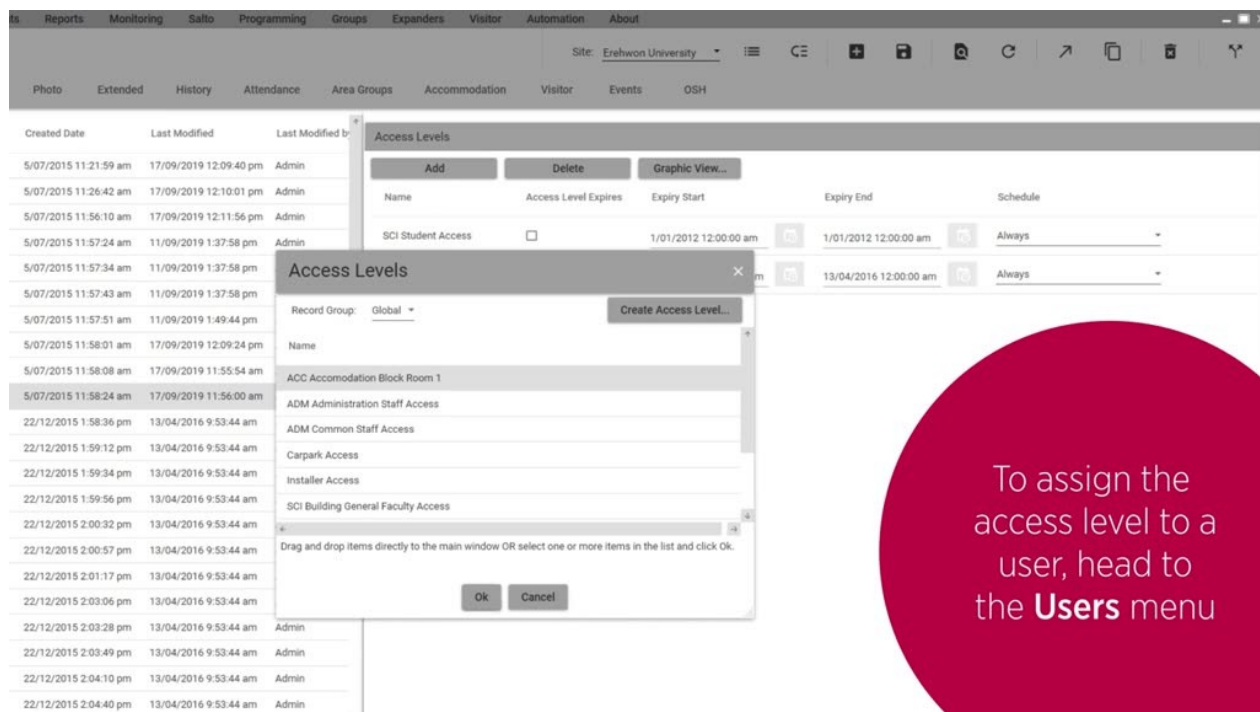


Figure 4 — Select the approved access level and confirm. Do not choose by name alone if your site has similarly named records.

3. Add a user from an unknown/raw fob read

AMBER • REVERSIBLE CHANGE

WHAT THIS DOES

Uses a live 'Read Raw Data' event to start a user record when the fob number is not printed or known.

Use this when: Your approved enrollment method is to present the fob at a reader and capture its raw event.

Before you click

- Use only the designated enrollment reader and confirm nobody else is presenting a credential.
- Have the user's identity and approved access level ready.
- If you cannot see the right-click action, your operator role may not permit it.

MENU PATH

Monitoring → Status Page View → right-click Read Raw Data event

Exact steps

1. Open Monitoring → Status Page View and choose the status page containing the reader's event window.
2. Present the new fob once at the approved reader.
3. Find the newest Read Raw Data event and confirm its time and reader.
4. Right-click that event and choose Add new user.
5. Open the new user record if it does not open automatically.
6. Enter the person's name and required dates.
7. Open Access levels, add the approved level, and Save.
8. Test and verify in Events.

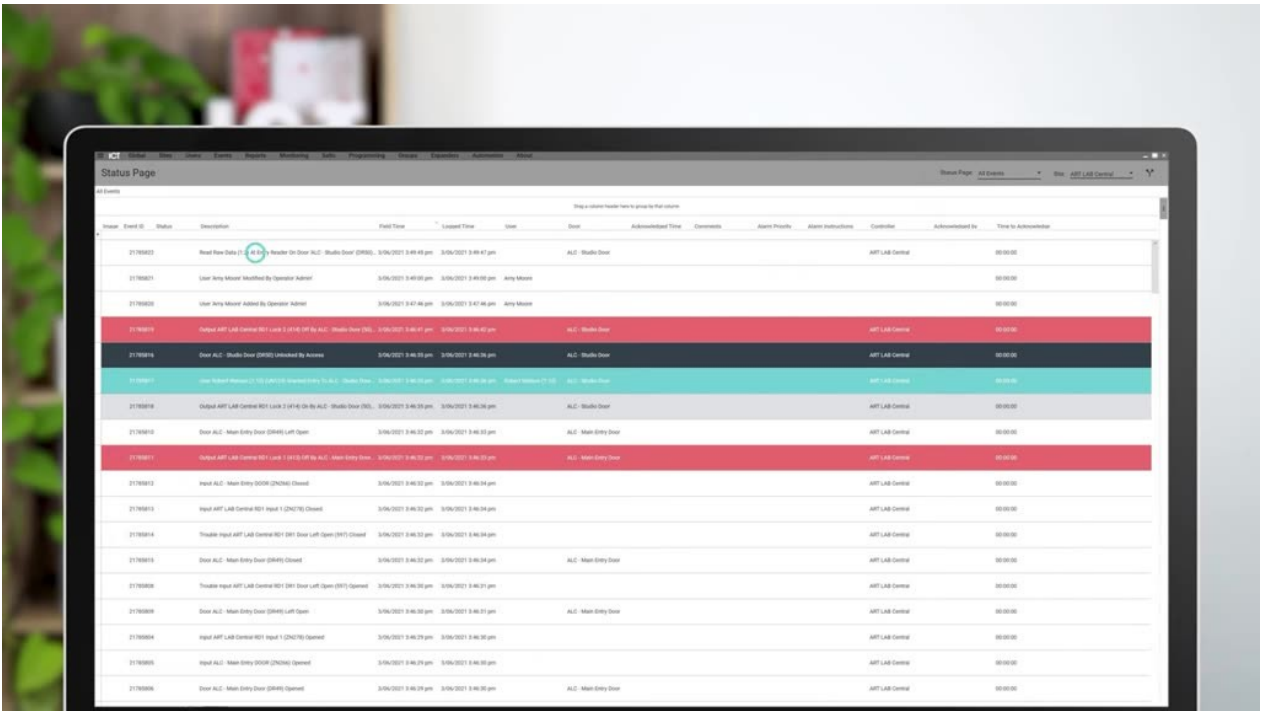


Figure 5 — Status page/event method shown in the official ICT Adding a User video.

VERIFY	The new user shows the credential captured from the event and receives only the approved access.
UNDO	Disable the captured credential immediately if the wrong read was selected, then repeat with a clean event window.
WATCH FOR	Selecting an older raw event, using the wrong reader, another person badging at the same moment, or forgetting the access level.

Source: [Official ICT video: Adding a User in Protege GX, 2:08–3:12](#) • [ICT Protege GX Operator Reference Manual \(18 Dec 2025\)](#), p. 114

4. Change a user’s access level

AMBER • REVERSIBLE CHANGE

WHAT THIS DOES

Changes the reusable permission packages assigned to one person.

Use this when: A person moves roles, changes suite/floor, or needs approved temporary access.

Before you click

- Confirm the target access level is approved and already exists.
- Read every currently assigned level. One remaining level may still grant the same door or floor.
- If removing access, identify the exact door/floor that must become denied.

MENU PATH	Users → Users → select user → Access levels
-----------	---

Exact steps

1. Find and confirm the correct user.
2. Open the Access levels tab.
3. To grant new access, click Add, select the approved level, and click OK.
4. Save, wait for synchronization, and test the new allowed door/floor.
5. Return to the Access levels tab.
6. Select the old level that is no longer approved and click Remove—not Delete.
7. Save again.
8. Test both an allowed location and the location that should now be denied.

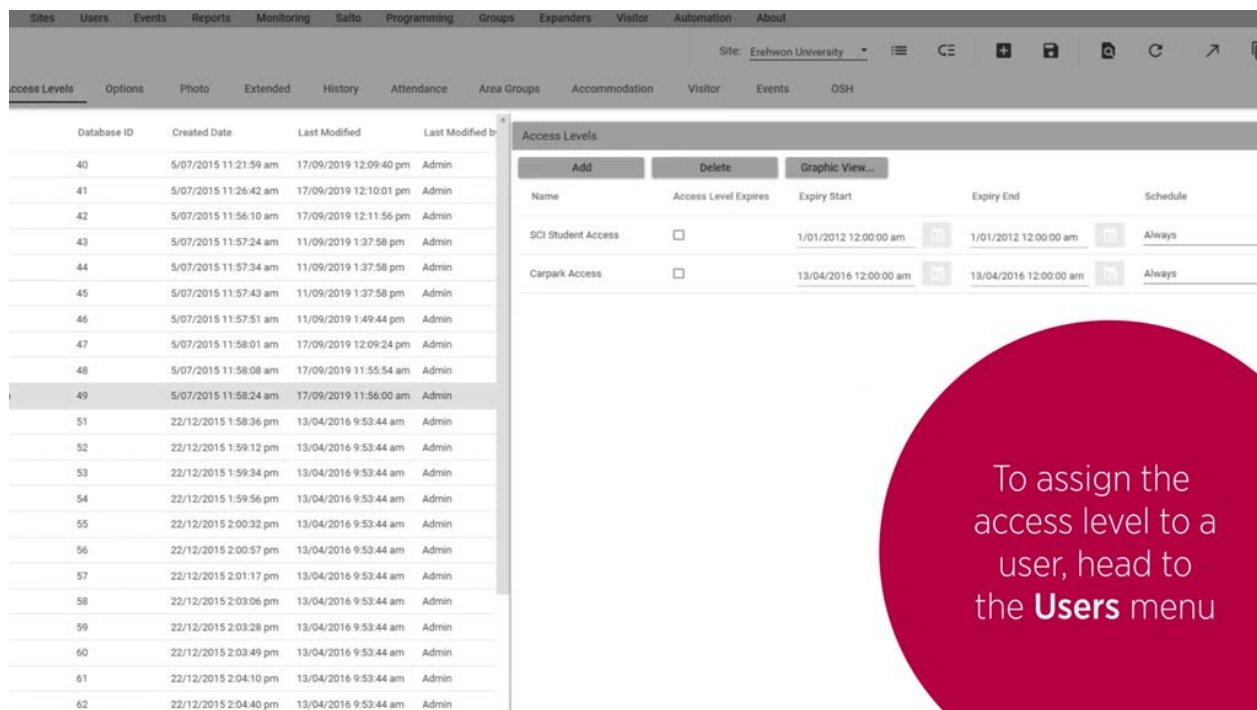


Figure 6 — User-level assignment screen. Remove the row from this user; do not delete the shared access-level record.

VERIFY	The Access levels list contains only approved levels. A granted test succeeds and a revoked door/floor is denied. Events names the expected access level.
UNDO	Re-add the prior approved level if rollback is authorized, Save, and retest.
WATCH FOR	Deleting the shared access-level record, removing one level while another still grants access, or skipping the denied test.

source: [ICT Protege GX Operator Reference Manual \(18 Dec 2025\)](#), pp. 118 and 128–132 • [Official ICT video: Configuring a Basic Access Level, 0:52–1:07](#)

5. Remove fob access: choose the right action

DO NOT TREAT EVERY REQUEST AS 'DELETE THE USER'

A lost fob, a suspended person, an expiring contractor, and a permanently departed person are four different cases.

CASE	SAFE ACTION	RESULT	RISK
One lost/stolen fob	Mark Card disabled for that credential row.	Other credentials on the user can keep working.	Amber
Temporarily stop all access	Open Options and enable Disable user.	The person and credentials stay on file; all access stops.	Amber
Access ends at a known time	Set the user end date/time or approved access-level expiry.	Access stops automatically; verify the time zone.	Amber
Permanent authorized removal	Capture evidence, then delete the user record.	Irreversible; follow retention and audit policy.	Red

Source: [ICT Protege GX End User Guide \(30 Jul 2025\), p. 14](#) • [ICT Protege GX Operator Reference Manual \(18 Dec 2025\), pp. 115–116](#)

5A. Disable one lost fob

AMBER • REVERSIBLE CHANGE

WHAT THIS DOES

Stops one credential while preserving the person and any other approved credentials.

Use this when: A person has lost one fob but may still use another credential.

Before you click

- Confirm exactly which fob is lost; compare facility/card number if known.
- Check whether the user has more than one credential row.
- Record the report time and person authorizing the disable.

MENU PATH

Users → Users → select user → General → credential row

Exact steps

1. Find and confirm the correct user.
2. Locate the exact credential row.
3. Enable Card disabled for that credential.
4. Do not clear or replace the numbers unless your site policy requires it.
5. Click Save and wait for normal synchronization.
6. Test the lost credential if it is available, or confirm a denied event when it is next presented.

VERIFY

The credential remains recorded but is marked disabled; Events shows it denied if presented.

UNDO	Clear Card disabled only after the fob is recovered and reactivation is authorized; Save and test.
WATCH FOR	Disabling the wrong credential row, disabling the whole user, or issuing a replacement without disabling the lost fob.

Source: [ICT Protege GX Operator Reference Manual \(18 Dec 2025\), pp. 115–116](#) • [ICT Protege GX End User Guide \(30 Jul 2025\), p. 14](#)

5B. Disable the whole user or set an end time

AMBER • REVERSIBLE CHANGE

WHAT THIS DOES

Stops every credential for one user now, or at a defined future time, while preserving the record.

Use this when: A person is suspended, a contractor's shift ends, or access is temporary.

Before you click

- Confirm whether access stops immediately or at a specific local date/time.
- Check whether the person has multiple credentials and access levels.
- Confirm the system/site time zone and daylight-saving behavior.

MENU PATH

Users → Users → select user → Options / General dates

Exact steps

1. Find and confirm the correct user.
2. For an immediate stop, open Options and enable Disable user.
3. For a scheduled stop, set the approved user end date/time instead.
4. Click Save.
5. Refresh and reopen the user.
6. Test at the correct time and check Events.

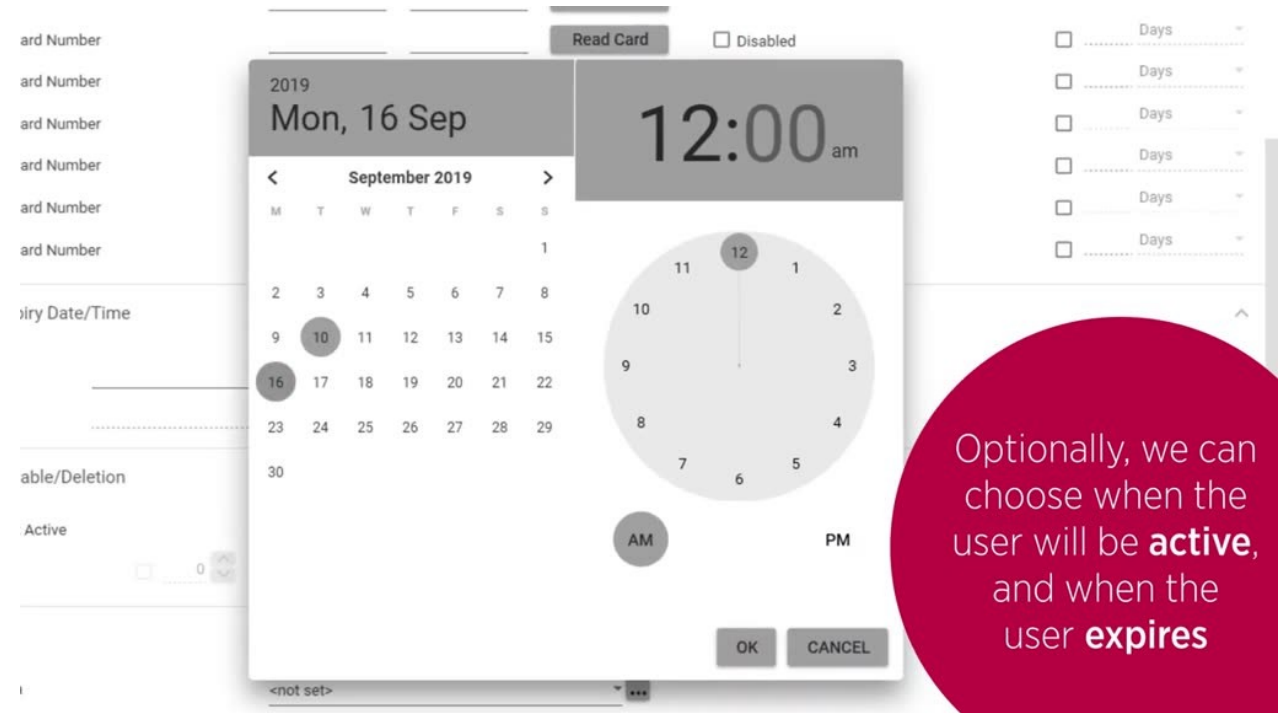


Figure 7 — Date selection in the official ICT user-management video. Confirm local date and time before saving.

VERIFY	All credentials for the user are denied now—or become denied at the approved end time.
UNDO	Clear Disable user or change the end time only with authorization, then Save and retest.
WATCH FOR	Using a server-time assumption, changing only one access level while another remains valid, or forgetting to document reactivation.

Source: [ICT Protege GX Operator Reference Manual \(18 Dec 2025\), pp. 115–116](#) • [ICT Protege GX End User Guide \(30 Jul 2025\), p. 14](#)

6. Delete a user permanently

RED • SHARED OR HIGH IMPACT

WHAT THIS DOES

Removes the user record. This is not the recommended first response to a lost fob or temporary suspension.

Use this when: Retention policy permits deletion and an authorized person has confirmed the record is no longer needed.

Before you click

- Prefer Disable user until permanent deletion is confirmed.
- Capture the record, access levels, credential numbers, relevant Events, and History according to policy.
- Select exactly one user and reconfirm the name plus second identifier.
- Never use this routine on an access level, schedule, group, door, floor, or elevator record.

MENU PATH	Users → Users → select exactly one record → Delete
-----------	--

Exact steps

1. Find and confirm the correct user.
2. Open History and Usage if available; retain required evidence.
3. Return to the user list and ensure only one row is selected.
4. Re-read the name and credential immediately before deleting.
5. Click Delete on the toolbar.
6. Read the confirmation/impact prompt and confirm only if it names the intended user.
7. Search again to confirm the record no longer appears.
8. Present the credential at a test location if available and verify it is denied.

VERIFY	The user no longer appears, the credential is denied, and an operator/audit event records the deletion.
UNDO	Deletion is not a routine undo. Restore requires your approved backup/retention process or recreating the user from authorized evidence.
WATCH FOR	Deleting a shared programming record, multiple selected rows, confusing Copy with duplication, or deleting before retaining audit evidence.

Source: [ICT Protege GX End User Guide \(30 Jul 2025\), p. 14](#) • [ICT Protege GX Operator Reference Manual \(18 Dec 2025\), pp. 20–22 and 114–116](#)

7. Temporarily unlock a door

AMBER • REVERSIBLE CHANGE

WHAT THIS DOES

Releases one door for its programmed lock activation time. It is not the same as leaving the door unlocked.

Use this when: An authorized visitor, delivery, or staff member needs one supervised entry.

Before you click

- Confirm the exact door by name and live status.
- Confirm visual/CCTV or voice authorization under your local SOP.
- Check that the command is Unlock—not Unlock latched and not a lockdown command.
- If right-click commands are absent, the door may not support manual commands or your operator role lacks permission.

MENU PATH **Programming → Doors, or Monitoring → Status Page/Floor Plan → right-click door**

Exact steps

1. Open the approved status page/floor plan, or Programming → Doors.
2. Select or right-click the exact door.
3. Choose Unlock.
4. Watch the live state change and supervise the entry.

5. Wait for the programmed lock activation time to expire.
6. Confirm the door returns to Locked/Secure and physically closes.
7. Open View recent events or the event window and verify the operator command and restore.

- **Flash when unlocked by key:** With this option enabled, the reader will flash blue three times when the door is unlocked with a key. This occurs when the door latch is fully retracted (not when the deadbolt is retracted).
- **Allow emergency opening:** Enable this option to allow operators to send the **Emergency open** manual command to the door. An authorized config app user can retrieve the command from an update point reader and use it to unlock the door once. This allows a building manager to open the door when the owner or tenant locks themselves out, but does not grant them permanent access.
- **Exit leaves door unlocked time period:** When the lock is in Exit leaves door unlocked or Exit leaves door unlocked + toggle mode (**Programming | Door types | Options**), by default when someone exits the door will remain unlocked until a user badges a credential to relock it. With this option enabled, the door will automatically lock when the defined period expires. It can still be manually relocked by badging a credential.
- **Schedule operates late to open:** When this option is enabled the door will not latch unlock on schedule until a user unlocks the door. This can be used to prevent the door from automatically unlocking on days when nobody arrives on site.

Advanced options

- **Lock activation time:** Determines the length of time (in seconds) that the door will unlock for when a user is granted access. This does not apply in modes that toggle the lock.
- **Door extended access time:** When a user with **User operates extended door access function** enabled (**Users | Users | Options**) unlocks this door, it will be unlocked for this period instead of the standard lock activation time.

Manual Door Commands

Right clicking a door record in **Programming | Doors** or a door icon on a floor plan or status page opens a menu with manual commands for that door.

Door control

These commands allow you to control basic door functionality. The available commands are:

- **Lock**
- **Unlock** (temporarily activate the lock)
- **Unlock latched** (activate the lock and keep the door unlocked)

Door lockdown

These commands allow you to lock down individual doors. Any lockdown command will lock the door regardless of any other function causing it to be unlocked. Some lockdown modes allow entry or exit with valid credentials or REX/REN, while others deny access. The available commands are:

- **Allow entry**
- **Allow exit**
- **Allow entry and exit**
- **Deny entry and exit**
- **Clear** (remove the lockdown from the door)

To implement automatic lockdown procedures across multiple doors, use **Door control** programmable functions (**Automation | Programmable functions**).

View recent events

This command automatically runs an event search in a breakout window, showing all recent events for this door.

For sorting, grouping, filtering and exporting this report, see [Viewing Reports](#) (see page 167).

Figure 8 — Official Operator Reference Manual p. 211: Lock, Unlock, Unlock latched, and separate lockdown commands.

VERIFY	Live status and Events show the intended door unlocked temporarily and returned to the secure state.
UNDO	If it remains open, choose Lock, confirm the door closes, and escalate a mechanical/door-held condition.
WATCH FOR	Choosing Unlock latched, confusing Lock with Lockdown, unlocking the wrong similarly named door, or assuming a closed door is electrically locked.

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

8. Lock a temporarily or latched-unlocked door again

AMBER • REVERSIBLE CHANGE

WHAT THIS DOES

Sends a normal Lock command. It does not create an emergency lockdown.

Use this when: A door was manually unlocked and must return to normal secure operation.

Before you click

- Confirm nobody is in the door path and egress remains safe.
- Check whether an unlock schedule is currently valid; it may unlock the door again.
- Do not choose a lockdown command unless following the emergency SOP.

MENU PATH

Monitoring → Status Page/Floor Plan → right-click door → Lock

Exact steps

1. Right-click the exact door.
2. Choose Lock.
3. Watch live status and confirm the lock state changes.
4. Physically confirm the door closes and latches.
5. Check Events for the operator command.
6. If the door immediately unlocks again, check its Unlock schedule and options; escalate rather than repeatedly commanding Lock.

VERIFY	Door status is secure, the physical latch holds, and the event log records the normal Lock command.
UNDO	If a normal Unlock is authorized, use Unlock. Do not use Clear unless you are intentionally clearing an active lockdown.
WATCH FOR	Using Lockdown instead of Lock, using Clear as a normal unlock, or fighting a valid enforced schedule.

Source: [ICT Protege GX Operator Reference Manual \(18 Dec 2025\), pp. 199 and 211](#)

9. Verify every change

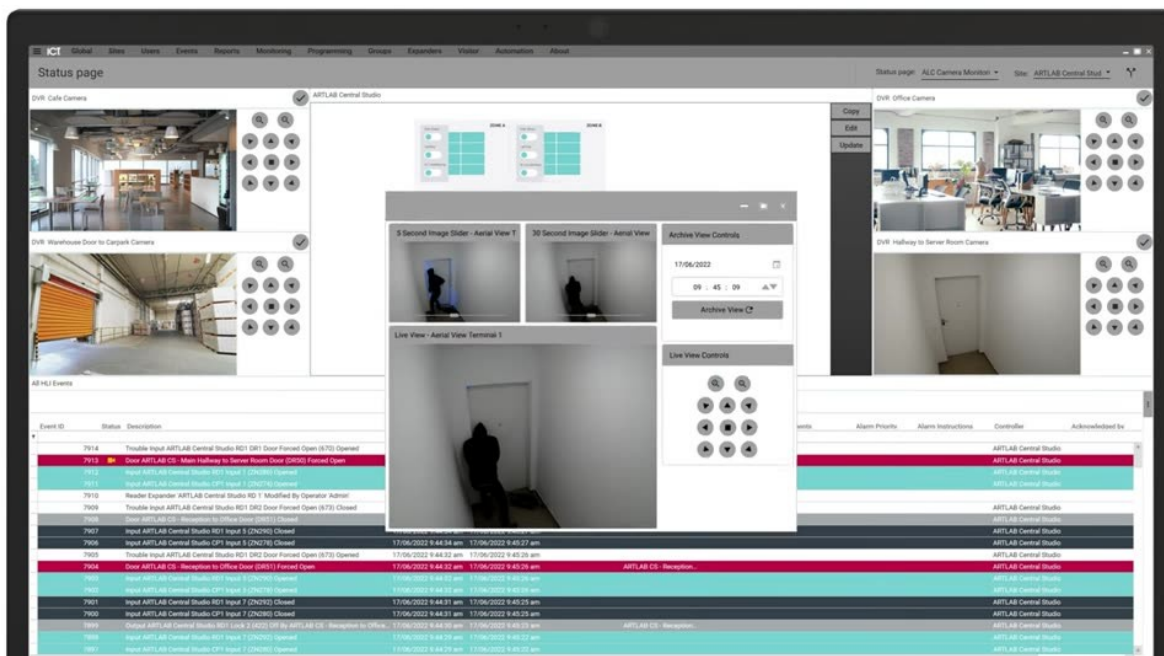


Figure 9 — A finished ICT status page can combine cameras, floor plans, live events, and device status.

1. Refresh and reopen the record; never rely only on the Save click.
2. Confirm the controller's normal download/synchronization completes.
3. Test one action that should be allowed.
4. Test one action that should be denied.
5. Open Reports → Events, choose the approved report, set the time range, and Run.
6. Filter by the exact user, credential, or door.
7. Read the reason and access level named in the event.
8. Capture/export evidence only if policy permits personal-access data to be retained.



10. Safe troubleshooting

Internal training guide • Verify against your site SOP • 17

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.