

AN-191

Programming Operator Roles in Protege GX

Application Note



The specifications and descriptions of products and services contained in this document were correct at the time of printing. Integrated Control Technology Limited reserves the right to change specifications or withdraw products without notice. No part of this document may be reproduced, photocopied, or transmitted in any form or by any means (electronic or mechanical), for any purpose, without the express written permission of Integrated Control Technology Limited. Designed and manufactured by Integrated Control Technology Limited, Protege® and the Protege® Logo are registered trademarks of Integrated Control Technology Limited. All other brand or product names are trademarks or registered trademarks of their respective holders.

Copyright © Integrated Control Technology Limited 2003-2025. All rights reserved.

Last Published: 30-Jul-25 3:41 PM

Contents

| | |
|----------------------------------|----|
| Introduction | 4 |
| Programming Roles | 5 |
| Programming Basic Roles | 5 |
| Programming Complex Roles | 5 |
| Example: HR Operator | 7 |
| Example: Security Guard Operator | 8 |
| Reference Tables | 10 |
| Role Presets and Tables | 10 |
| Security Level Tables | 14 |
| Security Level Manual Commands | 17 |

Introduction

Roles in Protege GX determine what each operator has permission to see and do in the software. They define which items in the Protege GX menu are visible, enabling you to limit access to specific functions and records based on the requirements of the operator. For example, operators in an HR position are typically granted full access to view and edit users and run reports on access data, but denied permission to records related to the physical operation of the site such as doors and outputs.

This document provides instructions and programming examples for creating roles in Protege GX. It also includes detailed reference tables to help you select and modify role presets and security levels.

Programming Roles

When creating a role in **Global | Roles**, you start by assigning one of the four presets:

- **Administrator** or **Installer**: Can perform all actions in the system without any restrictions.
- **End user**: Can perform most actions related to user access and scheduling. Can view status pages and floor plans and run event reports.
- **Guard**: Can view status pages and floor plans and run event reports.

You can then refine the permissions for that specific role by adjusting the settings in the other tabs:

- **Tables**: The menu items and functions available to the operator. By default these are set to Inherit from preset. You can modify each table to Deny, Grant full access or Grant read only access.
- **Sites**: By default the operator has access to all sites. You can enable or disable access to each site individually.
- **Security levels**: To further refine the operator's permissions, you can set the security level within a site or record group. Security levels (**Sites | Security levels**) provide a more granular breakdown of the functions that are available to the operator. This also allows you to restrict the operator to one or more record groups, which may represent different regions or companies within the Protege GX system.
- **Display**: This tab provides options for alarm and camera popups. You can disable popups for operators who are not expected to respond to incidents, set the frequency of alarm notifications and the rules for disabling or delaying them.

Before you begin, it is useful to review the [Reference Tables](#) section to get an idea of the default settings for each preset and the permissions granted by the options in the role and security level.

If you are editing a role, any changes to the menu will not take effect until the next time that operator logs in.

Programming Basic Roles

Basic roles use a role record but not a security level. They are useful where the broad groups of permissions provided by the role tables are sufficient.

To program a basic role:

1. Determine what permissions are needed by the operator.
2. In **Global | Roles**, add a new role.
3. Select a **Preset** to determine the base access rights.
4. If you need to change the default permissions granted by the preset, modify the settings in the **Tables** tab.
5. The role has access to all sites by default. If you need to restrict access:
 - In the **Sites** tab, disable **Has access to all sites**.
 - Select **Active** next to the sites the operator will have access to.
6. In the **Display** tab, set the operator's alarm and camera popup options.
7. Save the role.
8. In **Global | Operators**, select or create an operator record. Set the **Role** to the new role you have created.

Programming Complex Roles

Complex roles use security levels to achieve more precise control over the operator's permissions. They are required when the tables provided in the role programming are too broad. For example, the **Controller programming windows** table in the role groups together a large number of different permissions which can be adjusted separately via a security level. They must also be used when access needs to be restricted by record group.

To program a complex role with a security level:

1. Determine what permissions are needed by the operator.
2. In **Sites | Security levels**, add a new security level.
3. In the **Tables** tab, modify the permissions for each table to override the settings from the role.
4. In the **Manual commands** tab, set the operator's permissions for manual commands such as locking and unlocking doors. By default these are inherited from the **Manual commands** setting in the role.
For areas, doors, elevators, floors, keypads and outputs you can select a specific group that the operator will be allowed to control. If no group is selected, the operator can control all records of that type.
5. Save the security level.
6. In **Global | Roles**, add a new role.
7. Select a **Preset** to determine the base access rights.
8. The role has access to all sites by default. If you need to restrict access:
 - In the **Sites** tab, disable **Has access to all sites**.
 - Select **Active** next to the sites the operator will have access to.
9. In the **Security levels** tab, click **Add**.
 - Select the relevant **Site**.
 - Select the **Security level** that you just created.
 - Select one or more record groups that the operator will have access to, or enable **Access all record groups**.

Record groups on the same site must have the **same** security level. Record groups on different sites may have different security levels.
10. In the **Display** tab, set the operator's alarm and camera popup options.
11. Save the role.
12. In **Global | Operators**, select or create an operator record. Set the **Role** to the new role you have created.

Example: HR Operator

As an example of a basic role, we will demonstrate how to program an operator record for a member of human resources on a small, single-location Protege GX site.

First, we must assess how the employee will be using Protege GX, and therefore what records they need access to.

- This employee's role involves adding new staff members to the system, assigning credentials and access levels and running reports on users.
- They do not need access to view, program or control any of the site's hardware or schedules.
- They do not need to respond to alarms or camera popups.

As a starting point, we will use the End User preset. This preset has permission to add and edit users and access levels, but also allows some other operations which this operator does not need (see page 10). We need to remove some permissions from the role.

Programming Steps

First, create the role:

1. Navigate to **Global | Roles** and add a new role with the name Human Resources.
2. Set the **Preset** to End user.
3. In the **Tables** tab, set the following tables to Deny:
 - Holidays
 - Record groups
 - Schedules
 - Credential types
 - Controller programming windows
 - Floor plans
 - Status pages
 - Event reports

All other tables can be left as Inherit from preset.

4. In the **Display** tab, disable the following:
 - Pop up while alarms present
 - Allow camera popup

5. Click **Save**.

Then, create an operator who will use this role:

1. Navigate to **Global | Operators** and add a new operator called Gianna Pistrucci.
2. Set the **Username** and **Password** to unique values. Ensure that you use a strong password or pass phrase.
3. Set the **Role** to Human Resources.
4. Check **Enable operator timeout** and set the **Operator timeout in seconds** to 600 (10 minutes). If the operator is not active for this length of time, the Protege GX client will give a 30 second warning and then close.
5. Click **Save**.

To test the programming, open a new Protege GX client and log in as the HR operator. Ensure that you can see and control only the records that have been specified in the job description.

Status lists are available by default without a security level. This is a known issue.

Example: Security Guard Operator

As an example of a complex role, we will demonstrate how to program an operator record for a security guard in a large Protege GX system with multiple sites and regions.

First, we must assess how the security guard will be using Protege GX, and therefore what records they need access to.

- The guard is employed by ACME Incorporated, and should therefore be restricted to viewing records on the ACME site.
- The guard is responsible for monitoring only ACME's Singapore location. They should be restricted to viewing records in the *Singapore* record group.
- The guard's duties include:
 - Monitoring door and area status from a floor plan or status page.
 - Monitoring events and security camera footage.
 - Controlling doors and areas from the Protege GX software. However, they are not permitted to bypass inputs.
 - Comparing user photos to the users entering the building. However, they are not permitted to add or edit user records.

As a starting point, we will use the *Guard* role preset. This preset has permission to view status pages, floor plans and event reports, but few other permissions (see page 10). This allows us to add only what is required for this particular operator.

Programming Steps

Before we begin, it is assumed that the *ACME* site and *Singapore* record group already exist, and that the record group has been applied to the relevant records (including status pages and floor plans).

Because the guard's access must be restricted to a specific record group, we need to create a *security level*. The security level also determines how this operator's access differs from the standard *Guard* preset.

1. In Protege GX, navigate to **Sites | Security levels**.
2. In the toolbar, set the **Site** to *ACME*.
3. Add a new security level with the name *Security Guard (ACME)*.
4. The **Tables** tab allows you to set the access individually for each record type.
 - Most records can be left as *Inherit from role* to retain the settings from the *Guard* preset.
 - The **Users** table should be set to *Grant Read Only Access*. This overrides the setting from the role preset (no user access permitted).
5. The **Manual commands** tab allows you to set whether the guard can control each type of device.
 - Most records can be left as *Inherit from role*. The *Guard* preset is permitted to control doors and areas from a status page by default.
 - Set **Input control** to *Deny*. This will prevent the guard from bypassing inputs.
6. Click **Save**.

Now we can apply the security level to a role:

1. Navigate to **Global | Roles** and add a new role with the name *Security Guard (ACME Singapore)*.
2. Set the **Preset** to *Guard*.
3. Open the **Sites** tab and uncheck **Has access to all sites**.
4. Check the box next to the *ACME* site. This ensures that the operator only has access to records in this site.
5. Open the **Security levels** tab and click **Add**.

- Set the **Site** to ACME.
- Set the **Security level** to Security Guard (ACME).
- Select the Singapore record group.
- Click **Ok**.

6. Keep the default settings in the **Display** tab.

7. Click **Save**.

Finally, we must create an operator who uses the new role:

1. Navigate to **Global | Operators** and add a new operator called Zhang San (ACME Singapore).
2. Set the **Username** and **Password** to unique values. Ensure that you use a strong password or pass phrase.
3. Set the **Role** to Security Guard (ACME Singapore).
4. Set the **Time Zone** to GMT+08:00 Singapore Standard Time Singapore.
5. Ensure that **Show PIN numbers for users** is disabled. This ensures that the guard cannot see users' PIN codes.
6. Check **Enable operator timeout** and set the **Operator timeout in seconds** to 600 (10 minutes). If the operator is not active for this length of time, the Protege GX client will give a 30 second warning and then close.
7. Click **Save**.

To test the programming, open a new Protege GX client and log in as the guard operator. Ensure that you can see and control only the records which have been specified in the job description above. For example, the guard should be able to view only user records in the Singapore record group (excluding their PIN codes), and should not be able to edit them.

Reference Tables

Role Presets and Tables

When programming a basic role, you begin from a role preset with fixed permissions then customize the role's permissions to each specific table. Each table in the role controls access to one or more menu items in the software (or another software feature such as manual commands).

This reference table contains the following information:

- What permissions are granted/denied by each role table.
- The default permissions for the End User and Guard presets. The Administrator and Installer presets have full access to everything by default.



= Read and edit access by default



= Read only access by default



= Access denied by default



All roles have access to the **Visitor** and **About** menus by default.

| Table | Permissions | End User | Guard |
|----------------------|---|----------|-------|
| Global tables | | | |
| Sites | <ul style="list-style-type: none">Global Sites | ✕ | ✕ |
| Operators | <ul style="list-style-type: none">Global OperatorsReports Central station reportReports Operator permission report <p>Requires access to User reports.</p> | ✕ | ✕ |
| Roles | <ul style="list-style-type: none">Global Roles | ✕ | ✕ |
| Event servers | <ul style="list-style-type: none">Global Event server | ✕ | ✕ |
| Download servers | <ul style="list-style-type: none">Global Download server | ✕ | ✕ |
| Device states | Not used. | | |
| Event logs | <ul style="list-style-type: none">Salto Salto log <p>Requires access to Salto programming windows.</p> | ✕ | ✕ |
| System | <ul style="list-style-type: none">Global Global settingsGlobal Color maps <p>Not available for End User or Guard presets.</p> <ul style="list-style-type: none">Global Floor plan symbols <p>Not available for End User or Guard presets.</p> <ul style="list-style-type: none">Global Event types <p>Not available for End User or Guard presets.</p> | ✕ | ✕ |

| Table | Permissions | End User | Guard |
|----------------------|--|----------|-------|
| Modems | <ul style="list-style-type: none"> Global Modem (not used) | ✕ | ✕ |
| Event types | Not used. | | |
| Site tables | | | |
| Access levels | <ul style="list-style-type: none"> Users Access levels | ✓ | ✕ |
| Alarms | <ul style="list-style-type: none"> Events Alarms | ✕ | ✕ |
| Card template editor | <ul style="list-style-type: none"> Users Card template editor | ✕ | ✕ |
| Custom fields | <ul style="list-style-type: none"> Users Custom fields Users Custom field tabs | ✓ | ✕ |
| Door groups | <ul style="list-style-type: none"> Groups Door groups | ✕ | ✕ |
| Holidays | <ul style="list-style-type: none"> Sites Holiday groups | ✓ | ✕ |
| Jobs | Not used. | | |
| Record groups | <ul style="list-style-type: none"> Sites Record groups | ✓ | ✕ |
| Schedules | <ul style="list-style-type: none"> Sites Schedules | ✓ | ✕ |
| Calendar actions | <ul style="list-style-type: none"> Sites Calendar actions | ✕ | ✕ |
| Security levels | <ul style="list-style-type: none"> Sites Security levels | ✕ | ✕ |
| Users | <ul style="list-style-type: none"> Sites Import users Sites Batch add users Users Users <p>The End User and Guard presets do not have access to edit user PIN codes without Generate PINs enabled in the security level.</p> | ✓ | ✕ |
| Credential types | <ul style="list-style-type: none"> Sites Credential types | ✓ | ✕ |
| Card profiles | <ul style="list-style-type: none"> Sites Card profiles | ✓ | ✕ |

| Table | Permissions | End User | Guard |
|--------------------------------|---|----------|-------|
| Controller programming windows | <ul style="list-style-type: none"> Sites Controllers <p>Grants access to perform all controller manual commands except for setting the date/time (see Manual commands).</p> <ul style="list-style-type: none"> Programming Doors Programming Inputs Programming Door types Programming Input types Programming Areas Programming Outputs Programming Trouble inputs Programming Elevator cars Programming Floors Programming Phone numbers Programming Services Groups Area groups Groups Keypad groups Groups Menu groups Groups Output groups Groups Elevator groups Groups Floor groups Expanders Keypads Expanders Analog expanders Expanders Input expanders Expanders Output expanders Expanders Reader expanders Automation Automation Automation Programmable functions Automation Data values Automation Variables | ✕ | ✕ |
| | <ul style="list-style-type: none"> Programming Daylight savings <p>The End User preset has access to edit daylight savings records by default.</p> | ✓ | ✕ |
| Salto programming windows | <ul style="list-style-type: none"> Salto Doors Salto Door groups Salto Calendars Salto Salto log <p>Requires access to Event logs.</p> | ✕ | ✕ |
| Smart readers | <ul style="list-style-type: none"> Expanders Smart readers | ✕ | ✕ |
| Apartments | <ul style="list-style-type: none"> Programming Apartments Programming Batch add apartments <p>Requires access to Controller programming windows.</p> | ✕ | ✕ |

| Table | Permissions | End User | Guard |
|------------------------------------|---|----------|-------|
| Function codes | <ul style="list-style-type: none"> Sites Function codes | ✗ | ✗ |
| Site monitoring and control | | | |
| Floor plans | <ul style="list-style-type: none"> Monitoring Floor plan view Monitoring Setup Floor plan editor Monitoring Setup Floor plan editor (batch) Monitoring Setup Add bulk floor plans | ✓ | ✓ |
| Status pages | <ul style="list-style-type: none"> Monitoring Status page view The role must also have access to view the status lists, event reports and other objects on the status page. Monitoring Setup Status page editor Monitoring Setup Status page editor (batch) Monitoring Setup Status lists Monitoring Setup Web links | ✓ | ✓ |
| Cameras | <ul style="list-style-type: none"> Monitoring Setup DVRs Monitoring Setup Cameras Monitoring Setup PTZ commands | ✗ | ✗ |
| Manual commands | Grants access to perform manual commands on devices. Grants access to set the controller date/time. | ✗ | ✓ |
| Acknowledge alarm | Grants access to acknowledge alarms. | ✗ | ✓ |
| Intercoms | <ul style="list-style-type: none"> Monitoring Setup Intercoms | ✗ | ✗ |
| Site reports | | | |
| Event reports | <ul style="list-style-type: none"> Events Event search Events Event filters Reports Setup Event | ✗ | ✗ |
| | <ul style="list-style-type: none"> Reports Event The Guard and End User presets have access to run event reports by default. Reports Central station report | ✓ | ✓ |
| Muster reports | <ul style="list-style-type: none"> Reports Muster Reports Central station report Reports Setup Muster | ✗ | ✗ |
| Attendance reports | <ul style="list-style-type: none"> Reports Attendance Reports Central station report Reports Setup Attendance Reports Setup Shift type | ✗ | ✗ |

| Table | Permissions | End User | Guard |
|--------------|--|---|---|
| User reports | <ul style="list-style-type: none"> Sites Jobs (not used) Sites User import job step (not used) Users User search Reports Users Reports Central station report Reports Setup User |  |  |

Security Level Tables

The tables in the security level provide more granular permissions than those in the role, enabling you to control the operator's access to specific menu items. Each security level table inherits its default setting from a parent table in the role, but when you update the setting in the security level it overrides that in the role.

This reference table contains the following information:

- The menu items and other features that each security level table provides access to.
- The parent role table that each security level table inherits from.

| Table | Permissions | Parent Role Table |
|------------------|---|--------------------------------|
| Access levels | <ul style="list-style-type: none"> Users Access levels | Access levels |
| Actions | Not used - see Event filters . | |
| Alarm priorities | Not used - see Event filters . | |
| Alarms | Not used - enable Alarms in the role. | |
| Analog expanders | <ul style="list-style-type: none"> Expanders Analog expanders | Controller programming windows |
| Apartments | <ul style="list-style-type: none"> Programming Apartments Programming Batch add apartments | Apartments |
| Area groups | <ul style="list-style-type: none"> Groups Area groups | Controller programming windows |
| Areas | <ul style="list-style-type: none"> Programming Areas | Controller programming windows |
| Automation | <ul style="list-style-type: none"> Automation Automation | Controller programming windows |
| Bit data values | Not used. | |
| Calendar actions | <ul style="list-style-type: none"> Sites Calendar actions | Calendar actions |
| Cameras | <ul style="list-style-type: none"> Monitoring Setup Cameras | Cameras |
| Card profiles | <ul style="list-style-type: none"> Sites Card profiles | Card profiles |
| Controllers | <ul style="list-style-type: none"> Sites Controllers <div>Grants access to perform all controller manual commands except for setting the date/time (see Manual commands tab).</div> | Controller programming windows |
| Credential types | <ul style="list-style-type: none"> Sites Credential types | Credential types |

| Table | Permissions | Parent Role Table |
|------------------|---|--------------------------------|
| Custom fields | <ul style="list-style-type: none"> Users Custom fields Users Custom field tabs | Custom fields |
| Data values | <ul style="list-style-type: none"> Automation Data values | Controller programming windows |
| Daylight savings | <ul style="list-style-type: none"> Programming Daylight savings | Controller programming windows |
| Door groups | <ul style="list-style-type: none"> Groups Door groups | Controller programming windows |
| Door types | <ul style="list-style-type: none"> Programming Door types | Controller programming windows |
| Doors | <ul style="list-style-type: none"> Programming Doors | Controller programming windows |
| DVRs | <ul style="list-style-type: none"> Monitoring Setup DVRs | Cameras |
| Elevator cars | <ul style="list-style-type: none"> Programming Elevator cars | Controller programming windows |
| Elevator groups | <ul style="list-style-type: none"> Groups Elevator groups | Controller programming windows |
| Event filters | <ul style="list-style-type: none"> Events Event filters Events Actions Events Alarm priorities | Event reports |
| Event groups | Not used. | |
| Event logs | <ul style="list-style-type: none"> Salto Salto log Requires access to Salto programming windows in the role. | Event logs |
| Event reports | <ul style="list-style-type: none"> Reports Event Reports Central station report Reports Setup Event | Event reports |
| Filters | Not used. | |
| Floor groups | <ul style="list-style-type: none"> Groups Floor groups | Controller programming windows |
| Floor plans | <ul style="list-style-type: none"> Monitoring Floor plan view Monitoring Setup Floor plan editor Monitoring Setup Floor plan editor (batch) Monitoring Setup Add bulk floor plans | Floor plans |
| Floors | <ul style="list-style-type: none"> Programming Floors | Controller programming windows |
| Function codes | <ul style="list-style-type: none"> Sites Function codes | Function codes |
| Generate PINs | Grants access to program user PIN codes. Also requires access to the Users table. | Users |
| Holidays | <ul style="list-style-type: none"> Sites Holiday groups | Holidays |

| Table | Permissions | Parent Role Table |
|------------------------|---|--------------------------------|
| Input expanders | <ul style="list-style-type: none"> Expanders Input expanders | Controller programming windows |
| Input types | <ul style="list-style-type: none"> Programming Input types | Controller programming windows |
| Inputs | <ul style="list-style-type: none"> Programming Inputs | Controller programming windows |
| Intercoms | <ul style="list-style-type: none"> Monitoring Setup Intercoms | Intercoms |
| Jobs | Not used. | |
| Keypad groups | <ul style="list-style-type: none"> Groups Keypad groups | Controller programming windows |
| Keypads | <ul style="list-style-type: none"> Expanders Keypads | Controller programming windows |
| Menu groups | <ul style="list-style-type: none"> Groups Menu groups | Controller programming windows |
| Modems | Not used. | |
| Muster reports | Not used - enable Muster reports in the role. | |
| Output expanders | <ul style="list-style-type: none"> Expanders Output expanders | Controller programming windows |
| Output groups | <ul style="list-style-type: none"> Groups Output groups | Controller programming windows |
| Outputs | <ul style="list-style-type: none"> Programming Outputs | Controller programming windows |
| Phone numbers | <ul style="list-style-type: none"> Programming Phone numbers | Controller programming windows |
| PhotoID | <ul style="list-style-type: none"> Users Card template editor | Card template editor |
| Programmable functions | <ul style="list-style-type: none"> Automation Programmable functions | Controller programming windows |
| PTZ setup | <ul style="list-style-type: none"> Monitoring Setup PTZ commands Requires access to cameras or DVRs. | Cameras |
| Reader expanders | <ul style="list-style-type: none"> Expanders Reader expanders | Controller programming windows |
| Record groups | <ul style="list-style-type: none"> Sites Record groups | Record groups |
| Record history | Not used. | |
| Salto calendars | Not used - enable Salto programming windows in the role. | |
| Salto door groups | Not used - enable Salto programming windows in the role. | |
| Salto doors | Not used - enable Salto programming windows in the role. | |
| Salto outputs | Not used - enable Salto programming windows in the role. | |

| Table | Permissions | Parent Role Table |
|------------------------|--|--|
| Salto time periods | Not used - enable Salto programming windows in the role. | |
| Scheduled user imports | Not used. | |
| Schedules | <ul style="list-style-type: none"> Sites Schedules | Schedules |
| Security levels | <ul style="list-style-type: none"> Sites Security levels | Security levels |
| Services | <ul style="list-style-type: none"> Programming Services | Controller programming windows |
| Smart readers | <ul style="list-style-type: none"> Expanders Smart readers | Controller programming windows |
| Status definitions | Not used. | |
| Status lists | <ul style="list-style-type: none"> Monitoring Setup Status lists | Available by default. |
| Status pages | <ul style="list-style-type: none"> Monitoring Status page view <div>The role must also have access to view the status lists, event reports and other objects on the status page.</div> <ul style="list-style-type: none"> Monitoring Setup Status page editor Monitoring Setup Status page editor (batch) | Status pages |
| Status table | Not used. | |
| Time and attendance | <ul style="list-style-type: none"> Reports Attendance report Reports Central station report Reports Setup Attendance Reports Setup Shift types | Attendance reports |
| Trouble inputs | <ul style="list-style-type: none"> Programming Trouble inputs | Controller programming windows |
| User reports | <ul style="list-style-type: none"> Users User search Reports User Reports Central station report Reports Setup User | User reports |
| Variables | <ul style="list-style-type: none"> Automation Variables | Controller programming windows |
| Web links | <ul style="list-style-type: none"> Monitoring Web links | Status pages |
| Workstations | <ul style="list-style-type: none"> Events Alarm routing Events Workstations Events Workstation groups | Available by default to Administrator and Installer presets. |

Security Level Manual Commands

The **Manual commands** tab enables you to control access to manual commands for specific records.

Areas, doors, floors, elevators, keypads and outputs also allow you to select a group that restricts the operator's access to specific records only. These records must also be available in the record groups that the operator has access to. If the group is left as <not set>, the operator will be able to control all records.

This reference table contains the following information:

- The menu items and other features that each manual command option refers to.
- The parent role table that each option inherits from.

| Setting | Permissions | Parent Role Table |
|----------------------------------|---|---------------------------|
| Area control | All commands for areas (e.g. arming/disarming) | Manual commands |
| Door control | All commands for doors (e.g. locking/unlocking) | Manual commands |
| Elevator control | Locking and unlocking floors in elevators. | Manual commands |
| Keypad control commands | Module update command for keypads | Manual commands |
| Output control commands | Activating and deactivating outputs | Manual commands |
| Input control | Bypassing inputs and removing bypasses | Manual commands |
| Restart and stop services | Stopping and starting services | Manual commands |
| Reset user commands | Reset antipassback command for users | Manual commands |
| Update module commands | Module update command for all expander types | Manual commands |
| Variable control | Updating variables from a floor plan | Manual commands |
| Programmable function control | Stopping and starting programmable functions | Manual commands |
| Update controller time | Setting controller date/time | Manual commands |
| Change audit opening in the keys | Edit the Audit on keys setting for Salto locks and user records. | Salto programming windows |
| Allegion commands | Locking and unlocking Allegion doors | Manual commands |

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.
Copyright © Integrated Control Technology Limited 2003-2025. All rights reserved.

Disclaimer: Whilst every effort has been made to ensure accuracy in the representation of this product, neither Integrated Control Technology Ltd nor its employees shall be liable under any circumstances to any party in respect of decisions or actions they may make as a result of using this information. In accordance with the ICT policy of enhanced development, design and specifications are subject to change without notice.