AN-361

Protege GX KONE Office Flow Integration

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 2003-2026. All rights reserved.

Last Published: 07-Jul-26 9:39 AM

Contents

Introduction 5
KONE Integration Comparison 5
Integration Architecture 6
KONE and Protege GX Terminology 7
Prerequisites 7
Credentials 8
Limitations 8
Initial Setup 9
KONE Setup 9
Installing OpenSSL 9
Enabling SQL Server Communication 10
Creating the SQL Server Login 10
Creating an Integration Operator 11
Installation 12
Validating the Installation 13
Disabling Sync Logging 13
Programming in Protege GX 15
Programming KONE Credential Types 15
Configuring Protege GX Doors 15
Card Readers 15
Door Types 16
Enabling the KONE Mobile Experience 17
Understanding Access in KONE Office Flow 18
KONE Records 18
Access Levels 18
Users 19
Programming Scenarios 21
Scenario 1: Two Companies 21
Part 1: Create Groups 22
Part 2: Create User Access Levels for KONE 23
Part 3: Create Public Access Levels 26
Part 4: Create the Home Floor Access Levels 28
Part 5: Assign Access Levels to Users 30
Scenario 2: Goods Elevator 31

Part 1: Create Groups 31
Part 2: Create Access Levels 31
Elevator Calls (Virtual Swipe) from Protege GX 34
Enabling Virtual Swipe 34
Calling Elevators 34
Troubleshooting 36
Events 36
Service Logs 36
Certificates 36
Resynchronizing with Office Flow 37
Known Issues 38
Certificate of Completion for KONE Site API Integration 39

Introduction

The Protege GX integration with KONE Office Flow enables you to manage access to the KONE elevator system in Protege GX, simplifying your access control system and eliminating the time spent programming user records in two separate systems. End users can use a single card to access both doors and elevator terminals throughout the building.

This application note covers the prerequisites, installation and programming instructions for integrating KONE Office Flow with Protege GX. It also includes programming scenarios for setting up user access.

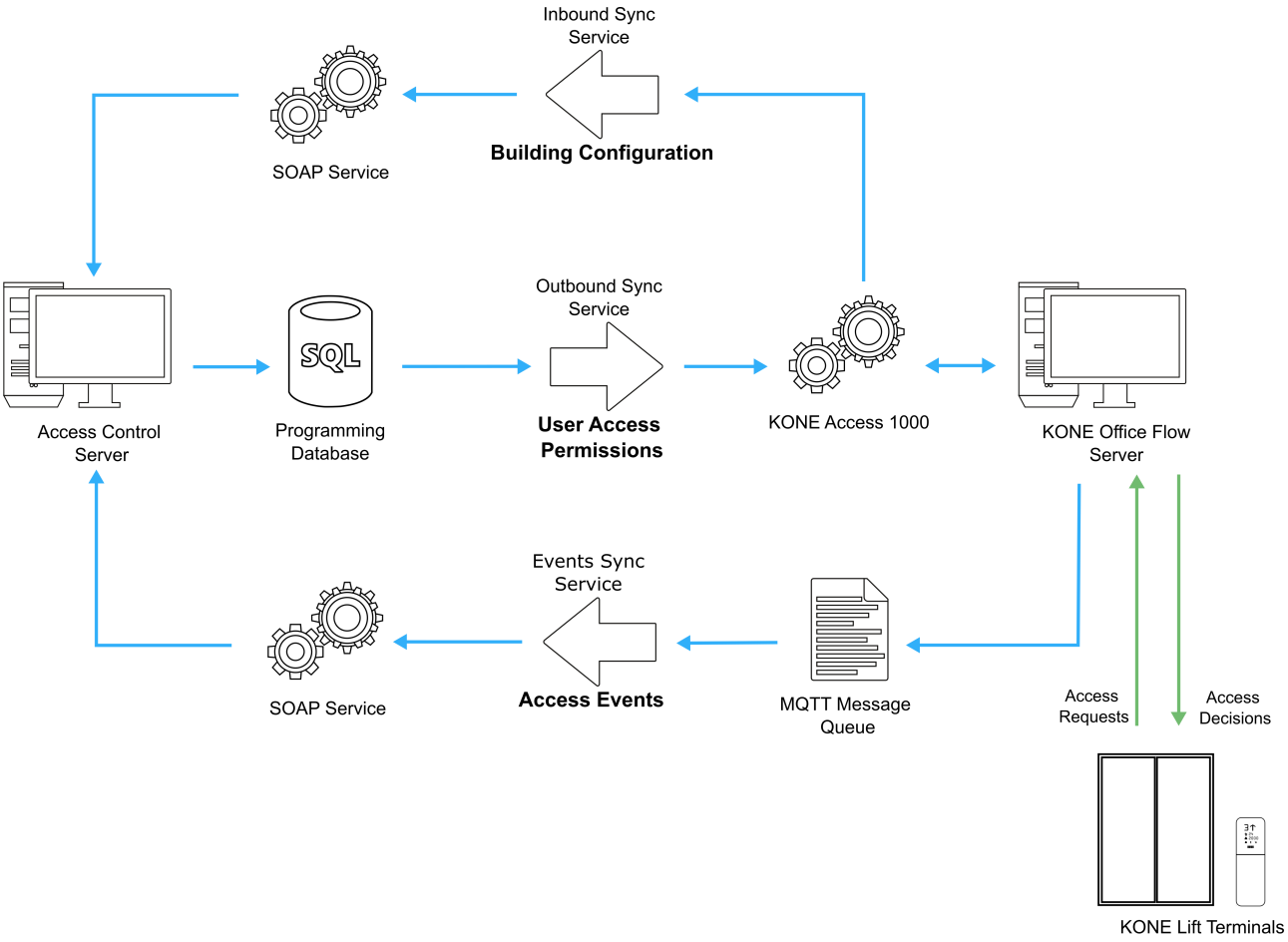
KONE Integration Comparison

Protege GX has multiple integrations available for KONE systems. The table below will help you understand the differences and select the right integration for your site.

	KONE HLI Integration	KONE Destination 880 Integration	KONE Office Flow Integration
Architecture	Protege GX controller to KONE group controller	Protege GX controller to KONE group controllers Extension of the KONE HLI Integration	Protege GX server to KONE Office Flow server
KONE System	KONE group controllers (primary and backup)	KONE group controllers (up to 32)	KONE Office Flow
Application Programming Interface	KONE API, GCAC and RCGIF	Destination 880	Access 1000
Card Readers for Elevator Access	ICT card readers	ICT card readers	KONE terminals
Application Note	Application Note 170	Application Note 274	Application Note 361

Integration Architecture

The Protege GX KONE Office Flow Sync Service manages the synchronization of the two systems using three main services: the inbound sync service, the outbound sync service and the events sync service. Additional services manage health monitoring and certificate renewal.



It works as follows:

- Lifts, floors and terminals (DOPs/COPs) are configured in KONE Office Flow.
- The inbound sync service imports these records to Protege GX (via KONE Access 1000 and the Protege GX SOAP Service), creating elevator car, floor and door records.
- Users, credentials, access levels and schedules are programmed in Protege GX. The outbound sync service synchronizes these changes to the KONE system as people, profiles and access rights. Access records are synchronized every 60 seconds by default.
- When a user requests access at a KONE terminal, Office Flow uses the access permissions from Protege GX to decide which floors they can travel to.
- The KONE system sends access events to an MQTT message queue, where the events sync service picks them up and synchronizes them to Protege GX.

KONE and Protege GX Terminology

KONE Record	Protege GX Record
Person	User
Profile / Access Right	Access Level
Allowed Time	Schedule
Special Day	Holiday Group
Lift	Elevator Car
Group	Elevator Group
Area	Floor
Source Terminal DOP COP Turnstile	Door

Prerequisites

The following software must be installed and operational.

Software	Version	Notes
Protege GX	4.3.387.2 or higher	
Protege GX SOAP Service	1.7.0.0 or higher	
Protege GX KONE Office Flow Sync Service	1.0.5.0 or higher	Installation instructions are included below (see page 12).
KONE Access 1000	1.1.5	This is the **only** tested and supported version for this integration.
KONE Office Flow	-	Version must be compatible with the KONE Access 1000 version stated above.
OpenSSL	Latest version	Installation instructions are included below (see page 9).

It is the responsibility of the installation professional to verify the version of the proposed third-party system and supported components with the version listed in this document. ICT will not accept responsibility for the failure to verify integrated system versions and requirements.

Licensing

The following licenses are required for this integration:

License	Order Code	Notes
Protege GX KONE Office Flow License	PRT-GX-ELV-HLI-KNOF	1 per integrated site.

License	Order Code	Notes
Protege GX KONE Office Flow Annual Care Plan	PRT-GX-ELV-HLI-KNOF-ACP	The annual care plan must be purchased alongside the base integration license. It is charged annually for ongoing support and integration updates.
Protege GX Door License	PRT-GX-DOR-1	1 license per KONE terminal (DOP, COP or turnstile).
	PRT-GX-DOR-10	
	PRT-GX-DOR-50	

Credentials

This integration supports ICT MIFARE DESFire cards on both KONE terminals and card readers connected to Protege GX. Your KONE representative will help you configure your KONE terminals to read ICT cards. Up to five Wiegand credential formats are supported per site.

The **facility numbers** of your cards must match the **company codes** programmed in the KONE system. If the facility number does not match a company code, the user will fail to sync.

Before you begin, contact ICT Customer Services or Technical Support (Contact Us) to obtain the following information about your cards:

- Wiegand format
- Application ID of the open Wiegand file
- MIFARE DESFire read key

KONE Bluetooth credentials may be used on KONE terminals, but not on ICT card readers. Only one Bluetooth credential format is supported per site.

One QR code credential format is supported per site.

Limitations

- Antipassback in KONE Office Flow is not supported.
- Only English is supported as the user language.

Initial Setup

A few setup steps are required before installing the integration.

KONE Setup

We strongly recommend that you do not install the sync service until all **building configuration** is completed in Office Flow. Any subsequent changes to the elevator system will not be automatically synchronized to Protege GX, so you will need to manually clear and resync the integration (see page 37).

Once the KONE system has been set up, request the following information and files from your KONE representative:

1. The Host Name for the KONE system (by default, est.localsite).
2. If an API security certificate has already been created for this site, you will need the following:
   - CRT file
   - PFX file
   - Passphrase
3. If the certificate has not yet been created, you can instead use the following details:
   - IP Address
   - Activation Code (six-digit alphanumeric code)

     The activation code is only valid for 24 hours, so ensure that you install the sync service before the code expires.
   - Client Code
4. The connection details for the MQTT event queue (if they have been changed from the defaults):
   - Group ID
   - Client ID
   - Port Number

In addition, provide the card details supplied by ICT (see previous page) and the cards' **facility numbers** to your KONE representative. This will enable them to:

- Program your KONE terminals to read ICT MIFARE DESFire credentials.
- Add the facility numbers to Office Flow as company codes.

Installing OpenSSL

OpenSSL is used to generate and renew security certificates for the connection between the sync service and KONE Office Flow. It must be installed on the same machine where you will install the sync service.

To install OpenSSL:

1. Download the installer from Shining Light Productions. Select the most recent **Win64** installer in either EXE or MSI format. You can install either the light or standard version.
2. Run the installer on the machine where you will install the sync service.
3. Accept the license agreement and click **Next**.
4. Ensure that the **Destination Location** is set to *C:\Program Files\OpenSSL-Win64*. Click **Next**.
5. Click **Next**.

6. Select **The Windows system directory**. Click **Next**.
7. Click **Install**.

Enabling SQL Server Communication

To ensure that SQL Server can communicate with the sync service:

1. Open SQL Server Configuration Manager as an administrator.
2. Under **SQL Server Network Configuration**, select **Protocols for ProtegeGX**.
3. Double click on **TCP/IP**.
4. Ensure that **Enabled** is set to *Yes*.
5. In the **IP Addresses** tab, scroll down to the **IPAll** section. Ensure that the **TCP Port** is set to *1433*.
6. Click **Ok**.
7. Open **Services** as an administrator:
   - Press the **Windows + R** keys.
   - Type **services.msc**.
   - Press **Control + Shift + Enter**.
8. Locate *SQL Server (ProtegeGX)*. Right click on the service and click **Restart**.

Creating the SQL Server Login

The sync service needs access to the Protege GX database in order to synchronize user records. To create an operator:

1. Run SQL Server Management Studio on the machine with the Protege GX databases installed.
2. Connect to the ProtegeGX server instance.
3. Right click on the instance name in the Object Explorer and select **Properties**.
4. Make a note of the **Name** displayed on the **General** page.
5. Navigate to the **Security** page.
6. Set **Server authentication** to **SQL Server and Windows Authentication mode**.
7. Click **OK**.
8. In the Object Explorer, expand the **Security** folder and right click on **Logins**.
9. Select **New Login...**
10. Enter a **Login name**.
11. Select **SQL Server authentication**.
12. Enter a secure **Password** and repeat it to confirm.

    Save this password to a password manager or other secure location.

13. Disable **Enforce password expiration**. This prevents the service from periodically losing access to the database when the password expires.
14. Disable **User must change password at next login**.
15. In the **Server Roles** tab, enable the **public** and **sysadmin** roles.
16. Click **OK**.
17. Right click on the instance name and select **Restart**.

This will also stop some Protege GX services.

18. To ensure that the new user is configured correctly, open a new instance of SQL Server Management Studio.
19. Set **Authentication** to *SQL Server Authentication* and attempt to log in with the new credentials. You should be able to log in successfully and view the ProtegeGX database.
20. Open the Services manager. Start the **Protege GX Data Service** and **Protege GX Download Service**.

Creating an Integration Operator

It is best practice to create a unique operator for use by the sync service. This ensures that automatic programming changes made by the sync service can be distinguished from changes by other Protege GX operators.

1. Navigate to **Global | Operators**.
2. Add a new operator with a descriptive name, e.g. *KONE Integration Sync Service*.
3. Set a new **Username** and temporary **Password**.
4. Set the **Role** to *Administrator*.
5. Click **Save**.
6. Open a new Protege GX client window and log in as the new operator. Give the operator a new, strong password.

Installation

Before you begin, ensure that you have all of the required information from KONE (see page 9) and the building configuration has been completed in KONE Office Flow. To simplify the security configuration, it is recommended to install the sync service on the same machine as the Protege GX server.

To install the Protege GX KONE Office Flow Sync Service:

1. Right click on the installer provided by ICT and select **Run as administrator**.
2. Enter the Database ID of the site you are integrating with (1 by default).
3. Enter the SOAP connection details:
   - **API URL**: The endpoint for the SOAP service WSDL. By default this is: https://<pcname>:8040/ProtegeGXSOAPService/service.svc?wsdl
   - **Username**: The username of the Protege GX operator created above.
   - **Password**: The password of the Protege GX operator created above.

   Click **Next**.
4. Enter the **Host Name** for the KONE system.
5. Under the **Certificates** section, you can either upload an existing certificate for the connection or generate a new one.

   If KONE has provided a certificate, or a certificate already exists from a previous installation:
   - Click **Select Existing Certificate**.
   - Upload the CRT and PFX files.
   - Enter the **Passphrase** provided for the PFX file.

   If KONE has not provided a certificate:
   - Click **Generate New Certificate**.
   - Enter the **IP Address**, **Client Code** and **Activation Code** (six-digit alphanumeric code) provided by KONE.
   - Create a new secure **Passphrase** for protecting the PFX file. Only alphanumeric characters are supported.

     Save this passphrase to a password manager or other secure location.
6. Enter the **MQTT Topic Details** provided by the KONE representative. The installer shows the default settings, but these may be different for your installation.
7. Click **Next**.
8. Enter the connection information for the ProtegeGX database:
   - **Database Server**: The name of the Protege GX server instance that you copied above (see page 10).
   - **Database Name**: The name of the Protege GX programming database (ProtegeGX by default).
   - **User Name**: The name of the SQL login created above.
   - **Password**: The password of the SQL login created above.

   Click **Next**.
9. Click **Install** to complete the installation.

Validating the Installation

To ensure that the installation has been completed correctly, open the Windows Service Manager. Confirm that five services have been created and have the status *Running*.

- Protege GX KONE Cert Renewal Service
- Protege GX KONE Health Check Service
- Protege GX KONE Office Flow Events Sync Service
- Protege GX KONE Office Flow Inbound Sync Service
- Protege GX KONE Office Flow Outbound Sync Service

Start any services that are not running.

You can also validate the new records that have been created in Protege GX:

Location	Records Created	Usage
Global | Download server	KONE	Manages synchronization with the KONE Office Flow system.
Sites | Schedules	Direct Call Enabled - KONE Integration - DO NOT DELETE Source Areas Enabled - KONE Integration - DO NOT DELETE	Specify direct call destinations and source floors in access levels. Not used as regular schedules.
Sites | Controllers	KONE Controller - DO NOT DELETE	Provides a host controller for records synchronized from KONE. No physical controller is required.
Sites | Credential types	• Five KONE RFID credential types for card formats • KONE Bluetooth for mobile credentials • KONE QR for QR codes	Used to assign credentials to users. KONE RFID credentials can be used at card readers connected to Protege GX. Only credential types that are configured in Office Flow will appear in Protege GX.
Programming | Doors	DOPs and COPs synced from Office Flow.	Used to assign KONE terminals (DOPs/COPs) to access levels.
Programming | Floors	Floors synced from Office Flow	Used to assign KONE floors to access levels
Programming | Elevator cars	Lifts synced from Office Flow	Used to assign KONE lifts to access levels
Groups | Elevator groups	Groups synced from Office Flow	Used to assign KONE groups to access levels

You can change the names of these records, but do not otherwise edit or delete them except as advised in this document.

Disabling Sync Logging

By default, the integration service saves the sync history to the Protege GX database. This can fill up the database quickly, especially in systems that use SQL Express. . We recommend that you disable sync logging to prevent this issue.

1. In a File Explorer, navigate to **C:\Program Files (x86)\Integrated Control Technology\Protege GX KONE Office Flow Sync Service**
2. Make a copy of **appsettings.json** as a backup, then edit the original file.

   Files in this directory require administrator permissions. To edit a file, run Notepad or Notepad++ as an administrator, then open the file from the application. Alternatively, make a copy in a different directory, edit the copy, then replace the original.

3. Locate `ShouldUpdateSyncHistory` and change the value to `false`.

```
"KoneUsersBulkUpdateThreshold": 100,
"ShouldUpdateSyncHistory": false,
"KoneConnectionSettings": {
    ...
},
```

4. Open **Services** as an administrator:
   - Press the **Windows + R** keys.
   - Type **services.msc**.
   - Press **Control + Shift + Enter**.
5. Locate the **Protege GX KONE Office Flow Outbound Sync Service**. Right click and select **Restart**.

Programming in Protege GX

This section covers the programming required in Protege GX to sync user access to the KONE system.

Programming KONE Credential Types

You must program the Wiegand format of the KONE credential types created by the installer. This ensures that Protege GX controllers can interpret the format of RFID cards, and that all credentials sync to Office Flow correctly.

To set up the credential formats:

1. In **Sites | Credential types**, open the *KONE RFID 1* credential type.
2. Optionally, you can change the name of this credential type.
3. In the **Wiegand or TLV format** field, enter the format code for your cards. The most common formats for ICT cards are HID 26 bit and HID 34 bit:
   - `#HID26bit__#Variables__A,FACILITY,8,MSB,BIN__B,CARD,16,MSB,BIN__ #Format__PAAAAAAAABBBBBBBBBBBBBBBP__#Parity__ EXXXXXXXX.................__.........XXXXXXXXXXXXXXXXO`
   - `#HID34bit__#Variables__A,FACILITY,16,MSB,BIN__B,CARD,16,MSB,BIN__ #Format__PAAAAAAAAAAAAAAAABBBBBBBBBBBBBBBBP__#Parity__ EXXXXXXXXXXXXXXXX.................._ _.................XXXXXXXXXXXXXXXXO`

   If your cards use a different Wiegand format, program it following the instructions in *Application Note 276: Configuring Credential Types in Protege GX*.
4. Click **Save**.
5. Repeat for all KONE credential types that your site uses, including *KONE Bluetooth* and *KONE QR*.

Configuring Protege GX Doors

The KONE RFID credential types will be used for both KONE terminals and Protege GX doors. This means that the operator can enter the credential once for each user instead of entering the same credential twice (in the Cards section *and* the Credentials section).

This requires some additional configuration for the normal Protege GX doors in the system.

Card Readers

You must configure all standard ICT card readers on site to recognize the *KONE RFID* credential types programmed above.

For ICT RS-485 readers:

1. Navigate to **Expanders | Reader expanders** and select each reader expander with standard card readers connected.
2. Set the **Port 1/2 network type** to *Wiegand* temporarily.
3. In the **Reader 1** tab, set the **Reader 1 format** to *Custom credential*.
4. Repeat in the **Reader 2** tab.
5. Return to the **General** tab and change the **Port 1/2 network type** back to *ICT RS485*.
6. Click **Save**.

7. Wait for the changes to download to the controller, then right click on the reader expander and select **Update module**.

For OSDP readers:

1. Navigate to **Expanders | Smart readers** and select each smart reader with a standard card reader connected.
2. In the **Reader one** tab, set the **Reader one format** to *Custom credential*.
3. Click **Save**.

For Wiegand readers:

1. Navigate to **Expanders | Reader expanders** and select each reader expander with standard card readers connected.
2. In the **Reader 1** tab, set the **Reader 1 format** to *Custom credential*.
3. Repeat in the **Reader 2** tab.
4. Click **Save**.
5. Wait for the changes to download to the controller, then right click on the reader expander and select **Update module**.

Door Types

You will also need a door type for reading the custom credentials:

1. Add a new door type with a descriptive name (e.g. *KONE/ICT Cards*).
2. Set the **Entry reading mode** to *Custom*.
3. Under **Entry credential types**, add the *KONE RFID 1* credential type.
4. Repeat for the **Exit reading mode**.
5. Click **Save**.
6. Create additional door types for each KONE RFID credential type that is in use on the site.
7. If one door needs to recognize two or more credential types, return to the first door type and set the **Fallback door type** to different door type. This may be another KONE RFID door type or different credential such as PIN.

   To add a third alternative credential, set the **Fallback door type** of the second door type, and so on.
8. Navigate to **Programming | Doors**.
9. Use *Shift + Click* or *Ctrl + Click* to select all of the standard Protege GX doors that will use this door type.

   Do not program the doors that represent KONE terminals.
10. Set the **Door type** to the one created above.
11. Click **Save**.

Enabling the KONE Mobile Experience

The KONE Mobile Experience enables users to call elevators with their smartphones. If your site uses the KONE Mobile Experience, you must first display the extended user settings to allow you to enable the mobile experience for each user.

1. Navigate to **Global | Sites**.
2. In the **Display** tab, enable **Display predefined custom fields in users**.
3. Click **Save**.

Understanding Access in KONE Office Flow

Access in KONE Office Flow works differently from normal Protege GX access levels. This section covers the key concepts you need to understand to program access to KONE floors, elevator cars and DOPs/turnstiles.

When you're ready to get hands-on, jump to the detailed examples below: *Programming Scenarios*

KONE Records

In a Protege GX system that is integrated with KONE, users need access to the following records:

- **Destination floors**: The floors that people are allowed to travel to.
- **Source floors**: The floors that people are allowed to travel from.
- **Home floors** (called direct call destinations in Office Flow): Users can travel to their home floor with a quick swipe.
- **Elevator cars**: The elevator cars that people are allowed to call.
- **DOPs and turnstiles**: The operating panels that people can use to call elevators. These are represented by **doors** in Protege GX.

You will need to create floor, elevator and door groups to program access. Before you begin, we recommend you create the following groups:

- Any **destination floor groups** that are needed for site access.
- A floor group containing **all source floors**. You can create additional source floor groups, or program source floors individually.
- An elevator group containing **all elevator cars**. You can create additional elevator groups to restrict access to specific elevator cars.
- A door group containing **all DOPs and turnstiles**. You can create additional door groups to restrict access to specific DOPs and turnstiles.

It is not possible to mix KONE and Protege GX records in a single group or access level. To prevent operators from creating mixed access levels, we strongly recommend including the term **KONE** in the name for each group.

Access Levels

This integration uses several different types of access levels to represent different functions in the Office Flow system. You will need to create four types of access level:

- **Protege GX User Access Levels**: Provide access to doors, areas and so on in the Protege GX system.
- **KONE User Access Levels**: Provide access to KONE floors, elevator cars and DOPs/turnstiles. When a user swipes their credential, they can access anything in their KONE user access level.
- **KONE Home Floor Access Levels**: Define the home floor for each user.
- **KONE Public Access Levels**: Define which floors, elevator cars and DOPs/turnstiles allow free access without a credential. These are not assigned to users.

For KONE access levels, there is a new **Integration options** tab. This tab contains:

- **Actions**: These are synchronized from the KONE system, and determine what types of call the user can make. You must select at least one action in KONE user access levels and public access levels.

  If the access level uses multiple actions, enable them in order of priority. The first action you enable will be the default action for these users.

- **Company codes**: For information only.

- **Options**: The following options are available:
  - **Allow public access**: Enable for public access levels, but not user access levels.
  - **Allow group call to elevator**
  - **Allow direct action**: The *first* action that was enabled above will be the user's direct action.

Rules for programming access levels:

- Access levels cannot contain both KONE and Protege GX doors, floors or elevator cars. Any access levels that contain both types of records will not sync to Office Flow, and you will receive a 400 error from the Office Flow system.

  Use a naming convention for your access levels to help operators understand which access levels are used for KONE and which for Protege GX.

- You must select at least one **Action** in the **Integration options** tab (for user and public access levels).
- Every KONE user access level and public access level must contain access rules for destination floors, source floors, elevator cars *and* DOPs/turnstiles. If the access level contains nothing for a specific record, Office Flow will grant access to *everything*.

  We recommend using 'All KONE Source Floors', 'All KONE Elevator Cars' and 'All KONE DOPs/Turnstiles' groups instead of leaving access levels empty.

- Home floor access levels should only contain the home floor or floors. The user must also have access to that floor in a KONE user access level.
- If someone has a source floor in their access level, they can travel from there to any destination floor *in the same access level*. In general, access is only consistent within a single access level. This also applies to public access levels.
- Use the **Operating schedule** to control when the user has access.
- The **Schedule** setting in the **Floors** and **Floor groups** tabs determines what type of floor is being programmed.
  - *Always*: Destination floor
  - *Source Areas Enabled - KONE Integration - DO NOT DELETE*: Source floor
  - *Direct Call Enabled - KONE Integration - DO NOT DELETE*: Home floor

See *Scenario 1: Two Companies* for how to set up access levels in practice.

Users

Credentials

In the **Credentials** section, you will see the credentials that are available in the Office Flow system: RFID, Bluetooth and/or QR code. Enter all credentials in the format *FacilityNumber:CredentialNumber*, e.g. 10256:59249.

The RFID credentials can also be used at Protege GX card readers.

You can only assign credentials from the companies that have been defined in the KONE system. Users with undefined credentials will fail to sync. For more information, see *Credentials* (page 8).

Access Levels

Each user can have three types of access levels:

- Protege GX user access levels
- KONE user access levels
- KONE home floor access levels (optional)

Never assign public access levels to users.

KONE Mobile Experience

To enable the KONE mobile experience:

- Enter the user's **Email** (in the **General** tab)
- Enter the following in the **Extended** tab:
  - **Service Number**: The user's phone number.
  - **Custom field 1**: `EnableKONEMobile=true`

Other Rules for Programming Users

- The maximum length for the first name and last name combined is 48 characters.
- To control user expiry, use the **User expiry date/time** (**General** tab) or the **Start** and **End** for credentials. Do not use the expiry settings in the **Access levels** tab.
- To control schedules, use the **Operating schedule** in the access level. Do not use the schedule in the user record.

Programming Scenarios

This section contains the following scenarios to help you plan and program your site's access permissions:

- *Scenario 1: Two Companies*: Covers basic access requirements including destination floors, source floors, home floors and public access levels.
- *Scenario 2: Goods Elevator*: Demonstrates how to restrict access to a specific elevator car. The same technique can be applied to DOPs/turnstiles.

Scenario 1: Two Companies

This scenario demonstrates how to program a system with two companies, using destination floors, source floors, home floors and public access levels. To simplify the scenario, we will assume that every user has access to every elevator car and every DOP and turnstile.

Consider a building with six floors.

Floor	Usage
Floor 6	Company B
Floor 5	
Floor 4	Company A
Floor 3	
Floor 2	Shared Cafeteria
Floor 1	Public Lobby

The table below shows one possible plan for access in this building:

Access Level	Public	Source Floors	Destination Floors	Home Floors	Description
KONE-Common-Public	Yes	(All)	Floor 1		Anyone can travel to the lobby from anywhere in the building without a credential.
KONE-Company A	No	(All)	Floor 2 Floor 3 Floor 4		Employees of Company A can travel to the cafeteria and their company premises with a credential. All source floors are enabled, so if someone accidentally travels to Company B's premises they can leave again.
KONE-Company A-Public	Yes	Floor 3 Floor 4	Floor 2 Floor 3 Floor 4		Once someone is in the Company A premises, they can freely travel between floors belonging to that company. They can also go to the cafeteria freely, but they will need a credential to return to the company premises.
KONE-Company A-Home (3)	No			Floor 3	Some employees of Company A have Floor 3 as their home floor.

Access Level	Public	Source Floors	Destination Floors	Home Floors	Description
KONE-Company A-Home (4)	No			Floor 4	Some employees of Company A have Floor 4 as their home floor.
KONE-Company B	No	(All)	Floor 2 Floor 5 Floor 6		Employees of Company B can travel to the cafeteria and their company premises with a credential. All source floors are enabled, so if someone accidentally travels to Company A's premises they can leave again.
KONE-Company B-Public	Yes	Floor 5 Floor 6	Floor 2 Floor 5 Floor 6		Once someone is in the Company B premises, they can freely travel between floors belonging to that company. They can also go to the cafeteria freely, but they will need a credential to return to the company premises.
KONE-Company B-Home (5)	No			Floor 5	Some employees of Company B have Floor 5 as their home floor.
KONE-Company B-Home (6)	No			Floor 6	Some employees of Company B have Floor 6 as their home floor.

Note the naming convention. This was designed so that access levels for the same company are together when the list is sorted alphabetically.

Part 1: Create Groups

Before creating our access levels, we need to create floor, door and elevator groups based on the access needs we identified above.

First we need to create floor groups that contain any destination floors we need for the access levels. It is also helpful to create an *All Source Floors* group for the access levels that allow any source floor.

In **Groups | Floor groups**, create the following:

Floor Group	Floors
KONE - Company A - Destination Floors	Floor 2 Floor 3 Floor 4
KONE - Company B - Destination Floors	Floor 2 Floor 5 Floor 6
KONE - Public Destination Floors	Floor 1

Floor Group	Floors
KONE - All Source Floors	Floor 1 Floor 2 Floor 3 Floor 4 Floor 5 Floor 6

The prefix KONE at the start of each name helps operators identify which records they are allowed to add to KONE access levels.

In this scenario, everyone is allowed to use any DOP or turnstile. Navigate to **Groups | Door groups** and create the following:

Door Group	Doors
KONE - All DOPs and Turnstiles	Every DOP and turnstile record synced from KONE.

Everyone is allowed to use any elevator car, so navigate to **Groups | Elevator groups** and create the following:

Elevator Group	Elevator Cars
KONE - All Elevators	Every elevator car synced from KONE.

Part 2: Create User Access Levels for KONE

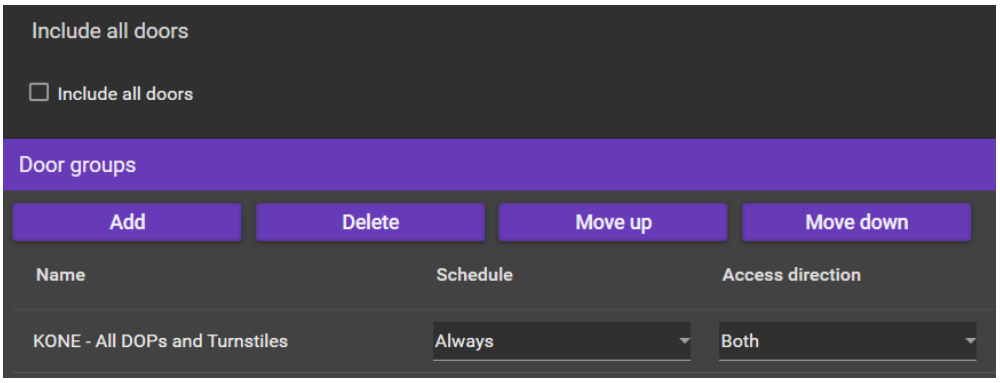
We need to create the access levels described in the table above. It's not possible to give instructions for all of these access levels here, but we will demonstrate a few examples.

First we will create the *KONE - Company A* access level, which is the normal access level for employees of Company A.

1. Navigate to **Users | Access levels** and add a new access level.
2. Enter the name *KONE - Company A*.

   Here you could set the **Operating schedule** to restrict access to certain times and days.

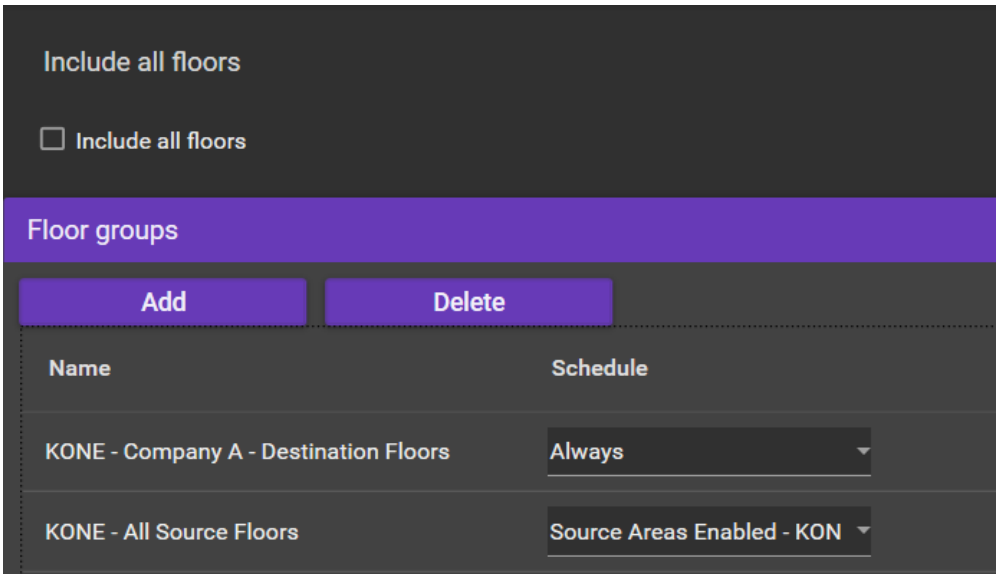
3. In the **Door groups** tab, add *KONE - All DOPs and Turnstiles*. This grants access to every KONE terminal.



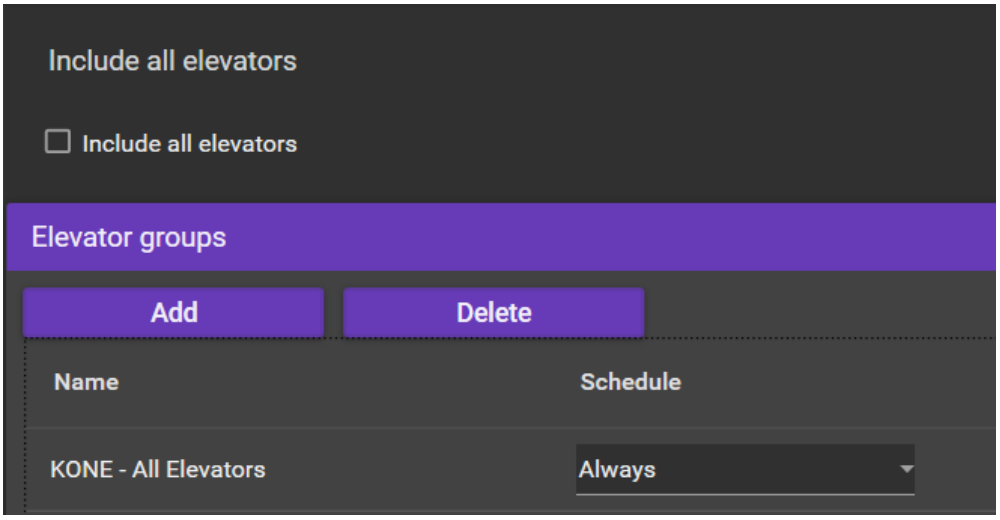
4. In the **Floor groups** tab, add *KONE - Company A - Destination Floors* to allow employees to travel to their company's floors.

5. To allow the Company A employees to leave any floor, add *KONE - All Source Floors* and set the **Schedule** to *Source Areas Enabled - KONE Integration - DO NOT DELETE*.

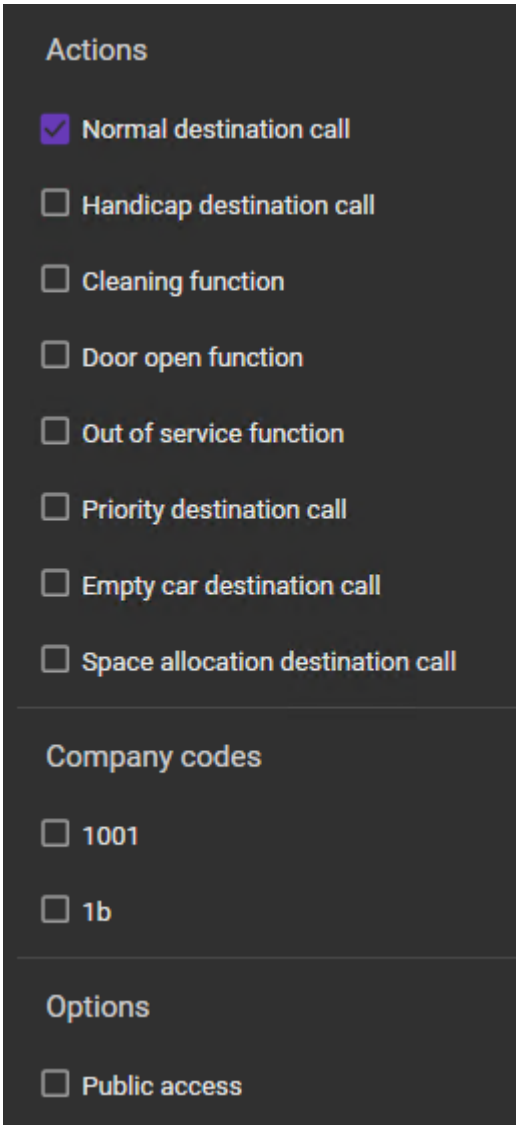
   The **Schedule** setting determines which floors are the source floors.



6. In the **Elevator groups** tab, add *KONE - All Elevators*.



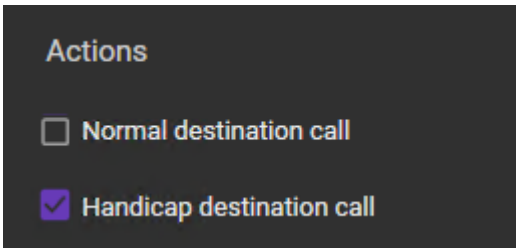
7. In the **Integration options** tab, enable at least one of the **Actions**. The available actions are different depending on how the KONE system was set up—in this case, we will use **Normal Destination Call**.



8. Do not add any normal Protege GX doors or other records to this access level. Click **Save**.

You can create the user access level for Company B with the same process, using their destination floor group.

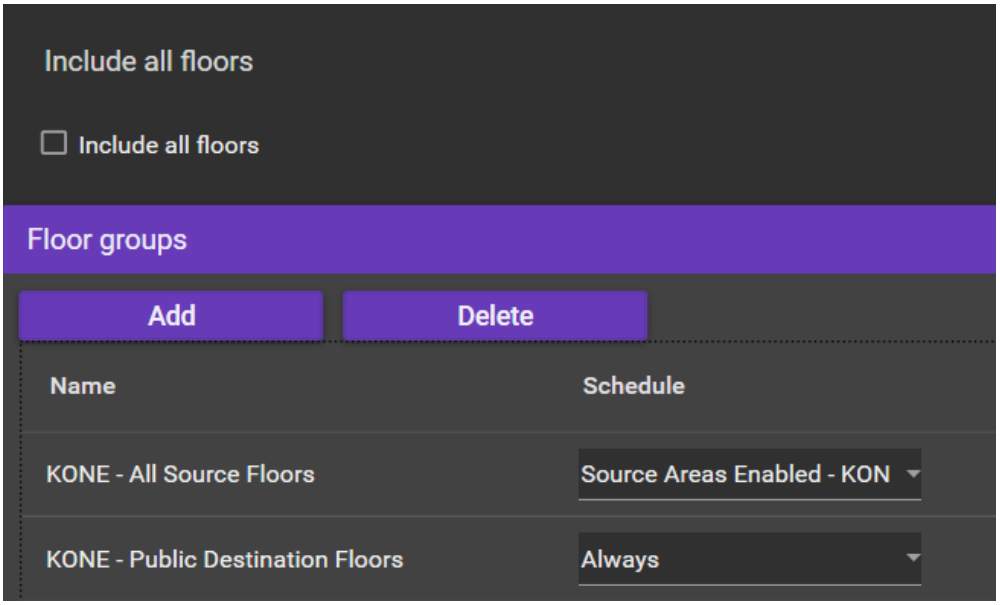
For a real site, you might need to create alternative versions of the access levels with different **Actions**. For example, you could create an access level for disabled employees using the **Handicap destination call** action.



Part 3: Create Public Access Levels

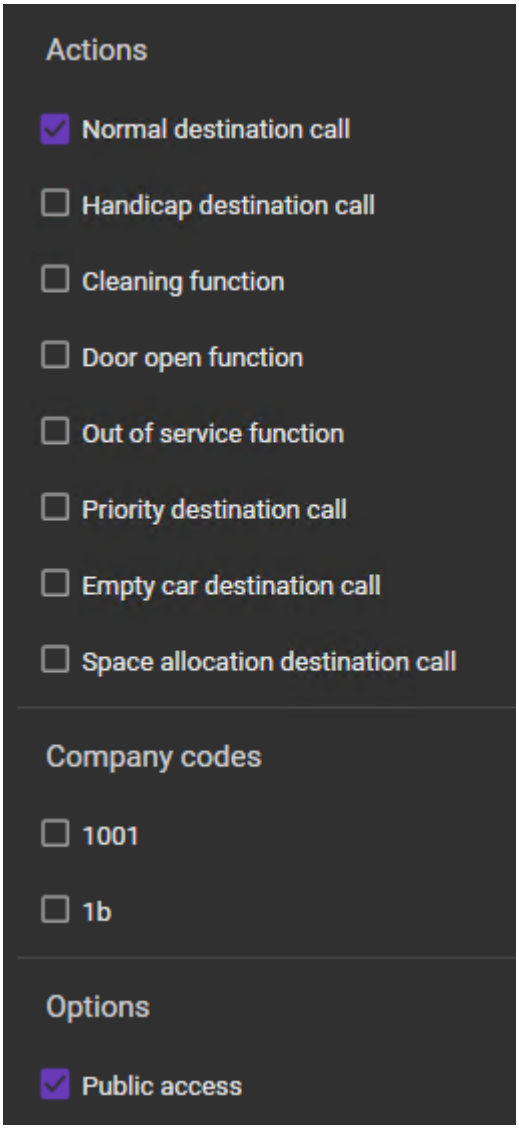
Public access levels determine where people can travel without a credential. First, create the access level for the lobby floor:

1. Add a new access level called *KONE-Common-Public*.
2. In the **Door groups** tab, add *KONE - All DOPs and Turnstiles*.
3. In the **Floor groups** tab, add *KONE - Public Destination Floors*.
4. Add *KONE - All Source Floors* and set the **Schedule** to *Source Areas Enabled - KONE Integration - DO NOT DELETE*.



5. In the **Elevator groups** tab, add *KONE - All Elevators*.
6. In the **Integration options** tab, enable at least one of the **Actions**.

7. Enable **Public access**.

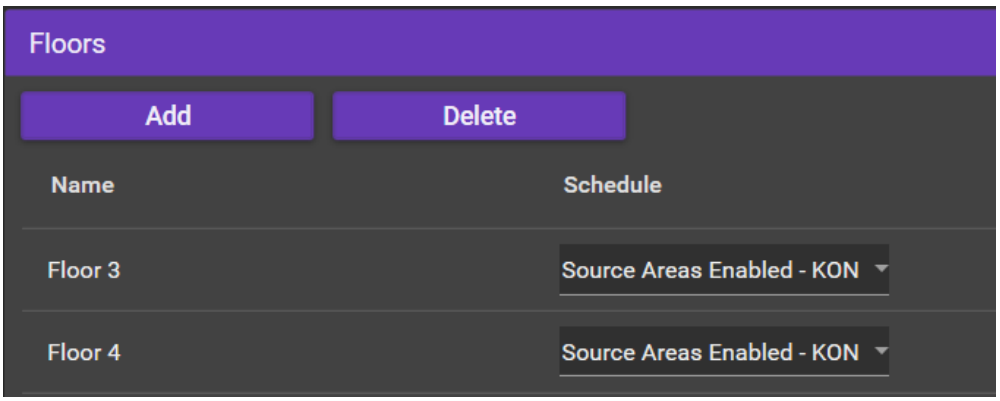


8. Do not add any normal Protege GX doors or other records to this access level. Click **Save**.

Now we can create the *KONE - Company A - Public* access level. This allows people to travel between Company A's floors without a credential.

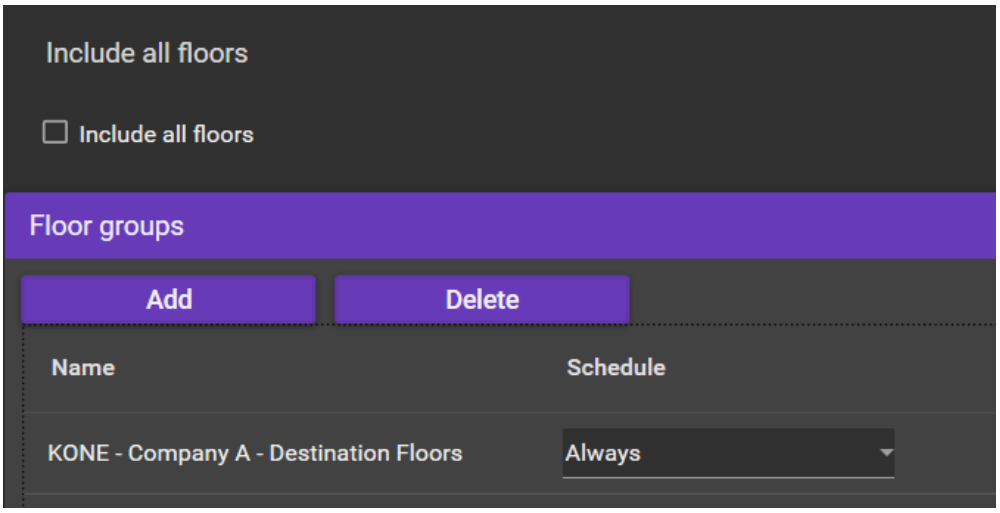
1. Add a new access level called *KONE - Company A - Public*.
2. In the **Door groups** tab, add *KONE - All DOPs and Turnstiles*.

3. This access level has specific source floors, which we will add in the **Floors** tab.
   Add *Floor 3* and *Floor 4*, then set the **Schedule** for both to *Source Areas Enabled - KONE Integration - DO NOT DELETE*.



Alternatively, you could create a floor group for the Company A source floors.

4. In the **Floor groups** tab, add *KONE - Company A - Destination Floors*.



5. In the **Elevator groups** tab, add *KONE - All Elevators*.
6. In the **Integration options** tab, enable at least one of the **Actions** and the **Public access** setting.
7. Do not add any normal Protege GX doors or other records to this access level. Click **Save**.

Repeat to create the public access level for Company B. These public access levels will not be assigned to users.

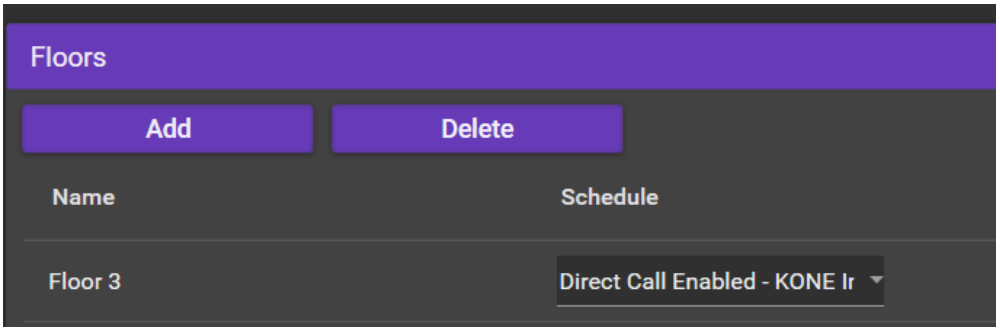
Part 4: Create the Home Floor Access Levels

Home floor access levels allow employees to travel to their home floors with a quick swipe.

To create a home floor access level for Company A:

1. Add a new access level called *KONE - Company A - Home (3)*.
2. In the **Floors** tab, add *Floor 3*.

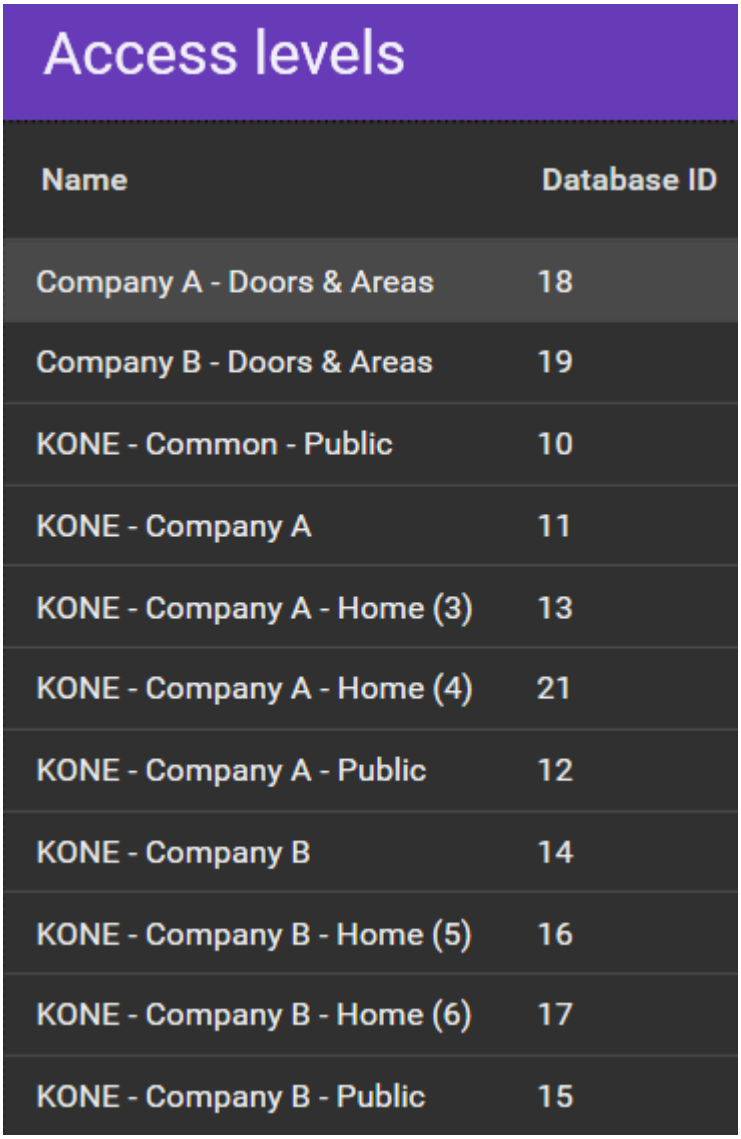
3. Set the **Schedule** to *Direct Call Enabled - KONE Integration - DO NOT DELETE.*



4. Do not add any normal Protege GX doors or other records to this access level. Click **Save**.

Repeat to create the home floor access levels for Company A (floor 4) and Company B (one for Floor 5 and one for Floor 6).

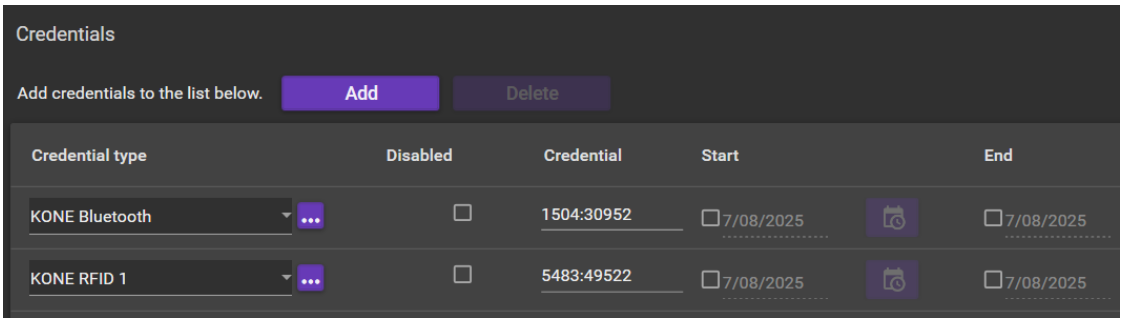
You have now created all the basic access levels needed for the KONE system. You can create additional access levels for access to the Protege GX system, including doors, areas and so on. **Do not** add any KONE records to these access levels.



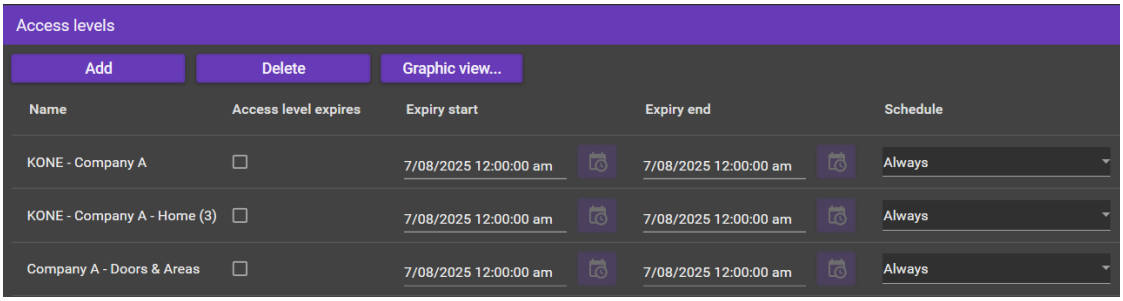
Part 5: Assign Access Levels to Users

You can now add users and assign them access levels. You can assign the standard KONE access levels and the home floor access levels, but not the public access levels.

1. Navigate to **Users | Users**.
2. Add a new user (an employee of Company A).
3. Scroll down to **Credentials**. Enter the user's RFID, Bluetooth and/or QR code credentials.



4. In the **Access levels** tab, add the following:
   - KONE - Company A
   - KONE - Company A - Home
   - Any Protege GX access levels that the user needs.



> Do not add public access levels to any user.

5. Click **Save**.

This user record will be synchronized to the KONE system so they can gain access to Company A's floors.

Scenario 2: Goods Elevator

This scenario demonstrates how to restrict access to a specific elevator car. The same technique can be used to restrict access to particular DOPs and turnstiles.

In this scenario, the building has three elevator cars:

Elevator Car	Description
Elevator 1	Accessible to staff and the public.
Elevator 2	Accessible to staff and the public.
Goods Elevator	Accessible to maintenance and delivery staff only.

Part 1: Create Groups

To simplify this scenario, we will assume that you have already created the destination floor groups, source floor groups and door groups required for user access. See *Scenario 1: Two Companies* for assistance with this process.

In **Groups | Elevator groups**, create two elevator groups: one for all elevators, and one for only the publicly accessible ones.

Elevator Group	Elevator Cars
KONE - All Elevators	Elevator 1 Elevator 2 Goods Elevator
KONE - Public Elevators	Elevator 1 Elevator 2

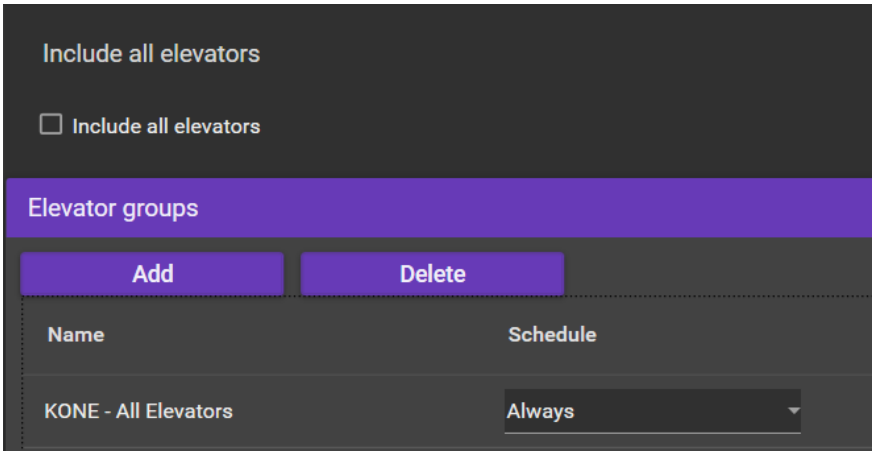
There may already be some elevator groups synchronized from Office Flow. You do not need to create new elevator groups if the ones you need already exist.

Part 2: Create Access Levels

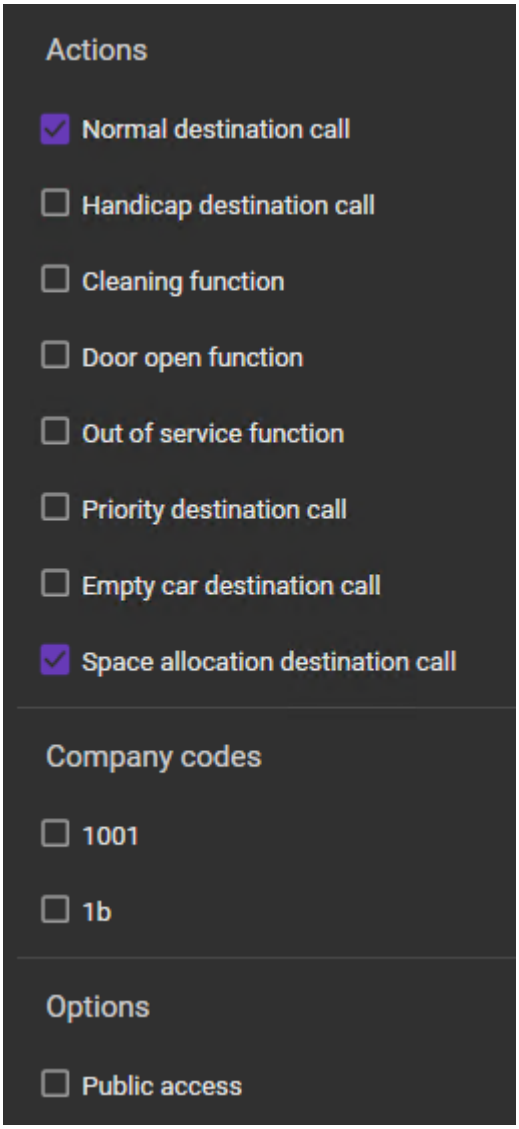
First we will create an access level for maintenance and delivery workers that allows access to all elevators, including the goods elevator.

1. Navigate to **Users | Access levels**.
2. Add a new access level called *KONE - Maintenance and Delivery*.
3. Optionally, set the **Operating schedule** to limit the time of access.
4. In the **Door groups** tab, add *KONE - All DOPs and Turnstiles*.
5. In the **Floor groups** tab, add the destination floor groups that these workers will have access to.
6. Add *KONE - All Source Floors* and set the **Schedule** to *Source Areas Enabled - KONE Integration - DO NOT DELETE*.

7. In the **Elevator groups** tab, add *KONE - All Elevators*.



8. In the **Integration options** tab, select at least one action. If available, choose an action that allows the user to call the goods elevator, such as the **Space allocation destination call** (sometimes called a freight call).

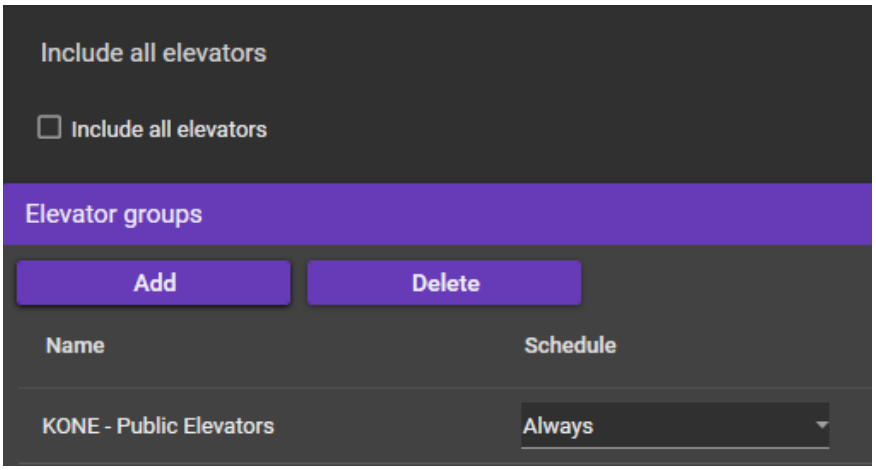


If you are selecting two actions, select the most commonly-used action *first*.

9. Click **Save**.

Next, create user access levels for regular staff members that restrict their elevator access. For example:

1. Add a new access level with a descriptive name.
2. Add the **Operating schedule**, DOPs/turnstiles, destination floors and source floors required.
3. In the **Elevator groups** tab, add *KONE - Public Elevators*.



4. In the **Integration options** tab, enable at least one of the **Actions**.
5. Click **Save**.

Similarly, when you create a public access level, assign the *KONE - Public Elevators* group in the **Elevator groups** tab. This prevents members of the public from calling the goods elevator when they travel between public floors.

Assign the *KONE - Maintenance and Delivery* access level to users who need to access the goods elevator, and assign the other access levels to regular staff members as usual. This ensures that people who need the goods elevator can call it, while regular employees and members of the public do not have access.

If you needed to restrict access to specific DOPs or turnstiles, you would create an 'All DOPs/Turnstiles' door group and restricted doors groups, then apply them to access levels the same way.

Elevator Calls (Virtual Swipe) from Protege GX

Protege GX operators can call an elevator for a specific user using a 'virtual swipe'. For example, a receptionist could use this to call an elevator for someone who has forgotten their credential. This unlocks the DOP, allowing the user to select a destination floor.

This feature is disabled by default and must be enabled if required.

Enabling Virtual Swipe

To enable this feature, you must edit the appsettings.json file for the integration service:

1. In the File Explorer, navigate to **C:/Program Files (x86)/Integrated Control Technology/Protege GX KONE Office Flow Sync Service**
2. Open *appsettings.json* in a text editor.

   Files in this directory require administrator permissions. To edit a file, run Notepad or Notepad++ as an administrator, then open the file from the application. Alternatively, make a copy in a different directory, edit the copy, then replace the original.

3. Locate the following line:

   ```
   "EnableSwipeEvent": false,
   ```

4. Change `false` to `true`.
5. Save the file.
6. Open the Windows Services Manager and restart the **Protege GX KONE Office Flow Events Sync Service**.

Calling Elevators

To call an elevator:

1. Navigate to **Users | Users**.
2. Locate the user who you wish to call an elevator for and right click to open the control menu.
3. Select **Call Elevator**.
4. Select the **Elevator Group** to call, the **Floor** they are traveling from and the **Door** (DOP) where they are currently located.
5. Enable **Direct Action** to send the user's direct action call (the first call enabled in their access level).
6. Click **OK**.

Protege GX will send an access request to KONE as if the user had swiped their card at that terminal. Two events will be saved to the Protege GX event log:

```
Operator Requested Swipe for User with credentials xxx:yyy
Sent Swipe for Elevator Group at Door from Floor with Direct Action State
true/false for User
```

The integration service will return an event when it successfully sends the message to KONE or fails to do so:

```
Successfully sent a swipe event for terminal:a at area:b of elevator
group:c, with credential:dddd:eeee of credentialType:RFID/Bluetooth/QR,
with direct action as enabled/disabled
OR
```

```
Failed to send a swipe event for terminal:a at area:b of elevator
group:c, with credential:dddd:eeee of credentialType:RFID/Bluetooth/QR,
with direct action as enabled/disabled
```

Troubleshooting

Events

Events are generated in Protege GX when the sync service loses or restores its connection to Office Flow:

- `KONE Office Flow Connection Failure to [URL]`
- `KONE Office Flow Connection Restored to [URL]`

Service Logs

Logs are available for each individual service in **C:/Program Files (x86)/Integrated Control Technology/Protege GX KONE Office Flow Sync Service/Logs**

To investigate syncing errors, see the outbound-log files. You may see the following errors:

- **400 (Bad Request)**: The KONE system will reject any access levels that contain Protege GX doors (see page 18). If some users fail to sync, review their access levels. Make sure that:
  - No KONE access levels contain standard Protege GX doors, areas or other records.
  - No Protege GX access levels contain KONE doors, floors or elevator cars.
- **503 (Service Unavailable)**: This error often indicates that KONE Office Flow is rate limiting the synchronization, causing communications from Protege GX to fail. Relaxing the rate limiting can resolve this error, especially during initial synchronization between the two systems. Discuss with your KONE technician.

Certificates

The sync service installer generates a certificate to secure the connection between the sync service and KONE Office Flow. The *Protege GX KONE Cert Renewal Service* will renew that certificate 30 days before its expiry date, retrying daily if the renewal fails. If the certificate does expire without being renewed, the sync service will lose connection to Office Flow.

You can find the relevant logs in the folder above (cert-renewal-log.txt).

Resynchronizing with Office Flow

Minor changes to the Office Flow system (e.g. name changes) will be synchronized automatically. If there are major changes (e.g. floors added or removed), you must manually clear the access data from KONE and resynchronize the two systems.

When the configuration has been updated in KONE, complete the following steps:

1. On the Protege GX server, open a File Explorer and navigate to *C:\Program Files (x86)\Integrated Control Technology\Protege GX KONE Office Flow Sync Service*.
2. Double click the file *Run_ConfigSyncReload_CLEAR.bat*.

   This batch file will clear the Protege GX access data from KONE and pause the synchronization.
3. Once all configuration changes in KONE are complete, double click the file *Run_ConfigSyncReload_RUN_CONFIG_SYNC.bat*.

   This batch file will synchronize the new configuration from KONE to Protege GX. When this is complete, it will resychronize the Protege GX access and user data to the KONE system.

After this, the resychronization is complete and you can continue programming users and access levels in Protege GX as normal. No access levels will be changed apart from removing records that no longer exist.

Known Issues

- When you send a **Call Elevator** command, the dropdowns will show elevator groups, floors and doors created in Protege GX as well as those created in KONE. The operator must select the correct records to include in the call.

API Consumer Certificate of Completion for KONE Site API Integration

is hereby granted to

Integrated Control Technology

To certify that the software and version below has been successfully tested according to product set

Protege GX KONE Office Flow Sync Service [Protege GX] .version1.0.5.0

API	A1000 v1; ConnectivitySuite v4.2

X	A1000 API		Connectivity Suite API

Granted: APRIL 17, 2025

Raymond Ogienoyevbede, Digital Operations Lead

Name, title

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.
Copyright © Integrated Control Technology Limited 2003-2026. 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.