

AN-367

Integrating Hikvision Face Terminals with 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 2003-2026. All rights reserved.

Last Published: 31-Jul-26 1:16 PM

Contents

Introduction	5
Key Benefits	5
Features	5
Integration Architecture	6
How It Works	6
Prerequisites	7
Permissions	8
Biometric Data	8
PIN Codes	9
Connecting the Hikvision Terminals	10
Wiegand Connection	10
Combining Card Readers and Face Terminals	10
Networking Requirements	10
Configuring the Hikvision Terminals	12
Network Settings	12
Wiegand Output	12
PIN Entry	13
Initial Protege GX Setup	14
Adding Reader Expanders and Doors	14
Creating an Operator for the Connect Service	14
Creating a Facial Recognition Consent Setting	15
Setting up the Protege GX Connect Service	16
Installing the Connect Service	16
Logging In to the Connect Service	16
Adding a Site	16
Linking the Service Operator	17
Adding Devices to the Connect Service	17
Additional Protege GX Setup	19
Creating Door Types	19
Assigning Door Types	19
Creating Access Levels	19
Enrolling Users	20
Photo Requirements	20
Enrolling a User from the Client Software	20

Enrolling a User from the Web App	21
End-to-End Validation	22
Monitoring	23
Resynchronizing a User	23
Resynchronizing a Device	23
System Maintenance	24
Refreshing Your License	24
Rotating the Service Operator's Token	24
Backup and Restore	24
Backing Up Data	24
Restoring Data	25
HTTPS Certificates	25
Renewing the Self-Signed Certificate	25
Uploading a Trusted Certificate	25

Introduction

Integrating Hikvision face terminals with Protege GX gives your sites the convenience of facial recognition alongside Protege GX's powerful access control features.

This application note provides instructions for installing and configuring the facial recognition integration using the Protege GX Connect Service.

ICT also offers an integration with Hikvision DVRs. For more information, see [*Application Note 190: Hikvision Video Integration with Protege GX*](#).

Key Benefits

- **Convenient for the end user:** The end user just submits a photo of their face to the site administrator. The next time they walk up to the door, the face terminal authenticates them and unlocks the door before they can even get their card out.
- **Easy for the administrator:** When the site administrator sets up a new user, they upload the user's photo to Protege GX. The system picks up the new user within 30 seconds and synchronizes their photo with the Hikvision face terminals.
- **Simple to install and manage:** The integration is quick to install and configure. The web interface makes it easy to monitor, troubleshoot and maintain the integration with extensive dashboards, logging and device management features.
- **Ready for automation:** Using the ICT Data Sync Service, you can easily combine this integration with visitor management systems and other third-party systems that collect user photos.
- **Cost-effective:** Hikvision devices provide a low-cost entry into biometric authentication. With standalone terminals, you get the benefits of facial recognition without installing a second access management platform.
- **Protects users' privacy:** All data is stored and processed on-premises by default, with no internet connection required. Optionally, the system can require the user's consent to be recorded before it sends their photo to any terminals.

Features

The integration supports the following features:

- Facial recognition
- PIN codes
- Dual authentication (alongside a card reader)
- Automatic synchronization every 30 seconds
- Manual synchronization
- Audit log
- Facial recognition consent setting
- Multiple Protege GX sites

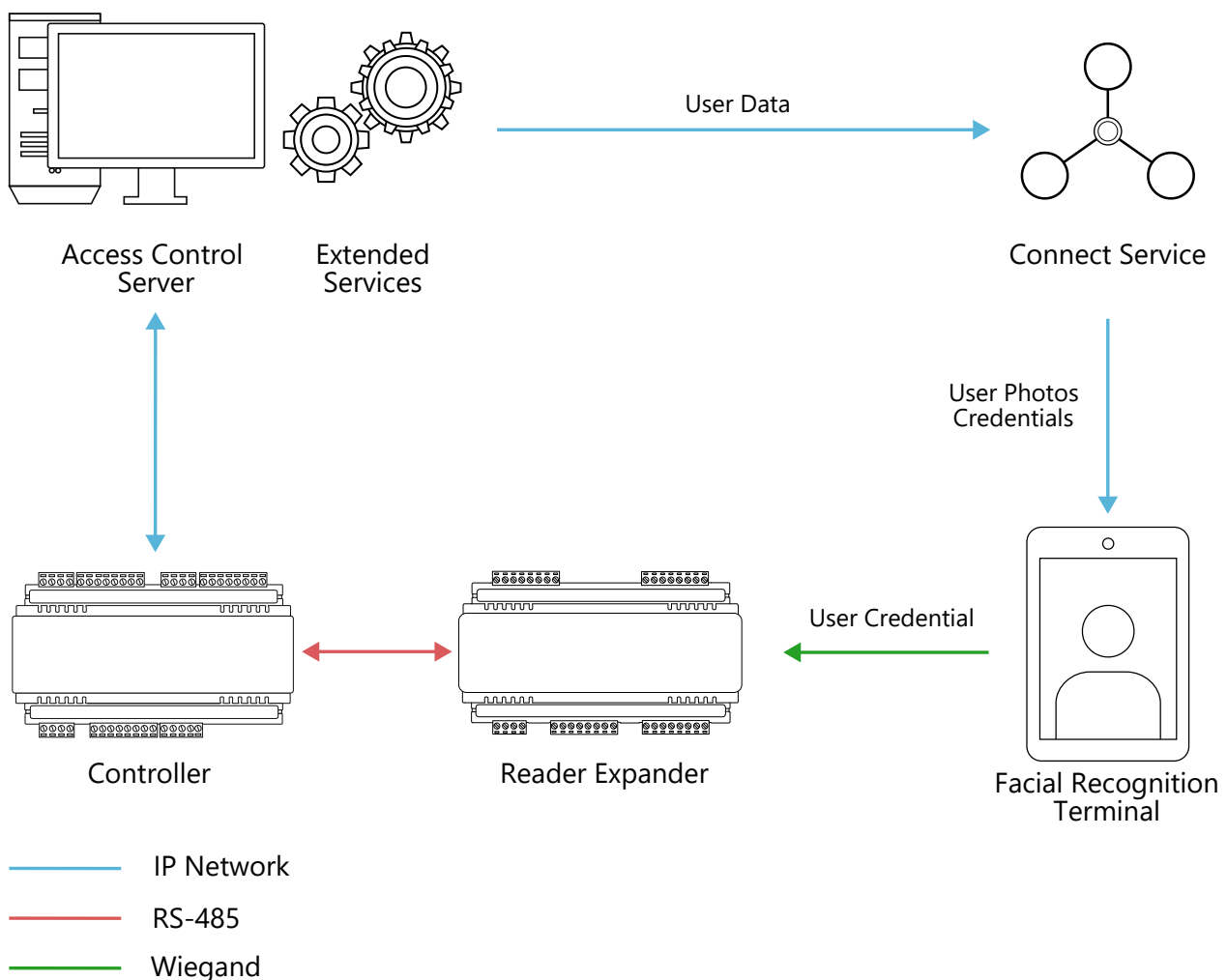
Integration Architecture

This integration uses the **Protege GX Connect Service**, a multi-purpose interface for connecting Protege GX with first-party and third-party systems.

The connect service is responsible for synchronizing data between Protege GX and the Hikvision face terminals. It also provides a convenient web interface for configuring and maintaining the integration.

How It Works

1. Administrators add and update photos, credentials and access rights in the **Protege GX software** or **web app**.
2. The **Protege GX Connect Service** monitors Protege GX for changes, via the **Protege GX Extended Services**.
3. When the connect service detects changes, it sends the latest user photos and credentials to the **Hikvision face terminals** over the ethernet network.
4. Face terminals store the user photos locally. When a terminal detects someone at the door, it matches their face against a known user, then sends that user's credential to the **Protege GX controller or reader expander** over Wiegand.
5. The Protege GX controller processes the access request, then unlocks the door if the user has access.



Prerequisites

Protege GX Components

Component	Version	Notes
Protege GX	4.3.398.2 or higher	
Protege GX Web App	1.38.2 or higher	The connect service relies on the extended services that are bundled with the web app, so you must install the web app even if it will not be used as a web interface.
Protege GX Connect Service	1.30.2 or higher	
Protege GX Controllers	2.08.766 or higher	Controllers must be online and operational.

Third-Party Components

Component	Version	Notes
PowerShell	7	Install the latest version available from the Microsoft website .

Supported Hikvision Devices

This integration supports Hikvision face terminals with ISAPI-capable firmware. It has been validated with the following models:

Component	Version
Pro Face Access Terminal (DS-K1T673DWX)	4.39.20

Other models may work, but have not been validated by ICT. We recommend validating any other models on the test bench before deploying to a site.

Licensing

License	Order Code	Notes
Protege GX Hikvision Biometric Integration License	PRT-GX-HIK	1 license per Hikvision device.
Protege GX Hikvision Biometric Integration Annual Care Plan	PRT-GX-HIK-ACP	1 annual care plan must be purchased for each Hikvision device. It is charged annually for ongoing support and integration updates.
Protege GX Photo ID License	PRT-GX-PHOTO	This license is required to add photos to users in the Protege GX software. No license is required to add photos to users in the Protege GX Web App.
Protege GX Door License	PRT-GX-DOR-1	1 license per door record.
	PRT-GX-DOR-10	
	PRT-GX-DOR-50	

Permissions

- **Installation:** You will need local administrator permissions on the computer where you are installing the connect service.
- **Web Interface:** To access the connect service user interface, you must have a Protege GX operator account with the *Administrator* role.
- **Databases:** If the connect service is running under a restricted account, the account must have **db_datareader** and **db_datawriter** permissions for both the ProtegeGX and ProtegeGXEvents databases.

Biometric Data

Facial recognition data is sensitive personal data that is controlled by laws such as the GDPR and New Zealand Privacy Act (2020). The following information is provided to help the system owner and end users understand the implications of this data storage and processing.

- **Purpose:** Names and face photos are stored for the purpose of access control. Terminals installed beside doors use facial recognition to authenticate users and grant or deny access.
- **Method:** Access control administrators add users to the system and take photos or upload provided photos.
- **Storage:** Data is stored within the ProtegeGX database, primarily on-premises. Some system owners deploy the database to cloud-hosted environments.
User photos are also stored on facial recognition devices, installed on-premises. All communications between Protege GX and the devices are encrypted.
- **Consent:** Depending on your local laws and the organization's policies, you may be required to collect consent before saving photos in Protege GX and using them for facial recognition.
Optionally, Protege GX can track users' consent. In this case, photos will only be synchronized to the devices once the consent is recorded in Protege GX.

See [Creating a Facial Recognition Consent Setting](#) and [Adding a Site](#) for setup instructions.

- **Retention:**
 - User photos are retained in Protege GX until the photo or user record is deleted by an operator. Users cannot self-delete, but can ask an access control administrator to remove their data.
 - Deleted user data may be retained in system backups for a certain period of time, depending on the system owner's policies.
 - Each user photo is only stored on terminals that the user needs access to. If the user does not have access to a door, the terminal at that door does not store their face data.
 - If the user no longer meets the criteria for a specific door, their data is removed from that device. User photos are removed when:
 - The user withdraws consent for facial recognition.
 - An administrator removes the user's access rights.
 - The photo or user record is deleted.
 - The user record is disabled.
 - The device is unlinked from Protege GX.

If the device is physically disconnected from the network before it is unlinked from Protege GX, you must remove the user data from the device separately (e.g. using a factory reset).

- **Recommendations:**
 - Review your local laws and organizational policy before implementing the biometric access control system.
 - Always inform users that their photos will be used for access control, even if consent is not required.

- Offer alternative access methods for users who do not consent to facial recognition (e.g. PIN code, card).

For more information about how ICT processes personal data, see the [ICT Data Management Overview](#).

PIN Codes

Hikvision devices support PIN code entry as an alternative to facial recognition. However, the device is not able to pass received PIN codes directly to the Protege GX controller or reader expander.

If you enable PIN code authentication, it works as follows:

1. The connect service syncs each user's PIN codes to the Hikvision terminals.
2. When the user enters their PIN code, the Hikvision terminal matches the PIN to a known user.
3. The Hikvision terminal sends the user's biometric credential to the controller or reader expander to request access.

There are a few key implications that you should be aware of:

- PIN codes are saved to the Hikvision device and are visible to device admins.
- Users are able to use expired PIN codes on Hikvision terminals. Protege GX has no way to tell the terminal that the code has expired.
- The event log will state that the user gained access using their facial recognition credential rather than a PIN code.
- It is not possible to use a Face and PIN credential sequence with only the Hikvision terminal. However, you can achieve this by connecting a card reader to the same reader port ([see next page](#)).
- Duplicate PIN codes are not supported.
- Features that rely on specific codes being entered into the reader (e.g. function codes) are not supported.

Connecting the Hikvision Terminals

Each Hikvision terminal has two connections to the Protege GX system:

1. **Ethernet connection** to the network, allowing Protege GX to send biometric data to the terminals. The terminals must be reachable from the computer where the connect service is installed.
2. **Wiegand connection** to the Protege GX controllers and reader expanders. When a user presents their face, the face terminal sends a facility and card number over the reader port, in the same way as a standard card reader.

Hikvision terminals only support OSDP as controllers, not as peripheral devices. Therefore, it is not possible to connect a Hikvision terminal to the controller or reader expander over OSDP.

Wiegand Connection

To connect the face terminal over Wiegand, use the following wiring connections:

Face Terminal Wire	Typical Wire Color	Pin on Protege Reader Port
Wiegand W0	Green	Wiegand D0
Wiegand W1	White	Wiegand D1
Power +12V	Red	V+
Ground GND	Black	V-

Wire colors may be different for different devices. Confirm with the device's installation manual before you make the connection.

To use Hikvision terminals for entry and exit on the same door, you can multiplex them into a single reader port. For the exit reader, connect **Wiegand W1** to the **D1** terminal of the other reader port. See the installation manual for your controller or reader expander for more information.

Do not connect the Hikvision device's relays to the door locks. The locks must be controlled by the Protege modules.

Combining Card Readers and Face Terminals

To allow users to access the door with a card, you can combine a card reader with the face terminal. This also enables you to use dual credentials (face and card, face and PIN).

To connect a card reader alongside a terminal:

- Wire the biometric device and the card reader to the same reader port.
- The ICT card reader must be in Wiegand mode.

See the *ICT Card Reader Configuration Guide* for instructions for enabling Wiegand mode.

- The door type determines which credentials each door will use—see [Creating Door Types](#).

Networking Requirements

This integration requires the following networking configuration:

- Each Hikvision device must have a static IP address.
- The following communication path must be open on the relevant firewalls:

From	To	Description
Connect Service TCP 5080	Hikvision Terminals TCP 443	Receive polls and user data from the connect service.

Configuring the Hikvision Terminals

This section covers the basic settings required to connect Hikvision terminals to the Protege GX system and controller.

For more information about device settings, see the relevant product manual, e.g. [Pro Face Access Terminal Manual](#).

Network Settings

1. Use an ethernet cable to connect the terminal to a laptop or computer.
2. Change the IP address of the network adapter to 192.0.0.x.

See [How to change the IP address of a network adapter](#) in the Microsoft Knowledge Base.
3. Open a web browser and navigate to the default IP address of the Hikvision device. For the Pro Face Access Terminal, this is **192.0.0.64**.
4. Create a new admin password and activate the device.
5. Log in to the web interface.
6. Navigate to **System and Maintenance > System Configuration > Network**.
7. On the **Network Settings** tab, enter the required network settings and click **Save**.
8. You can now disconnect the device from the laptop and connect it to its intended network.

Wiegand Output

1. Log in to the Hikvision terminal's web interface.
2. Navigate to **System and Maintenance > System Configuration > Access Configuration**.
3. On the **RS-485** tab, disable **Serial Port Parameter**.
4. On the **Wiegand Settings** tab, set the following:
 - **Wiegand**: Enabled
 - **Wiegand Direction**: Output
 - **Wiegand Mode**: Wiegand34

HID 34-bit is the default credential format in the connect service, but Wiegand26 can also be used if preferred.

 - **Time Interval**: 1
 - **Pulse Width**: 100

Click **Save**.
5. Because this integration does not support card reading, we recommend that you disable all card types on the terminal.
Navigate to **Access Control > Access Control Parameters**.
6. In the **Card Settings** tab, disable all card types and click **Save**.

PIN Entry

To enable PIN code entry on the Hikvision terminal, you must change the device's PIN mode setting:

1. On the **Access Control > Access Control Parameters** page, open the **Privacy Settings** tab.
2. Set the **PIN Mode** to **Device-Set Personal PIN**.
3. Click **Save**.

Repeat all required configuration for each Hikvision terminal.

Initial Protege GX Setup

Some configuration is required in Protege GX before you set up the connect service.

Make sure you update your software license in **About | License | License update**.

Adding Reader Expanders and Doors

Each terminal is configured the same way as a card reader in Protege GX. Before you connect the terminals to the connect service, you must create and configure the reader expanders and doors that they will be physically connected to.

1. In Protege GX, navigate to **Expanders | Reader expanders**.
2. In the toolbar, select the **Controller** that the terminals will be connected to.
3. Click **Add** to add a new reader expander, or select an existing one.
4. Set the **Physical address** of the reader expander.
5. If there is a face terminal connected to reader port 1, set the **Port 1 network type** to *Wiegand*.
6. If this reader port uses multiplexed entry/exit readers, enable **Multiple reader input port 1**.
7. In the **Reader 1** tab:
 - Set the **Reader 1 format** to *Custom credential*.
 - Disable **Intelligent reader tamper mode**.
8. If there is a face terminal connected to reader port 2, repeat the above steps for the reader port 2 settings.
9. Configure any other settings required.
10. Click **Save**.
11. If you are adding a new reader expander, ensure that **Add doors** is enabled. Click **Add now**.
12. Repeat to add and configure all reader expanders required for this integration.
13. If you have added new doors, navigate to **Programming | Doors** and give them descriptive names.

We will create the required door types later ([see page 19](#)).

Creating an Operator for the Connect Service

The connect service automatically generates credentials for users before syncing them to the face terminals. By default, events and the History tab attribute these changes to the SYSTEM operator.

We recommend creating a unique operator record for use by the connect service. This ensures that the events and record history accurately indicate where the edits came from.

You must create an operator and register them in the web app:

1. In Protege GX, navigate to **Global | Operators**.
2. Add a new operator with a descriptive name (e.g. *Connect Service*).
3. Enter a **Username** and **Password** for the operator.
4. Give the operator a **Role**. This operator will need access to edit users, so an **End User** role is appropriate.
5. Click **Save**.

Creating a Facial Recognition Consent Setting

Depending on your local laws or company policies, administrators may need to collect consent from users before using their photos for facial recognition ([see page 8](#)).

Optionally, you can record users' consent in Protege GX. If you use this feature, user photos will not be sent to the face terminals unless the user has consented and the consent is recorded. You do not need to use this feature if the organization will manage photo consent outside of Protege GX.

To record consent in Protege GX, you can create a custom field:

1. In Protege GX, navigate to **Users | Custom fields**.
2. Add a new custom field with a descriptive name, e.g. *Facial recognition consent*.
3. The **Tab** determines where this custom field will appear on the users page. Select an existing custom field tab, or click the ellipsis [...] to add a new one with a descriptive name (e.g. *Consent*).
4. Set the **Field type** to *Option*.
5. Click **Save**.
6. Navigate to **Users | Users**. You will find your new setting in the tab that you specified above.

Later, you will link this custom field to the connect service to manage consent ([see next page](#)).

Setting up the Protege GX Connect Service

This section covers how to install and log in to the connect service, and how to connect terminals.

Installing the Connect Service

The connect service uses the Protege GX Extended Services to authenticate operators and retrieve connection settings. Before you install the connect service, you must install the Protege GX Web App, which includes the extended services.

See the [Protege GX Web App Installation Manual](#) for instructions.

To install the connect service:

1. Run the connect service installer on the same machine where the web app is installed.
2. If you have a backup file from a previous installation, select **Restore from backup**. Otherwise, select **Install new** and click **Next**.
3. Click **Install**. The installer will install the new service and automatically connect it to Protege GX.
4. When the installation is complete, click **Finish**. The web interface will open automatically at **<https://localhost:8084>**

If needed, you can find the log file for the installation process (install.log) in the installation directory:

C:\Program Files (x86)\Integrated Control Technology\ConnectService

Logging In to the Connect Service

You can log in to the connect service using your Protege GX operator credentials, along with the two-factor authentication app that you use to access the web app.

Only operators with the *Administrator* role can log in to the connect service. This is the **role** with **Database ID 0**.

To log in to the connect service:

1. If you have not yet set up your web app account, open the web app in a browser. On the server computer, you can use the URL: **<https://localhost:8083>**
2. Sign in using your Protege GX operator credentials. When prompted, set up an authenticator app for two-factor authentication.
3. Browse to the connect service: **<https://localhost:8084>**

On other computers, the URL will be: **<https://servername.domainname:8084>**

4. Enter your Protege GX **Username** and **Password**.
5. When prompted, enter the code from your authenticator app and click **Verify**.

You will see the **Dashboard**, which provides an overview of your devices, sync status, warnings and errors.

Adding a Site

Before you can add devices, you must set up your site. The site settings determine whether Protege GX will record users' consent for facial recognition.

You need a custom field in Protege GX before you can enable the consent setting for your site ([see previous page](#)).

To add a site:

1. Navigate to **Sites**.
2. Click **Add site**.
3. Under **Facial-recognition consent**, select either:
 - **No facial-recognition consent required**
 - **Use a consent field** (i.e. consent is required to synchronize user photos)
4. If consent is required, set the **Consent field** to the custom field you created above.
5. If the consent field is a text field, enter a **Match pattern** (e.g. *Yes, Approved or Consented*).
6. Click **Save changes**.

Linking the Service Operator

If you want to use a dedicated service operator, you must link the operator record created above (see page 14) to the connect service. This ensures that automated edits are correctly attributed to the connect service in the event log and record history.

To link the operator:

1. Navigate to **Credentials**.
2. Under **Automated Background Changes**, click **Set sync identity**.
3. Select the **Service operator** created above.
4. Set an appropriate **Token expiry** time. The default is 1 year, but you can select a shorter period if required.
5. Click **Save**.

Make a note of the token's expiry date. Before the token expires, someone must log in and click the **Rotate** button to generate a new token (see page 24).

Adding Devices to the Connect Service

You can now add Hikvision terminals to the connect service so that they can receive user credentials and photos from Protege GX.

Before you begin, ensure that all terminals are connected and available over the network. You must also configure your site in the connect service first (see previous page).

To link a new device:

1. In the connect service, navigate to **Devices**.
2. Click **Add device**.
3. On the **Connection** tab, enter the following details:
 - Set the **Vendor** to *Hikvision*.
 - Enter the **IP address** and **Port** used to communicate with this device.
 - Enter the **Username** and **Password** for the device's administrator login.
4. Click **Test connection** to check whether the connect service can reach the device. If this fails, check the IP address and credentials. Ensure that your firewall is not blocking the outbound connection on this port.

You can check your connection settings by opening the face terminal's web interface in your browser. If you can't access the terminal, neither can the connect service.

Click **Next**.

5. On the **Identify** tab, enter a **Device name**, e.g. *Reception Door Face Terminal*. This will be displayed within the connect service.
Click **Next**.
 6. On the **Assign** tab, select the **Door** that this terminal will control. You can find the door using its name or Database ID.
 7. Select the **Direction** that the terminal will control (*Entry* or *Exit*).
 8. The first time you set up a biometric device, you should create a new credential type to represent the biometric credentials:
 - Select **Create a new credential type**.
 - Enter the **Credential type name** (e.g. *Face/PIN*). This will appear on each user record in Protege GX.

This credential type will be sent by the terminal regardless of whether the user presents their face or their PIN code, so we recommend calling it *Face/PIN* to avoid confusion.
 - Enter a **Facility code**. This must be a unique code that is not used for any cards on the site.

For subsequent devices, you can select the existing credential type from the list.
 9. Set up a **Credential profile**. This determines the *Wiegand format* used to structure the credentials.
 - For most situations, the **Default HID 34-bit** format is appropriate. This corresponds to **Wiegand34** in the Hikvision devices.
 - Alternatively, Hikvision devices also support Wiegand26 (standard HID 26-bit). If the terminals are using the 26-bit format, click **Add profile** and enter the credential format details. See [Everything ID](#) for the format structure.
 10. On the **Capabilities** tab, select whether this terminal will support face, PIN or both.
Click **Next**.
 11. Review the settings, then click **Add device** to complete.
- Repeat to add all of your Hikvision devices.

Additional Protege GX Setup

A few additional steps are needed in Protege GX to complete the integration setup.

Creating Door Types

The connect service has created a *Facial Recognition* credential type for use by the terminals (in **Sites | Credential types**). Now you can create a door type that accepts that credential type, for use by doors with face terminals connected.

Facial Recognition Door Type

1. In Protege GX, navigate to **Programming | Door types**.
2. Add a new door type with a descriptive name (e.g. *Face Terminal*).
3. Set the **Entry reading mode** to *Custom*.
4. Under **Entry credential types**, add the *Face/PIN* credential type created above.
5. Repeat for the **Exit reading mode** if exit readers use the same credentials.
6. Click **Save**.

Alternative Credentials

- **Face or PIN:** When the terminal receives a PIN code, it authenticates the PIN code on the device and sends the *Face/PIN* credential to the controller. Therefore, no additional configuration is required to support Face or PIN.
- **Face or Card:** Set the **Fallback door type** to *Card*. Requires a card reader connected to the same reader port as the terminal.

Dual Credentials

- **Face and PIN:** Add *PIN* to the **Entry/Exit credential types**. Requires a card reader connected to the same reader port as the terminal.
- **Face and Card:** Add *Card* to the **Entry/Exit credential types**. Requires a card reader connected to the same reader port as the terminal.

Assigning Door Types

Next, assign the relevant door types to doors:

1. Navigate to **Programming | Doors**.
2. Select each door controlled by a terminal and set the **Door type** as required.
3. Click **Save**.

Creating Access Levels

Finally, you will need access levels to grant access to the face terminals.

1. Navigate to **Users | Access levels**.
2. Add a new access level or edit an existing one.
3. Add the doors controlled by face terminals to the **Doors** or **Door groups** tabs.
4. Click **Save**.

Enrolling Users

The connect service synchronizes user details to face terminals when they meet specific requirements:

- The user needs an **access level** that grants access to the door. The connect service only sends user details to terminals that they have access to.
- **For facial recognition:**
 - The user record must have a **valid photo**. See the guidelines below.
 - If consent is required, the **consent custom field** must be filled in.
- **For PIN code authentication**, the user must have a PIN code.

The connect service detects changes to user records every 30 seconds. It will automatically generate a unique credential for each user, then synchronize their credential, photo and/or PIN code to the terminals that the user has access to.

If you update the user's name, credential, PIN code or photo on the terminal, the connect service will overwrite those changes the next time it syncs that user.

Photo Requirements

Before you upload photos to Protege GX, check that they meet the following requirements. This ensures that the face terminal will accept the photo and can use it for facial recognition.

- **Composition:** Photo contains one face only, which is front-facing and unobstructed. Eyes are open and looking at the camera. The subject is not wearing sunglasses.
- **Lighting:** Evenly lit. Avoid strong shadows or backlighting.
- **Background:** Plain or neutral preferred.
- **Recency:** Photo must have been taken in the last 24 months.

The service will automatically compress and convert photos if required before transmitting them to the face terminals.

Photos that do not meet these requirements will be rejected by the face terminal. To see failed syncs, in the connect service navigate to the **Sync** page and select **Failures only**.

If a sync fails, you must ask the user to supply another image that meets the requirements above.

Enrolling a User from the Client Software

To enroll a user from the Protege GX client:

1. Request a suitable photo from the user. Alternatively, if the user is present in person you can take a photo using your computer's webcam (below).

Ensure that the user gives their consent to use their photo for facial recognition, if required by your organization.

2. In the software, navigate to **Users | Users**.
3. Add a new user or select an existing one.
4. Set a PIN for the user if required.
5. On the **Access levels** tab, add their required access levels.
6. On the **Photo** tab, click **Add photo**.
7. Click the ellipsis [...] to upload a photo. Click **Next**.

To take a photo, set the **Image source** to *Integrated webcam*, click **Next**, then capture the photo.

8. Crop the image as required, then click **Ok**.
9. If your organization records user consent in Protege GX, open the **Consent** tab and enable **Facial recognition consent** (or similar).
10. Click **Save**.

The connect service will automatically create a unique *Face/PIN* credential for the user, then synchronize their data to the face terminals. The user should now be able to gain access to doors using their face or PIN code.

Enrolling a User from the Web App

To enroll a user from the Protege GX Web App:

1. Request a suitable photo from the user. Alternatively, if the user is present in person you can take a photo using your computer's webcam (below).

Ensure that the user gives their consent to use their photo for facial recognition, if required by your organization.

2. In the web app, navigate to  **Users, Manage**.
3. Add a new user or select an existing one.
4. Select  **Take picture** or  **Upload picture**. Follow the prompts to crop the image.

The image must be between 900x900 and 1024x1024 pixels. The maximum file size is 5MB.

5. Scroll down to the  **Access levels** section and click **+ Add access levels** or **View access level details**.
6. Select the access levels that this user needs.
7. Click **Add**, then **Done**.
8. Under  **Credentials**, set a **PIN code** if required.
9. If your organization records user consent in Protege GX, expand the **Consent** section and enable **Facial recognition consent** (or similar).
10. Click **Save**.

The connect service will automatically create a unique *Face/PIN* credential for the user, then synchronize their data to the face terminals. The user should now be able to gain access to doors using their face or PIN code.

End-to-End Validation

To validate the integration end-to-end, you can set up a new user, take your own photo and sync it to the Hikvision terminal, then gain access.

These instructions use the Protege GX software, but you can use the web app if preferred.

1. In the Protege GX software, navigate to **Users | Users**.
2. Add a new user.
3. Enter a **PIN**.
4. In the **Access levels** tab, select an access level that contains the relevant door.
5. In the **Photo** tab, click **Add photo**.
6. Set the **Image source** to *Integrated webcam* and take a photo of yourself.
7. Crop the image, then click **Ok**.
8. If consent is required, open the **Consent** tab and enable **Facial recognition consent** (or similar).
9. Click **Save**.
10. Wait for 30 seconds.
11. In the connect service, open or refresh the **Sync** page. Your new user should appear in the list with the message "Synced".
12. Present your face to the Hikvision terminal. It should authenticate you and display your name. The door should unlock.
13. In Protege GX, refresh the user record. Under **Credentials**, you should see the new *Face/PIN* credential.
14. Open a status page or floor plan. You should see events similar to the following:

```
User 'Petra Logan' Modified By Operator 'Connect Service'  
User Petra Logan Granted Entry to Reception Door Access Level Installer  
Using Credential 9010:3
```
15. Enter the user's PIN code.
16. The terminal should display **Access Granted** and the door should unlock. The status page will display the same access event as above.

Monitoring

The connect service makes it easy to monitor the status of your integration. Use the following pages to check the system:

- **Dashboard:** Shows a summary of online and offline devices, recent activity and sync failures.
- **Devices:** Displays each device's status, the results of the last sync, and the audit trail for operator actions.
- **Sync:** Displays the users that have been synced to the terminals.
Any users that have failed to sync will be displayed in the **Failures only** tab. This usually happens because the photo does not meet the requirements for facial recognition. Expand the user to see the error message.
- **Audit Trail:** Records operator actions, including changes to the connect service configuration and forced syncs. Audit logs are retained for 90 days.

Resynchronizing a User

When you update a user, the connect service will pick up the change and push it to devices within 30 seconds. Alternatively, you can manually force a resync.

1. In the connect service, navigate to **Sync**.
2. Use the search bar to find the required user.
3. Expand the user, then expand the device you want to resync.
4. Click **Resync**.

Resynchronizing a Device

If a device goes offline, then comes online again, the connect service will resend the latest sync data. You can speed this up by manually forcing a sync.

1. In the connect service, navigate to **Devices**.
2. Select the device you want to resync.
3. Click **Sync now**.

System Maintenance

This section covers key steps for maintaining your system.

Refreshing Your License

The connect service checks the Protege GX license for changes every 6 hours. If you update the Protege GX license (e.g. adding more devices), you can manually refresh the license to update the connect service immediately.

To refresh the license:

1. Update the license in Protege GX (**About | License | License update**).
2. In the connect service, navigate to **System**, then **Licensing**.
3. Click **Refresh license now**.

Rotating the Service Operator's Token

When you link an operator to the connect service, the service generates an **API token**. This allows the operator to connect to the extended services API whenever it needs to edit the database. This token will expire after a set time, so you must log in to the connect service and rotate the token at least once per year.

If the token expires, the connect service will no longer be able to add facial recognition credentials to users.

When you first set up the operator ([see page 17](#)), make a note of the token's expiry date.

Before the token expires, rotate it as follows:

1. Log in to the connect service.
2. Navigate to **Credentials**.
3. Click the  **Rotate** button.
4. Make a note of the new expiry date.

Backup and Restore

The connect service stores data in a dedicated database that is not hosted in SQL Server with the standard Protege GX databases. You must back up and restore the connect service separately.

Backing Up Data

From the connect service web interface, you can take a one-off backup or enable regular automated backups. Backup files are in the **.csbak** format and include all configuration and audit logs.

1. In the connect service, navigate to **System**, then **Backup**.
2. **To enable daily automated backups:**
Enter a **Backup passphrase** and click **Set passphrase**. This immediately enables automated backups. Automated backups will be saved to: **C:\Backups**. 7 days of backups will be retained.
3. **To take a backup immediately:**
Under **Back up now**, select **Saved passphrase** or **One-time passphrase**. Click **Create & download backup**.

You must store passphrases in a safe location such as a password manager. **If you do not have the passphrase, you will not be able to restore the backup.**

Restoring Data

If you need to recover data or migrate the software to another computer, you can restore a backup when you install the connect service.

1. Uninstall the Protege GX Connect Service (if already installed).
2. Select **Restore from backup**. Click **Next**.
3. Click **Browse** and select the **.csbak** file to restore.
4. Enter the **Passphrase** used to create the backup.
5. Click **Save**.

HTTPS Certificates

When you install the connect service, it generates a self-signed HTTPS certificate to secure the connection with your web browser. This certificate is a copy of the certificate used by the web app.

Renewing the Self-Signed Certificate

The connect service certificate will expire at the same time as the web app certificate—i.e., 2 years after the web app was installed. You can see the certificate's expiry date in the connect service interface, under **System, HTTPS certificate**.

Before the certificate expires, you must either renew it, or install a new certificate (see below). The easiest method for renewing the certificate is:

1. Renew or replace the web app certificate.
2. Run the connect service installer again. There is no need to uninstall the service before running the installer.

If you do not renew the certificate, users will see a security warning when they open the web interface. Depending on their web browser's security settings, they may be unable to access the interface.

Uploading a Trusted Certificate

Optionally, you can install a trusted certificate from an internal PKI or third-party CA. This will remove the security warning that may appear when you visit the web interface.

1. Acquire a certificate in **.pem** or **.pfx** format.
2. In the connect service, navigate to **System**, then **HTTPS certificate**.
3. Select the **Format** of your certificate.
4. Enter the certificate details or upload the file.
5. Click **Validate & save**.
6. Open **Services** as an administrator:
 - Press the **Windows + R** keys.
 - Type **services.msc**.
 - Press **Control + Shift + Enter**.

7. Locate the **Protege GX Connect Web Server**.
8. Right click and select **Restart**.

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.