



Integrated Control Technology

Protege GX

Release Notes | Version 4.3.402



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: 08-May-26 11:47 AM

Contents

Introduction	5
Important Updates	5
Upgrading Protege GX to 4.3.402	6
64-Bit Software	7
Supported Operating Systems	7
SQL Server Compatible Versions	7
Firmware Versions	8
Protege GX Software Version 4.3.402	9
Password Security Enhancements	9
Integration Updates (4.3.402)	10
Feature Enhancements (4.3.402)	12
Issues Resolved (4.3.402)	14
Previous Software Release History	17
Protege GX Software Version 4.3.352.10	17
Feature Enhancements (4.3.352.10)	17
Issues Resolved (4.3.352.10)	17
Protege GX Software Version 4.3.352.7	17
Feature Enhancements (4.3.352.7)	17
Issues Resolved (4.3.352.7)	18
Protege GX Software Version 4.3.342	20
Issues Resolved (4.3.342)	20
Protege GX Software Version 4.3.341	20
New Features (4.3.341)	20
Feature Enhancements (4.3.341)	21
Issues Resolved (4.3.341)	22
Protege GX Software Version 4.3.327	23
New Features (4.3.327)	23
Feature Enhancements (4.3.327)	24
Issues Resolved (4.3.327)	24
Protege GX Software Version 4.3.322	25
Feature Enhancements (4.3.322)	25
Issues Resolved (4.3.322)	25
Protege GX Software Version 4.3.319	26
Feature Enhancements (4.3.319)	26
Issues Resolved (4.3.319)	26

Introduction

This document provides information on the new features, enhancements and resolved issues released with:

- Protege GX software version 4.3.402

A release history for previous versions is also included.

Important Updates

This version includes some significant changes that may affect your Protege GX site. Read this document carefully to understand what preparation and actions are required when you upgrade to this version.

In particular, be aware of the following changes:

- If your Protege GX server uses a 32-bit operating system, it is not possible to upgrade the software to this version. For more information, see [64-Bit Software](#) (page 7).
- Due to cybersecurity enhancements, Protege GX no longer allows unencrypted connections. If your system currently uses unencrypted connections, you must update them to use TLS 1.2 or HTTPS encryption before you upgrade the software. **If you do not implement encryption, parts of your system may lose connection to each other after the upgrade.**

For more information and the actions you need to take, see [Upgrading Protege GX to 4.3.402](#) or [Application Note 366: Upgrading Protege GX to Version 4.3.402](#).

- If your system uses the Suprema biometric integration, your existing devices may not be supported in this Protege GX version, or may need firmware upgrades. For more information, see [Integration Updates \(4.3.402\)](#) (page 10).

Upgrading Protege GX to 4.3.402

The latest versions of Protege GX, SOAP service and web client include major enhancements to password and encryption security (see page 9). Because of these changes, you must complete additional configuration when you upgrade the system.

This page provides a summary of the actions you must take when you upgrade the software from version 4.3.352 (or earlier) to 4.3.402. **Failure to complete these actions may lead to parts of the system losing connection with each other.**

For detailed information and instructions, see [Application Note 366: Upgrading Protege GX to Version 4.3.402](#).

Before You Upgrade

Before performing this upgrade, ensure that you have read these release notes and understand the system changes that have been introduced in this version. In particular, be aware of the following:

- If your server uses a 32-bit operating system, you cannot upgrade the software. You must migrate your operating system to a 64-bit version first (see next page).
- If your system currently uses unencrypted connections, we recommend updating all components to use TLS 1.2 or HTTPS before you upgrade the software. This includes:
 - Enable TLS 1.2 on the Protege GX server and clients
 - Enable TLS 1.2 on the SOAP Service
 - Update all applications connected to the SOAP service to use HTTPS. This includes:
 - ICT Data Sync Service
 - Protege Entry Station Directory Integration
Requires a firmware upgrade to version 1.12.203.
 - Protege Tenancy Portal Sync Service
 - Protege Access+
 - Protege Mobile App
 - KeyWatcher Integration Service
Requires a software upgrade to version 1.0.0.11.
 - KeySecure Integration Service
 - Any custom integration using the SOAP service
 - Validate the web client HTTPS connection
- Upgrade third-party SOAP integrations to support the latest SOAP service

Upgrading the Software

You must upgrade the server, clients, SOAP service and web client to the latest versions **at the same time**. Any components that are not upgraded will not be able to connect to other parts of the system.

Ensure that you upgrade all components to the following versions:

Software	Required Version
Protege GX Server and Client	4.3.399.40 or higher
Protege GX SOAP Service	1.7.0.0 or higher
Protege GX Web Client	1.48.2.1 or higher

When upgrading, you must select either TLS or Windows Authentication for the security mode. The None option is no longer available. Ensure that all components use the same protocol.

After Upgrading

- When an operator first logs in to the Protege GX client or web client, Protege GX will force them to change their password.
- If an operator using the mobile app has a non-compliant password, they must update their password in the thick client or web client, then reconnect to their place in the app. We recommend transitioning operators to the new Protege Access+ app for a better experience.
- Any operator passwords used by applications connected to SOAP must be updated. To update a password, log in to Protege GX using the SOAP operator's details. Update the password in the operator record, then enter the same password into the configuration for the integration service or application.

64-Bit Software

The Protege GX Download Service has been upgraded from a 32-bit service to a 64-bit service. Because of this, this software version is **not** compatible with 32-bit operating systems. If you attempt to upgrade the software to this version on a 32-bit platform, the upgrade will fail.

If your Protege GX server is 32-bit, you must upgrade it to a 64-bit operating system that is listed in [Supported Operating Systems](#). When you change your operating system, you must also contact ICT to update the server profile in your Protege GX license.

For advice on server migration, see these knowledge base articles:

- [Server Migration Preparation](#)
- [Protege GX Server Migration Process](#)

In addition, if your system uses the Suprema Biometric integration, you must add specific 64-bit DLL files into the Protege GX installation folder. For more information and instructions, see [Application Note 264: Suprema Biometrics Integration with Protege GX](#).

Supported Operating Systems

Operating System	Edition	Architecture
Microsoft Windows Server 2025	Standard, Datacenter	64-bit
Microsoft Windows Server 2022	Standard, Datacenter	64-bit
Microsoft Windows Server 2019	Standard, Datacenter	64-bit
Microsoft Windows Server 2016	Standard, Datacenter	64-bit
Microsoft Windows 11	Pro, Business, Enterprise	64-bit
Microsoft Windows 10	Professional, Enterprise	64-bit

SQL Server Compatible Versions

The Protege GX application uses a non-proprietary open SQL database engine to store and share information. The software is compatible with SQL 2016, 2017, 2019 and 2022 in Standard, Express, and Enterprise editions.

The Express edition is a scaled down, free edition of SQL Server that includes the core database engine and functionality. The Express version of SQL supports a database size of up to 10 GB.

To obtain either SQL or SQL Express, download the appropriate installer from the Microsoft website. It is also recommended to download SQL Server Management Studio from Microsoft in order to configure SQL. Download the latest general availability (GA) version of SSMS from the Microsoft website.

Firmware Versions

The Protege system is a high-performance integrated system. To ensure your installations are running at the optimal performance we recommend that all installed modules use the latest firmware releases.

For a complete list of current firmware versions, please refer to the ICT website (www.ict.co/Firmware).

Firmware updates are available online from the ICT website or through your distribution channel. If you are having difficulty downloading any firmware or finding the appropriate version, please contact the ICT Technical Support team.

Protege GX Software Version 4.3.402

Password Security Enhancements

This version of Protege GX includes improvements to the security of passwords used by system operators. All operator passwords must now meet the following requirements:

- 8-32 characters long
- Does not contain any part of your username or email address
- Contains at least three out of four character types:
 - Uppercase letter
 - Lowercase letter
 - Number
 - Special character

In addition, Protege GX has introduced more protections around the communication of operator passwords.

- **One-time passwords:** It is not possible for anyone to set a permanent password for another operator, ensuring that only the operator knows their own password. When someone else sets an operator's password, the **Change password on next login** checkbox will be enabled. The operator will be required to set a new password the next time they log in.
- **Encrypted connections:** Protege GX no longer accepts unencrypted connections, preventing passwords and other sensitive data from being sent in the clear. It now requires:
 - Encrypted connections between server and clients (TLS 1.2)
 - Encrypted connection between server and SOAP service (TLS 1.2)
 - Encrypted connections between the SOAP service and integrated applications (HTTPS)
 - Encrypted connections between the web client and web browsers (HTTPS)
- **SOAP API Changes:** Applications must log in to the SOAP service using LogonType 0. LogonType 1 has been deprecated.

Altogether, these enhancements ensure that all Protege GX operators have strong passwords, and those passwords are never sent over unencrypted connections.

Due to these changes, you must complete additional configuration when you upgrade the system. See [Upgrading Protege GX to 4.3.402](#) or [Application Note 366: Upgrading Protege GX to Version 4.3.402](#) for more information.

Integration Updates (4.3.402)

This version includes the following new integrations and enhancements to existing integrations.

KONE Office Flow Integration

This version of Protege GX includes support for the KONE Office Flow integration, allowing Protege GX users to seamlessly access card readers in a KONE Office Flow system. All user records, credentials and access are managed in Protege GX, simplifying the access control system and eliminating the time spent programming duplicate records in two different systems.

For more information about this integration, see Application Note 361: Protege GX KONE Office Flow Integration.

Milestone XProtect Access Integration

The Protege GX XProtect Access Integration synchronizes Protege GX records and events with the Milestone XProtect video management system (VMS), unlocking a wide range of functionality within the XProtect Smart Client. It enables you to:

- View the status of doors, controllers, areas and other devices in XProtect.
- Monitor live and archived footage from doors.
- Use manual commands to lock, unlock and lock down doors, arm and disarm areas and activate and deactivate outputs.
- Add Protege GX doors and other records to XProtect maps, creating a unified view of the whole building.
- Monitor and report on access control and intrusion events within XProtect and view archived camera footage for each event.
- Set up custom alarms in XProtect based on Protege GX events. Acknowledging alarms in either XProtect or Protege GX will also acknowledge them in the other software, preventing double-handling.
- Receive an access request notification with camera footage whenever a user is denied access at a door, enabling operators to assess the situation and unlock the door remotely.
- View Protege GX users and photos within the XProtect Smart Client.

For more information about this integration, see Application Note 358: Milestone XProtect Access Integration with Protege GX.

FLIR Latitude Integration

This Protege GX version includes support for FLIR Latitude versions 9.0 and 9.2. Along with seamless integration of FLIR Latitude cameras with Protege GX records, events, alarms and status pages, this version also supports some convenient new features:

- Create a bookmark in the FLIR Latitude system whenever specific events occur in Protege GX.
- Alter the length of the looping video playback in the camera popup window, between 5-30 seconds.

For more information about this integration, see Application Note 267: FLIR Latitude Integration with Protege GX.

IDEMIA MorphoManager Biometric Integration

The Protege GX integration with IDEMIA MorphoManager combines the security and convenience of biometric identification with powerful access control functionality.

- Synchronize user data from Protege GX to MorphoManager, enroll fingerprints and faces and automatically download the data to biometric readers.
- Connect IDEMIA biometric readers to Protege reader expanders using OSDP with Secure Channel.
- Use any combination of fingerprint, face and card to access doors.
- Use biometrics to control powerful Protege GX features such as arming and disarming areas and activating automation.

For more information and instructions, see Application Note 360: Protege GX IDEMIA MorphoManager Integration.

Suprema Biometrics Integration

The Protege GX integration with Suprema now supports the currently available Generation 2 face and fingerprint readers, including the FaceStation F2 and BioStation 3.

To use this integration, you must also acquire the **Suprema DLL** files from ICT. Copy and paste these files into your Protege GX installation directory. You must update the files even if you have used this integration previously.

Please be aware that we have deprecated support for some Generation 1 Suprema devices. If your site is using this integration with Generation 1 devices, you may need to replace or upgrade your existing devices before installing this Protege GX software version.

For a full list of supported devices and integration instructions, see Application Note 264: Suprema Biometrics Integration with Protege GX.

Allegion Integration

Added new events which are generated when the Allegion door is locked or unlocked in apartment mode:

- Door Unit 1A Unlocked By Apartment Mode
- Door Unit 1A Locked By Apartment Mode

Feature Enhancements (4.3.402)

The following enhancements have been made to existing features in this release.

Resetting Door and Keypad Duress

After a user activates the duress trouble input at a door or keypad, you can now deactivate the trouble input using a manual command from Protege GX. This makes it much quicker and easier for security staff to resolve false alarms from the control center, without needing to physically access the door or keypad.

To reset the duress trouble input:

- For doors, right click the door record and select **Reset duress**.
- For keypads, right click the keypad record and select **Reset duress**.

To use this feature, your controllers must have firmware version 2.08.1567 or higher.

Operator Alarms

You can now right click on an operator alarm and select **Silence Workstation Sound** to stop the alarm audio without acknowledging it. This allows security guards to suppress the notification sound and investigate the issue before acknowledging the alarm.

When an operator silences or acknowledges an alarm, the system will generate an event:

- Alarm 43928 Silenced by Operator Sally Ye (OP34)
- Alarm 39042 Acknowledged by Operator Sally Ye (OP34)

In addition, when an alarm occurs the sound will play for all operators with permission to view and acknowledge that alarm, even if they do not have alarm popups enabled.

Floor Plans

You can now add clickable web links to floor plans, putting reports, incident response instructions, company portals and external data at the operator's fingertips. To add a link to a floor plan, first create the link in **Monitoring | Setup | Web links**. Then add a button to the floor plan and select your web link in the **Actions** section for that button. Clicking the button opens the selected URL in the default browser for the system.

When an operator clicks on a web link button on a floor plan, Protege GX will save an event for auditing purposes. The web links programming page now also has a **History** tab to record any changes to the programming of the web link.

Offline Wireless Locks

This software version includes support for Protege offline wireless locks, along with the following enhancements:

- It is now possible to choose whether user records and credentials will be added to the blocklist when they are deleted. Use the new **Blocklist creation** setting in **Global | Sites | Offline wireless locking** to select whether blocklisting will be enabled or disabled for the whole site, or whether operators will be prompted to add credentials to the blocklist on a case-by-case basis.
- Door open events are now disabled by default for offline wireless locks, reducing the number of events that must be stored on user cards. You can use the new **Enable door open events** option to enable these events again for specific locks (**Programming | Doors | Offline wireless locking**) or all locks on site (**Global | Sites | Offline wireless locking**).

Access Events

Previously, some types of 'Access Denied' events displayed the reader expander port where access was denied instead of the door. These now display the door's name and Database ID, making it easier for operations teams to understand where the incident occurred.

The updated events now display the following text:

- User Jane Smith (UN175) Record Expired At Door Front Door (DR12)
- User Jane Smith (UN175) Record Expired At Door Front Door (DR12) Using Credentials 100:4306
- User Jane Smith (UN175) Record Disabled At Door Front Door (DR12)
- User Jane Smith (UN175) Record Disabled At Door Front Door (DR12) Using Credentials 100:4306
- User INVALID USER PIN Not Valid at Door Front Door (DR12)

You must add the new events to your **event filters** to ensure that they appear in relevant event reports and status pages. After upgrading to this version, navigate to **Events | Event filters** and add the new events to any event filters that contain the 'Record Expired', 'Record Disabled' or 'PIN Not Valid' events.

To receive these new events, you must also upgrade the controller firmware to version 2.08.1535 or higher. If either the software or the controller does not support the new events, you will continue to receive the existing events.

Operator Events

Added new events to record when operators have been added, modified and deleted, enabling you to run reports on operator changes. The new events are:

- Operator JDoe Added By Operator Admin
- Operator JDoe Modified By Operator Admin
- Operator JDoe Deleted By Operator Admin

When creating an event filter, you can find the new operator events under **All PC Events**.

System Updates

- Protege GX now supports Windows Server 2025 operating systems.
- The Protege GX software now supports **Hungarian**.
- Protege GX can now generate a diagnostic bundle, making it easier for you to share system information and application event logs with ICT Technical Support. To export a diagnostic bundle, navigate to **About | Diagnostics**.

Issues Resolved (4.3.402)

The following issues were resolved with this release.

Services

- Resolved an issue where all controllers on a site would occasionally drop offline from the event service.
- When the event service crashes, the data service now attempts to restart it. Controllers will only be marked as offline if the event service is still down after a grace period.

The grace period is 30 seconds by default. If you wish to adjust this value, you must add the following lines to **GXSV.exe.config** in the position shown:

```
<configSections>
    ...
</configSections>
<appSettings>
    <add key="EventServiceRecoveryTimeoutSeconds" value="120" />
</appSettings>
<microsoft.scripting>
    ...
</microsoft.scripting>
```

Restart the Protege GX services after editing the config file. The minimum grace period is 30 seconds.

- Upgraded the Protege GX Download Service to a 64-bit application. This resolves an issue where the service would crash when processing very large downloads. For more information, see [64-Bit Software](#) (page 7).
- Mitigated an issue where the download service could silently fail. Now the download server will be automatically restarted if it is running but not generating diagnostic messages.
- Resolved an issue where the download service could fail to download access levels if a database error occurred while downloading the user record. This could cause unexpected 'Read Raw Data' events.

Events

- Resolved an issue where no events were recorded when an operator instant armed or instant force armed an area.
- Resolved an issue where the field time recorded for 'Controller Online/Offline with Event Server' events could be one hour earlier than the actual server time.
- Resolved an issue where duplicate events were generated whenever an operator failed to log in.

Integrations

- Resolved an issue with the Schindler integration where the **SOM primary/secondary terminal ID** settings displayed sliders instead of numeric boxes.
- Corrected misleading event descriptions for enabling and disabling privacy mode on Allegion locks.
- Resolved an issue where it was not possible to set an expiry time for Salto SHIP users.
- Resolved an issue where it was not possible to read and program cards in the Salto SHIP integration.
- Resolved an issue where Protege GX could not encode Salto SHIP data onto dual-technology cards (DESFire EV3 and iClass).
- Resolved an issue where the KeyWatcher integration did not sync with Protege GX 4.3.344.29 and higher. You must also upgrade the integration service to version 1.0.0.11.
- 152795** - Resolved an issue where camera popups would sometimes display footage from the wrong time span, potentially missing the triggering incident.
- Resolved an issue where it was not possible to assign a camera to a PTZ command.
- 157315** - Resolved an issue where leaving the login page open with Windows Authentication enabled caused the software to continuously log error messages.

Offline Wireless Locks

- Resolved an issue where the **Connection type** field did not appear in the Find tool on the doors page.
- Resolved an issue where the emergency unlock feature did not work correctly when there were multiple controllers using offline wireless locks.
- Updated the names for wireless lock programming options, tabs and error messages for more clarity.
- Updated the maximum, minimum and default settings in the card profile programming to prevent the operator from creating impractical card profiles.
- Resolved an issue where operators with restricted sites could not enroll credentials for offline wireless locks.
- Resolved an issue where wireless lock doors could remain in the **Initialization required** state in the software even after they were initialized successfully. This typically occurred when initializing large batches of locks (more than 50).

This fix requires Protege GX controller firmware version 2.08.1577 or higher.

Cybersecurity

- Resolved a cybersecurity issue where malicious code could be included in CSVs exported from Protege GX.
- Resolved a cybersecurity issue where it was possible to launch an executable from a user custom field. Now only URLs beginning with `http://` or `https://` will be opened.
- Updated a third-party component due to a cybersecurity vulnerability.
- Removed SQL injection risks.

Reports

- Resolved an issue with 'Shift First and Last User Event' and 'Shift First In Last Out' attendance reports where time was not deducted correctly when the user was late in and late out.
- Resolved an issue where user reports containing 150,000 or more users would never complete.
- Resolved an issue where the **All users included** in the following access levels report would never complete.
- Resolved an issue where report exports would fail if scheduled exactly on the hour (except for user reports).

SOAP and Web Client

- Resolved an issue where the SOAP service did not return calendar actions to a **ListRecord** request.
- Resolved an issue where it was not possible to search for users by card number in the web client.

Photo ID

- Resolved an issue where cards were not printed double-sided, even when the **Print on both sides** setting was enabled.
- Resolved an issue where user images were not deleted from the database when the corresponding user records were deleted.

User Interface

- Resolved an issue where saving or refreshing an access level would delete the output group assigned to the access level, if there was no door group assigned.
- Resolved an issue where clicking **Open user** from an event would not open the correct record if the user list was paginated.
- Resolved an issue where the users tree view loaded slowly when there were a large number of users in a record group.
- Resolved an issue where the quick search on the users page did not support special or non-English characters. The quick search now supports all non-Latin characters including Hebrew, Cyrillic and Chinese characters.
- Resolved an issue where the **Load events** button was sometimes disabled for operators with read only permissions.

- Resolved an issue where the **Load events** button could become disabled when toggling between tabs in the users programming window.
- Resolved an issue where the Find tool could not find user data in custom fields if the data included special or non-English characters.
- Resolved an issue where floor plans in large systems could take several seconds to respond to operator input.
- Resolved an issue where the user interface would freeze for 10-15 seconds after loading a floor plan.
- Resolved an issue where the **Floor plan** dropdown would take a long time to load if there were 1000+ records.
- Resolved an issue where the tabs on the access levels page would take a long time to load if there were 1000+ records linked in them.
- Resolved an issue where closing a **Recent Events** report window would cause the main Protege GX window to become unresponsive.
- Resolved an issue where right clicking an alarm to navigate to a floor plan could be very slow on large sites.
- Resolved an issue where the user interface could crash when the operator used the keyboard within the output manual command window.
- Resolved an issue where operators with restricted site access were not able to open the **Usage** tab.
- Fixed an issue where the **History** tab did not show details when group membership changed. Now when you add or remove objects in door groups, area groups, keypad groups, menu groups, output groups, elevator groups, or floor groups, the History tab will correctly display what was changed.
- Resolved an issue where the **Start** and **End** fields for credentials only allowed one input at a time.
- Resolved an issue where the user interface could freeze up when an alarm popup occurred.
- Resolved an issue where alarms did not save after editing the event filter.
- Resolved an issue where visibility for elevator cars, floors and areas was incorrectly restricted by the operator's record groups. This occurred when the records were not associated with the correct controller.
- Resolved an issue where the right-click manual commands window was sometimes displayed off-screen.
- Resolved an issue where it was not possible to open a floor plan from a trouble input event.

Previous Software Release History

This section includes information on the changes and enhancements made in earlier versions.

Protege GX Software Version 4.3.352.10

Feature Enhancements (4.3.352.10)

The following enhancements have been made to existing features in this release.

Power Supply Support

This version of Protege GX supports two new power supply modules:

- PRT-PSU-DIN-5A: Protege DIN Rail 5A Intelligent Power Supply
- PRT-PSU-DIN-10A: Protege DIN Rail 10A Intelligent Power Supply

To support the new power supplies, you must also upgrade the controller firmware to version 2.08.1535 or higher.

Code Signing

Protege GX software installers are now digitally signed.

Issues Resolved (4.3.352.10)

The following issues were resolved with this release.

- Improved the resilience of the Protege GX Event Service. The updated service now robustly handles:
 - Unreliable or unstable data connections
 - Database latency, locking and transient failures
 - Network latency and connectivity issues
 - Large numbers of events received from controllers immediately after an outage

This enhancement ensures that all events are reliably captured and persisted, even under adverse conditions. This prevents data loss and improves overall system reliability.

- Resolved an issue where controllers could drop offline from the event service over time. Some processes that mitigated this issue are no longer needed and have been disabled. In most installations these mitigations will be automatically turned off when you upgrade the software. However, if you have added related configuration to the Protege GX config files, we recommend that you remove it when you upgrade.

Remove the following lines from the config files:

- **GXSV.exe.config:**

```
<add key="gx:EnableUnknownStatusMitigation" value="true" />
```

- **GXEvtSvr.exe.config:**

```
<add key="EnableControllerConnectionWatchdog" value="1" />
```

Restart the Protege GX services after editing the config files.

- Resolved an issue where the License.dll file could be incorrectly quarantined or deleted by antivirus programs.

Protege GX Software Version 4.3.352.7

Feature Enhancements (4.3.352.7)

The following enhancements have been made to existing features in this release.

Access Events

- Added new events that are used when a user attempts to gain access at a door or elevator car, but does not have any access levels which allow access to that record. The events are:
 - User John Doe Door Not Allowed Office Door Using any Access Level
 - User John Doe Access Level Schedule Not Valid Office Door Using any Access Level
 - User John Doe Denied by Elevator Group at South Elevator Using any Access Level

This feature requires controller firmware version 2.08.1373. You may need to edit existing event filters to ensure that these events are displayed in reports and status pages.

Performance Improvements

- The door and access level lists are now paginated, improving the loading times for pages when there are large numbers of records.
- Added a search bar to the door and access level pages for quickly filtering the record list.
- Improved the loading times for the doors and access levels pages and system navigator.

Language Support

- The Protege GX thick client now supports Traditional Chinese.

Issues Resolved (4.3.352.7)

The following issues were resolved with this release.

- Resolved an issue where the single record download service would trigger a download when a user record was saved without any changes, or with changes only to fields that are not downloaded to the controller. Now user downloads are only triggered when there are changes to fields which need to be downloaded to the controller.
- Resolved an issue where running an event report for a period which had no events would return an error. Now it returns an empty event report.
- Resolved an issue where the **Detach** (breakout) button did not have a tooltip.
- Resolved an issue where the default schedule for elevator floors was displayed as *Always* instead of *Never*.
- Resolved an issue where the **Access direction** dropdown in **Users | Access levels | Door groups** was not populated when it was first opened.
- Resolved an issue where the incorrect Site ID was used when deleting smart readers, causing the delete event to not appear in reports for that site.
- Resolved an issue with custom reader formats where the even and odd parity settings were reversed.
- Resolved an issue where Salto door groups could not be added to access levels.
- Resolved an issue where the module addressing window would crash when there were a large number of modules connected.
- Resolved an issue where Protege GX installations using SQL Server versions older than 2016 could not download to the controller, add/edit door groups, or add/edit access levels containing door groups after upgrading to version 4.3.341.5.
- Resolved an issue where muster reports did not complete when there were a large number of access events with custom credentials in the reporting period.
- Resolved an issue where opening a user from an event could open the wrong user record if the list was paginated.
- Resolved an issue where the default inactivity periods were not being applied when a user was added from a credential event.
- Resolved an issue where status pages did not display the record names of muster reports.
- Fixed a visual issue with the pagination and quick search features in detached windows.
- Resolved an issue where the maximum value for the **Function 3 activation time** was incorrectly set to 128. It is now correctly set to 86,400.
- Resolved an issue where doors were assigned an incorrect host controller based on an unrelated output group.
- Resolved an issue where attendance reports did not deduct the early in time if the user was also late out.

- Resolved an issue where the **Forced open output** was not assigned to doors when a reader expander was added manually.
- Resolved an issue where the Door Duress trouble inputs were not created when a door was added manually.
- Resolved an issue where calendar actions were not filtered by record groups in the web client.
- Resolved an issue where logging in with Windows Authentication randomly failed approximately 25% of the time.

If your site uses Windows Authentication, when you upgrade to this version of the Protege GX software you must also upgrade the Protege GX Web Client to version 1.47.1.3.

- Resolved an issue where upgrading a system with PIN encryption enabled would cause errors in the database.
- Resolved an issue where the download service would crash when there were a large number of users to download.
- Resolved performance issues with the data service in large systems.
- Resolved download service crashes in large systems.
- Resolved an issue where changing an output group from the areas page could cause the **Bell output group** to be reassigned to the **Exit delay output group**.
- Resolved an issue where navigating from the **Function outputs** tab to another door record tab would remove the outputs assigned in the **Outputs** tab.
- Resolved an issue where the users page would show a 'Save Changes' prompt when navigating away from the first user, even if no changes had been made.
- Resolved an issue where only the first custom alarm sound would be played, even when multiple custom sounds were programmed.
- Resolved an issue where saving a programmable function would blank out the **Door to control**, and saving a second time would remove the door record.
- Resolved an issue where deleting a door record would automatically delete its associated trouble inputs, but no 'Trouble Input Deleted' events were logged.
- Resolved an issue where changing an operator with the No Access role caused a network error.
- Resolved an issue with the Finnish language version where the controller wizard did not add reader expanders if a keypad was also added.
- Resolved an issue with the Schindler integration where it was not possible to select the controller used for the integration in the SOM output programming.
- Resolved an issue where visitor notification emails failed to send, preventing visitors from signing in.
- Resolved an issue where the Salto SHIP integration periodically went offline and the Protege GX download server crashed.
- Resolved an issue where controllers would drop offline and come back online regularly.
- Resolved an issue where entry and exit events using credential types were not included in the **Users | Users | Attendance** tab.
- Resolved an issue where clicking **Refresh** on the module addressing page would cause an error or crash the client.
- Resolved errors and crashes which occurred when switching between sites on the doors page.
- Resolved an issue where, on a site with no users, the Users page displayed users from other sites when the number of records on the page was set to All.
- Improved the performance of the client user interface.
- Resolved an issue where the access level programming displayed the **Include all elevators** checkbox as blank even when it should have been enabled.
- Resolved an issue where the download service regularly crashed while the Suprema biometric integration was running.

High Data Usage on 4G Modems

In some recent versions of Protege GX there is unexpectedly high data usage on controllers connected by 4G modems. This can be caused by the Protege GX regularly contacting all controllers to improve status reporting from the event service.

If you are experiencing high data usage on metered (low data) connections, you can turn off these regular "check-ins". Be aware that this may increase the chance of controllers dropping offline.

1. Stop the Protege GX services.
2. In the File Explorer, navigate to the installation directory: C:\Program Files (x86)\Integrated Control Technology\Protege GX
3. Open GXSV.exe.config.

Files in this directory require administrator permissions to edit. You may need to open the file as an administrator using an application like Notepad++, or make a copy in a different directory to edit and replace the original.

4. Add the following code under the `<configuration>` node, between `</configSections>` and `<microsoft.scripting>`:

```
<appSettings>
  <add key="gx:EnableUnknownStatusMitigation" value="false" />
</appSettings>
```

5. Save the file.
6. Open GXEvtSvr.exe.config.
7. Directly under the `<appSettings>` tag, add the following code:

```
<add key="EnableControllerConnectionWatchdog" value="0" />
```

8. Save the file.
9. Restart the Protege GX services.

Protege GX Software Version 4.3.342

Issues Resolved (4.3.342)

The following issues were resolved with this release.

- Resolved an issue where Protege GX installations using SQL Server versions older than 2016 could not download to the controller, add/edit door groups, or add/edit access levels containing door groups after upgrading to version 4.3.341.5.
- Resolved an issue where logging in with Windows Authentication randomly failed approximately 25% of the time.

If your site uses Windows Authentication, when you upgrade to this version of the Protege GX software you must also upgrade the Protege GX Web Client to version 1.47.1.3.

Protege GX Software Version 4.3.341

New Features (4.3.341)

The following new features have been included with this release.

OSDP 2.2 Support

Protege GX now supports the OSDP 2.2 standard. This includes a number of changes which make setting up OSDP card readers quicker and easier.

- To program OSDP readers in Protege GX, you can now simply set the **Port 1/2 network type** of the reader expander to OSDP. When you save the record, Protege GX will automatically create the smart reader records that are required for the entry and exit readers, ready to be programmed with the reader address and door configuration.

When programmed using the method above, ICT 485 smart reader licenses are no longer required to connect OSDP readers.

- Protege modules now support OSDP installation mode, allowing them to establish a secure channel session with readers using a randomly generated encryption key. After putting the card reader into installation mode, simply right click on the reader expander record and select **Activate OSDP install mode**. This prompts the reader expander to initiate an OSDP session with the card reader, in which it will establish the reader's Baud rate and negotiate an encryption key for a secure session.
- Alternatively, it is possible to manage custom encryption keys manually if preferred. One encryption key can be programmed per reader, and the key will be diversified by the controller to establish a secure session with the card reader.

For complete prerequisites and programming instructions, see Application Note 254: Configuring OSDP Readers in Protege. If you have previously programmed OSDP readers using commands, it is recommended that you remove these commands and replace them with the new programming available in the UI.

Custom Alarm Sounds

Protege GX now includes the ability to program unique custom sounds for operator alarms in the system, enabling you to differentiate between the types of alarms which need to be monitored on site. Use custom alarm sounds to enable personnel to quickly recognize what is happening and respond appropriately.

To program this feature:

- In **Global | Global settings | Sound**, add any number of wave files in the **Sounds** field and give them descriptive names. The original **Wave file path** option will provide a fallback for any alarms which do not have a custom alarm sound.
- Select alarms in the **Events | Alarms** programming and set the new **Alarm sound** option to the desired custom sound. Any sounds which are assigned to an alarm record will be automatically synchronized with client installations.

Feature Enhancements (4.3.341)

The following enhancements have been made to existing features in this release.

Users Page Improvements

- The user list is now paginated so it can be loaded faster when there are large numbers of users. By default 200 records are displayed per page, but this can be changed using the dropdown at the bottom of the window.
- The search field at the top of the users page enables you to quickly filter user records by their display name.
- It is now possible to sort user records by first name and last name, making it easier to find users in the list. To enable this feature, navigate to **Global | Sites | Display** and enable **Display first name and last name columns in users**. On the users page, you can click the column headers to sort the records as required.
- There are new options for automatically formatting the display names of users based on the entered first and last names. The **User display name auto format** field in **Global | Global settings | General** now includes:
 - Reverse short format (Smith, J)
 - Reverse long format (Smith, John)

Licensing

- Protege GX operators can now activate and update their license from client workstations, not only from the server.

Alarms

- It is now possible to include a camera popup alongside an alarm event, allowing operators to see what is happening on site immediately. When you enable **Allow camera popup** in the alarms programming, whenever there is an alarm on a record such as a door or input the associated camera will pop up.

Function Outputs

- It is now possible to activate function outputs for up to 86,400 seconds (24 hours).

Language Support

- Protege GX is now available in Ukrainian.

Issues Resolved (4.3.341)

The following issues were resolved with this release.

- Resolved an issue where the 'Read Raw Credential Data At Reader Expander' event did not allow operators to right click and add the custom credential to a user.
- Resolved an issue where it was possible to view and edit the User ID credential type from the Protege GX web client.

This fix requires SOAP version 1.6.0.10 or higher and web client version 1.47.0.66 or higher.

- Resolved an issue where muster reports did not display the correct details for a user if their last access event used a custom credential type.
- Resolved an issue where floor plans would display an error when the operator viewed sorted event window tabs.
- Added the **Exclude report header and footer** option to user and muster reports (previously available for event reports only). This resolves an issue where extra blank columns were sometimes added to exported and emailed CSV reports.
- Resolved an issue where some extended user fields could be added to card templates, but were not editable and disappeared when the template was saved.
- Resolved an issue where the **Instructions** and **Instructions 2** fields did not appear in alarm popups.
- Resolved an issue where the "All users by events" report was not being populated correctly if the report included a large number of events (c. 100,000).
- Resolved an issue where the Find tool displayed duplicate field names on some pages, making it difficult to search for the correct field. The repeated field names are now combined into a single search option (e.g. **Facility/Card number**) or distinguished using numbers (e.g. **Area 1, Area 2**, etc.) or tab names (e.g. **Disarm area for door on access (Reader 1)**).
- Resolved an issue where area groups assigned to users were not correctly removed from the database when the area group was unassigned or the user record was deleted.
- Resolved multiple issues where operators who did not have access to all sites could not perform certain actions:
 - Resolved an issue where these operators could not filter the inputs list by controller.
 - Resolved an issue where these operators could not view trouble inputs.
 - Resolved an issue where these operators could not control areas via a status page.
- Resolved an issue in the March Networks video integration where the camera stream intermittently would not open.
- Resolved an issue in the March Networks video integration where PTZ commands would not work correctly unless there was a video stream open in another window.

This fix requires Protege GX March Video Service version 1.0.0.7 or higher.

- Resolved an issue where custom field displayed 'Invalid String ID' instead of the field name in the user history page.
- Resolved an issue where the **User last active** field was not included in emailed or exported reports.
- Resolved an issue where the Find tool did not correctly find user records without a specific access level assigned.
- Resolved an issue where some third-party DLL files in the Protege GX installation were not compiled with ASLR and DEP flags. These files have been removed from new installations, but will not be deleted when the software is upgraded from a previous installation.

If you are setting up the Suprema or Geutebrück integrations for the first time, you will need to add these files to the main Protege GX directory. For more information, see the relevant application note.

- Resolved an issue where the Protege GX Download Service was vulnerable to dumb fuzzing on ports 51212-51213. This was caused by the Suprema DLLs that have been removed from the default installation as mentioned above. To resolve this issue, uninstall Protege GX and install the new version (do not upgrade the software).
- Resolved an issue where the download and event server diagnostic windows on the controllers page would display the bottom of the list first and force users to scroll up to see the latest events. This was caused by a change in Windows Update KB5018410.
- Resolved an issue where the client could crash when switching between two sites in **Global | Sites** if the first site had security enhancements enabled.
- Resolved an issue where the record group assigned to a door would not restrict which operators received any camera popups.
- Resolved an issue where schedule periods would not save the correct times when an operator in a different time zone from the server entered times by typing them in manually.
- The Protege GX Download Server will now restart once every 24 hours, mitigating issues where it can silently fail. The server will only restart when there is no controller download pending.

Secondary download servers will not be restarted by this process. If required, a Windows scheduled task can be used to restart any secondary servers periodically.

- Resolved an issue where an exported event report for Last month did not contain all of the events for the month.
- Resolved an issue where the second language name of the Red R2 Output was not populated when a reader expander was created.
- Improved loading times for a number of pages when there are large numbers of records.
- Resolved an issue where user PINs could be viewed in user reports even when site security enhancements were enabled.
- Resolved an issue where trouble inputs without a host controller were not displayed using the <Unassigned> filter.
- Resolved an issue where controllers would drop offline, requiring an event service restart.
- Resolved a number of significant cybersecurity issues.

Protege GX Software Version 4.3.327

New Features (4.3.327)

The following new features have been included with this release.

Tenancy Portal Sync

The Protege Tenancy Portal is designed as the central point for synchronizing contacts for an entry station directory. With this version of Protege GX you can synchronize your Protege GX user records with the tenancy portal and subsequently import them to a Protege entry station directory, allowing building visitors to call or video call Protege GX users directly from the entry station.

- You can enable this feature in Protege GX by checking **Enable portal synchronization** in **Global | Sites | Portal** and entering your login credentials for the tenancy portal.
- Each synchronized site will create a place and a phonebook in the tenancy portal.
- To automatically sync a user to the tenancy portal, enter their email address and/or phone number, along with a tenancy name.
- A mobile app account and SIP account will be added for each user (if they do not have one already), and the user will be assigned to a tenancy and added to the phonebook.
- The phonebook can be manually imported or automatically synchronized with the Protege entry station directory, updated every 60 minutes.
- Visitors can now video call Protege Mobile App users directly from the entry station, or voice call using the phone number.
- Users can also use their PIN to unlock doors and activate devices at the entry station.

This feature requires a tenancy portal login and the separate sync service, available from the ICT website. For more information, see the [Protege Tenancy Portal User Guide](#).

Feature Enhancements (4.3.327)

The following enhancements have been made to existing features in this release.

Door Groups

- Added the ability to set expiry start and end dates for door groups. This can be used to disable or enable a group of doors across all user access levels at a defined date and time - for example, allowing you to pre-program a section of the building that is under construction, and activate the door group on the day it is opened to staff.

Issues Resolved (4.3.327)

The following issues were resolved with this release.

- Improved cybersecurity measures where a number of IGXService methods did not have access controls.
- Improved cybersecurity measures where a certain method was vulnerable to SQL injection.
- Upgraded the log4net application to version 2.0.14.
- Resolved an issue where the alarm window would disappear after receiving more than 200 events when alarm routing was in use.
- Resolved an issue where the time for a scheduled report email or file export could be incorrectly changed when the report was edited by an operator in a different time zone from the server.
- Resolved an issue with the Salto SHIP integration where the door state was not displayed in Protege GX.
- Resolved an issue where data for dropdown custom fields was not included in automatically exported or emailed reports.
- Resolved an issue in the SOAP service where it was not possible to find users by credential.

This fix requires SOAP service version 1.6.0.9.

- Resolved an issue where a record group could not be assigned to the first programmed door group until it had been saved.
- Resolved an issue where the 'DVR Generic' and 'Camera Generic' events were not functioning correctly.
- Resolved an issue where the Find tool could not filter certain records (including doors) by record group.
- Resolved an issue where the credential types which could be viewed and edited in a user record were not restricted by the operator's record groups.

- Resolved an issue where the History tab would display "Invalid String ID" for some fields.
- Resolved an issue where extra blank columns were sometimes added to exported and emailed CSV reports. This was caused by the additional header and footer rows in the CSV report (e.g. report name, date of export) and can be prevented by enabling the new **Exclude report header and footer** option in the report programming.

Protege GX Software Version 4.3.322

Feature Enhancements (4.3.322)

The following enhancements have been made to existing features in this release.

OS Support

- Protege GX is now supported on the Windows 11 operating system (Pro, Business and Enterprise editions).

Limiting Cards/Credentials per User

- Added the ability to restrict the number of cards which can be assigned to each user to one. To apply this limitation to the whole site, enable the **Display only one card slot** option in **Global | Sites | Display**.
- Added the ability to limit the number of instances of a credential type which can be assigned to each user. When programming a credential type in **Sites | Credential types | General**, you can set the **Credential limit per user** to a number from 1-10, or leave it as unlimited.

It is not possible to enable card or credential limits if there are any users with more than the desired limit currently assigned. Delete any excess credentials from users before enabling these settings.

Issues Resolved (4.3.322)

The following issues were resolved with this release.

- Resolved an issue where some text in the second language was displayed with excess quotation marks.
- Resolved an issue where the data sync service sometimes created duplicate user records when two instances of the service were running at the same time.

This fix requires ICT Data Sync Service version 2.0.10.18 or higher.

- Resolved an issue in the Chinese language build where column headers were missing from event and muster reports.
- Resolved an issue where adding and immediately deleting a user record while a full download was in progress could cause the single record download service to fail and not recover.

This fix requires single record download service version 1.0.0.4 or higher.

- Resolved an issue where the single record download service could not successfully install a self-signed certificate on the controller in environments with operating systems prior to Windows 10.

This fix requires single record download service version 1.0.0.4 or higher.

- Resolved an issue where the download service failed to start.
- Reinstated the **Download retry delay** setting in **Sites | Controllers | Configuration**.
- Resolved an issue where the download service was continually crashing when attempting to download a large user database including Suprema biometric credentials.
- Resolved an issue where the SOAP service was not respecting the nStart and nNumberOfRows parameters when getting user reports.

This fix requires SOAP service version 1.6.0.7 or higher.

- Resolved an issue where some UI translations in second language versions were incorrectly reverted to English.

- Resolved an issue where updating the **Password** field in **Sites | Controllers** would result in multiple unnecessary save prompts.
- Resolved an issue where attempting to delete a credential type from a new, unsaved user record would result in the first credential type on the list being deleted, regardless of which one was selected.

Protege GX Software Version 4.3.319

Feature Enhancements (4.3.319)

The following enhancements have been made to existing features in this release.

Programming Efficiency

- When a site has only one controller, the **Controller** field in the toolbar is automatically set to this controller. This improves efficiency when programming records such as programmable functions, services and expander modules.

Failed Login Attempt Events

- Protege GX can now generate events whenever there is a failed login attempt on the thick client. This enables you to audit and report on failed attempts to access the software. To enable this feature, check the **Save failed operator login events to event database** option in **Global | Global settings**.

The new events are:

- **Operator login failed attempt: Unknown operator**
- **Operator login failed attempt: Incorrect password: <OPERATOR NAME>**
- **Operator login failed attempt: No role access: <OPERATOR NAME>**

Credential Types

- Added the ability to set an inactivity period for each credential type assigned to a user. If the credential is not used within this period, it will be disabled. Inactivity periods can be set individually for each credential assigned in **Users | Users | General**, or you can set a default inactivity period for the credential type in **Sites | Credential Types**.

For more information, see Application Note 276: Credential Types in Protege GX.

Login Page

- The **Server** field on the Protege GX login page now includes a dropdown menu, allowing you to select previously used server addresses. The **Clear** button allows you to delete the currently selected address from the dropdown.

Photo ID

- It is now possible to display a user's credential types on a Photo ID card template. For example, this allows you to include custom card numbers, license plates and User IDs on user cards.

For more information, see Application Note 149: Creating a Photo ID Template in Protege GX.

Language Support

- Added Danish as a supported language.
- Added Chinese (Simplified) as a supported language.
- Updated Russian translations.

Issues Resolved (4.3.319)

The following issues were resolved with this release.

- Resolved an issue where the **Service Port** field was not visible in the second language.
- Resolved an issue where the 3 badge latch door 8 hours and User Key Watcher ID columns could be duplicated in user reports, and would be impossible to delete.
- Resolved an issue where Protege GX would stop receiving live events from controllers, requiring a restart of the event service.
- Resolved an issue where holiday date formats would be changed unexpectedly, preventing the software from correctly converting the date format.
- Fixed an issue where some user cards which were about to expire would not be included in the Cards about to Expire user report.
- Resolved an issue where emailed reports were not being sent when a custom TLS certificate was in use.
- Resolved an issue where a controller's username and password could be displayed in event reports.
- Resolved an issue where recurring calendar actions would end before the set date.
- Resolved an issue where floors could not be filtered by record group when being added to an elevator car record.
- Resolved an issue where for some Windows regions the time was incorrectly displayed in 12hr format instead of 24hr format.
- Resolved an issue where operators with roles that could not access the <not set> record group were not able to set User IDs, making it impossible to add new users.
- Resolved an issue where enabling the **Autopopulate User ID Credential Value** option could cause controllers to drop offline.
- Resolved an issue where emailed reports were not translated correctly.
- Resolved an issue where deleted record groups were not removed from some types of records, which caused lists to load slowly for operators who only had access to specific record groups.
- Renamed the **Last Month** field in the report email tab to **Previous Calendar Month** to more accurately describe the effect of the setting.
- Resolved an issue where a SOAP GetRecord call would return an empty PIN record for users when the site had **Require Dual Credential for Keypad Access** and **Allow PIN Duplication** enabled.
- Removed the **Email** and **File Export** tabs from the user search page.
- Resolved an issue where user reports for All Users By Access Level would not be automatically emailed.
- Improved the performance of status page loading on large sites.
- Resolved an issue where changing a schedule on a disarming area group would also change the schedule on the arming area group, and vice versa.
- Resolved an issue where increasing the size of the user image column on a status page would not resize the photo ID images.
- Resolved an issue where muster reports which included the record group column would not be automatically exported or emailed if at least one user did not have a record group set.
- Resolved an issue where the **Solid**, **Gradient** and **Null** tabs did not appear above the color picker in the card template editor and other locations. This could prevent operators from selecting the background, border and/or foreground colors for objects.
- Resolved an issue where adding more than one custom field column to an event report caused file exports and emails to fail.
- Fixed a regression where alarms were sent to all workstations instead of following the programmed alarm routing rules.
- Amended and updated textual display in the user interface, including fixes to spelling, grammar and capitalization.
- Resolved an issue where legacy credentials were stored in plain text in a config file.
- Resolved an issue where the server could become unlicensed when the computer restarted.
- Resolved an issue where event reports could not be created in the web client.
- Resolved an issue where the required Visual C++ 2017 Redistributable prerequisite was not installed.

- Resolved an issue where clicking the **Load default report layout** button for a user report could cause the client to crash.
- Resolved an issue where operators with the Guard or End user role presets could not view elevator floors on status pages and floor plans.
- Resolved an issue where attendance reports would not run using the Summary report layout.
- Resolved an issue where the All users not in events report could return users who were included in events.
- Resolved an issue where the **Unlock latched** and **Extended lock time** options were not displayed correctly in the calendar action programming.
- Resolved an issue where some programming tabs did not appear in second language builds.
- Resolved an issue where navigating away while a report was loading could cause a memory leak, resulting in the client crashing.
- Resolved an issue where the All users not in events report did not return correct data when exported.
- Resolved an issue where some password entry fields were not masked.
- Resolved an issue where custom field data was not loaded correctly in event, user, muster or attendance reports.
- Resolved an issue where the search functionality in the online help was not functioning.
- Resolved an issue where the **Load events** button on the **Events** tab was returning an error.

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.