Integrated Control Technology

Protege GX

Release Notes | Version 4.3.352

Last Published: 23-Jul-24 8:58 AM

Contents

Introduction

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

- Protege GX software version 4.3.352

The release history for previous Protege GX, Protege GX SOAP Service and Protege GX Web Client versions is also included.

When you upgrade Protege GX to this version, we recommend you also upgrade the Protege GX SOAP service to version 1.6.0.11 or higher and the Protege GX Web Client to version 1.47.1.3 or higher. This is required if you are using Windows Authentication.

Changes to Supported Versions

In this version, ICT is dropping support for some Windows operating systems and SQL Server versions. These versions have reached end-of-life and are no longer supported by Microsoft.

- Windows 8.1 (Microsoft ended support in January 2023)
- Windows Server 2012 (Microsoft ended support in October 2023)
- SQL Server 2008 (Microsoft ended support in September 2019)
- SQL Server 2012 (Microsoft ended support in July 2022)

ICT recommends upgrading to the latest supported versions (see next page) to ensure that your site receives cybersecurity updates, bug fixes and features from Microsoft and ICT.

New software versions, including this one, will not be tested on unsupported Windows and SQL Server versions. Sites may continue to use these unsupported versions, but upgrading the Protege GX software is at the customer's own risk and new features may not work correctly. ICT Technical Support reserves the right to request that any issues be replicated on a supported operating system and/or SQL Server version.

Important Note on Software / Firmware Compatibility

The release of Protege GX version 4 introduced cross controller operations, which enables controllers to operate as a unified system and share hardware resources. This makes all physically connected items on a controller accessible and usable by various functions and records within Protege GX. Version 4 also introduced many new features that were unavailable in previous versions.

In order to use these features, you must also be using a Protege GX DIN Rail Controller or Protege GX PCB Integrated System Controller (PRT-GX-PCB) running firmware version 2.08.583 or above.

If you are running an earlier version of the firmware, or if you are using an older PCB Controller (PRT-CTRL-GX), these features are not available. If you are running firmware version 2.08.583 or later with an earlier version of the software, it will result in unexpected operation.

	Firmware 2.08.499 and below	Firmware 2.08.583 and above
Below software version 4.0.128	❌ Cross controller operations and new features not available	❌ **Software/Firmware versions incompatible. Controller will not accept programming downloads**

	Firmware 2.08.499 and below	Firmware 2.08.583 and above
Software version 4.0.128 and above	❌ Controller download will not be allowed if any cross controller links are made in programming. All new features will be ignored.	✅ Feature available

For more information about cross controller operations and how this functionality affects the operation of Protege GX, refer to AN-180: Cross Controller Operations. We strongly advise that you read this document thoroughly before proceeding with the upgrade.

Supported Operating Systems

Operating System	Edition	Architecture
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	32 / 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 2014, 2016, 2017 and 2019 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.

Note: SQL Server 2014 (SP2) for 32-bit installation or SQL 2016 (SP2) for 64-bit installation.

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.

Upgrading Protege GX to the Latest Build

To upgrade to the latest version, you may be required to uninstall the previous version first. The installer will inform you if this is the case.

1. Prior to performing an upgrade, you should always back up your database:
   - Open the Protege GX application and log in using an operator account with administrative permissions, or at minimum the ability to perform system functions.
   - Select **Global | Global settings** from the main menu.
   - Under the **Main database backup** options, select **Backup now**.

   Wait for the backup to be completed before proceeding.

2. Run the installation for the server:
   - Run the supplied setup file (setup.exe) and follow the onscreen instructions.
   - When the installer is launched it looks for the previous version of Protege GX installed on the local workstation and upgrades it to the latest build.
   - Progress is displayed as the database is upgraded and the application installed.

3. Run the installer again on each client machine to update the client interface.

Detailed installation instructions can be found in the Protege GX Installation Manual.

Protege GX Software Version 4.3.352

Feature Enhancements (4.3.352)

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)

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.

Previous Software Release History

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

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.

Protege GX Software Version 4.3.308

Note: The installer for this version will automatically install ODBC Driver 17 for SQL Server on your workstation before beginning the Protege GX installation. This is required for the User PIN Encryption feature described below. No action is required from you.

New Features (4.3.308)

The following new features are included with this release.

User PIN Encryption

By default, the Protege GX database stores user PINs in plaintext, allowing operators with the appropriate permissions to view and edit PIN codes. However, on some high security sites it is vital that only one person has access to a user's PIN code: the user themselves. The **Encrypt User PINs** option in **Global | Global Settings** allows you to permanently encrypt PINs for all users, with the following effects:

- User PINs are encrypted in the SQL database using the SQL Always Encrypted feature.
- Protege GX operators can no longer view PINs defined by users.
- Protege GX operators can no longer manually enter PINs for users.
- Randomly generated PINs expire immediately, requiring users to define a new PIN the first time they log on to a keypad.

Warning: User PIN encryption is **permanent** and can only be reversed by restoring a database backup taken before encryption was implemented.

For more information, see Application Note 306: Configuring User PIN Encryption in Protege GX.

Single Record Download Support

Normally when you save a record in the Protege GX software, the Protege GX Download Service performs a full download to each controller that requires the change. In contrast, the Protege GX Single Record Download Service uses a differential download process, only downloading the specific records and fields that have changed in the database.

This service runs in parallel to the existing download service, providing an independent path for single-record changes that need to be downloaded to the controller in a timely fashion. Record changes downloaded by this service are typically received by a controller in under 30 seconds. This reduces download times considerably, especially on large sites with many controllers.

The single record download service receives updates for changes to user, access level and schedule records and immediately downloads these changes to the associated controllers. All other changes are handled by the standard download service as normal.

The Protege GX Single Record Download Service must be installed separately. For more information, see Application Note 309: Single Record Downloads in Protege GX.

Feature Enhancements (4.3.308)

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

Autopopulate User IDs

- When site security enhancements are in use, you can now enable the **Autopopulate User ID Credential Value** option in **Global | Sites | Site Defaults**. When you first enable this feature, all existing user records that do not currently have a User ID are assigned a unique number based on their Database ID. From then on, all new user records will be automatically assigned a unique, randomly generated 8-digit User ID. It is still possible to override the pre-generated ID with a custom value.
- Even when the **Autopopulate User ID Credential Value** feature is not in use, you can type the word SYSTEM into the User ID credential to automatically generate a unique 8-digit value when you save the user record.

For more information, see Application Note 275: Configuring Site Security Enhancements in Protege GX.

User Reports

- After running a user report, you are able to filter and/or group the results using the column headers, or by adding a text filter on any column. Now this layout can be saved for an individual operator by clicking the **Save Report Layout** toolbar button, and will be displayed automatically whenever the operator opens that report.
- In addition, a layout can be saved as a default for all operators using the **Save Default Report Layout** toolbar button. Operators can load this default layout using the **Load Default Report Layout** toolbar button.
- Any filter criteria used by the saved default report layout can now be viewed on the user report setup page. This field shows the current filter criteria and provides a button to navigate directly to the loaded report view so that you can edit the filters as necessary.

Alarms

- Added the ability to set whether comments are required, optional or not permitted when acknowledging alarms. This can be set in the **Events | Alarms** programming for each alarm.
- The available options are:
  - **Must**: Comments must be entered when acknowledging alarms
  - **Optional**: Operators may leave a comment when acknowledging alarms
  - **Never**: There is no prompt to leave a comment when acknowledging alarms

User PIN Security Enhancements

- Added the ability to restrict operators from generating new user PINs in the security level programming.

Language Support

- Added Turkish language support.

Low Level Elevator Integration

- Added the ability to configure the credentials required for elevator access. The options are: card, card or PIN, card and PIN, and PIN only.

Delete User Photos

- Added the ability to delete user photos.

KONE Destination 880 Integration

- The following access level options are now available in the software when the KONE integration is in use:
  - Enable Normal Call
  - Enable Handicap Call
  - Enable Priority Call

- Enable Empty Car Call
- Enable Space Allocation Call

Issues Resolved (4.3.308)

The following issues have been resolved with this release.

- Fixed an issue where the User ID credential type was available as a door type credential, even when site security enhancements were not implemented.
- Resolved an issue where the event filter programming displayed additional options in breakout windows that were not available in the main window.
- Resolved an issue where the 'All Users not in Events' user report type was not returning correct details.
- Fixed an issue with the date/time sorting in events and reports.
- Resolved an issue where the text of some buttons could be cut off in second languages.
- Resolved an issue where random numbers appeared before the 'Do you want to log out' message in Canadian French.
- Fixed an issue where central station reports were not populating inputs and areas.
- Resolved an issue where the 'Confirm New Password' text was truncated in Canadian French.
- Resolved an issue where, when a copy of an existing controller was created, programmable functions were not copied to the new controller.
- Resolved an issue where exported or emailed muster reports were being sorted incorrectly.
- Resolved an issue where exported or emailed muster reports were being formatted incorrectly.
- Resolved an issue where exported or emailed muster reports which included custom fields did not include users without those custom fields configured.
- Resolved an issue where automatically exported attendance reports were missing information.
- Resolved an issue where manually unlocking elevator floors from a status page or floor plan did not function, and generated a 'System Assertion 51' event.
- Resolved an issue where times could not be set to PM for some Windows regions.
- Fixed an issue where only 100 events were being displayed on a status page event window.
- Fixed an issue where seconds were not shown for event times in event reports or on the status page.
- Fixed an issue where event reports would not display more than one custom user field.
- Resolved an issue where connecting a microphone and speaker to a SIP workstation could cause Protege GX to crash.
- Fixed an issue in the Princeton Identity integration where users beyond the first were not enrolled correctly in the Princeton system.
- Resolved an issue with the graphical schedule display not being filled correctly with some Windows languages.
- Resolved an issue where multi-selecting and deleting credential types from a user record caused the user interface to crash.
- Resolved an issue where no scroll bar was displayed when selecting a record group in the user find tool.
- Resolved an issue where the saved report filter details were not displaying correctly and would generate an error in the **Reports | Setup | Events** page.
- Resolved an issue where editing a visitor record prevented the visitor card from being made available when the visitor signed out.
- Fixed an issue in the Suprema Biometric integration with user credentials not being added correctly.
- Resolved an issue where extended/predefined custom user fields were not being populated in exported user reports.
- Resolved an issue where attendance reports did not display events from the correct period.
- Resolved an issue where the device status could not be retrieved via the SOAP service.
- Resolved an issue where copying a controller caused additional phone number records to be generated.
- Resolved an issue where default column widths were not set correctly in event reports.
- Resolved an issue where the field time and logged time for alarm popups were out by several hours (the logged time was incorrect).

- Resolved an issue where the **Schedule** dropdown in **Users | Users | Access Levels** was displayed as transparent.
- Resolved an issue where columns were missing from manually exported event reports.
- Resolved an issue where some popup windows were cut off at the bottom.
- Resolved an issue where the report filter editor was difficult to read in the dark theme.
- Resolved an issue where some column text was cut off in automatically exported attendance reports.
- Resolved an issue where fields on the **Events | Actions** page were not being enabled/disabled correctly based on the **Type** of action.
- Resolved an issue where the alarm counter in the status bar did not display any number of alarms above 10.
- Resolved an issue where it was not possible to generate a central station report for reporting services with a space at the end of the name.
- Resolved an issue where security level restrictions were not followed on status pages.
- Resolved an issue where pressing any key when the Type field in **Monitoring | Setup | Status Page Editor** was open would crash the client.
- Resolved an issue where the **Read Card** function did not function correctly with 26 bit DESFire cards.
- Resolved an issue where emailed event reports would not be sent to operators when Windows Authentication was in use.
- Resolved an issue where the controller export feature was not working correctly and displayed an error.
- Resolved an issue where records exported to CSV did not have the data aligned correctly with the column headers.
- Resolved an issue where copying an access level record did not also copy the records assigned to it (e.g. doors, area groups, etc.)
- Resolved an issue where the date pickers in **Programming | Apartments | Users | Access Levels** did not follow the material design theme.
- Resolved an issue where the 'Save to Database' action was able to be edited for new sites beyond the first.
- Resolved an issue where a floor plan would not update record statuses correctly when it was opened from a link on another floor plan.
- Resolved an issue where right clicking on a camera icon in an event report did not function correctly.
- Resolved an issue where the **User Last Active** field would not be updated when the user used a credential type to gain access.
- Resolved an issue which occurred when an operator was acknowledging an alarm and a second alarm popped up. The first alarm window incorrectly lost focus on the alarm which was being acknowledged.
- Resolved an issue where the schedule graphical display was not operating correctly in Protege GX when French Canadian was set as the Windows language.
- Resolved an issue where some objects on a floor plan would sometimes be displayed as gray icons, even though they were online.
- Resolved an issue where the 'Save Changes' dialogue would appear on the **Users | Users | Access Levels** tab even when there were no changes to save.
- Resolved an issue where, when editing a schedule in a breakout window on a system with a 24 hour time setting, afternoon times would be incorrectly changed to morning times.
- Resolved an issue where some areas would not appear on a floor plan, even though they should have been visible to operators.
- Resolved an issue where the **Service Port** field was missing from the DVR programming when using the second language.
- Resolved an issue where saving an event report with a blank email time could cause the client to crash.
- Resolved an issue where user PINs sent from the software could not be used by controllers with firmware version 2.08.788 or earlier.

Previous SOAP Service Release History

Protege GX SOAP Service (1.6.0.11)

Feature Enhancements

- When you request user records with ListRecords, SOAP now provides the <a:SpareString1> and <a:SpareString2> fields containing the user's first name and last name respectively. This allows you to sort the user list by first name and last name.

  This feature requires Protege GX 4.3.337.3 or higher.

Issues Resolved

- Resolved an issue where it was not possible to search users by credential using the FindRecord API.

  This fix requires Protege GX version 4.3.324.2.

- Resolved an issue where the system-generated User ID credential type could be edited in the web client.

  This fix requires Protege GX version 4.3.329.6 or higher and web client version 1.47.0.66 or higher.

Protege GX SOAP Service (1.6.0.7)

Feature Enhancements

- Added support for the KeySecure integration.

Issues Resolved

- Resolved an issue where the SOAP service was not respecting the nStart and nNumberOfRows parameters when getting user reports.

  This fix requires Protege GX version 4.3.321.3.

Protege GX SOAP Service (1.6.0.5)

Feature Enhancements

- Added the ability to randomly generate user PINs via the SOAP service.
- When you update a user record, you can now instruct the SOAP service to immediately return the updated user record. If the user PIN has been updated by this SOAP call, this will allow you to view the newly updated user PIN.

For more information, see the Protege GX SOAP Service API Specification.

Issues Resolved

- Resolved an issue that occurred when the SOAP service attempted to write an error to the Windows Event Log without sufficient permissions. This caused it to generate an additional error and not report the original error.
- Resolved an issue where the SOAP service could time out (endless loading) when pulling user events. This issue affected the web client, and requires the corresponding Protege GX server version from this release.

Protege GX SOAP Service (1.6.0.1)

Feature Enhancements

- This version includes improvements for TLS 1.2 security.
- The SOAP installer now populates or overwrites the data server address with the current hostname instead of 'localhost' on installation or upgrade.
- Added the ability to create, program and use function codes via the SOAP Service.

Protege GX SOAP Service (1.6.0.0)

New Features

- Transport Layer Security (TLS) has been implemented and is now the default security setting when installing the SOAP service with options to select None or Windows Authentication. See "Enhanced Communication Security" in Protege GX New Features for more information.

Feature Enhancements

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

- Added the ability for the Protege GX SOAP service to check the Protege GX Data Service in order to validate license requirements.

Issues Resolved

The following issues have been resolved in this release:

- Fixed an issue where the SOAP service installer options of "Modify" or "Repair" would do nothing at all.
- Fixed an issue where SOAP was able to add Doors to a controller that did not exist in the database.
- Fixed an Issue where SOAP was able to insert a schedule record and apply it to another record that did not exist in the database.
- Fixed an issue where door type credential type fields were not exposed in the GetTableSchema API.
- Fixed an issue where the installer was not applying TLS settings when updating from version 1.5.0.30 or earlier.
- Fixed an issue where the GetStatusListStatus request was failing to retrieve data values assigned to variables.
- Fixed an issue where the Access level option "Use Access Level Door Type" was being set to "True" when adding access levels. This has been changed to "False" by default.

Previous Web Client Release History

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

Protege GX Web Client (1.47.1.3)

Issues Resolved

- Resolved an issue where it was not possible to log in to the web client using Windows Authentication.

  This fix requires Protege GX software version 4.3.342.2.

Protege GX Web Client (1.47.1.2)

Issues Resolved

- Resolved an issue where exported user report CSVs did not separate the values with commas.
- Resolved an issue where event reports did not handle time picking correctly when the system was set to 24 hour time.
- Resolved an issue where it was not possible to find users by credential in the web client.

  This fix requires Protege GX version 4.3.324.2 and SOAP version 1.6.0.9.

- Resolved an issue where it was not possible to type in time fields.
- Resolved an issue where the Lock calendar action displayed a blank action field.
- Resolved an issue where adding access levels to multiple users simultaneously was not saved correctly.
- Resolved an issue where editing a user assigned to a particular record group, using an operator role restricted to that record group only, could cause an access level assigned to the same record group to be removed from the user. This occurred when the user had at least one access level that was not visible to the operator.
- Resolved an issue where the system-generated User ID credential type could be edited in the web client.

  This fix requires Protege GX version 4.3.329.6 or higher and SOAP version 1.6.0.10 or higher.

- Resolved an issue where the < and > characters in user display names were not correctly handled when using the find tool, preventing it from displaying any user records after the first one with an angle bracket character.
- Resolved an issue where, when the operator's language was set to a language other than English, the final user in the user list was not displayed.
- Resolved an issue where the clickable area of some buttons was smaller than the visual size of the button.

Protege GX Web Client (1.47.0.56)

Feature Enhancements

- The web client now prevents editing of fields while the record list is loading. This prevents operators from entering data until all records have been loaded.
- The web client now shows a 'Saving' popup while it is saving a record.
- Added the ability to view and enter inactivity periods for credential types. If the user does not use the credential to access a door during this period, it will be disabled.

  Inactivity periods can be applied to credentials in individual user records, or as a default setting for each credential type.

  This feature requires Protege GX version 4.3.319 or higher.

- Added the ability to view elevator floor status in the web client.

  This feature requires Protege GX version 4.3.321 or higher.

Issues Resolved

- Resolved an issue where attempting to load events for a specific user would result in endless loading.
- Resolved an issue where event reports could not be created in the web client.
- Resolved an issue where saving a report record in the web client would remove operators assigned to that report.
- Resolved an issue where user PINs were displayed in plain text even when the operator had **Show PIN numbers for users** disabled.
- Resolved an issue where the default Administrator role could be edited in the web client.
- Resolved an issue where recurring calendar actions configured in the web client would recur on Mondays, even when they were programmed to recur on a different day.

Protege GX Web Client (1.47.0.45)

New Features

- Added the ability to select a display theme (light or dark) and display color when you log in to the web client. Your selection will persist whenever you log in to the web client from the same browser.

Feature Enhancements

- Improved web security by preventing cross-site scripting (XSS).
- Upgraded jQuery to version 3.5.1 to include an internal security patch.

Issues Resolved

- Resolved an issue where the **Credentials** tab was sometimes not displayed in the users programming.
- Resolved an issue where attendance reports generated through the web client displayed the incorrect month.
- Resolved an issue where user reports displayed the **value** of drop down custom fields instead of the display text.
- Resolved an issue where user reports did not display the default value for custom fields if a user did not have that field configured.
- Resolved an issue where user photos could not be viewed or added through the web client.
- Removed an ellipsis button which caused a 404 error.
- Resolved an issue where in some instances the Web Client failed to apply the correct operator role and security level access restrictions, allowing operators to view or edit menus and programming that they should not have access to.
- Resolved an issue where event filtered reports were not displayed correctly via the Web Client.
- Resolved an issue where the **Operator Logged In** time was not being displayed correctly.
- Resolved an issue where HTTP headers were not set on web client pages.
- Resolved an issue where performing a user search using any binary option (checkbox) returned no records.
- Removed the 'Copy' button from the areas page.
- Resolved an issue where door records had blank names and could not be saved by operators with restricted site access.
- Resolved an issue where area records had blank names and could not be saved.
- Resolved an issue where the credential types page was not displayed correctly in Internet Explorer browsers.
- Resolved an issue where the access levels page was not displayed correctly.
- Resolved an issue where the controller drop down menu on the daylight savings page was empty.

- Resolved an issue where the export PDF function was not working on the user reports page.
- Resolved an issue where the user page did not include scroll bars when the users were displayed in groups.

Protege GX Web Client (1.47.0.35)

New Features

- Web Client Cookies now have the HTTPOnly flag set, and are also now regenerated uniquely for every session. Both of these changes help mitigate the risk of client side scripts accessing the protected cookies.

Feature Enhancements

- Added the ability to multi-select records to apply common setting changes.
- Added the ability to filter an Event Report by individual controllers.
- Improved performance of the User list to make loading and switching between large numbers of users quicker.

Issues Resolved

- Fixed minor display and presentation issues.
- Fixed an issue where the **Use Access Level Door Type** setting was being enabled by default when adding an Access Level via the Web Client.
- Fixed a number of issues relating to the Find tool:
  - Where clicking the Find button on the User page would simply just refresh the page.
  - Where the Find tool was not displaying User Custom fields as it does in the Protege GX User Interface.
  - Where a number of blank lines were displayed in the Find tool search list on the Areas and Output Groups pages.
- Fixed an issue where adding Enterprise Muster Reports would cause blank pages to be displayed.
- Fixed an issue with Attendance Reports not showing any data in the Web Client.
- Fixed an issue where the Name2 field was being incorrectly served to the Mobile App through the Web Client.
- Fixed a bug where the Areas page would incorrectly load a blank page with editable fields allowing a new Area to be created through the Web Client.
- Fixed a bug where the Elevators page would incorrectly load a blank page with editable fields allowing a new Elevator to be created through the Web Client.
- Fixed instances of Fast CGI Handler error messages by adding Microsoft Visual C++ Runtime 2015 x86 to the Web Client installer.
- Fixed an issue on User Reports where PINs were being starred out (****) for an Operator that had permissions to view PINs.
- Fixed an issue where adding a card to an existing from a 'Read Raw Credential Data' event was clearing the user's PIN and resetting any card expiry options.
- Fixed a number of issues with the User Custom Fields tab:
  - Where the User Custom Field tab was not displaying special characters correctly.
  - Where Time and Date values and date picker were not working correctly.
  - Where the Custom Fields would appear in a random order each time the page was loaded.
- Fixed an issue where the text entered and saved into a Command field was disappearing when the page was refreshed.
- Fixed issues with text display and minor inconsistencies in button positions.
- Fixed an issue causing slowdown in the Web Client.
- Fixed an issue where printing reports to PDF was failing.
- Fixed an issue with changes to the operator password policy not taking effect when saved.

Protege GX Web Client (1.47.0.16)

New Features

The following new features have been included in this release:

- The Protege GX Web Client has been completely revamped and updated to match the Protege GX User Interface changes outlined earlier in this document.
- The Protege GX Web Client Installer has been updated to utilize PHP version 7.3.6.

Feature Enhancements

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

- Operator Passwords now support the use of the special characters # and &.
- Updated Door Statuses and Icons on status pages.

Issues Resolved

The following issues have been resolved in this release:

- Fixed an issue where changing an Operator password actually changed the Admin Operator password and not the password of the logged in Operator.
- Fixed an issue where the Name and Name2 fields were being switched around when logging in using a secondary language.
- Fixed an issue where User properties were not saved using the Web Client if a Custom Field and Custom Field Tab existed in programming.
- Fixed an issue where language translations were displaying the incorrect second language value for installations where a different alternative language was used to log into the web client.