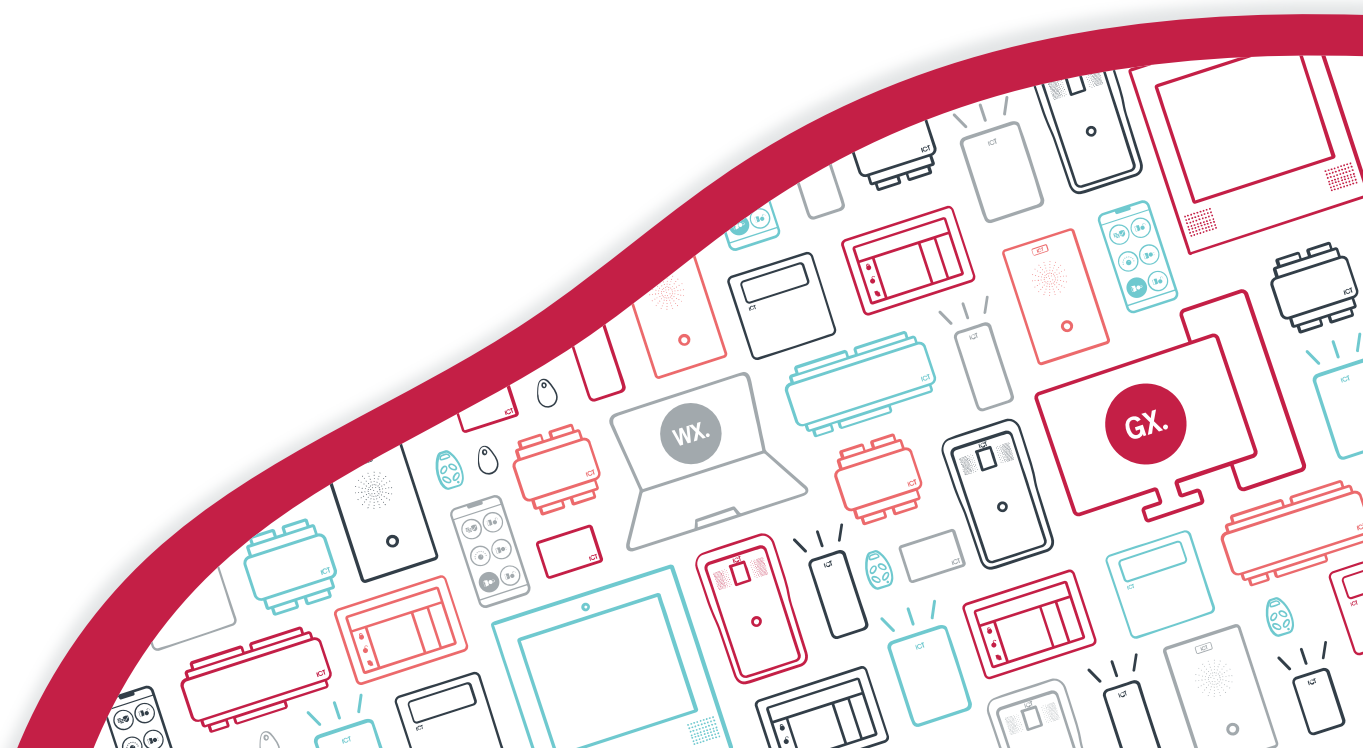
AN-331

KeySecure Integration with Protege GX

Application Note



Last Published: 01-Jul-21 12:20 PM

Contents

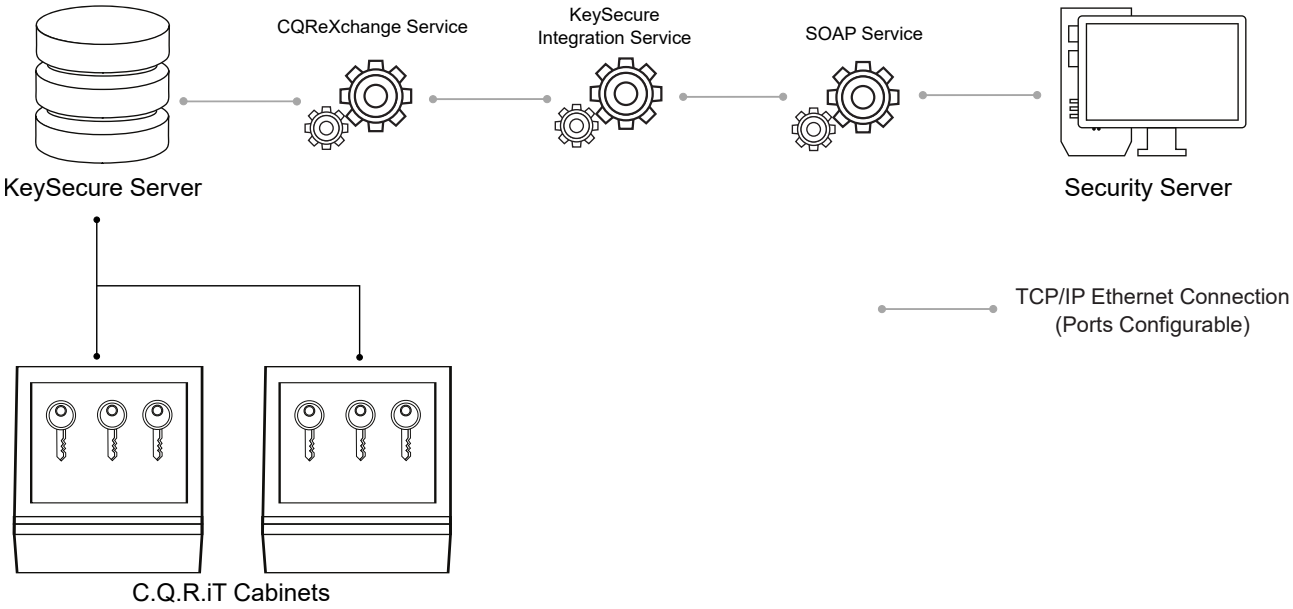
Introduction

The KeySecure system by CIC Technology enables centralized management of C.Q.R.iT electronic lockers and key cabinets, providing high levels of security, accountability and convenience. Their range of cabinets offers secure storage for a variety of items including keys, phones, laptops and briefcases, with options for both high and low security situations.

Protege GX integration with KeySecure enables you to control access to KeySecure items and cabinets using Protege GX users, access levels and schedules. Integration between the two systems also allows the extensive reporting and alarm functionality available in Protege GX to be used with KeySecure events.

Integration Architecture

This integration involves bi-directional synchronization of information between Protege GX and KeySecure, managed by the Protege GX KeySecure Integration Service. This service monitors the two systems and synchronizes any added, modified or deleted records based on the interval defined by the installer. In addition, the service continuously transfers any events triggered in KeySecure to Protege GX.



Synchronized Record Types

Each record type involved in this integration is synchronized in **one direction only**, as indicated by the table below.

Protege GX Record Type	KeySecure Record Type	Sync Direction
Cabinets	Cabinets	KeySecure to Protege GX
Keys	Items	KeySecure to Protege GX
Schedules	Time Profiles	Protege GX to KeySecure
Access Levels	User Groups	Protege GX to KeySecure
Users	Users	Protege GX to KeySecure

Prerequisites

The following software prerequisites must be installed and operational prior to beginning unless otherwise stated.

Software	Version	Notes
Protege GX	4.3.313.1 or higher	
Protege GX SOAP Service	1.6.0.6 or higher	Ensure that you know the endpoint address for the SOAP service. For installation instructions, see the Protege GX SOAP Service Installation Manual.
Protege GX KeySecure Integration Service	1.0.0.0 or higher	Instructions for installing this service are included in this application note.
KeySecure	1.3.5.2	This is the **only** tested and supported version for this integration.
CQReXchange	1.0.1.5	This is the **only** tested and supported version for this integration. Ensure that you know the endpoint address for the service.
C.Q.R.iT Cabinet Firmware	2.0808b (primary) / 2.007 (secondary)	These are the **only** tested and supported versions for this integration. The cabinet models supported by this integration are determined by the KeySecure system. For more information, see the KeySecure documentation available from CIC Technologies.
Microsoft .NET	4.8 or higher	

The following licensing is required:

License	Order Code	Notes
Protege GX KeySecure Integration License	PRT-GX-KSI	1 license per Protege GX server

Limitations

The following limitations apply when configuring and using this integration.

C.Q.R.iT Cabinet Limitations

Each C.Q.R.iT cabinet has limitations on the number of users, user groups, time profiles, item groups and access profiles it can support. The maximum supported number for each record type can be found in the CQReXchange Development Guide, available from CIC Technology.

Any number of records can be synchronized with the KeySecure system, as long as the number of records assigned to each cabinet does not exceed the supported maximum. The integration **does not** check these limits and it is the responsibility of the installer/operator to ensure that they are not exceeded.

Integration-Specific Limitations

The following features in KeySecure are not supported with this integration:

- Programming item groups in KeySecure is not supported. Items (keys) can be grouped together in an access level in Protege GX.
- The following features in a time profile:
  - **Effective From**: When a schedule is synchronized, this field is set to the current date.
  - **Cycle Type**: Only Weekly is supported.
  - **Exceptions**: All exception-related functionality is currently supported.
- Only those KeySecure events included in the appendix (see page 14) are supported in Protege GX.

The following limitations should be considered when implementing programming in Protege GX:

- This integration only supports one site in Protege GX and cannot be enabled for multiple sites.
- This integration cannot be used in a Protege GX system that has a Morse Watchmans KeyWatcher integration enabled (even on a different site).
- Time profiles in KeySecure only support a start time and end time. Therefore, only the first period of a schedule programmed in Protege GX will be synchronized to KeySecure. Any further periods will be ignored by the integration.
- Protege GX holiday groups are not supported in KeySecure. Scheduled periods cannot be changed on holidays.
- The maximum PIN length that can be assigned to a KeySecure user is 6 digits. If a PIN programmed in Protege GX exceeds this length the user record will be synchronized to KeySecure without a PIN. In addition, a warning will be logged in the log file for the integration service (see page 9).
- Only those user settings included in the user programming (see page 11) are supported in KeySecure.

Configuring KeySecure

This section outlines the configuration required in KeySecure and CQReXchange before configuring this integration. For more information about configuring the software, see the user documentation available from CIC Technologies.

Cabinets

All cabinets should be programmed in KeySecure. The KeySecure system must have at least one cabinet programmed prior to setting up the integration.

CQReXchange Settings

The following settings must be programmed in CQReXchange prior to setting up the integration:

- The **Third Party System** must be set to Generic Interface. This can be configured during installation of CQReXchange, or using the CQReXchange configuration app.
- You must know the **Security Token** to allow connection to CQReXchange. This can be found on the **Connection Configuration** tab of the CQReXchange configuration app.
- On the **Events** tab of the CQReXchange configuration app, select the event types that will be sent to Protege GX. For a list of event types supported in Protege GX, see the appendix (see page 14).
- If users will use cards to access cabinets, a data mask must be configured to define the expected card format. This can be programmed in either CQReXchange or KeySecure itself.

  Important: KeySecure is not able to interpret parity bits in a Wiegand card format. If you are programming a Wiegand card format as a data mask, ensure that you set the **Start Bit** and **End Bit** of each section appropriately so that any parity bits are ignored by KeySecure. For more information, refer to the KeySecure User Guide.

Setting Up the Integration

This section outlines the necessary steps for enabling the integration in Protege GX and installing the integration service.

Creating an Integration Operator

It is strongly recommended that you create a new Protege GX operator solely for use with this integration. This will ensure that the integration service has sufficient permissions to synchronize the data, and makes it simple to identify and audit changes made by the integration service.

1. In Protege GX, navigate to **Global | Operators**.
2. Click **Add** to create a new operator with a descriptive **Name** (e.g. KeySecure Integration Service).
3. Enter a **User Name** and **Password** for this operator. These will be used when configuring the integration service.
4. Set the **Role** to Administrator.
5. Enable the **Show PIN Numbers for Users** option. Click **OK** to clear the warning.
6. Click **Save**.

Enabling the Integration

1. Navigate to **Global | Sites** and select the site which will use this integration (or create a new one).
2. In the **Key Cabinets** tab, check the **Enable Integration** option.
3. Set the **Integration Type** to KeySecure - CIC Technology.
4. If desired, check the **Enable Logging** option. When this option is enabled, all KeySecure integration activity is logged by the integration service. When disabled, activity will not be logged.
   For more information, see Running and Troubleshooting the Integration (next page).

   This option is useful for setting up and debugging the integration, but should be deactivated during normal operation.
5. Click **Save**.

Creating the Credential Type

If cards will be used to access cabinets on site, you must program a credential type in Protege GX. This will be used to enter the KeySecure credentials in user records. This is not necessary if only PIN codes will be used for user access.

1. Navigate to **Sites | Credential Types**.
2. **Add** a new credential type with a descriptive **Name** (e.g. KeySecure Wiegand 26 Bit).
3. Set the **Format** to Wiegand.

   There is no need to enter a **Wiegand or TLV Format** unless the same credentials will be used at card readers in the Protege GX system.
4. If this credential type will also be used to access doors and elevator cars within the Protege GX system, enter the **Wiegand or TLV Format**. For more information on configuring Wiegand card formats, see Application Note 276: Configuring Credential Types in Protege GX.
5. Click **Save**.

Installing the Integration Service

1. Run the installation executable to launch the installation wizard.
2. Click **Next**.
3. Click **Next**.
4. Click **Next** to install the service in the default directory, or **Change...** to select a different directory.
5. When the installation is complete, enable **Launch on click "Finish"**, then click **Finish**.

The installation wizard will close and the Protege GX KeySecure Integration Manager will be launched.

Configuring the Integration Service

A number of settings must be configured in the Protege GX KeySecure Integration Manager to allow communication between the Protege GX and KeySecure systems.

Integration Settings

- **Sync Interval**: How frequently data will be synchronized between KeySecure and Protege GX. Set a number of seconds, minutes or hours.

Protege GX Settings

- **SOAP Service Address**: The endpoint address of the Protege GX SOAP Service. Upon installation, this address will be set to https://localhost:8040/ProtegeGXSOAPService/service.svc.

  If you see an error that reads 'Could not establish trust relationship for the SSL/TLS secure channel', resolve this issue by replacing the localhost portion of the address with the full hostname for the SOAP service.

- **Operator Username / Password**: The login credentials for the integration operator created above (see previous page).
- **Site**: The Protege GX site that has KeySecure integration enabled (see previous page).
- **Credential Type**: The credential type that will be used for cards in this integration (see previous page).

KeySecure Settings

- **CQReXchange Service Address**: The endpoint address of the CQReXchange service.
- **Security Token**: The security token retrieved from CQReXchange above (see page 7).

Running and Troubleshooting the Integration

When all necessary details have been configured, click **Start** to start the Protege GX KeySecure Integration Service and begin synchronization. To stop the service, open the integration service manager and click **Stop**.

Important: If any changes are made within the Protege GX KeySecure Integration Manager you must stop and start the service again before the changes will take effect.

When the **Enable Logging** option is enabled in **Global | Sites | Key Cabinets** the integration service will log events in a log.txt file. By default this can be found in C:\Program Files (x86)\Integrated Control Technology\KeySecure Integration Service. Logging may be useful for initial setup and troubleshooting but should be disabled during normal operation.

Programming in Protege GX

This section outlines the programming required to configure user access to C.Q.R.iT cabinets and keys in Protege GX.

Programming Schedules

Protege GX schedules can be used to manage when users are able to gain access to specific keys. When the schedule is valid, access will be permitted; when the schedule is invalid, access will be denied.

1. Navigate to **Sites | Schedules**.
2. **Add** a new schedule with a descriptive **Name** (e.g. Opening Hours).
3. In the **Period 1** row, set the **Start Time**, **End Time** and days of the week.

   Only the first programmed period will be synchronized with KeySecure. Holiday modes are ignored.

4. Click **Save**.

If a user requires access to the same key in multiple discontinuous periods (e.g. morning and evening, an overnight period, or different hours for weekends), it is necessary to create two schedules that each cover part of the necessary access period. An example of this programming is provided below (see page 12).

Programming Access Levels

Once keys have been synchronized from KeySecure they can be added to access levels to grant access to users. Multiple keys can be added to an access level, even if they are associated with different cabinets. The same access levels can also include Protege GX records such as doors and areas, enabling you to integrate key access with other access required on site.

The **Keys** tab will not be visible in the access level programming until the integration service has synchronized with KeySecure.

1. Navigate to **Users | Access Levels**.
2. **Add** a new access level, or select an existing record.
3. In the **Keys** tab, click **Add**.

   You will see the keys that have been synchronized from KeySecure. The name of each key in Protege GX is based on the cabinet ID, item ID and item name in KeySecure, e.g. [CB005:IT012] Basement Carpark.
4. Select one or more keys and click **OK**.
5. If required, set the **Schedule** for each key to one of the schedules created above.

   This is the **only** schedule option that will affect user access to keys. The integration will not respect schedules set in the **General** tab or the user record.

6. Click **Save**.

Configuring Users

Finally, the access levels and credential type created above can be assigned to new or existing user records. Only user records with one or more keys assigned to their access levels will be synchronized with KeySecure.

1. Navigate to **Users | Users**.
2. **Add** a new user or select an existing record.

3. Enter the user's **First Name** and **Last Name**. These fields are required to synchronize the user record to KeySecure.
4. In the **Access Levels** tab, click **Add** and select one or more access levels that have keys assigned. Click **OK**.
5. Return to the **General** tab.
6. Enter a **PIN** if the user does not already have one. This cannot exceed 6 digits.
7. Scroll down to the **Key Cabinet Integration** section. Note that the user's **Third Party User ID** field has been automatically filled.

   This is the User ID that the user must enter at a C.Q.R.iT cabinet to identify themselves. It can be edited manually if required.

8. Scroll down to the **Credentials** section and locate the credential type created for this integration (see page 8). Enter the user's card number, with a colon between the facility and card number (e.g. 1234:5678).

   Only one instance of this credential can be assigned to each user. If there are multiple instances, all will be ignored by the integration service and the user record will be synchronized to KeySecure without a card number.

9. Click **Save**.

Supported User Fields

The user fields listed below are supported by this integration. All other fields may be used within the Protege GX system as normal, but will not be synchronized with KeySecure.

Protege GX User Fields	KeySecure User Fields
First Name	First Name
Last Name	Surname
PIN	PIN
Third Party User ID	User ID (C.Q.R.iT access)
Disable User	Deactivate (marked orange in KeySecure)
Credential xxxx:yyyy	Facility Code Card/ID Code

Note: The KeySecure duress function is supported by this integration, and does not require additional configuration. Any user can activate a duress event by entering a 5 at the end of their PIN when logging in to a cabinet.

Programming Example: Day and Night Shifts

In this scenario, a security company has a company vehicle which guards can check out during their shifts to access the work site. There are two shifts: the day shift from 9am - 9pm, and the night shift from 9pm - 9am. Lucy Sun works the day shift and Te Kengo Black works the night shift. Both need an access level which will grant them access to take the car keys ([CB001:IT001] Company Car) during their working hours.

Programming the Day Shift

1. Navigate to **Sites | Schedules** and add a new schedule called Day Shift 9am-9pm.
2. Set the hours for **Period 1**:
   - **Start Time**: 09:00 AM
   - **End Time**: 09:00 PM
   - **Days**: Monday - Friday
3. Click **Save**.
4. Navigate to **Users | Access Levels** and add a new access level called Day Shift.
5. In the **Keys** tab, add the [CB001:IT001] Company Car key.
6. Set the **Schedule** to Day Shift 9am-9pm.
7. Click **Save**.
8. Navigate to **Users | Users** and add a new user with **First Name** Lucy, **Last Name** Sun.
9. In the **Access Levels** tab, add the Day Shift access level.
10. In the **General** tab, set the following:
    - **PIN**: Enter a 6-digit PIN or click the **[6]** button to generate a new PIN.
    - **Third Party User ID**: This field is filled automatically with a unique ID.
    - **Credentials**: Enter a card number in the credential type for this integration, e.g. 1234:5678.
11. Click **Save**.

Programming the Night Shift

Because the night shift spans over midnight, multiple schedule periods are required to cover the entire length of the shift. As the KeySecure integration does not support multiple periods per schedule, it is necessary to assign the same key to the user record twice, with each instance covering part of the shift. This requires two schedule and two access level records.

1. Navigate to **Sites | Schedules** and add a new schedule with the name Night Shift 9pm-12am.
2. Set the hours for **Period 1**:
   - **Start Time**: 09:00 PM
   - **End Time**: 12:00 AM
   - **Days**: Monday - Friday
3. Click **Save**.
4. Add a second schedule with the name Night Shift 12am-9am.
5. Set the hours for **Period 1**:
   - **Start Time**: 12:00 AM
   - **End Time**: 09:00 AM
   - **Days**: Tuesday - Saturday
6. Click **Save**.
7. Navigate to **Users | Access Levels** and add a new access level with the name Night Shift Part 1.

8. In the **Keys** tab, add the [CB001:IT001] Company Car key.
9. Set the **Schedule** to Night Shift 9pm-12am.
10. Click **Save**.
11. Add a second access level with the name Night Shift Part 2.
12. In the **Keys** tab, add the [CB001:IT001] Company Car key.
13. Set the **Schedule** to Night Shift 12am - 9am.
14. Click **Save**.
15. Navigate to **Users | Users** and add a new user with **First Name** Te Kengo, **Last Name** Black.
16. In the **Access Levels** tab, add both Night Shift Part 1 and Night Shift Part 2.
17. In the **General** tab, set the following:
    - **PIN**: Enter a 6-digit PIN or click the **[6]** button to generate a new PIN.
    - **Third Party User ID**: This field is filled automatically with a unique ID.
    - **Credentials**: Enter a card number in the credential type for this integration, e.g. 1234:9012.
18. Click **Save**.

When all programming has been completed, verify that Lucy Sun's PIN/card can be used to withdraw the key during the day, and Te Kengo Black's PIN/card can be used at night.

Appendix: Event Types

The table below indicates which KeySecure events are supported by this integration, and which event types these correspond to in Protege GX. Event types must be enabled in CQReXchange (see page 7).

KeySecure Event Type	KeySecure Event Description	Protege GX Event Type	Protege GX Event Description
3	Access Attempt (Known User)	30103	Access Attempt by User <USER_NAME> at Cabinet <CABINET_NAME>
4	Session Initiated	30104	User <USER_NAME> Initiated Session at Cabinet <CABINET_NAME>
5	Session Terminated	30105	User <USER_NAME> Terminated Session at Cabinet <CABINET_NAME>
6	Door Opened	30106	User <USER_NAME> Opened Door at Cabinet <CABINET_NAME>
7	Item Taken	30107	User <USER_NAME> Removed Item <ITEM_NAME> from Cabinet <CABINET_NAME>
8	Item Returned	30108	User <USER_NAME> Returned Item <ITEM_NAME> from Cabinet <CABINET_NAME>
11	Door Left Open	30111	Door Left Open at Cabinet <CABINET_NAME>
13	Tamper	30113	Tampering Detected at Cabinet <CABINET_NAME>
19	Door Forced Open	30119	Door Forced Open at Cabinet <CABINET_NAME>
20	Access Attempt (Unknown User)	30120	Access Attempt by Unknown User at Cabinet <CABINET_NAME>
21	Item Forced Out	30121	Item <ITEM_NAME> Forced Out at Cabinet <CABINET_NAME>
26	Locked by Administrator	30126	User <USER_NAME> Locked Cabinet <CABINET_NAME> as Administrator
27	Unlocked by Administrator	30127	User <USER_NAME> Unlocked Cabinet <CABINET_NAME> as Administrator
28	Locked by Software	30128	Cabinet <CABINET_NAME> Locked by Software
29	Unlocked by Software	30129	Cabinet <CABINET_NAME> Unlocked by Software
35	Power Restored	30135	Power Restored at Cabinet <CABINET_NAME>
39	Item Timer Expired	30139	User <USER_NAME> Timer Expired for Item <ITEM_NAME> at Cabinet <CABINET_NAME>
45	AC Power Outage	30145	Power Outage Detected at Cabinet <CABINET_NAME>
46	Low Battery Voltage	30146	Low Battery Voltage Detected at Cabinet <CABINET_NAME>
47	Duress Alarm	30147	User <USER_NAME> Duress Logon Received at Cabinet <CABINET_NAME>
48	Door Closed After Left Open	30148	Door Closed After Left Open at Cabinet <CABINET_NAME>

KeySecure Event Type	KeySecure Event Description	Protege GX Event Type	Protege GX Event Description
55	Item Forced In - Checkpoint	30155	Item <ITEM_NAME> Forced In as Checkpoint at Cabinet <CABINET_NAME>
56	Item Returned - Override Return	30156	User <USER_NAME> Override Return of Item <ITEM_NAME> at Cabinet <CABINET_NAME>
64	Item Forced In	30164	Item <ITEM_NAME> Forced In at Cabinet <CABINET_NAME>
65	Item Forced Out - Checkpoint	30165	Item <ITEM_NAME> Forced Out as Checkpoint at Cabinet <CABINET_NAME>
200	Synchronisation Fault Detected	30300	Synchronisation Fault Detected at Cabinet <CABINET_NAME>

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.