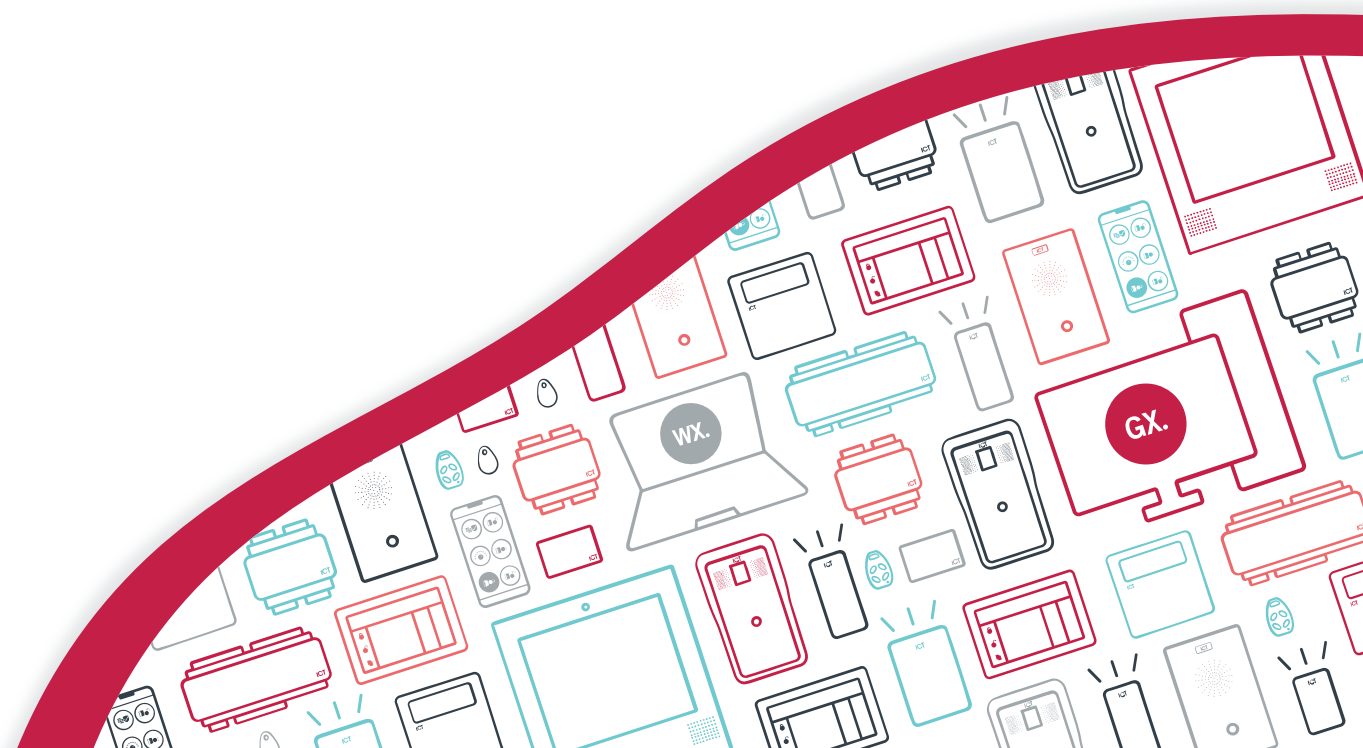
AN-335

Salto SHIP ProAccess SPACE Integration with Protege GX

Application Note



Last Published: 23-Feb-23 02:26 PM

Contents

Salto SHIP ProAccess SPACE Integration

High level integration between Protege GX and Salto SHIP enables you to seamlessly combine the real-time power of online doors with the versatility and cost effectiveness of offline doors to give your access control system true flexibility.

Salto integration enables you to:

- Take advantage of a single, comprehensive access control solution by bringing all of the day to day Salto lock management tasks into Protege GX.
- Control Salto online and offline locks from within Protege GX.
- View searchable audit trails of online and offline events.
- View archived footage from all related cameras, including those for offline locks.
- Monitor Salto wireless doors in real time.
- Encode cards in a single operation from the Protege GX interface.

This guide covers:

- Integration prerequisites and tested software and hardware versions (see page 7)
- Instructions for configuring the Salto software (see page 9)
- Instructions for configuring Salto integration within Protege GX (see page 13)

This application note covers integration with Salto SHIP ProAccess SPACE. For integration with Salto SHIP RW Pro Access, see AN-188: Salto SHIP RW Pro Access Integration with Protege GX.

Before You Begin

Who This Guide is For

This guide is intended for anyone who administers a Protege GX system and wants to integrate with Salto SHIP.

What You Should Already Know

This guide assumes that you are familiar with configuring, integrating and installing Protege GX, as well as configuring and understanding the security principles and policies within the facility you are working in.

You should also have completed Salto training and be currently certified.

This guide is limited to configuring the Protege GX Salto SHIP integration and does not cover:

- Protege GX server or client installation
- Salto ProAccess SPACE installation
- Configuring the firewall
- Installing Salto locks and configuring locks with a PPD
- Changing the IP addresses of the Salto controller/Ubox/hotspots/wireless locks
- Wiring of the Salto or ICT hardware

Important

- This integration supports synchronization between a single Protege GX site and a single Salto SHIP server only. Attempting to sync multiple Protege GX sites and/or multiple Salto SHIP servers will result in SHIP records being incorrectly overwritten.
- Protege GX acts as the host for this integration. Records are maintained in Protege GX and updated to Salto. This means that Protege GX controls what information the Salto system contains. Records must not be modified within Salto as doing so is likely to result in a loss of information and may cause further issues.
- Protege GX checks for changes regularly and updates the Salto system as required. Some functionality is reliant upon these updates. For example, when a new user is added you must wait for the update to complete before you can program a card. Before changing any records, always ensure that the Salto indicator icon (see page 14) is green, indicating that all Protege GX records have successfully downloaded.
- As of Protege GX version 3.2.77.0 the Salto Sync Service has been integrated with the standard Protege GX installation. If the service has previously been installed separately, it must be uninstalled.
- Salto records are limited to 24 characters in length.

Prerequisites

All software, firmware and hardware must be installed and operational before beginning this integration.

Component	Version	Notes
Software		
Protege GX Software	Version 4.2.251.19 or higher	
Salto SHIP	Version 1.40d	This is the **only** tested and supported version for this integration.
Salto ProAccess SPACE	Version 6.6.4.2	This is the **only** tested and supported version for this integration. This installation must have a blank database.
Firmware		
Protege GX Controller	Version 2.08.918 or higher	
Hardware		
Salto NCoder	Ethernet	
ICT USB Desktop Encoder	PRX-ENC-DT	

Encoder.ini File

This integration requires a custom encoder.ini file, programmed specifically for your installation. You will need to request the file from ICT, and provide the Protege GX **SSN** and the **CP#** (Credential Profile) for the cards.

Before beginning the installation the encoder.ini file issued by ICT must be copied to the installation directory of the Protege GX server and all Protege GX client installations that will be used for card encoding.

Licensing

License	Order Code	Notes
Protege GX Salto SHIP Door License	PRT-GX-DOR-IP	1 license per connected Salto door
	PRT-GX-DOR-IP-100	

Supported Salto Devices

The following Salto controllers have been tested and validated with this integration:

- CU42E0
- UBOX4000

The following Salto BLUEnet devices have been tested and validated with this integration:

- Salto BLUEnet Gateway
- Salto BLUEnet Node
- Salto XS4 One Escutcheon
- Salto XS4 Mini Escutcheon
- Ælement Fusion - ANSI

Other devices may be suitable for this integration but have not been validated and may require testing.

Record Names in Protege GX and Salto

Protege GX	Salto
User	User
Door	Door
Door group	Zone
Access level	Access level (group)
Schedule	Time zone or time period
Calendar	Calendar

Integration with Multiple Download Servers

This integration does not work correctly when multiple download servers can communicate with the Salto SHIP interface.

To mitigate this issue, block the outbound IP port that would be used to communicate with Salto SHIP on every download server machine/VM beyond the first. If the single record download service is in use, block outbound messages from that service on the SHIP port. This ensures that only the first download server can send data to SHIP.

Configuring Salto ProAccess SPACE

SAM the Salto Database

Before the Salto SHIP integration can be enabled, the Salto database needs to be SAM'd to allow operation with the SAM (Secure Access Module) cards. The integration will not function unless this is performed.

SAMing of the Salto database can only be performed by ICT technical support, and this needs to be completed before beginning the integration. You will need to contact ICT technical support and provide:

- A current **backup** of the Salto database
- A valid **login** for the Salto database
- The exact **ProAccess SPACE version** being used
- The exact **SQL Server version** being used with the Salto database

Important: For GDPR sites and secure sites that cannot ship their database backups, the database should be SAM'd before any users or user data is transferred from Protege GX.

Enabling the SHIP Interface

The SHIP interface must first be enabled in the Salto software.

1. Open the Salto application and log in using the relevant credentials.
2. Navigate to **General Options** and click the **SHIP** tab.
3. Enable the **SALTO server (SHIP)** option.
4. Set the **TCP/IP port**.

   If you are using the service version of Salto, ensure that this value does not interfere with the TCP/IP port of the Salto client, which is 8099 by default.
5. Click **Save** and close the window.
6. Upon closing, a warning appears informing you that changes won't take effect until the Salto Service is restarted. Ignore this warning until you have completed the entire setup.

Advanced Options

1. To enable the advanced features required for the integration, navigate to the **General Options** menu and select the **Advanced** tab. Enable and configure the following options from the **Parameters** section:
   - `EXIT_LEAVES_OPEN=1`

     Only select `EXIT_LEAVES_OPEN` if the site uses the exit leaves open open modes(see page 15).
   - `PROX_ANTICLONING=0`

     Ensure that `PROX_ANTICLONING` is set to **0**.
   - `RF_ENABLED=1`

     Only select the `RF_ENABLED` option if the site uses RF Salto locks.
   - `SHOW_EXT_ID=1`
   - `SHOW_ROM_CODE=1`
2. Click **Save**.

Configuring the Wiegand Code

Configure the Controller

For Salto installations using a **CU42E0 controller**:

1. Navigate to **System | Salto Network**.
2. In the list, click the breakout button beside the **CU4200** then click on the node to enter the device.
3. Under **Inputs** select **IN3** and click **Edit**.
   - Set the **Type** to CUADAP
   - Set the **Interface and data type** to 24. WIEGAND - WIEGAND CODE - Software defined
   - Set the **Reader number** to #1
4. Click **OK**.
5. Under **Inputs** select **IN5** and click **Edit**.
   - Set the **Type** to CUADAP
   - Set the **Interface and data type** to 24. WIEGAND - WIEGAND CODE - Software defined
   - Set the **Reader number** to #2
6. Click **OK**.

Configure the Ubox

For Salto installations using a **Ubox**:

Ensure that the Ubox's dipswitch settings match the following table.

Switch	Setting
1	ON
2	ON
3	OFF
4	OFF
5	ON
6	OFF
7	ON
8	OFF

Configure the Wiegand Code

1. Navigate to the **General Options** menu and select the **Users** tab.
2. From the **Wiegand Format** section, select **Configure**.
3. Click **Add Code**.
4. Enter the following details:
   - **Code**: A
   - **Description**: Facility Code
   - **Bit Order**: MSB
   - **Number of Digits**: 5
   - **Digital Format**: Decimal
5. Click **OK** to save.

6. Repeat steps **3 and 4** with the following details:
   - **Code**: B
   - **Description**: Card Number
   - **Bit Order**: MSB
   - **Number of Digits**: 5
   - **Digital Format**: Decimal
7. Click **OK** to save.
8. When the A and B codes have been created, enter **AB** into the **Interface Format** section.
9. Enter the following details to enable 34 bit Wiegand configuration:
   - **Bit composition**: PAAAAAAAAAAAAAAAABBBBBBBBBBBBBBBP
   - **Parity rule1**: EXXXXXXXXXXXXXXX----------
   - **Parity rule2**: ----------XXXXXXXXXXXXXXXO
10. Click **OK** to save the configuration.
11. In the **Tracks of User Key** section, ensure that **Wiegand Code** is enabled and **Profile Code** is selected.
12. Click **Save**.

Configuring the Salto Ethernet NCoder

Salto SHIP integration with Protege GX requires that a Salto Ethernet NCoder is connected and configured. The Ethernet NCoder acts like a dongle to validate the integration and is often stored in an IT closet, connected to a network switch. Optionally, it can also be used to read encoded cards to assist with troubleshooting.

The Salto Ethernet NCoder cannot be used to encode cards for this integration. Refer to Encoding Salto Cards (see page 19) for information on the card encoding process.

To configure a Salto Ethernet NCoder for use with the SHIP integration:

1. Select the **Devices** tab from the **General Options** menu.
2. From the **Dongle Encoder** section, ensure that the Ethernet Encoder is selected from the drop down.
3. Click **Save** to update.

Configuring the Operator's Editor

The operator's editor function is used for reading encoded Salto cards, to identify who the credentials belong to and what access they have been assigned.

You can also use the operator's editor to update a cardholder's credentials, much like a hotspot.

This functionality **does not** enable you to encode cards.

1. Navigate to the **Settings** menu.
2. From the **Local Settings** section configure the **Encoder Settings** as required:
   - If you are using a Salto USB encoder for this function, enable the **Local** option.
   - If you are using a Salto ethernet encoder for this function, enable the **Online** option and select the Ethernet Encoder from the drop-down menu.
3. Click **Save** to update.

In most situations a Salto USB encoder is used for this function as the ethernet encoder is generally not as accessible. Please note that ICT USB encoders do not support this function.

Restarting the Salto Service

Once configuration is complete you need to restart the Salto Service to activate the new settings.

1. Launch the Salto **ProAccess Space Configurator**.
2. Select the **SERVICE PROPERTIES** tab.
3. In the **Service Startup Control** section, click **STOP**.
4. Once the service has successfully stopped, click **START** to restart the service.
5. Click **CLOSE**.

Configuring the Integration in Protege GX

Copying the encoder.ini File

A customized encoder.ini file needs to be requested from ICT (see the Prerequisites section).

Before the Salto SHIP integration can be enabled, the **encoder.ini** file must be copied to the installation directory of the Protege GX server and all Protege GX client installation workstations that will be used for card encoding.

The default installation directory is C:\Program Files (x86)\Integrated Control Technology\Protege GX

Enabling Salto Integration

Launch the Protege GX client and log in.

You will need the necessary Salto door licenses applied to your SSN, and the Protege GX license file updated with the licenses, before you can access the Salto configuration menus and settings.

1. Navigate to **Global | Sites**.
2. Select the site that requires Salto SHIP integration.
3. Select the **Salto** tab.
4. Select the **Enable Salto (SHIP) Integration** option.
5. If you want to view error messages in the Salto error log during the configuration process, select the **Enable Logging** option.

This option is helpful for setup and troubleshooting but **should not be enabled during normal operation** as it saves events to the database. Remember to disable this option once setup is complete.

Configuring Salto Integration Settings

The parameters you enter here **must** match the settings in the Salto SHIP interface programming section.

1. Enter the **IP Address** and **IP Port** of the SHIP server.
2. If encoding MIFARE Classic cards from the Protege GX interface, you need to identify the sectors allocated to Salto. The allocated sectors are site specific and can be viewed in the **encoder.ini** file, which should be located in the installation folder: C:\Program Files (x86)\Integrated Control Technology\Protege GX (see above).

   For encoding MIFARE DESFire cards it is not necessary to identify and select sectors.
3. Select the **sectors** displayed in the encoder.ini file.

   Sector 14 must be left for use by the ICT format.
4. Click **Save**.

Once complete, Protege GX is able to sync with the Salto SHIP system. A complete download takes from a minute to two hours depending on the size of the site. During this time some integration features may be unavailable.

- A full download is only ever carried out the first time Salto integration is enabled, when the Protege GX software is upgraded, or when a database is restored.
- If the Salto database is changed or deleted, the **Enable Salto Integration** option within Protege GX must be disabled, the site saved, and the integration enabled again. This forces all of the records to resynchronize.

Salto Indicator Icon

After enabling Salto SHIP integration, a Salto status indicator icon is displayed in the Protege GX status bar. The Salto status indicator icon displays the current state of the integration. You can use this icon to ensure that the integration is running correctly or to diagnose problems.

- **Salto SHIP Status Failed (Red)**: Indicates that at least one record has failed to download correctly. For more information, refer to the Salto error log (see page 18).
- **Salto SHIP Status Synchronized (Green)**: Indicates that all Protege GX records have been successfully downloaded.
- **Salto SHIP Status Unknown (Gray)**: Indicates that there is a connection issue between the Protege GX interface and the Protege GX Download Service. If you encounter this error, ensure that the download service is running or check the Windows Event Viewer application log to diagnose any problems.
- **Salto SHIP Status Updating (Orange)**: Indicates that Protege GX is currently downloading to Salto.

  You can hover over the popup to see the exact number of items completed.

Background Update Icon

The background update icon is displayed in the Protege GX status bar and displays the active background operations. These operations include deleting an access level, a schedule or a Salto calendar.

When one of these records is being deleted, all other records tied to them cannot be modified. For example, if a Salto calendar assigned to a user is deleted, the user record won't be editable until the operation is complete.

- **Background Update Processing (Orange)**: An operation is currently being processed.
- **Background Update Success (Green)**: The operation completed successfully. These messages disappear automatically after a short period of time.
- **Background Update Failure (Red)**: The operation failed. This is often due to the system attempting to complete multiple operations at one time. For more information, refer to the Windows Event Viewer application log.

  Failure alert messages must be acknowledged by the operator, by clicking on the individual item or clicking the heading at the top of the list.
- The Background Updates Failed warning window is displayed when there is a failure that has not been acknowledged before the operator attempts to close the Protege GX user interface.

Schedules

Schedules are equivalent to Salto time periods, and can be used to control automatic door unlocking and user access. When used in conjunction with Salto calendars (see page 17), different periods can become valid on specific days (Holiday, Special 1 and Special 2).

To program a schedule:

1. In Protege GX, navigate to **Sites | Schedules** and click **Add**.
2. Give the schedule a **Name**.
3. Enter one or more periods. To the right of each period there is a **Salto** section with columns for **H** (Holiday), **S1** (Special 1) and **S2** (Special 2). For each period, either leave this column blank (so that the period will be valid on normal days) or select which type of day this period will become valid on.

   For example, a user might have access during their 9am - 5pm shift on normal days, but work a shorter shift (10am - 2pm) on public holidays. In this situation, you would create a 10am - 2pm period and select **H** in the **Salto** column so that the period will only become valid on holidays.
4. Click **Save**.

Unlike Protege GX holiday groups, Salto calendars must be applied to individual user and door records, not to the schedule itself.

Doors

The maximum number of doors that Salto currently supports is 64,000 per database. A maximum of 96 doors (individual doors or doors within a group) can be assigned to a user. This rule applies to adding doors/door groups to a user directly or via an access level.

When integrating existing Salto systems the doors that are being integrated must first be added in Protege GX. Once this is complete the locks will need to be reinitialized via the Salto PPD.

To configure Doors from within Protege GX:

1. Navigate to **Salto | Doors** and click **Add**.
2. Enter a **Name** for the Salto door.

   We advise naming doors in a way that will be easily recognizable in both Protege GX and Salto.
3. In the **Settings** section, configure an **Open Time**. If required, you can also set an **Increase Open Time** for users tagged as requiring extended access. This option is enabled from the users menu (see page 19).
4. If required, select the **Enable Antipassback** option from the **Antipassback** section. Some installations require the system to prevent users from entering through the same door twice before they have gone through the exit. This ensures that users cannot pass their credentials back to another user to grant access.

   In order for antipassback to function correctly, this option must also be enabled for each user required.
5. If antipassback is enabled, select the **Direction** of control, **From outside to inside** or **From inside to outside.**
6. The **Audit on Keys** option available from the **Audit Options** section enables you to keep a log of any door opening events that occur for the door. \

   In order for this to function correctly, this option must also be enabled for each user required.
7. The **Open Mode and Periods** section enables you to define the Open Mode and unlock schedule Periods to determine the behavior of the door.
   - **Open mode**: This field determines the operating mode for this electronic lock, i.e. how it can be accessed during different scheduled periods.
     - **Standard**: Users must badge an authorized Salto key to gain access.
     - **Office**: Users can set the door to office mode. Office mode is activated by presenting a Salto key while holding the inside handle down, and canceled by repeating the procedure. While in office mode the door is latch unlocked and can be accessed by any user without a credential.

       Only users with the **Office** option enabled can set a door to office mode (**Users | Users | Salto**).
     - **Toggle**: When this option is selected, users can activate and cancel office mode by badging their card, without holding down the inside handle.

       Only users with the **Office** option enabled can set a door to office mode (**Users | Users | Salto**).
     - **Automatic changes**: This option allows the door to operate under different modes at different times. The operation of this setting can be configured in the Salto software.
     - **Automatic open**: In this mode the door will automatically latch unlock when the **Open periods** schedule becomes valid. When the schedule is invalid the door will automatically lock and operate in standard mode.
     - **Automatic opening + office**: In this mode the door will automatically latch unlock when the schedule becomes valid. The door locks when the schedule becomes invalid, but users can still activate office mode by badging a card with the inside handle held down.

- **Automatic opening + toggle**: In this mode the door will automatically latch unlock when the schedule becomes valid. The door locks when the schedule becomes invalid, but users can still activate office mode by badging a card.
- **Key + PIN**: The door requires both a valid Salto key/card and a valid PIN to be entered at the keypad. This is valid at all times.

  The **PIN** option must be enabled in the **Users | Users | Salto** tab.
- **Keypad only**: The door can be opened by entering a valid code at the keypad. This is valid at all times.
- **Timed key + PIN**: This mode is the same as Key + PIN except a PIN is only required when the **Open periods** schedule is valid. Outside this period only a card is required for access.
- **Timed keypad**: This mode is the same as Keypad except the code can only be used when the **Open periods** schedule is valid. Outside this period a card can be used for access.
- **Timed office**: This option is similar to Office except office mode can be activated only when the **Open periods** schedule is valid. The door will automatically lock and operate in standard mode when the schedule period ends.
- **Timed toggle**: This option is the same as Toggle except office mode can only be activated when the **Open periods** schedule is valid. The door will automatically lock and operate in standard mode when the schedule period ends.
- **Exit leaves open**: When this option is selected the door operates in standard mode. However, when the inside handle is held down the door will latch unlock.

  The `EXIT_LEAVES_OPEN` option must also be enabled in the Salto software (**Advanced options**).
- **Toggle + exit leaves open:** This is a combination of the two modes. When a valid card is presented the door will begin to work in Toggle mode. Using the inner handle activates Exit Leaves Open mode.

  The `EXIT_LEAVES_OPEN` option must also be enabled in the Salto software (**Advanced options**).

- **Open periods**: The schedule that is associated with the Salto door. This is equivalent to a time periods record in the Salto software. The operation of this schedule will depend on the **Open mode** selected above.

8. The **Cameras** section enables you to assign a camera to the Salto door, allowing you to view a camera feed from an event associated with the door.
9. Click **Save** to complete the configuration of the Salto door.

When all door records have been added the locks will need to be reinitialized via the Salto PPD.

Door Commands

Right clicking on a Salto door record, or multiple Salto door records, in Protege GX launches a command window enabling you to send the following commands to the Salto system:

- Open
- Emergency open
- Emergency close
- Cancel emergency

These commands are only relevant for online locks. Using these commands with offline locks causes Protege GX to return an error. At this stage there is no way to distinguish between online and offline locks.

Door Groups

Salto door groups enable you to bring Salto doors together into logical groups and define which doors particular users are able to access/control. Within the Salto software, door groups are referred to as zones.

A maximum of 96 doors (individual doors or doors within a group) can be assigned to a user. This rule applies to adding doors/door groups to a user directly or via an access level.

To create Salto Door Groups from within Protege GX:

1. Navigate to **Salto | Door Groups** and click **Add**.
2. Enter a **Name** for the door group.

   We advise naming door groups in a way that will be easily recognizable in both Protege GX and Salto.
3. Click the **Doors** tab.
4. Click **Add** and highlight the doors you want included in the group.
5. Click **Ok**.
6. Click **Save.**

Door Group Commands

Right clicking on a Salto door group record in Protege GX launches a command window enabling you to send the following commands to the Salto system:

- Open
- Emergency open
- Emergency close
- Cancel emergency

These commands are only relevant for online locks. Using these commands with offline locks causes Protege GX to return an error. At this stage there is no way to distinguish between online and offline locks.

Calendars

Salto calendars enable you to use an alternative time period for a record on specific dates. Each calendar can define three different types of day: Holiday, Special 1 and Special 2. When one of these special days occurs the periods marked for those days in the schedule (see page 14) will be used instead of the default periods.

Salto locks use calendars when operating in a timed mode, such as Automatic Open or Timed Key + PIN. They can also define when a user has access to a door.

To create a Calendar in Protege GX:

1. Navigate to **Salto | Calendars** and click **Add**.
2. Enter a **Name** for the calendar.

   We advise naming calendars in a way that will be easily recognizable in both Protege GX and Salto.
3. Click the **Dates** tab.
4. Click **Add**.
5. Complete the following fields:
   - **Name**: Used to describe the date (e.g. Christmas).
   - **Date**: The date of the Holiday/Special day.
   - **Type**: The type of date. Choose from Holiday, Special 1 or Special 2.
6. Repeat steps 4 and 5 to add more dates to the calendar.
7. Click **Save**.

Salto Error Log

When the **Enable Salto logging** option is enabled in the **Global | Sites | Salto** menu, the Salto error log shows events of all the data sent to the Salto system. This information is used for debugging.

Messages stored in the error log are generally logged in pairs, with one message showing the information sent to the Salto system and the other showing the reply from the Salto system.

Common events include:

- **GetInfo**: This message is logged once each time the download server starts, and displays the current SHIP version that the Salto system is running.
- **InsertOrUpdate**: This message indicates that Protege GX is updating the records within the Salto system.

To view the Salto error log, navigate to **Salto | Salto Log**.

Access Levels

Access levels are assigned to users to determine access conditions. Integration with Salto allows you to add Salto doors and Salto door groups to an access level, and specify the access schedule for each door/door group.

Important: Access schedules for Salto doors must be assigned directly to each Salto door or door group assigned in the access level, in **Users | Access Levels | Salto Doors** or **Salto Door Groups**. Schedules assigned to the access level itself **do not** impact access to Salto doors.

To add Salto doors or door groups to an access level, navigate to **Users | Access Levels**.

Access Levels | Salto Doors

A maximum of 96 doors (individual doors or doors within a group) can be assigned to a user. This rule applies to adding doors/door groups to a user directly or via an access level.

1. Select the **Salto Doors** tab.
2. Click **Add** and highlight the required records.
3. Click **OK**.
4. The **Schedule** determines when users with this access level will have access to each Salto door.
5. Click **Save**.

Access Levels | Salto Door Groups

A maximum of 96 doors (individual doors or doors within a group) can be assigned to a user. This rule applies to adding doors/door groups to a user directly or via an access level.

1. Select the **Salto Door Groups** tab.
2. Click **Add** and highlight the required records.
3. Click **OK**.
4. The **Schedule** determines when users with this access level will have access to each Salto door group.
5. Click **Save**.

Users

Integration with Salto SHIP enables you to encode cards for use with Salto locks, configure various Salto related user options, and add Salto doors and door groups directly to a user.

The Salto JustIN Mobile app and credentials are currently not supported by this integration.

To configure user requirements for Salto SHIP integration, navigate to **Users | Users**.

Encoding Salto Cards

The database must be SAM'd with a valid encoder.ini file (see page 9) before Salto cards can be encoded.

Card encoding is core functionality for this integration. Cards will not be usable on Salto locks until they have been correctly encoded.

Important: Only an ICT USB Desktop Encoder can be used to encode cards for use in this integration. Salto encoders are not able to communicate with Protege GX for card encoding.

Before encoding any Salto cards, ensure that the Salto indicator icon (see page 14) is green, indicating that all Protege GX records have successfully downloaded.

Once the Salto SHIP integration has been enabled and correctly configured in Protege GX, a **Program Card** button will be available in the **General** tab of each user record, above the **Facility/Card Number** fields.

1. Navigate to **Users | Users** and select a user to encode a Salto card for.
2. Ensure that the first **Facility/Card Number** record contains the number to be encoded on the card.

   The encoding process will only read the facility/card number contained in this top position.
3. Place a valid programmable Salto card onto a connected ICT USB Desktop Encoder, then click **Program Card** to encode the card for operation with Salto locks.
4. During the encoding process, a dialog window displays the progress.
5. When encoding is complete, a message will advise that 'The smartcard was successfully programmed'.

If the encoding process returns a key error message, contact ICT Technical Support.

Users | Salto

The **Salto** tab enables you to set various Salto specific user options.

1. The following options are available from the **Salto Options** section:
   - **Calendar**: A Salto calendar defines the days when the user's access permissions have different hours (such as holidays).

     Calendars can be programmed in **Salto | Calendars**. The schedule(s) assigned to the user's access level define the periods that are active on different days (see the **Salto** column of **Sites | Schedules | Configuration**).
   - **Use extended opening time**: With this option enabled, whenever this user is granted access to a Salto door the lock will open for the **Increase open time** instead of the **Open Time** programmed in **Salto | Doors | General**. This should be used to grant people with mobility issues extended times to access doors.
   - **Office**: When this option is enabled the user can set Salto doors to 'office mode' (latch unlock). Office mode is activated by presenting a Salto key while holding the inside handle down, and canceled by repeating the procedure.

     The door's **Open mode** must support office mode (**Salto | Doors**).
   - **Use antipassback**: With this option enabled the user will be affected by any antipassback restrictions set on Salto doors.
   - **Audit openings in the key**: With this option enabled the Salto system will generate an audit trail on the Salto credential itself when this user opens a Salto door. The **Audit on keys** option must also be selected in the **Salto | Doors | General** programming.
   - **PIN**: When this option is enabled the user can use their PIN (**General** tab) to access keypad enabled Salto locks.
   - **User can override privacy**: When this option is enabled the user can access a Salto door even when it has been set to privacy mode (locked from the inside).
   - **User can override lockdown**: When this option is enabled the user can open a Salto door even when it has been closed by a lockdown (emergency close).
   - **User can lockdown door**: When this option is enabled the user can initiate a lockdown on compatible Salto doors (with AMOK escutcheons). The lockdown is initiated by holding the card to the AMOK reader (lower inside handle) and canceled the same way.
2. The following options are available from the **User and Key Expiration** section:
   - **Start**: When this option is enabled the user's Salto key will not become active until the date specified. They will not be able to gain access to Salto doors before this date.
   - **End**: When this option is enabled the user's Salto key will expire after the date specified. They will not be able to gain access to Salto doors after this date.
   - **Enable revalidation of key expiration**: When this option is enabled the Salto key will expire at the end of the **Update period**. Whenever the key is presented at a Ubox or online lock it is revalidated and the update period is renewed.
   - **Update period**: Defines how long the Salto key will remain valid after it is updated at a Ubox or online lock. For example, for a short term residency you might set the key to expire every 48 hours unless revalidated.
   - **Period**: Sets the **Update period** to days or hours.
   - **Cancel key**: This button deactivates the user's Salto key.
3. The **Key Status** section displays the key assigned to the user and when the key is due to expire.
4. Click **Save**.

Users | Salto Doors

A maximum of 96 doors (individual doors or doors within a group) can be assigned to a user. This rule applies to adding doors/door groups to a user directly or via an access level.

1. Select the **Salto Doors** tab.
2. Click **Add** and highlight the required records.
3. Click **OK**.
4. The **Schedule** determines when the user will have access to each Salto door.
5. Click **Save**.

Users | Salto Door Groups

A maximum of 96 doors (individual doors or doors within a group) can be assigned to a user. This rule applies to adding doors/door groups to a user directly or via an access level.

1. Select the **Salto Door Groups** tab.
2. Click **Add** and highlight the required records.
3. Click **OK**.
4. The **Schedule** determines when the user will have access to each Salto door group.
5. Click **Save**.

Status Pages

Salto integration enables you to add Salto doors and Salto door groups to a Protege GX status page.

- When included in a status page, a Salto door displays its current status if it is an online lock.

  The status displayed in Protege GX mirrors the lock state displayed in ProAccess SPACE **Online Monitoring**.

- Right clicking on a Salto door or door group launches a command window enabling you to send the following commands to the Salto system:
  - Open
  - Emergency open
  - Emergency close
  - Cancel emergency

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