AN-343

# Protege GX Aperio IP Hub Integration

Application Note

The specifications and descriptions of products and services contained in this document were correct at the time of printing. Integrated Control Technology Limited reserves the right to change specifications or withdraw products without notice. No part of this document may be reproduced, photocopied, or transmitted in any form or by any means (electronic or mechanical), for any purpose, without the express written permission of Integrated Control Technology Limited. Designed and manufactured by Integrated Control Technology Limited, Protege® and the Protege® Logo are registered trademarks of Integrated Control Technology Limited. All other brand or product names are trademarks or registered trademarks of their respective holders.

Copyright © Integrated Control Technology Limited 2003-2026. All rights reserved.

Last Published: 11-May-26 3:24 PM

# Contents


Introduction 5
Prerequisites 5
Aperio Customer Encryption Key File 6
MIFARE / DESFire Encryption Keys 6
Integration Capacity 6
Connections 6
Aperio Hardware Installation and RF Channels 7
Aperio Programming Application Setup 9
Creating a new Door Installation 9
Configuration for Aperio IP Hubs 9
Scanning for Communication Hubs 10
Pairing Locks with a Communication Hub 10
Finding the MAC Addresses 10
Configuring a Lock for Sector 13 Encrypted Card Operation 10
Configuring a Lock for DESFire Encrypted Card Operation 11
Protege GX Setup 12
Configuring the Onboard Ethernet Port 12
Bringing IP Hubs Online 12
Adding the Aperio Locks as Smart Readers 13
Changing the Credential Format 13
Using Cards with Reverse Byte Order 14
Adding the Trouble Inputs 14
Programming AES Encrypted Card Operation in Protege 14
Programming Encrypted Aperio Cards 14
Programming the Encryption Key for all Aperio Locks on a Controller 15
Programming the Encryption Key for Individual Aperio Locks 15
Appendix: Validated Features 16
Supported Protege GX Door Options 16
Supported Protege GX Door Type Options 18
Supported Protege GX Smart Reader Options 19
Supported Protege GX User Access Restrictions 20
Validated Card Formats 20
Supported Aperio Door Features 20
Known Issues 20

# Introduction

Aperio integration is a licensed feature that enables Aperio wireless locking devices to be used within the Protege GX system. Each Protege GX controller can communicate with up to four AH40 Aperio IP hubs, with each hub allowing 16 wireless locks to be added to the system.

This application note covers the requirements for integrating with Aperio IP hubs, the capabilities of the integration, and the required programming in the Aperio Programming Application and Protege GX.

For integration with Aperio RS-485 hubs, see Application Note 147: Protege GX Aperio Integration.

# Prerequisites

### Protege GX Components

| Component | Version | Notes |
|---|---|---|
| Protege GX | 3.2.62 or higher | |
| Protege GX Controller | 2.08.1535 or higher | |

### Required Aperio Components

Ensure that you are using the correct matching programming application, radio dongle, wireless hub and locks for your region.

The versions reported below are the only versions validated by ICT.

| Component | Version | Notes |
|---|---|---|
| Aperio Programming Application | 25.0.23 | To check which version you are using, navigate to **Help \| About Aperio Programming Application** from within the Aperio Programming Application. |
| Aperio Radio Dongle | - | The integration has been validated with the following model: TriBee USB, Model nr. 200300. |
| AH40 Wireless Hub (Gen 5) | 1.1.0 | |
| AH40 Wireless Hub (Gen 3) | 1.10.3476 | |

### Supported Aperio Locks

ICT has only validated this integration with the locks listed below. Other locks and versions supported by ASSA ABLOY may be used in this integration, but ICT cannot directly support them without a sample being supplied for testing.

It is highly recommended that V3 locks are used due to improved response times.

| Lock | Firmware Version |
|---|---|
| AU100 HF V3 | 3.15.55 |
| C100 V3 | 3.14.70 |
| E100 V3 | 3.14.70 |
| G100 V3 | 3.14.70 |
| H100 V3 | 3.14.70 |
| IN100 V3 | 3.16.38 |

| Lock | Firmware Version |
|---|---|
| KL100 V3 | 3.21.102 |
| KS100 V3 | 3.14.70 |
| P100 V3 | 3.14.70 |

It is the responsibility of the installation professional to verify the version of the proposed third-party system and supported components with the version listed in this document. ICT will not accept responsibility for the failure to verify integrated system versions and requirements.

**Licensing**

| License | Order Code | Notes |
|---|---|---|
| Protege GX Aperio IP Hub Door License | PRT-GX-DOR-AP-IP | 1 per Aperio door connected to an IP hub.<br>The required number of Protege GX door licenses will be added automatically. |

## Aperio Customer Encryption Key File

Configuring the Aperio integration requires an XML encryption key file which is used by the Aperio Programming Application to establish encrypted communication between Aperio devices. The customer encryption key is unique to each site.

The encryption key file must be obtained from ASSA ABLOY before beginning the integration process. Without it you will not be able to create a new installation in the Aperio Programming Application, and will not be able to register the Aperio hub and wireless locks.

Contact ASSA ABLOY to request the XML customer encryption key file before you begin.

## MIFARE / DESFire Encryption Keys

If you intend to use Sector 13 Encrypted MIFARE or DESFire cards in this installation, you must acquire your encryption key from ICT Technical Support before you begin.

# Integration Capacity

The Aperio integration currently supports the following quantities on each controller:

| Aperio Component | Supported Quantity |
|---|---|
| IP Hubs | 4 |
| Wireless Locks per Hub | 16 |
| **Total Wireless Locks Supported per Controller** | **64** |

# Connections

AH40 hubs can be connected to the controller using a standard ethernet segment via the local area network.

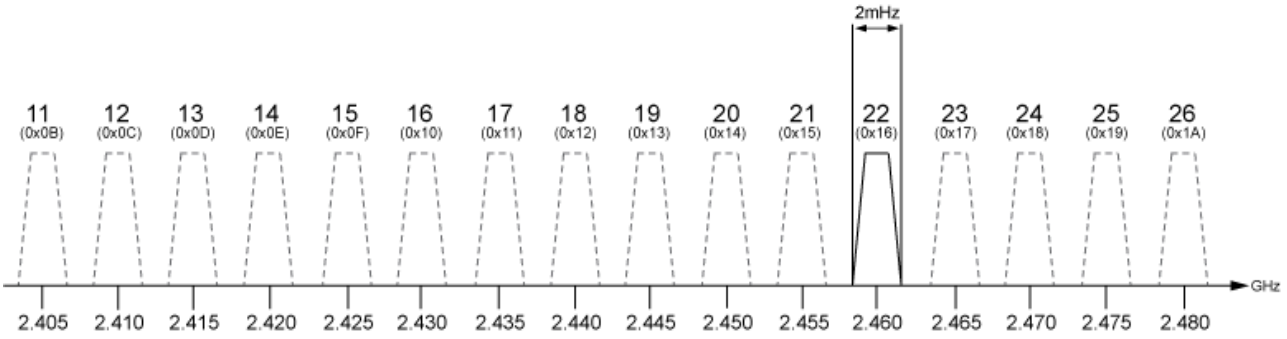
# Aperio Hardware Installation and RF Channels

Before installing any Aperio hardware, we recommend that you consult your Aperio installation guide for restrictions and installation guidelines.

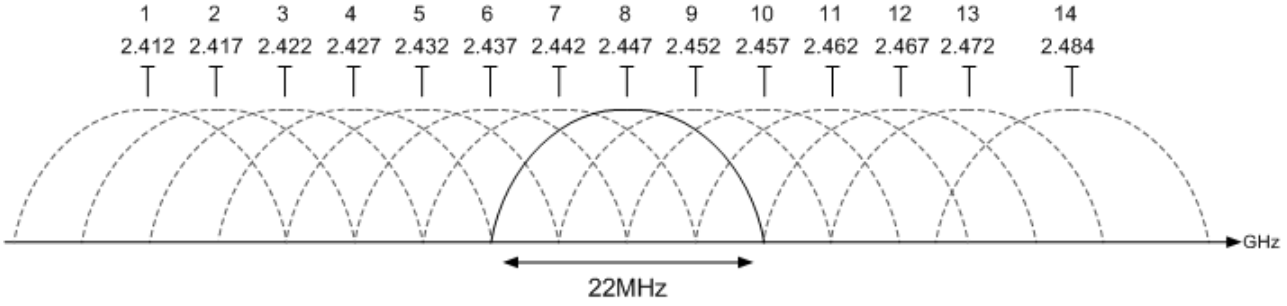
It is important to identify any devices that could affect the operation of your Aperio system. It is advised that any device operating on the 2.4GHz band be kept at least 3.5m (11.5ft) from the communication hub and lock.

Aperio communication hubs are able to establish a reliable radio link regardless of their mounting position and the type of lock used. However, Aperio devices operate on a 2.4GHz band - the same band as Wi-Fi, Bluetooth, cordless phones and even microwave ovens - so it is important to identify any devices that could affect the operation of your Aperio system before wiring and installing the hardware. Predicting the behavior of radio waves and detecting the presence of interfering signals can be difficult with wireless networks, so conducting an RF site survey is recommended.

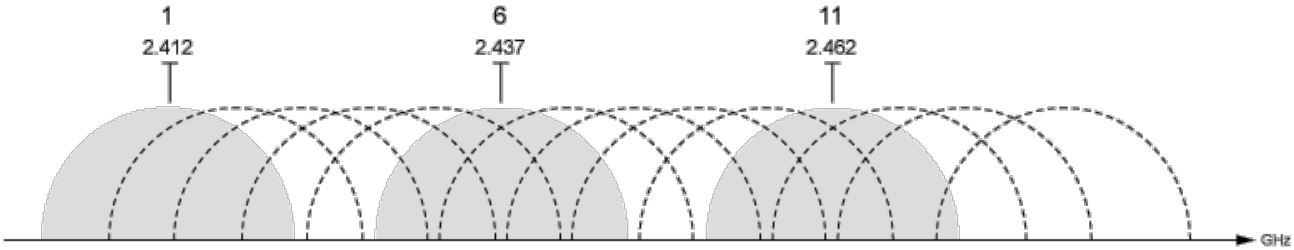
Aperio wireless locks use a communication protocol based on the IEEE 802.15.4 standard with 16 separate channels that occupy 2MHz of bandwidth from 2405MHz to 2480MHz. An RF site survey can determine which of the 16 channels the Aperio network should use.



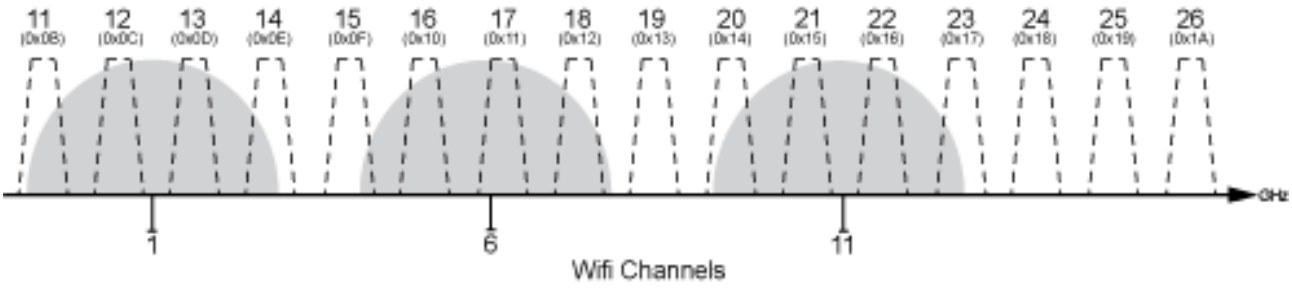

As an example, we can look at how Wi-Fi can affect the operation of Aperio when it is operating on the same 2.4GHz band. Wi-Fi generally operates on a standard of the IEEE 802.11 communication protocol divided into 14 channels, each occupying 22MHz of bandwidth from 2412MHz to 2484MHz.




The commonly used channels are 1, 6 and 11 as they are the only channels that do not share frequency space within the band.




From the results of an RF site survey, you can determine which of the channels the Wi-Fi network is using. With this information, you can see which of the Aperio channels will be least affected by the Wi-Fi network. The diagram below shows that channels 11, 14, 15, 19, 20, 23, 24, 25 and 26 are the least likely to incur interference from the Wi-Fi network, so these would be the most effective channels to use for your Aperio network.




By default, Aperio hubs are configured to automatically select the radio channel that is least affected by radio interference.

# Aperio Programming Application Setup

The Aperio Programming Application manages Aperio communication hubs, Aperio locks and cards.

This section is limited to a brief overview of the Aperio Programming Application and only addresses the configuration that is required for integration. For more information, consult the Aperio installation manual.

## Creating a new Door Installation

Before you can add the communication hub or lock, you need to create a new Installation Instance.

1. Insert the Aperio USB radio device into one of your PC's USB ports and open the Aperio Programming Application.
2. If you are using the program for the first time, complete any initial setup steps required.
3. From the **File** menu, select **New**.
4. Enter a name for the installation and click the ellipsis **(...)** button to locate the **Key file**.

   This is the .xml customer encryption key file obtained from ASSA ABLOY (see page 6).
5. Click **Create new**.
6. Enter a password of at least eight characters and click **OK**.

## Configuration for Aperio IP Hubs

All hubs used for the Aperio Integration must be configured using the following steps:

1. From the installation window, right click on the hub and navigate to **Communication Hub | Configure**.
2. Navigate to **EAC and Network Settings**.
3. Set the **ACU address** to the IP address of the controller, and the **ACU port** to the port which the hub will use to communicate with the controller. Enable TLS encryption for secure communications.

   Consult with your system administrator to select an available port. This port will be used as the controller's **Ethernet port** later in the setup (see page 12).
4. Navigate to **Electronic Access Controller Settings**.
5. Under **EAC Credential Settings** you must configure the **UID Reverse Byte Order** settings. The table below shows how the **UID Reverse Byte Order** settings should be configured, based on the hub version and the card format that will be used

| Card Format | Gen 3 Hubs | Gen 5 Hubs |
|---|---|---|
| MIFARE UID | ✓ | ✓ |
| MIFARE Classic with Sector Data | ✗ | ✗ |
| DESFire | ✓ | ✓ |

   ✓ = Enable all UID Reverse Byte Order settings

   ✗ = Disable all UID Reverse Byte Order settings
6. Complete the remaining configuration wizard steps to push the changes to the hub.
7. Repeat this process for all hubs to be used for the integration.

# Scanning for Communication Hubs

1. Upon saving the installation file, a scan will begin to locate communication hubs that are in reach of the radio device. Once the scan is complete, the window displays all communication hubs in reach of the radio device.

   You can identify a communication hub by the last four characters of the hub's MAC address (e.g. 01CF). These characters correspond to the label on the cover of the hub.

2. If the scan did not return all of the installed hubs, click **Rescan**
3. Select the hub(s) that you want to include in your installation, then click **Show Details** to open the Installation window

# Pairing Locks with a Communication Hub

Each lock to be used in the integration needs to be paired with a communication hub. The example below demonstrates the pairing process.

1. From the **Installation** window, right click on the hub and navigate to **Communication Hub | Pair with Lock or Sensor**.
2. A new window will appear prompting you to either show a card or engage a sensor to pair the lock.
3. Follow the prompt and click **Done** when pairing is complete.
4. If the pairing was successful, click **Close** to return to the **Installation** window.
5. Repeat this process to pair any remaining locks in reach of the USB radio device.

# Finding the MAC Addresses

When programming this integration, you will need the MAC address of each hub and lock that will be connected to the system. To find these addresses:

1. Click **Quick Scan** to scan for nearby hubs.
2. When the relevant hub is detected, select it and click **Show details**.
3. The **Communication Hub** column should display an ID with 6 numbers/letters. This represents the last 3 bytes of the hub's MAC address. Make a note of this 6-digit ID.
4. This page should also display the locks which have been paired to the hub. The **Lock/sensor** column will show the last 3 bytes of each lock's MAC address. Make a note of the 6-digit ID for each lock.

# Configuring a Lock for Sector 13 Encrypted Card Operation

This section is specific to integrations requiring Sector 13 MIFARE Classic programmed cards for sites using both Aperio wireless locks and ICT proximity readers and/or cards.

If you are using Aperio wireless locks and ICT proximity readers on the same site, follow the steps below to enable the reading of Sector 13 MIFARE Classic programmed cards on Aperio wireless locks.

This ensures that the same number is read by both Aperio wireless locks and ICT proximity readers.

**Configuring an Aperio Lock to read MIFARE Classic Sector Data**

1. Right click on the lock within the Aperio Programming Application and navigate to **Lock/Sensor | Configure**.
2. Click **Add/Change**.
3. From the **RFID Card Type** dropdown, select MIFARE Classic Sector.
4. Set the **Sector** option to 13.

5. Set the **Start Address in Sector** to 0.
6. Set the **Length to read in Sector** to 16.
7. Set the **MIFARE Authentication Key** to the 6 byte MIFARE key supplied by ICT.
8. Set the **Read Key** to MIFARE Key A.
9. Click **OK**.
10. Click **Next**.
11. Continue to click **Next** until the final screen, which displays the **Apply** option and prompts you to show a card. Present a MIFARE sector 13 encoded card to the Aperio lock.
12. When successful, click **Apply**.

# Configuring a Lock for DESFire Encrypted Card Operation

This section is specific to integrations where ICT encrypted DESFire programmed cards are required, for sites using both Aperio wireless locks and ICT proximity readers and/or cards.

If you are using Aperio wireless locks and ICT proximity readers on the same site, follow the steps below to enable the reading of ICT encrypted DESFire programmed cards on Aperio wireless locks.

This ensures that the same number is read by both Aperio wireless locks and ICT proximity readers.

**Configuring an Aperio Lock to read ICT Encrypted DESFire Sector Data**

1. Right click on the lock within the Aperio Programming Application and navigate to **Lock/Sensor | Configure**.
2. Click **Add/Change**.
3. Enable the **Use MIFARE DESFire RFID** option.
4. From the **RFID Card Type** dropdown, select DESFire.
5. Set the **Application ID** to the ID supplied by ICT.
6. Set the **File Identity** to 0.
7. Set the **File Start Position** to 0.
8. Set the **Length to read in File** to 16.
9. Set the **File Data Protection Level** to full Encryption.
10. Set the **Key Type** to AES 128.
11. If available, set the **Diversification Algorithm** to None. (This option is not available for all installations).
12. If available, set the **Diversification Type** to 1KTDES. (This option is not available for all installations).
13. Set the **Key** to the DESFire key supplied by ICT.
14. Set the **Key Number** to 1.
15. Click **OK**.
16. Click **Next**.
17. Continue to click **Next** until the final screen, which displays the **Apply** option and prompts you to show a card. Present an encrypted DESFire encoded card to the Aperio lock.
18. When successful, click **Close**.

# Protege GX Setup

Before you begin the programming specific to the Aperio integration, you should create all of the door records that will be controlled by Aperio locks in **Programming | Doors**.

## Configuring the Onboard Ethernet Port

The controller's ethernet port must be configured to connect to the Aperio IP hubs. This is done in the programming for the onboard reader expander.

1. Navigate to **Expanders | Reader expanders** and select the onboard reader.
2. Set the **Ethernet network type** to Third party generic.
3. Enter the **Ethernet port** which the controller will use to communicate with the Aperio hub. This should match the **ACU Settings** configured in the Aperio software (see page 9).
4. In the **Commands** section, enter the `AperioHubList` command. This command defines the Aperio hubs which this controller will communicate with. You can enter up to four hubs using the final 3 bytes of the MAC address noted earlier (see page 10), separated by commas.

   For example:

   `AperioHubList=0c369c,19f62c,221ab9,04c47b`
5. Click **Save**.

## Bringing IP Hubs Online

The system provides some debug events to indicate the status of the connection between the controller and each hub. To track the progress when bringing hubs online, enter the following command in the onboard reader expander programming:

`EnableDebugEvent = true`

Then right click on the reader expander record and click **Update module**. This will initiate the process of bringing the hubs online. Make sure that the hubs are powered up and connected to the local ethernet network.

As each hub comes online, you should see system debug events similar to the following:

```
System Debug Event 000 Sub 0 Data 0A69:0000:0000:0000
```

The onboard reader expander is connecting to an Aperio hub. The Event ID is **0A69**.

```
System Debug Event 000 Sub 0 Data 0A6A:0022:001A:00B9
```

The Aperio hub is online with the onboard reader expander. The Event ID is **0A6A** and the final three segments include the final three bytes of the hub's MAC address (in this case **22 1A B9**).

If a hub goes offline (for example, if it loses power), you will see the following debug event:

```
System Debug Event 000 Sub 0 Data 0A70:0022:001A:00B9
```

The Aperio hub is offline with the onboard reader expander. The Event ID is **0A70** and the final three segments include the final three bytes of the hub's MAC address (in this case **22 1A B9**).

After you have confirmed that all hubs have come online, it is recommended to remove the `EnableDebugEvent = true` command to prevent unnecessary events. Right click on the reader expander record and click **Update module**.

# Adding the Aperio Locks as Smart Readers

Each Aperio lock is represented by a smart reader record associated with the controller's ethernet port.

1. Navigate to **Expanders | Smart readers**.
2. Click **Add**.
3. Enter a **Name** for the lock.
4. Set the **Expander address** to that of the onboard reader (in most cases this will be 1).
5. Set the **Expander port** to Ethernet.
6. Enter the **Configured address** of the lock. This can be any unique address.
7. Expand the **Commands** section and enter the `AperioIPDeviceID` to specify the lock. Each lock is represented by the final three bytes of the its MAC address (see page 10).
   For example:
   `AperioIPDeviceID=040f9d`
8. Select the **Reader** tab.
9. Set the **Reader one location** to Entry or Exit.
10. Select the **Reader one door** that this lock will control.
11. Various options can also be enabled from the **Misc options** section.
    - When the **Disarm area for door on access** option is enabled, unlocking the door will disarm the defined **Inside area** if the lock is used for entry and the **Outside area** if the lock is used for exit. When this option is disabled the lock will not perform any disarm functions.
    - When the **Allow access when area armed** option is enabled, a user can gain access through the door even when the inside area is armed. When disabled, a user will be denied access through the door if they do not have permission to disarm the **Inside/Outside area**.
    - When the **Log reader events** option is enabled, events associated with the lock will be logged.
    - When the **Display card detail when invalid** option is enabled, full card data will be displayed when a user attempts to unlock the lock with an invalid card.
12. Click **Save**.

## Changing the Credential Format

If you are using Sector 13 MIFARE Classic, ICT encrypted DESFire or a custom credential type with this integration, some additional configuration is required for the smart reader.

1. In **Expanders | Smart readers**, select the relevant Aperio lock.
2. In the **General** tab, temporarily set the **Expander port** to Port 1.
3. In the **Reader** tab, set the **Reader one format**:
   - For Sector 13 MIFARE Classic or ICT encrypted DESFire, set this to HID 26/34 bit.
   - For custom credential types, set this to Custom credential.
4. Return to the **General** tab and set the **Expander port** back to Ethernet.
5. Click **Save**.

With this configuration, the door will use the custom credential types programmed in the door type as normal.

For more information on using custom credential types, see Application Note 276: Configuring Credential Types in Protege GX.

## Using Cards with Reverse Byte Order

This feature is available in controller firmware version **2.08.1329 or higher**.

Although Aperio locks do not support reading card sector data with a reverse byte order format, you can configure the controller to handle these cards correctly. Enter the following command in the **Commands** field of the smart reader programming for each Aperio lock:

```
ReverseByteOrder = true
```

This would typically be used with card serial number (CSN) or custom sector reading and will not work with standard ICT programmed cards.

# Adding the Trouble Inputs

The following table shows the trouble inputs that are available for Aperio doors. You must program these manually in **Programming | Trouble inputs**.

| Trouble Input Address | Name | Description |
|---|---|---|
| 1 | Door Forced | The Aperio lock has been forced open. |
| 2 | Door Left Open | The Aperio lock has been left open for the **Door left open alarm time**. |
| 4 | Battery Low | The Aperio lock has a low battery. |
| 6 | Door Offline | The Aperio lock is offline. |
| 9 | Battery Critical | The Aperio lock has a critically low or flat battery. |
| 10 | Privacy Mode | A user has activated privacy mode on the Aperio lock. |

To add trouble inputs for Aperio doors:

1. Navigate to **Programming | Trouble inputs**.
2. Give the trouble input a relevant name, such as Aperio Lock 1 Tamper.
3. Set the address of the trouble input:
   - **Module type**: Door (DR)
   - **Module address**: The door record this trouble input is monitoring.
   - **Module input**: The relevant Trouble Input Address from the table above.
4. In the **Areas and input types** tab, assign the trouble input to a system area and input type for trouble monitoring.
5. Click **Save**.

# Programming AES Encrypted Card Operation in Protege

This section is specific to integrations requiring encrypted cards for sites using both Aperio wireless locks and ICT proximity readers and/or cards.

The AES encryption key required for sector 13 MIFARE Classic programming or ICT encrypted DESFire programming is supplied by ICT. Please contact the ICT support team to obtain your encryption key.

## Programming Encrypted Aperio Cards

Programming sector 13 MIFARE and ICT encrypted DESFire on Aperio encoded cards is achieved using the ICT Encoder Client. For information on the steps required, refer to the ICT Encoder Client User Manual, or contact the ICT support team for assistance.

## Programming the Encryption Key for all Aperio Locks on a Controller

If you require the AES encryption key to apply to all devices connected to the controller, you need to enter the key into the **Custom reader format** section of the controller programming.

1. Navigate to **Sites | Controllers** and select the controller used for this integration.
2. Select the **Custom reader format** tab.
3. In the **Card data options** section, enter the **Card data AES encryption key** supplied by ICT.
4. Click **Save**.

## Programming the Encryption Key for Individual Aperio Locks

If you require the AES encryption key to apply only to specific Aperio wireless locks, you need to enter the key into the **Custom reader format** section of the corresponding smart reader record programming.

1. Navigate to the **Expanders | Smart readers** and select the lock's smart reader record.
2. Select the **Reader** tab.
3. Ensure that the **Reader format** is set to HID 26/34 bit.
4. In the **Card data options** section, enter the **Card data AES encryption key** supplied by ICT.
   - The **Read non ICT programmed sector data** option enables the reading of card sector data not programmed by ICT, but means that the reader / lock will no longer read ICT programmed sector data.

     Do not enable this option if you require the reader / lock to read ICT programmed sector data and additional sector data.
5. Click **Save**.

# Appendix: Validated Features

This appendix outlines which features of the Protege GX and Aperio systems have been validated to function correctly with this integration.

## Supported Protege GX Door Options

The following door options have been validated by ICT.

| Option | Supported? | Notes |
|---|---|---|
| Manual controls | ✓ | |
| **Doors \| General** | | |
| Door type | ✓ | Some door type options are not supported (see page 18). |
| Slave door | ✓ | Supported only when a hardwired door is used as the slave. |
| Area inside door | ✓ | |
| Area outside door | ✓ | |
| Unlock schedule | ✓ | |
| Door pre-alarm delay time | ✓ | |
| Door left open alarm time | ✓ | |
| Interlock door group | ✗ | |
| **Doors \| Outputs** | | |
| Lock output / output group | ✓ | |
| Lock activation time | ✓ | |
| Enable additional lock outputs | ✗ | |
| Pre alarm output / output group | ✓ | |
| Pre alarm pulse on/off time | ✓ | |
| Left open alarm output / output group | ✓ | |
| Left open alarm pulse on/off time | ✓ | |
| Forced open output / output group | ✓ | |
| Forced open pulse on/off time | ✓ | |
| **Doors \| Function outputs** | | |
| Function 1-3 output / output group | ✗ | |

| Option | Supported? | Notes |
|---|---|---|
| **Doors \| Options** | | |
| Always check unlock schedule | ✗ | |
| Enable open/close events on schedule | ✗ | |
| Relock on door close | ✗ | |
| Relock on door open | ✗ | |
| Unlock door on REX | ✗ | |
| Unlock door on REN | ✗ | |
| Schedule operates late to open | ✓ | |
| Door lock follows inside area | ✓ | |
| Door lock follows outside area | ✓ | |
| Prevent slave unlock on inside area | ✗ | |
| Prevent unlock on schedule if inside area armed | ✓ | |
| Prevent unlock on schedule if outside area armed | ✓ | |
| Area disarmed and schedule valid unlock door | ✓ | |
| Area disarmed or schedule valid unlock door | ✓ | |
| Enable access taken on REX/REN events | ✗ | |
| Schedule overrides latch | ✗ | |
| **Doors \| Advanced options** | | |
| Update user area when passback disabled | ✗ | |
| Lock out REX when inside area armed | ✗ | |
| Deny entry if inside area is armed | ✓ | |
| Deny exit if outside area is armed | ✓ | |
| Prompt user for access reason code | ✗ | |
| Enable access taken on door unlock events | ✓ | |
| Door extended access time | ✗ | |
| Antipassback entry/exit user reset time | ✗ | |

| Option | Supported? | Notes |
|---|---|---|
| Reset antipassback status on schedule | ✗ | |
| Enable timed user antipassback reset | ✗ | |
| Antipassback reset schedule | ✗ | |
| **Doors \| Alarm options** | | |
| Enable pre-alarm alarms | ✓ | |
| Disable during unlock schedule | ✗ | |
| Disable during manual commands | ✗ | |
| Disable during calendar actions | ✗ | |
| Disable whilst unlocked by area | ✗ | |
| Disable whilst unlocked by programmable function | ✗ | |
| Disable whilst unlocked by fire drop | ✗ | |
| Alarm operating schedule | ✗ | |
| Enable left open alarms | ✓ | |
| Disable during unlock schedule | ✗ | |
| Disable during manual commands | ✗ | |
| Disable during calendar actions | ✗ | |
| Disable whilst unlocked by area | ✗ | |
| Disable whilst unlocked by programmable function | ✗ | |
| Disable whilst unlocked by fire drop | ✗ | |
| Alarm operating schedule | ✗ | |
| Enable forced open alarms | ✓ | |
| Alarm operating schedule | ✗ | |

# Supported Protege GX Door Type Options

The following door type options have been validated by ICT.

| Option | Supported? | Notes |
|---|---|---|
| **Door types \| General** | | |

| Option | Supported? | Notes |
|---|---|---|
| Operating schedule | ✓ | |
| Secondary door type | ✓ | |
| Fallback door type | ✗ | |
| Access level door type | ✗ | |
| Entry/Exit passback is qualified with door opening | ✗ | |
| Entry/Exit passback mode | ✓ | |
| Entry/Exit reading mode | ✓ | Can be set to Card only, PIN only or Card and PIN depending on the lock type. The Custom option may be used to allow support for custom credential types (see page 13). |
| Door entry/exit requires verification | ✗ | |
| **Door types \| Options** | | |
| Door REX not allowed | ✗ | |
| Door REN not allowed | ✗ | |
| Requires dual authentication | ✓ | The following commands are available in **Expanders \| Reader expanders** to configure the dual authentication operation for the controller's onboard ethernet port:<br>• `DualAuthOutputEth = X`<br>Sets the output that will be activated when the first user enters their credentials at the door, where **X** is the output's Database ID.<br>• `DualAuthTimeEth = Y`<br>Sets the time that the door will wait for a second credential, where **Y** is the time in seconds. |
| Dual card provider can initiate access | ✓ | |

# Supported Protege GX Smart Reader Options

| Option | Supported? | Notes |
|---|---|---|
| **Smart readers \| Reader** | | |
| Disarm area for door on access | ✓ | |
| Allow access when area armed | ✓ | |
| Disarm users area on valid card | ✗ | |
| Log reader events | ✓ | |

| Option | Supported? | Notes |
|---|---|---|
| Activate access level output | ✗ | |
| Display card detail when invalid | ✓ | |
| Always allow REX | ✗ | |
| Recycle REX time | ✗ | |

# Supported Protege GX User Access Restrictions

ICT has validated that the following features can be used to deny access to a user at an Aperio lock.

- User disabled
- User record expired
- PIN expired
- Access level expired
- Access level schedule not valid (in **Users | Users | Access levels**)
- Access level schedule not valid (in **Users | Access levels | General**)
- Access level usage restriction
- Hard antipassback
- Inside/Outside area armed
- Maximum user count in area

# Validated Card Formats

The following card formats have been confirmed to function correctly with this integration. Other card formats may be functional, but have not yet been validated by ICT.

- ICT encrypted DESFire
- MIFARE Classic (UID only)
- MIFARE Classic (with sector data)

# Supported Aperio Door Features

**Privacy Mode**

When the inside push button is pressed on a compatible Aperio device, privacy mode will be initiated. The lock will deny user access until privacy mode has been released by a REX (turning the inside handle) or by a user with super user rights. An event will be generated in the event log each time privacy mode is activated or deactivated.

In addition, a door trouble input can be used to indicate when a door has entered privacy mode and report it to a monitoring station. This is programmed as trouble input address 10 on the relevant door record.

# Known Issues

**Aperio Door Features**

- No REX event is generated when the inside handle is turned, even when the lock supports REX.
  ASSA ABLOY has confirmed that this is caused by a known issue in the Aperio IP hub. This applies to the following hub firmware versions tested by ICT:

- Gen 5 hubs: 1.1.0
- Gen 3 hubs: 1.10.3476

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.
Copyright © Integrated Control Technology Limited 2003-2026. All rights reserved.

**Disclaimer:** Whilst every effort has been made to ensure accuracy in the representation of this product, neither Integrated Control Technology Ltd nor its employees shall be liable under any circumstances to any party in respect of decisions or actions they may make as a result of using this information. In accordance with the ICT policy of enhanced development, design and specifications are subject to change without notice.