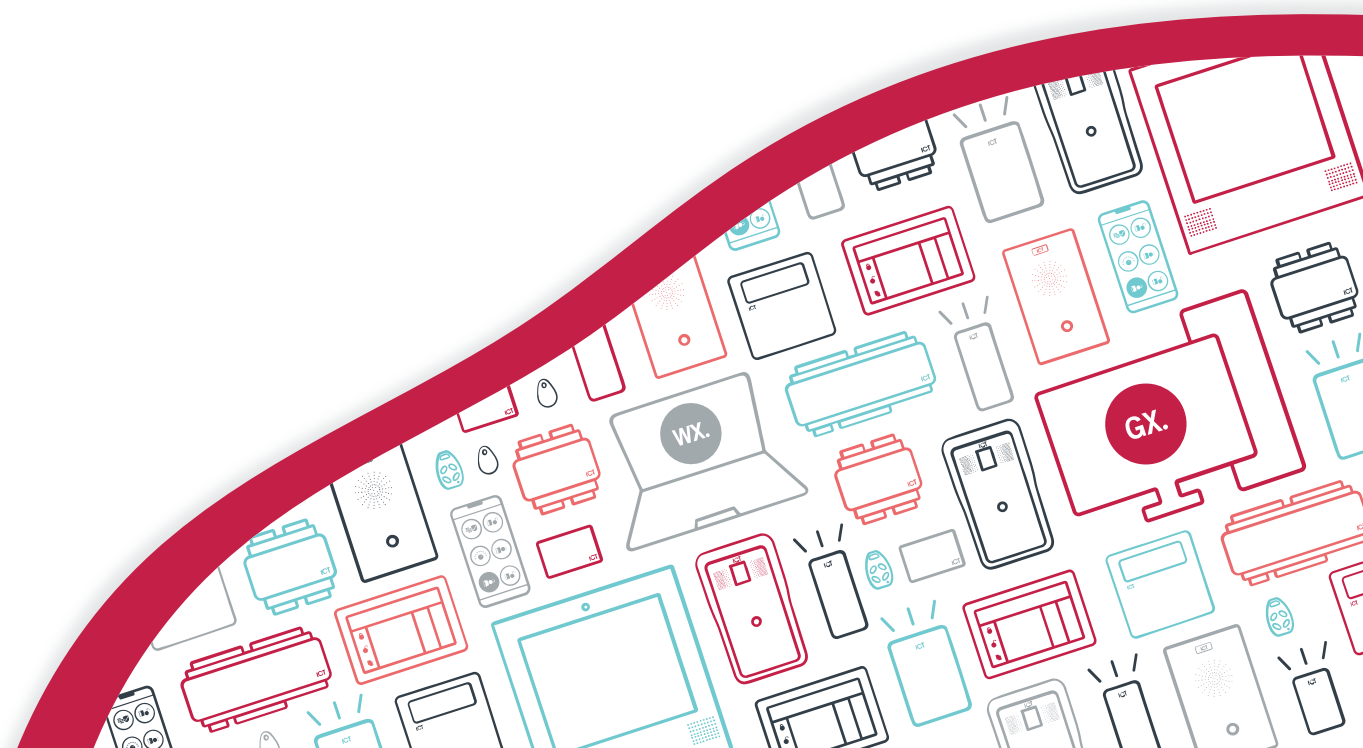
AN-155

Protege WX Aperio RS-485 Hub Integration

Application Note



Last Published: 28-Mar-23 02:52 PM

Contents

Introduction

Aperio integration is a licensed feature that enables you to use Aperio wireless locking devices within the Protege WX system. Aperio locks wirelessly communicate with Aperio communication hubs which are connected via RS-485 to a Protege WX controller. Both the standard Protege WX controller and the single door controller support communication with Aperio communication hubs.

This integration supports sector 13 encrypted MIFARE and DESFire cards, allowing it to be used on sites with a combination of ICT and Aperio card readers.

This document only covers the programming that is relevant to integration with Protege WX. For further information on Aperio configuration, refer to the Aperio installation manual.

Prerequisites

Protege WX Components

Component	Version	Notes
Protege WX Controller	2.10.030 or higher	Only controllers with RS-485 functionality on the reader ports support this integration. Older controllers may not have RS-485 reader ports. The following features require later firmware versions: • Sector 13 MIFARE Classic card configuration is available in version 4.00.274 or higher. • ICT encrypted DESFire card configuration is available in version 4.00.469 or higher. • Deadbolt operation is available in version 4.00.409 or higher. Protege WX advanced mode must also be activated. • Inside handle REX and privacy mode on IN100 locks is available in version 4.00.420 or higher.

Important:

Connection via RS-485 is only supported with hardware revisions of controllers that are equipped with the added RS-485 reader functionality on the reader ports. This is easily determined by checking the reader ports on the front panel of the controller. Hardware revisions that are equipped with RS-485 reader functionality have the NA and NB labels beneath the D0 and D1 labels, as shown below.

Earlier revisions of the controller hardware that do not have the NA and NB labels (as in the example below) do not have the added RS-485 reader functionality.

All one door controllers come equipped with RS-485 reader functionality.

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	• 15.1.32798 • 17.0.33829 • 19.0.29 • 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 (APRD1/PAP1)	-	
AH30 Wireless Hub (Gen 3)	Flavor: • RS485 • Multiple Lock [Aperio Protocol] Version: • 6.6.32718 • 6.7.34105 AA Code: 0	Note that Gen 5 hubs have different configuration requirements than older hubs.
AH30 Wireless Hub (Gen 5)	Flavor: • RS485 • Multiple Lock [Aperio Protocol] Flavor: • 1.0.2 AA Code: 0	

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	Radio Version
AU100 V3	Flavor: N/A Version: • 3.4.10720 • 3.14.70 AA Code: 0	Flavor: N/A Version: • 3.4.10720 • 3.14.70 AA Code: 0
IN100 V3	Flavor: N/A Version: • 3.8.56 AA Code: 0	Flavor: N/A Version: • 3.8.56 AA Code: 0

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
Aperio Door License	PRT-WX-LIC-AP-1	1 license per Aperio lock connected to the Protege WX system. Available as single licenses, or in bundles of 10.
	PRT-WX-LIC-AP-10	

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.

Aperio Hardware Installation

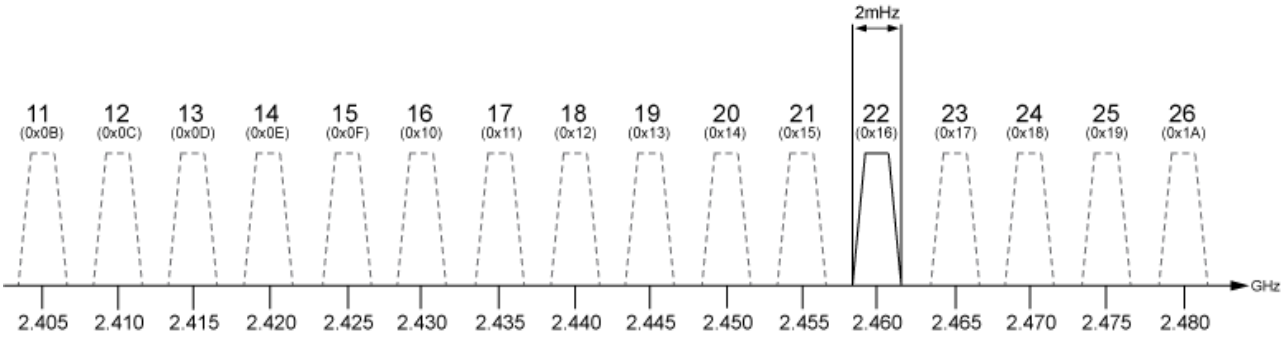
Aperio Hardware Installation and RF Channels

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

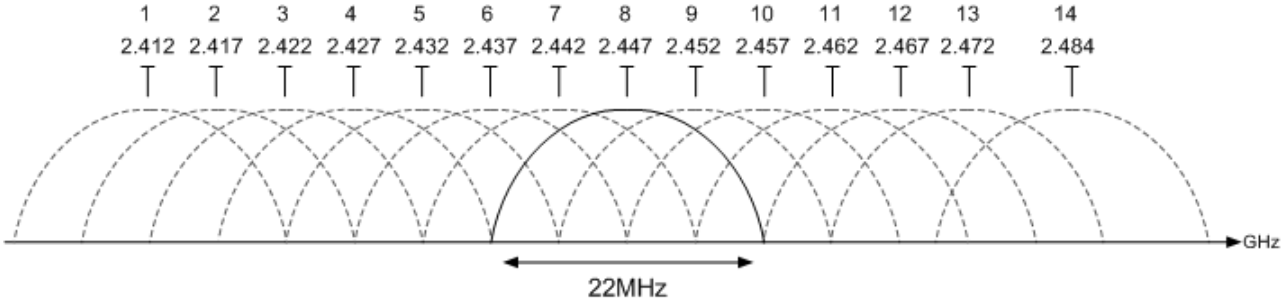
It is important to identify any devices that could affect the operation of your Aperio system. It is advised that any device operating on the 2.4GHz band be kept at least 3.5m (11.5ft) from the communication hub and lock.

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.

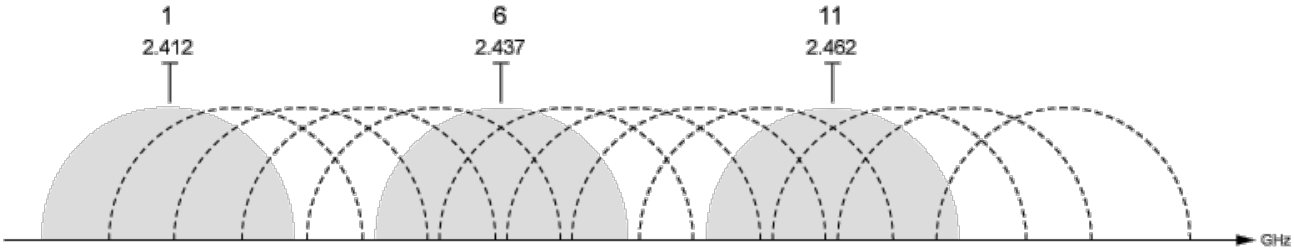
Aperio wireless locks use a communication protocol based on the IEEE 802.15.4 standard with 16 separate channels that occupy 2MHz of bandwidth from 2405MHz to 2480MHz. An RF site survey can determine which of the 16 channels the Aperio network should use.



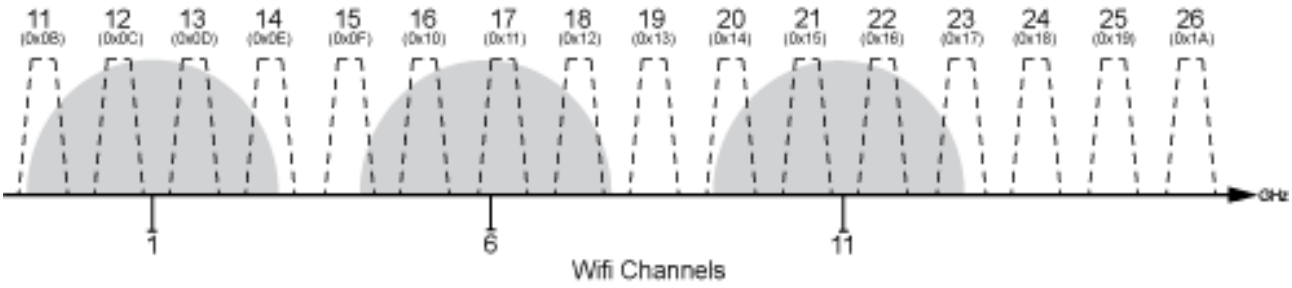
As an example, we can look at how Wi-Fi can affect the operation of Aperio when it is operating on the same 2.4GHz band. Wi-Fi generally operates on a standard of the IEEE 802.11 communication protocol divided into 14 channels, each occupying 22MHz of bandwidth from 2412MHz to 2484MHz.



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.

Wiring an Aperio Communication Hub to a Controller

In order to facilitate communications between the Protege system and the Aperio wireless locks, you need to wire an Aperio communication hub to a Protege controller.

This integration uses the AH30 1-to-8 standard Aperio RS-485 communication hub. Below are some key points to consider when connecting the hubs:

- You can pair up to eight locks with each AH30 hub prior to Gen 5, and up to 16 locks with each Gen 5 hub.
- You can connect a maximum of fifteen hubs to a single reader port on the controller.
- Each AH30 hub draws 250mA.
- Each DC output (auxiliary) on the controller is rated at 0.7A (typical) with electronic shutdown at 1.1A – this enables you to power up to four AH30 hubs on each of the two DC outputs on the controller.

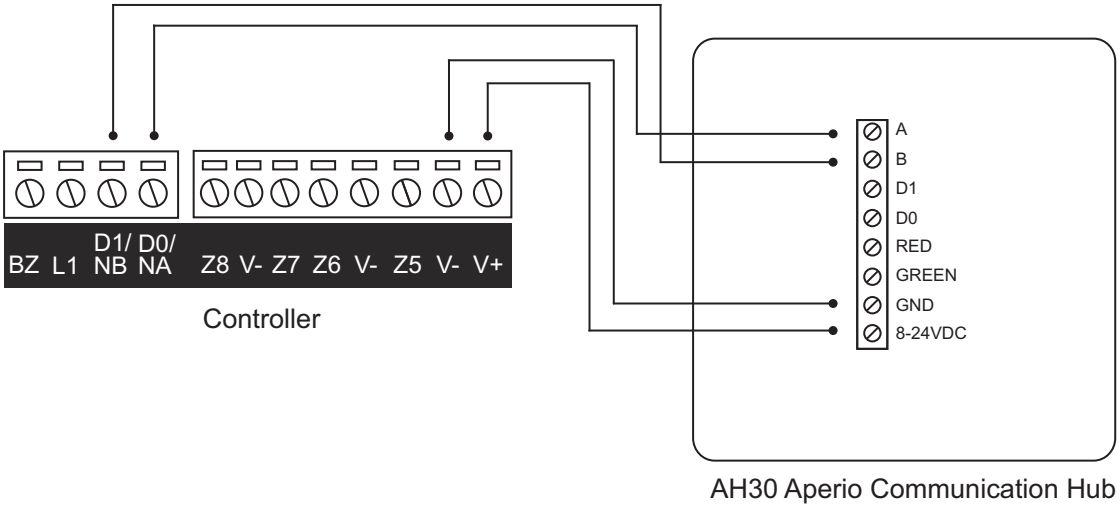
  If you need to connect more hubs, you must use an external power supply to power the hubs separately from the controller.

- Each controller supports a maximum of 120 locks. This limitation applies even if Gen 5 hubs are used.

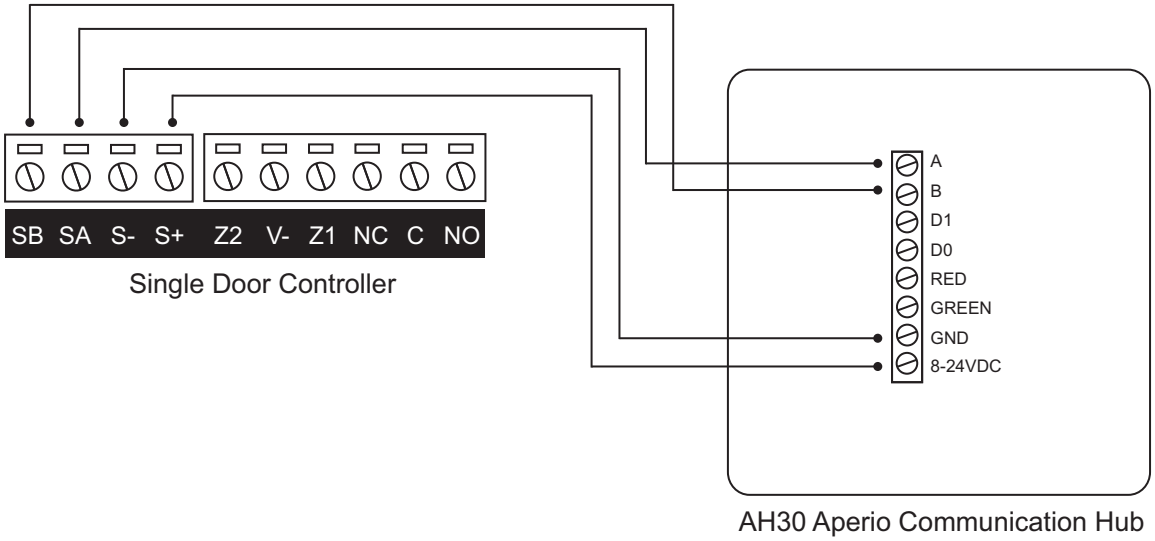
Connecting the Aperio Hubs

This integration uses the onboard RS-485 reader ports of the controller to provide the Aperio communication hub with a network connection and a power supply. The Aperio communication hub is compatible with both the standard and single door controllers as they are both equipped with onboard RS-485 enabled reader ports.

Controller to Aperio Communication Hub:



Single Door Controller to Aperio Communication Hub:



DIP Switch Configuration

The dip switches on the back of each Aperio hub must be used to set the hub's address, control the use of the resistors, and configure the antenna. Use of the dip switches differs between AH30 hub models. For information on the hardware configuration of hubs, see the Aperio AH20-AH30 Mounting Instructions available from ASSA ABLOY.

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**.

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

Configuration for Aperio RS-485 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 **Electronic Access Controller Settings**.
3. In the **EAC Addressing Mode** section, ensure that the hub is configured for Normal address offset.

   This is the default EAC addressing mode, in which the communication hub assigns the EAC address to the paired locks according to the address table within the Aperio Online Mechanical Installation manual. The legacy Address Offset mode is **not** supported in this integration.
4. Next, you must configure the **UID Reverse Byte Order** settings. Depending on your software version, these may be configured under the **EAC Credential 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

5. Under the **EAC Credential Settings** (if available), disable all **MIFARE AADP RS-485 Message Selection** settings.
6. Complete the remaining configuration wizard steps to push the changes to the hub.
7. Repeat this process for any hub to be used for the integration.

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.

Identifying the Lock's EAC Address

In order to use Aperio locks with Protege, you need to identify the lock's EAC address. The EAC address corresponds to the lock's **Configured address** in Protege and you will need to identify the EAC Address of all locks to be used in the integration.

The lock's EAC address is located under the EAC address column of the **Installation window**.

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 WX Setup

In order to control the Aperio wireless locks from within Protege WX, you need to configure the controller's onboard reader for use with an Aperio communication hub and add the wireless locks as Smart Readers.

Configuring the Onboard Reader Port

1. Navigate to **Expanders | Reader expanders** and select the onboard reader.
2. Set the **Port network type** to Aperio for the port that the Aperio communication hub is wired to.
3. Click **Save**.

Adding the Aperio Locks as Smart Readers

1. Navigate to **Expanders | Smart readers** and click **Add**.
2. Enter a **Name** for the lock.
3. Set the **Expander address** to that of the onboard reader (in most cases this will be 1).
4. Set the **Expander port** that the hub is wired to.
5. Enter the **Configured address** of the lock.

   This is the EAC address assigned in the Aperio Programming Application (see page 12).
6. Select the **Reader** tab.
7. Set the **Reader location** to Entry or Exit.
8. Select the door that you want the lock to be associated with.
9. 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 **Area inside door** if the lock is used for entry and the **Area outside door** 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.
10. Click **Save**.

Using Cards with Reverse Byte Order

This feature is available in Protege WX version **4.00.1306 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.

Aperio Locks with Deadbolts

If an Aperio lock is fitted with a deadbolt mechanism, the position of the deadbolt can be used when determining access to a door when the deadbolt is engaged.

In Protege WX controller firmware version 4.00.409 or higher, users are able to specify when an Aperio lock is fitted with a physical deadbolt.

1. Navigate to **Programming | Doors** and select the door controlled by the Aperio lock.
2. In the **Commands** section enter `HasAperioDeadbolt = true`.
3. Click **Save**.

Adding the Trouble Inputs

The following table shows the trouble inputs that are available for Aperio doors. Trouble inputs 1 and 2 are generated automatically when the door record is created, but others must be programmed 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**.
3	Lock Tamper	The Aperio lock tamper switch has been triggered.
4	Battery Low	The Aperio lock has a low battery.
6	Door Offline	The Aperio lock is offline.
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**.

Trouble Inputs in Older Versions

In older versions, Aperio lock trouble conditions were monitored by the controller's onboard reader expander. These can still be used for backwards compatibility with older sites if the equivalent door trouble inputs have not been created. The linked trouble inputs are:

Trouble Input Address	Name	Description
5	Door Forced	One of the Aperio locks has a door forced condition. The reader log records which lock it is.
7	Door Left Open	One of the Aperio locks has been left open. The reader log records which lock it is.

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 Reader Port

If you are using the same AES encryption key for each lock connected to the same reader port, you can apply the key globally to the reader port. To do this you need to change the network type of the reader port, as this feature is not available when the reader is configured for Aperio integration.

1. Navigate to **Expanders | Reader expanders** and select the controller's onboard reader expander.
2. Change the required **Port network type** from Aperio to ICT RS485 and click **Save**.
3. Select the corresponding **Reader** tab.
4. In the **Card Data Options** section, enter the **Card data AES encryption key** supplied by ICT and click **Save**.
5. Select the **General** tab and change the **Port network type** back to Aperio.
6. 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**.

Supported Door Options

Once an Aperio lock has been configured within Protege WX, it can be programmed with many of the features of hardwired doors. This section outlines which options are supported for Aperio locks.

Notes

- Aperio locks with an integrated door sensor can provide up-to-date door state feedback to Protege WX.
- Only single-badging is supported by Aperio locks: double- or triple-badging to arm an area or activate an output is not possible.
- Areas can be linked to Aperio doors to enable a user with suitable access to disarm the area.

Door Options

The following door options have been validated by ICT.

Option	Supported?	Notes
Doors | General		
Door Type	✔	Can be set to Card only or PIN only depending on the lock type.
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	✔	
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 | Options		

Option	Supported?	Notes
Always Check Unlock Schedule	✗	
Enable Open/Close Event 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	✓	Unlock schedules are not supported, but with this option enabled the lock will follow the state of the inside/outside area.
Enable Access Taken On REX/REN Events	✗	
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	✗	
Reset Antipassback Status On Schedule	✗	
Enable Timed User Antipassback Reset	✗	

Option	Supported?	Notes
Antipassback Reset Schedule	✗	
Doors | Alarm options		
Enable Pre-Alarm Alarms	✓	
Disable During Unlock Schedule	✗	
Disable During Manual Commands	✗	
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 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	✗	

Aperio Door Features

The following special features of Aperio doors are available in the Protege WX integration.

These features require Protege WX version 4.00.420 or higher.

Inside Handle REX

When the inside handle of an Aperio lock is turned, a REX (request to exit) event will be generated for that door.

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.

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