ASSA ABLOY

Aperio⁽ Online Programming Application Manua

Document No: ST-001321-C, Issue date: 8 October 2013



The global leader in door opening solutions

Table of Contents

1	Introduction	3
	Purpose	3
	Scope	3
	Applicable Products	3
	Aperio support in the EAC system	3
	Abbreviations and Definitions	3

2 System Overview4

The Aperio system	4
The Aperio programming application	4
Regulatory and security information	4
Communication hub versions and FAC	
interface	4

3 The Programming Application

E .
-

About the Programming Application	5
Main view	5
Status bar	5
User settings	6
Software version	6
USB radio indication	7
Installation View overview	7

4 Programming Application Functions 9

Opening/creating installations9
Scanning and adding communication hubs 9
Pairing locks/sensors with
communication hub10
Configure function - Wizard 12
RFID configuration (Lock/sensor)12
Advanced settings - Keypad configuration (Lock)24
Override credential (Lock)25
Security Mode Settings (Communication hub
and Lock/sensor)
RS-485 settings (Communication hub)
Advanced setting - Radio channel settings
(Communication hub or Lock/sensor)
Advanced Lock/sensor Settings
Applying a stored configuration to a
communication hub/lock/sensor
Get Event Log
Get Audit Trail
Retrieve system information

Change EAC address	45
Changing the Security Mode	46
Changing the radio channels	48
Setting the time of a lock	51
Change IP address (Communication	
hub AH40)	53
Importing and exporting configurations	54
Upgrade of communication hub/lock/	
sensor firmware	56

5 Installation of Programming Application and Drivers61

6 Regulatory Information Regarding the Aperio USB Radio Dongle64

Compliance	64
According to FCC15.247	64
According to FCC15.105 (b) Information	
to the user	64
Security Statement	64

byt alla aperio till aperio med R

-symbolö

Purpose

The main purpose of this manual is to provide information for installation and configuration of Aperio Online based products using the Aperio Online Programming Application.

The manual is intended for installation personnel, project managers and people with similar responsibilities.

Scope

This manual includes a complete description of all functionality and settings in the Aperio Online Programming Application.

For quick installation instructions of a standard Aperio online system including communication hubs and locks/sensors. refer to ref [2], Aperio Online Quick Installation Guide.

This manual is applicable to version 2.6.4 of the Aperio Online Programming Application.

Abbreviations and Definitions

Abbreviation Definition EAC Electronic Access Control. The system controlling access decisions. DIP Dual in-line Package. A manual electric switch used for settings on the communcation hub. RFID Radio Frequency Identification. The credential technology used. ACU Access Control Unit. The device within the EAC system that communicates with the communication hub TLS Transport Layer Security. Cryptographic protocol that provides secure communication over TCP/IP connections

References

[1]	ST-001323-Aperio Online Mechanical Installation Manual
[2]	ST-001322-Aperio Online Quick Installation Guide

Applicable Products

This manual can be used for all versions of communication hubs.

Aperio support in the EAC system

Note that the Aperio support may vary depending on the Aperio communication hub used and the level of integration. Please contact your OEM for details.

2 System Overview





The Aperio system

The Aperio system is used in the following way: The user holds an RFID card in front of the lock. The lock sends card credentials wirelessly to the communication hub and the communication hub (wired through RS-485, Ethernet or Wiegand) then communicates with an EAC (Electronic Access Control) system. The EAC system then makes the access decision. The decision is sent via the communication hub to the lock and access is granted or denied.

The Aperio programming application

The Programming Application is used for the configuration of a door installation. It is installed on a laptop. The laptop has an Aperio USB radio device connected to one of its USB ports. The USB radio device enables the application to connect via a communication hub to the door lock. The lock communicates via the communication hub either with the EAC or with the Programming Application. Read more in the Aperio Online Programming Application Manual.

Regulatory and security information

See section "6 Regulatory Information Regarding the Aperio USB Radio Dongle" on page 64.

Communication hub versions and EAC interface

There are four communication hub types according to the table below:

Version	Interface	Maximum number of locks/sensors
AH15	Wiegand/RS 485*	1
AH20	Wiegand	1
AH30	RS-485	8
AH40	IP (Ethernet)	8

*) The firmware type loaded into the communication hub controls what interface is enabled.

About the Programming Application

- Software running under 32-bit or 64-bit versions of Windows 7, Windows 8, Vista or XP.
- · Java Runtime Environment bundled with Aperio Programming Application.
- Multi-language installation management tool.
- · Encrypted installation database.

Refer to section "5 Installation of Programming Application and Drivers" on page 61 for installation and upgrade from earlier versions.

Main view

The main view of the Programming Application consists of three areas:

- Menu bar
- · View area
- Status bar



Status bar

The status bar contains the following information:

- USB Radio indication
- Date label

S USB Radio (COM 10)	May 14, 2013 3:43:55 PM

User settings

The User Settings (on the Settings menu) contains settings that are applicable to all installations:

🐵 User Settings 🛛 🔀
Language Settings Select the application language. You will have to restart Aperio [®] Programming Application. Application Language English
Serial Port Settings Select how the USB Radio device shall be detected. Image: Automatically detect USB radio at startup USB Radio Port Communication port 3 * Refresh port list
Advanced Settings Enable advanced device configuration in the configuration wizard. If advanced device configuration is enabled it is possible to change radio channels and perform advanced lock and sensor configurations. If solve advanced settings
Log Level Settings Log level TRACE This feature should be used only for support purposes.
OK Cancel

- Language settings: Select the language used by the Programming Application.
- Serial port settings: Automatically detects USB radio at start up: Uncheck this option to manually specify the port used by the USB Radio Dongle, in case of hardware conflict.
- **Advanced settings:** Check this box if you need to perform advanced hub and lock configurations: keypad configuration, advanced settings (changing the radio channel) and advanced lock settings.
- **Log Level Settings:** Used for trouble shooting purposes. Contact your Aperio supplier for more information.

Software version

To check the version of installed software, select About Aperio Programming Application on the Help menu:



USB radio indication

USB Radio together with a green check mark indicates that the serial port used is ok and the radio device is ready to transmit data.

SB Radio (COM 18)

USB Radio together with a red dot indicates that the serial port or the USB radio device is not ok.

😵 USB Radio

Installation View overview

The installation view is the main window when working with door installations. This window is automatically displayed after logging in to an installation and after the scanning process.

Aperio Programm	ning Application - [New_installa	ition]				
Lock/sensor	Communication Hub	EAC Address	UHF Link		Communication Hub [0216E1]	
011C43	0216F1	1		8		
013542	024521	1		80	MAC Address	00:17:7a:01:02:02:16:f1
0148E8	024521	2		80	Firmware Flavor	RS485 [Aperio protocol]
0148ED	024521	3		8	Firmware Version	6.0.22795
					Bootloader Version	1.2.5
					Radio protocol version	23
					Channel	19 (2.445 GHz)
					Radio channels	14, 19, 25
					PAN ID	16F1
					EAC addressing mode	Normal address offset
					DIP switch value	1
					EAC Address	[DIP Switch]
					Number of paired locks and sensors	: 1
					Device Status	EAC offline
					Lock/sensor [011C43]	
					MAC Address	00:17:7a:01:02:01:1c:43
					Assigned Address	0x115e
					EAC Address	1
					Radio protocol version	23
					Device Status	Lock/sensor offline
SB Radio (COM 1	10)					May 14, 2013 3:48:55 PM

The following information is shown:

- **Lock/sensor:** Indicates if there is a lock/sensor paired with the communication hub. If there is a paired lock/sensor the MAC address of the lock/sensor is shown.
- **Communication hub:** The MAC address of the communication hub.
- EAC Address: Shows the EAC address for the lock paired with this communication hub.
- **UHF Link:** Indicates the strength of the UHF wireless link (through the USB Radio device) between the communication hub and the Aperio Programming Application.

Green: Good Yellow: OK

Red: Not OK (firmware upgrade not allowed)

• **Security Mode:** Indicates the security mode of the communication hub. During final installation all locks and hubs must be changed from Manufacturer mode to Customer mode.

8	Customer mode	Door is using secure radio communication with the customer encryption key.
ſ	Manufacturer mode	Door is using insecure radio communication with the default encryption key.

• **Warning indications:** The following warning levels are given. Hoover with the mouse to see more information.

0	For example: Security mode for communication hub is undefined.
Û	For example: The communication hub firmware (rfif) version is older than Aperio Programming Application.
<u> </u>	For example: The communication hub is not paired with any lock.
8	For example: The security modes in communication hub and lock are not equal and should be changed, see section "Change EAC address" on page 45.

• Detailed information of selected hub and lock/sensor is shown on the right side of the window.

Right clicking a communication hub or lock/sensor will give access to the functions available in the Programming Application. See section "4 Programming Application Functions" on page 9 for an overview of all functions.

@ Aperio Program File Scan Settings	ming Application - [New_installatic Help	in]					_ • •
Lock/sensor	Communication Hub	EAC	Address	UHF Link	1	Communication Hub [0216F1]	
011C43	Apply configuration Configure Lock/sensor [011C43] Communication Hub [0216F1] Upgrade Firmware		1 Pair with I Retrieve sy Change ra Change pi Switch to	ock or sensor ystem information AC Address hysical location name. Customer Mode		MAC Address Firmware Flavor Firmware Version Bootloader Version Radio protocol version Channel Radio channels PAN ID EAC addressing mode DIP switch value EAC Address Number of paired locks and sensors Device Status Lock/sensor [011C43] MAC Address Radio protocol version Radio protocol version	00:17:7a:01:02:02:16:11 R5485 [Aperio protocol] 6.0.22795 1.2.5 23 19 (2.445 GHz) 14, 19, 25 16F1 Normal address offset 1 [DIP Switch] 1 EAC offline 00:17:7a:01:02:01:1c:43 0x117c 1 [Unknown]
Signal CON USB Radio (CON	110)						May 14, 2013 5:02:11 PM

Opening/creating installations

An installation is a password protected set of settings you need when you want to communicate with a hub and/or a lock. An installation is linked to an encryption file that is needed in order for the communication to work. (The encryption key file is provided by your local ASSA ABLOY company.)

• Select File - New or Open.



Scanning and adding communication hubs

1) After opening an installation the scanning process starts automatically. To manually scan for communication hubs, select *Scan* - *Quick Scan* (F7). (If your communication hub is not found on the default channels, retry and select *Scan* (*Ctrl+F7*), which searches on all channels.)

ĺ	🤕 Aperi	io Programm	ning Applica	a	
	File Sca	n Settings	Help		
	Loc	Quick scar	n F7	😔 Scanning	×
	011	Scan	Ctrl+F7	Please wait	
	013	Refresh	F5	0%	

Result: All communication hubs within reach of the USB Radio device of your computer are displayed in the scan result table.

4			
Select the Communica Check the boxes for eac retrieve detailed informa To select all, click in the	tion Hub to retrieve detaile th Communication Hub and ation. checkbox in the title row, or	d information from 1 press "Show detail press Ctrl + "A" or C	s" to :trl + "+".
Communication Hub	Radio channels	UHF Link	
29E6	12, 16, 24		<u>a</u> .
1C3D	15, 20		6
2A51	13, 18, 23		ê 👘
16F1	14, 19, 25		6
0D36	11, 16, 25		0
92FC	11, 16, 25		ê 🕦
29E8	11, 16, 26		6
2A2D	12, 25		<u> </u>
29F5	15, 20		é i
2A80	15, 20		ê 🕕
9367	13, 23		ê 🗌
2A10	14, 19		é 🗌
4521	11, 16, 25		8
29EA	14, 21		e l
C20C	14, 21		£ ·
Dec	can Show details	Cancel	

2) Locate a communication hub by the last four characters of the communication hub MAC address (ex. 01CF) in the scan result table. The same characters should be on a label on the cover of the communication hub. Click *Rescan* if the communication hubs that you want to configure are not shown in the list.

3) Select the communication hub(s) that you want to include in your installation. Click *Show details* to view detailed information in the installation view.



Pairing locks/sensors with communication hub

AH30/AH40 version of the communication hub can be paired with a combination of up to 8 locks/ sensors. AH15/AH20 can manage one lock/sensor.

1) Right click and select Communication hub - Pair with lock or sensor.



2) The pairing process starts. Hold the credential at the lock, or engage the magnet for the sensor to pair the hardware with the communication hub.



3) When the lock has stopped blinking you can click *Done* to see the pairing result. **Result:** The result is displayed.

🕾 Pair with lock or sensor 🗾	3
Pairing result The result of the pairing request is presented below.	
Communication hub paired successfully to: 0148ED	-
, Close	כ

Configure function - Wizard

Open the configure function by right clicking a communication hub or lock/sensor and selecting *Configure*.



Depending on the hardware, different windows will appear in the wizard.



If more than one lock is paired to the communication hub the *Configure menu* is found on the *lock* and *sensor* sub-menus respectively.

The following sections describe each window in the wizard.

RFID configuration (Lock/sensor)

A corresponding firmware for the given RFID type must be installed on the locks/sensors. Click *Add/Change* to enter the settings for each credential type.

Configure Lock/sen	sor [013542]				×
RFID Configuration Note that current RF RFID type you want	ID configuration to configure from	is in the Ape n the tabs b	rio™lock are not elow.	displayed. (Select the
MIFARE Classic	MIFARE Plus	DESFire	Low frequency	Legic	
Changes to be sent:					
			Remove changes	Add/C	hange
			Back	Next	Cancel

iCLASS RFID format is also supported by the programming application. However, no settings are necessary.

MIFARE Classic UID (Default)



No settings are made to MIFARE Classic UID.

If you want to prevent MIFARE Classic from being read at all by the lock, uncheck Use MIFARE Classic RFID.

MIFARE Classic Sector

Select MIFARE Classic Sector in the RFID Card Type drop down list.

left Change MIFARE Classic co	onfiguration 🛛 💌
👿 Use MIFARE Classic RFID	
RFID Card Type MIFARE C	lassic Sector 👻
Sector	1
Start Address in Sector	5
Length to read in Sector	15
MIFARE Authentication Key	112233445566
Read Key	MIFARE Key A 👻
OK	Cancel

- **Start Address in Sector:** Parts of blocks within a sector can be used for credential data: 0 to 47 for 1K MIFARE Classic credentials. For 4K MIFARE Classic credential 0-47 (Start sector 0 to 31) and 0 239 (Start sector above 31)
- Length to read in Sector: Length of the credential data: 1 48 (Start sector above 31 cannot be used in the current release of the Programming Application).
- **MIFARE Authentication Key:** A 6 bytes long hexadecimal key is required to read the credential data: For example: 112233445566
- **Read Key:** Select the read key that the credential is configured to use for sector reading. The lock/ sensor will give access only for this key.



If key B is selected as sector data read key, make sure that the access bits on the credential prevent reading of key B. If key B is readable on the credential, key B cannot be used to read the credential data.

Example:

To read the user data shown in the figure below, 17 10 19 80, and use the Authentication Key 001122334455 together with MIFARE Key A.



The configuration should look like this:

le Change MIFARE Classic co	onfiguration 🛛 🔼
👿 Use MIFARE Classic RFID	
RFID Card Type MIFARE C	lassic Sector 👻
Sector	14
Start Address in Sector	17
Length to read in Sector	4
MIFARE Authentication Key	001122334455
Read Key	MIFARE Key A 👻
ОК	Cancel

MIFARE Plus UID

The Change MIFARE Plus configuration	×
	\odot
Use MIFARE Plus RFID	
RFID Card Type MIFARE Plus UID 👻	
No parameters available	
OK Cancel	

No settings are made to MIFARE Classic UID.

If you want to prevent MIFARE Plus UID from being read at all by the lock, uncheck Use MIFARE Plus RFID.

MIFARE Plus Sector

Select MIFARE Plus Sector in the RFID Card Type drop down list.

left Change MIFARE Plus conf	iguration	×
🕼 Use MIFARE Plus RFID		
RFID Card Type MIFARE P	us Sector 👻	
Sector	1	
Start Address in Sector	5	
Length to read in Sector	15	
MIFARE Authentication Key	00112233445566778899AABBCCDDEEFF	
Read Key	MIFARE Key A	•
	OK Cancel	

- **Start Address in Sector:** Parts of blocks within a sector can be used for credential data: 0 to 47 for 1K MIFARE Classic credentials. For 4K MIFARE Classic credentials 0-47 (Start sector 0 to 31) and 0 239 (Start sector above 31)
- Length to read in Sector: Length of the credential data: 1 48 (Start sector above 31 cannot be used in the current release of the Programming Application).
- **MIFARE Authentication Key:** A 16 bytes long hexadecimal key is required to read the credential data: For example: 00112233445566778899AABBCCDDEEFF
- **Read Key:** Select the read key that the credential is configured to use for sector reading. The lock will give access only for this key.



If key B is selected as sector data read key, make sure that the access bits on the credential prevent reading of key B. If key B is readable on the credential, key B cannot be used to read the credential data.

Example:

Since MIFARE Plus has the same memory organization as MIFARE Classic, we can use the same configuration. We will also use Key A but here the length of this key should be 16 bytes, in this particular case: 00112233445566778899AABBCCDDEEFF.

The configuration should look like this:

left Change MIFARE Plus conf	iguration	X
		$\textcircled{\textbf{0}}$
📝 Use MIFARE Plus RFID		
RFID Card Type MIFARE PI	us Sector 💌	
Sector	14	
Start Address in Sector	15	
Length to read in Sector	4	
MIFARE Authentication Key	00112233445566778899AABBCCDDEEFF	
Read Key	MIFARE Key A	•
	OK Cancel	

DESFire UID

🐵 Change DESFire configuration
Use DESFire RFID
RFID Card Type DESFire UID 👻
No parameters available
No parameters available
OK Cancel

No settings are made to DESFire UID. If you want to prevent DESFire from being read at all by the lock, uncheck *Use DESFire RFID*.

DESFire Select DESFire in the RFID Card Type drop down list.

🐵 Change DESF	ire configu	iration 💌
💟 Use DESFire	RFID	
RFID Card Typ	DESFire	•
Application Id		1
File Identity		2
File Start Posit	ion	12
Length to read	l in File	6
File Data Prote	ection Level	Data authenticated by MAC \checkmark
Read Key (onfigurati	on
Кеу Туре	AES-128	
Кеу	OO11223 CDDEEFI	33445566778899AABBC F
Key Number	0	
	ОК	Cancel

- **Application Id:** To configure the lock for file credential reading, you need to set first the Application Id of the application which contains the file. A credential can have up to 32 applications. Application Ids range from 0 to 16777215.
- **File Identity:** You need to type the File Id of the file you want to read. Every application can have up to 28 files. File Ids range is 1 to 255.
- **File Start Position:** You need to indicate the byte index where you want to start to read the file. If you type 0 it will start from the beginning of the file.
- Length to read in File: Type the length of the data you want to read. The length is specified in bytes. Minimum length is 1 and the maximum length supported by the Aperio lock is 30 bytes (this is the current limitation that will be removed in the future).
- **File Data Protection Level:** Select one of the three options (Plain, Data Authenticity by MAC, Full Encryption) depending on the data type of the file.
- **Key Type:** Select one of the four options (DES, 2K3DES, 3K3DES, AES-128) depending on the crypto used by your application's key. Type the key value in hexadecimal. DES, 2K3DES and AES-128 are 16 bytes keys, 3K3DES is a 24 bytes key.
- **Key Number:** Each application can store up to 14 keys. Key 0 is always the application's master key. Enter which key number from the application you want to use. Key numbers range from 0 to 13.

Example:

AID: 1235	KEY AES -128 nr: 0 00112233445566778899AABBCCDDEEFF	
FID: 1		
		٦
FID: 2 En	crypted	_
17101980]
FID: 3		_

The configuration should look like this:

🤏 Change DES	Fire configu	ration	x
			\bigcirc
📝 Use DESFin	e RFID		
RFID Card Ty	pe DESFire	¥	
Application Id		1235	
File Identity		2	
File Start Posi	tion	0	
Length to rea	d in File	4	
File Data Prot	ection Level	Full encryption	•
Read Key	Configurati	ion	_
Кеу Туре	AES-128	•	
Key	OO1122 CDDEEF	33445566778899AABB F	с
Key Number	0		
	OK	Cancel	

Low frequency



In the list, select the low frequency credential type to use:

- HID Prox
- EM Prox



This credential type cannot be used together with any other credential types.



The following information is not applicable for the US market: Before the lock/sensor has been configured with the Programming Application, the lock/ sensor will accept any Low Frequency credential technology.

Once the lock has read any credential technology 3 times the lock/sensor will only accept this technology. If the power is toggled the lock/sensor will return to the initial state of accepting any credential.

Once a specific credential technology has been configured via the Programming Application, this will be the only accepted type of credential. The lock will remain in this condition after the power has been toggled.

Legic UID



In the list, select the card type to use: • Prime

- · ISO 15693 (Advant)
- ISO 14443 A (Advant)

No other settings are made to Legic UID.

Legic UID with data

Change Legic confi	guration 🛁	x	
		9	
Allowed card types			
At least one card typ	be must be selected.		
📝 Prime			
📝 ISO 15693			
📝 ISO 14443 A			
Configuration type	ID and data 👻		
Segment search			
Search string (hex)	30030009		
Segment type filter	Access		
Start segment	0		
Data Use the first by Start address Number of bytes 8	e of the search string as address 0 for Advant		
Checksum		1	
Туре	CRC 16-bit 👻		
Data start address	0		
Data length	6		
Checksum address	6		
	OK Cancel	_	

In the list, select the card type to use:

- Prime
- · ISO 15693 (Advant)
- · ISO 14443 A (Advant)

Select UID with data in the drop down list.

Segment search:

- Search string (hex): Max 24 characters hexadecimal, even number. For example: 30030009.
- Segment type filter: The type of segment, None, Access or Data.
- Start segment: Specifies the segment from which to start the search. It is useful in cases where more than one similar search string exists. Integer in the range of 0-255.

Data:

- Use the first byte of the search string as address 0 for Advant: Only for Advant card types, in order to change the data addressing of Advant. The first data byte will be the first search string/stamp byte.
- Start address: Specifies the start address of the data. Integer in the range of 0-255.
- Number of bytes: Specifies the number of bytes of data to be read. Integer in the range of 1-45.

Checksum:

- *Type*: "None" does not require any of the checksum related fields to be specified, but CRC 8-bit and 16-bit does.
- Data start address: Specifies the address where the data which checksum is to be calculated starts. Integer in the range of 0-255.

- *Data length*: Specifies the length of the data in number of bytes to be read. Integer in the range of 0-255.
- *Checksum address*: Specifies the address where the checksum is located. Integer in the range of 0-255.



The credential data start address differs between Legic Prime and Legic Advant: • For Legic Prime cards the first data byte starts with the first search string/stamp byte.

For Legic Advant cards the first data byte starts with the first byte in the data area.

Example: Legic Advant Card

Segment 0: Search String: 30 03 00 08 Segment type: Data Data length: 8 bytes Checksum: CRC 16 byte 0-5 Checksum address: 6

🗟 Change Legic configuration 🛛 🔤				
- Allowed card type	- Allowed card types			
At least one card ty	oe must be selected.			
Deine				
V Prime				
V 150 13093				
DOTITION				
Configuration type	ID and data 👻			
Segment search	[
Search string (hex)	30030008			
Segment type filter	None	•		
Start segment	0			
Data	Data			
I lice the first by	e of the search string as address 0 for Advant			
Cust address 0	o of the search se	_		
Start address 0		-1		
Number of bytes o				
Checksum				
Туре	CRC 8-bit	•		
Data start address	0			
Data length	Data length 6			
Checksum address	Checksum address 6			
	OK Cancel			

Segment 1: Search String: 30 03 00 09 Segment type: Access Data length: 24 bytes Checksum 1: CRC 16 byte 0-10 Checksum 1 address: 11

Checksum 2: CRC 16 byte 13-21 Checksum 2 address: 22

The Change Legic configuration	Change Legic configuration
	١
Allowed card types	Allowed card types
At least one card type must be selected.	At least one card type must be selected.
V Prime	V Prime
V ISO 15693	V ISO 15693
V ISO 14443 A	📝 ISO 14443 A
Configuration type UID and data 💌	Configuration type UID and data 💌
Segment search	Segment search
Search string (hex) 30030009	Search string (hex) 30030009
Segment type filter None 💌	Segment type filter Access
Start segment 0	Start segment 0
Data	Data
Use the first byte of the search string as address 0 for Advant	Use the first byte of the search string as address 0 for Advant
Start address 0	Start address 0
Number of bytes 24	Number of bytes 24
Checksum	Checksum
Type CRC 16-bit 👻	Type CRC 16-bit 👻
Data start address 13	Data start address 0
Data length 9	Data length 11
Checksum address 22	Checksum address 11
OK Cancel	OK Cancel
Calcor	or

Only one checksum can be selected.

To include the search string in the first data byte, check the Use the first byte of the search string as address 0 for Advant.

Example: Legic Prime Card Segment 0: (only segment) Search String: 30 03 00 08 Segment type: Data Data length: 8 bytes Checksum: CRC 8 byte 0-6 Checksum address: 7

🤏 Change Legic confi	guration	×	
- Allowed card type	6		
At least one card ty	e must be selected.		
2 Prime			
V ISO 15693			
👿 ISO 14443 A			
Configuration type	ID and data 👻		
configuration ()po			
Segment search			
Search string (hex)	30030008		
Segment type filter	None	•	
Start segment	0		
Data			
Use the first by	e of the search string as address 0 for Advant		
Start address 0			
Number of bytes 8		51	
Lhecksum	[_	
Туре	CRC 8-bit	•	
Data start address	0		
Data length	7	_	
Checksum address	/		
	OK Cancel		

Advanced settings - Keypad configuration (Lock)



This window is only visible if Show advanced settings is activated in User Settings window, see section "User settings" on page 6.

1) Click Change to enter specific Keypad configuration.

Configure Lock/sensor [013542]			x
Keypad configuration Set the keypad configuration if needed. C	lick "Next" to continue.		
Change Keypad configuration			1
Disable Keypad	Change	Remove changes	
	A Back	Next Cancel	

2) Choose between two reading modes:

🐵 Change Keypad configuration
📝 Enable Keypad
PIN reading mode Fixed length 👻
Enter PIN length 4
·
OK Cancel

- Fixed length: PIN is set to use a fixed length.
- Enter PIN length: A value between 1 and 16, as specified by the EAC.

🐵 Change Keypad configuration 📃 💌
🕼 Enable Keypad
PIN reading mode End Character 👻
Select character # + ASC# 35
OK Cancel

- End character: PIN is sent to the EAC after an end character is pressed.
- **Select Character:** One of the non-numeric characters on the keypad can be used to submit the pin. For example: The user enters the PIN followed by a # on the keypad.

Override credential (Lock)

The override credentials are used to gain access to an area when the EAC is offline or when the lock has lost connection with the communication hub. Only the credentials from the override list will be granted access when the system is offline. You may add 10 override credentials to a door.



Use of override credentials when using a Wiegand hub requires that DIP switch 1 is set to position ON.

Tip: You do not have to enter the override credential data manually for every door to be configured. This can be saved using the *Save configuration* function as the last step of the configuration wizard.

1) To add an override credential, select the desired card type in the drop down list and click Add.

🖗 Configure Lock/sensor [013542]	×
Override Credential Add and replace override credentials lock will be left unchanged. Note that loaded into the lock. If you load new o Click "Next" to continue.	If no changes are made, the credentials in the the list below does not show credentials currently cards into the lock the old cards are replaced.
MIFARE UID (Classic/Plus) MIFARE Sector (Classic/Plus) MIFARE Sector (Classic/Plus) MIFARE Sector and UID (Classic/Plus) ISO144488 UID DESfire Class HID Prox and EM Prox. PIN Seos Legic UID Legic Data	Add Description Delete Clear
Remove all credentials in lock	
	Back Next Cancel

See the list below for a description of each credential.



If you check Remove all credentials in the lock, all existing override credentials in the lock will be deleted during the configuration process.

MIFARE UID

lefter new override credential
Enter new override credential Enter UID for the credential. You may also enter a description of the credential.
Card Type
Card Type MIFARE Classic 👻
UID
The UID is entered using hexadecimal format For example: 25A78FA4
12345678
Description Janitor
OK Cancel

- Card Type: MIFARE Classic or MIFARE Plus UID: Card number
- **Description:** For example the credential owner.

MIFARE Sector

lefter new override credential	
Enter new override credential	
Enter sector data for the credential. You may also enter a description of the credential.	
Card Type	
Card Type MIFARE Classic 👻	
Sector data	
The sector data is entered in hex format For example: 99AABBCCDD	
00112233	
Description Janitor	

- Card Type: MIFARE Classic or MIFARE Plus
- Sector data: Sector data stored on the credential. This value is normally stored in the EAC.
- **Description:** For example the credential owner.

MIFARE Sector and UID

Enter new override credential	
Enter new override credential Enter UID and sector data for the credential. You may also enter a description of the credential.	
Card Type	
Card Type MIFARE Classic 👻	
UID	
The UID is entered using hexadecimal format For example: 25A78FA4	
11223344	
Sector data	
The sector data is entered in hex format For example: 99AABBCCDD	
12345ABCDE	
Description Janitor	
OK Cancel	

- Card Type: MIFARE Classic or MIFARE Plus
- **UID:** Card number
- Sector data: Sector data stored on the credential. This value is normally stored in the EAC.
 Description: For example the credential owner.

ISO 14443B UID

🐵 Enter new override credential 🛛 💌
Enter new override credential Enter UID for the credential. You may also enter a description of the credential.
UID The UID is entered using hexadecimal format For example: 25A78FA4
Description Janitor

- **UID:** Card number.
- **Description:** For example the credential owner.

DESFire

🐵 Enter new override credential 🛛 💌
Enter new override credential Enter the credential in hexadecimal format
File data
The sector data is entered in hex format For example: 99AABBCCDD
1234ABCD
Description Janitor OK Cancel

File data: The file data stored on the credential.
Description: For example the credential owner.

iCLASS

🐵 Enter new overri	de credential	×
Enter new overi Enter the creder Appended with 3 not fit into an ew example: 10 bit Appended with 3 Size in bits [1144]	ide credential tital in hexadecimal format. teros if the credential data does an number of bytes. For credential data 1111111101 teros 11111111000000 in hundralmal format.	• •
Credential	1122	
Description Janitor		
	OK Cancel	

- Size in bits [1...144]: Number of bits used for credential data on the iCLASS credential.
- **Credential:** Card credential appended with zeroes on the right side, and translated to hexadecimal format.
- **Description:** For example the credential owner.

HID prox and EM prox

🗢 Enter new overrid	e credential	×
Enter new overrin Enter the credent Appended with ze not fit into an ever example: 10 bit of Appended with ze	de credential ial in hexadecimal format. ros if the credential data does n number of bytes. For redential data 111111101 ros 1111111101000000	•
Size in bits [1144]	10	
Credential	FF40	
Description Janitor		
	Cancel	

- Size in bits [1...144]: Number of bits used for credential data on the credential.
- **Credential:** Card credential appended with zeroes on the right side, and translated to hexadecimal format.
- **Description:** For example the credential owner.

PIN

🖗 Enter	r new override credential
Enter Enter	new override credential the PIN for the credential.
PIN 2	2323
Descripti	on Janitor
	OK Cancel

- PIN: PIN code
- **Description:** For example the PIN user.

Seos

Enter new overrid	e credential	×
Enter new overrid Enter the credenti Appended with ze not fit into an ever example: 10 bit cr Appended with ze	de credential la in hexadecimal format. ros if the credential data does number of bytes. For redential data 111111101 ros 111111101000000. - Jonadeciment.	A III
Size in bits [1384]	10	
Credential	1111	
Description Janitor		
	Cancel	

- Size in bits [1...384]: Number of bits used for credential data on the credential.
- **Credential:** Card credential appended with zeroes on the right side, and translated to hexadecimal format.
- **Description:** For example the credential owner.

Legic UID

🛞 Enter new override credential
Enter new override credential Enter data for the credential. You may also enter a description of the credential.
UID The UID is entered using hexadecimal format For example: 25A78FA4
12345ABCDE
Description Janitor

- **UID:** Card number.
- **Description:** For example the credential owner.

Legic Data

🐵 Enter new override credential 🛛 🛛 💌
Enter new override credential Enter data for the credential. You may also enter a description of the credential.
Data
The sector data is entered in hex format For example: 99AABBCCDD
11222663&&BB
Description Janitor

• **Data:** Sector data stored on the credential.

• **Description:** For example the credential owner.

Security Mode Settings (Communication hub and Lock/sensor)

This setting will apply for both the communication hub and the lock if only one lock is paired.

The Configure Communication Hub [024521]	×
Security Mode Setting Set the security mode that will be used for encrypted radio commun to continue.	nication. Click "Next"
Security Mode Setting	
Security mode will not be changed	Change
A Back	ext Cancel

- 1) Click Change in the Security Mode Setting area if you want to change the security mode, or click Next.
- 2) To change to customer mode, check the checkbox and click OK.

-	
🐵 Security Mode Setting	×
Switch to Customer mode in d	evice
OK Cancel	



The default mode is Manufacturer mode, but you should always change it to Customer mode. If you change to Manufacturer mode key the lock will no longer be using secure radio communication.

RS-485 settings (Communication hub)

For use of RS-485 there are the following options. Click *Change*... for each option to enter the settings.

🐵 Configure Communication Hub [024521]	×
Electronic Access Controller Settings Change settings if needed. Click "Next" to continue.	
EAC addressing mode	
Legacy address offset	Change
Lock access decision timeout	
2 seconds	Change
Remote open	
Remote open is inactivated	Change
Enable EAC Address via DIP Switch	
DIP Switch enabled	Change
A Back	Cancel

EAC addressing mode



The default EAC addressing mode is Normal address offset, which means that the communication hub assigns the EAC address to the paired locks according to the addressing table, see the Aperio Online Mechanical Installation manual. This setting is used when the EAC can handle addresses without limit.

Legacy address offset is used when the EAC has a low limit for handling addresses, for example 32 or 64. The following example shows the addresses assigned to the locks on a communication hub with address 1:

- · Normal address offset: 1,17,33, 49,
- Legacy address offset: 1-8 (hub 1), 9-16 (hub 2), 17-24 (hub 3).

Lock access decision timeout



This value sets the time (in seconds) the lock will wait for an access decision from the EAC.

If this time is extended and the HUB is offline the response time when using the PAP will be longer. This is due to that each swipe of a credential will wait for the EAC response and with a longer timeout, the response in offline will also increase.

Remote open

ĭ

Remote open configuration	×
Enable remote open	
Default unlock duration for Wiegand: 8 hours and 0	minutes
·	
OK Cancel	

Checking the Enable remote open checkbox will enable the remote open functionality in the HUB. As the wiegand interface does not support setting an unlock duration from the EAC, this must be configured here.

Enable EAC Address via DIP Switch



Checking the *Enable DIP Switch* checkbox will restore the EAC addressing to what is configured with the DIP switches on the communication hub.



To disable the DIP switch the EAC address must digitally be set as well. To do this use the *Change the EAC address* function on the right click menu for the communication hub.

Advanced setting - Radio channel settings (Communication hub or Lock/sensor)

Always change the radio channel on the lock before changing on the communication hub. This function is also available on the right click menu in the *installation view*.

1) Click Change... to set the radio channel the communication.



2) Deselect one or several of the used channels to make a new selection of channels.



For the US market channel 26 is disabled.

Advanced Lock/sensor Settings

On this page you will be able to configure Battery Power Alarm Interval, Status Report Interval, Locking Parameters, Card Read Indication and Sensor Events.

🛞 Configure Lock/sensor [013542]	×
Advanced Lock/sensor Settings Change settings if needed. Click "Next" to continue.	
Battery Power Alarm Interval	Change
Status Report Interval	Chana
Locking Parameters	Change
	Change
Card Read Indication	Change
Sensor Events	Change
▲ Back ► Next	Cancel

Configure Battery Power Alarm



The battery power alarm is sent from the lock to the EAC system and is used to indicate when it is time to replace the battery. It may be necessary to configure the alarm triggering depending on the type of battery used and the surrounding temperature, e.g. in cold surroundings the battery runs out faster.



This only applies to products with lithium batteries that are using energy counter. For products with battery measurement on the secure side (P100/I100 currently), the interval you set translates into hours, i.e. 6 minutes = 6 hours on those products.

Status Report Interval

🐵 Configure Status Report Interval 🧧	x
Status Report Interval The value below is the default value, not the one currently in the Lock/sensor.	
Message Interval (minutes) 60	
OK Cancel	

The interval setting is normally set to 60 minutes. If *Remote Open* functionality is used, this parameter should be set to a shorter interval such somewhere in between 5 and 15 minutes.



Lowering the status interval time for any reason will have an adverse effect on the battery life of the product.

As the status message interval is used by the communication hub to detect if the lock has gone offline, any changes to this interval must be done on both lock and communication hub where the lock interval should be shorter than the interval in the communication hub. This is to ensure that no intermittent offline situations occur.

When using an AH30 communication hub it is also important that all locks have the same status interval as the communication hub will only have one 'offline' interval for all locks paired.

Locking Parameters

😔 Configure Locking Parameters		×
Try to unlock timeout (second: The time the lock tries to unlock a failure if it is not possible.	s) <, until it returns	
Lock open time (seconds) The time period during which th	ie lock is open	
Lock jammed alarm timeout (seconds) Time period during which the main controller constantly tries to lock a jammed lock until it sends a Lock Jammed Alarm to the EAC system and returns to sleep mode.		
Lock jammed retry period (see Time between the retries in loci	c onds) k jammed mode.	
Lock jammed indication mode The way in which the lock indica been jammed.	ates that it has	-
Try to unlock timeout (seconds)	2	
Lock open time (seconds)	5	
Lock jammed alarm timeout (seconds)	30	
Enable lock jammed retry		
Lock jammed retry period (seconds)	60	
Lock jammed indication mode	LED	-
ОК	LED Buzzer aLED and buzzer	

Here you configure timing for different operations in the lock:

- **Try to unlock timeout (seconds):** How long the lock tries to unlock before it returns a failure.
- Lock open time (seconds): How long the lock will be open in seconds (default = 5 s).

- Lock jammed alarm timeout (seconds): How long time the system tries to lock the lock before it sends an alarm to the EAC and goes back to idle state.
- **Enable lock jammed retry:** This enables a periodic retry to lock the lock according the settings under "Lock jammed retry period (seconds).
- Lock jammed retry period (seconds): How long the lock will wait before it retries to lock the lock in seconds (default = 2 s).
- Lock jammed indication mode: The way in which the lock indicates that it has been jammed. LED, Buzzer and LED and buzzer are the different indication modes.

Configure Card Read Indication

谷 Configure Card R	ead Indication 🛛 🔼
Card Read Indica Configure the war card read. Please card read indicati has since not all to every type of loo just default values never read from th	tion y in which the lock indicates a note that you must know what on capabilities the selected lock options here might be applicable k. Initial values shown here are s. The actual configuration is he lock.
Card Read Indication	None 🗸 🗸
	LED Buzzer LED and buzzer

Different locks can have a different mechanism for audio-visual indication of successful credential reading. Here it is possible to disable credential read indication or to set it to LED. Some Aperio locks have support for other mechanisms such as buzzers.

Sensor

😔 Configure Sensor Events
Disable sensor events for unlock durations greater than:
1 hours and 0 minutes
OK Cancel

This setting applies for locks with built in sensor. By activating this function, the lock sensor will stop sending passage events to the EAC for unlock durations longer than you set here. This setting will save battery life in high traffic doors.

Device update page – Saving Configuration

Constant Fockstearon (n722-m)		
Device Update		
The settings are now ready to be transm	ited to Lock/sensor. You might	need to Shaw
card/Engage sensor to Lock/sensor. Cli	S'Net".	
The following updates will be transmitted to the	Aperia#LadStensor	
Keypad		
Adding one override credentials		
- "Jentor" MEARE Classe: 12345678		
Card read indication		
- LED		
Time and date		
 Ourrent system time 		
	Save	artquster.

Here a summary of configurations that will be transferred to the unit. The Device Update dialog box shows a summary of the configuration tasks that will be downloaded to communication hub/lock/ sensor. The configuration may be used later to configure other devices with the same information, by clicking *Save configuration*:

- 1) The Save Configuration dialog box shows a summary of the configuration tasks that have been collected during the different steps in the Configuration Wizard. You can exclude some tasks by simply ticking the check box.
- 2) Recommended tasks to save could be:
 - RFID configuration
 - Change security mode
 - Override credential
 - Device time update
 - And optionally some advanced features like Battery Alarm, Status configuration and Locking parameters.

If you choose to save a configuration, keep in mind that some configuration settings should not be saved. Only save settings that are general for all locks in your installation. **Tip:** Create a set of configurations for the most common settings in your system.

Save configurat Select the config save. Then choo save.	ion to local storage urations in the table below that you want to se a name for the setting and click OK to
Configuration name	Default hub installation
Adding one ove	rride credentials
🔽 Remote open	
🔽 Card read indic	ation
👿 Time and date	
	OK Cancel

3) Enter a unique and suitable name for this configuration in the Configuration name field. Choose this name carefully, to make it clear what settings are changed in the lock/sensor or communication hub.. You could, for instance, name it according to the different configuration tasks or, if applicable, use a name that reflects the specific door type.

Save configurat Select the config save. Then choo save.	ion to local storage urrations in the table below that you want to use a name for the setting and click OK to
Configuration name	Default hub installation
Adding one over	erride credentials
Remote open	
🔽 Card read indic	ation
👿 Time and date	
(OK Cancel

4) Click OK.

Result: The configuration is saved in the local storage and the *Save configuration* window is closed. Clicking *Cancel* on the *Device Update* page does not affect the locally stored configuration.

The Configure Communication Hub [024521]
Device Update The settings are now ready to be transmitted to Lock/sensor. You might need to Show card/Engage sensor to Lock/sensor. Click "Next".
The following updates will be transmitted to the Aperio® Lock/sensor:
Adding one override credentials - "Janitor" MIFARE Classic: 1111111 Remote open - Activate Card read indication - LED Time and date - Current system time
Save Configuration
Back Next Cancel

Applying a stored configuration to a communication hub/lock/sensor

If you saved a configuration in the configuration wizard, you can apply it to numerous locks/sensors. This function is available on both the Lock/sensor menu and the communication hub menu and will only download settings that apply for the hardware selected.

Follow these steps to download a saved configuration to a lock/sensor:

1) In the *Installation view*, right click the desired lock/sensor and select *Apply configuration* and an earlier stored configuration.

Aperio Programmin File Scan Settings He	ig Application - elp	[New_insta	llation]					- • 💌
Lock/sensor	Communic	ation Hub	EAC Address	UHP	= Link	Communication F	tub [024521]	
011C43	0216F1		1		●● 	1		
013542	024521			9	. la	MAC Address		00:17:7a:01:02:
0148E8	024521	Lock/ser	isor [013542]	•	99 <u>8</u>	Physical Location		Office A
0148ED	024521	Commu	nication Hub (02452	1])	Apply configu	ration	Default	hub installation
		Upgrade	Firmware	_	Configure Pair with lock	or sensor	'n	1.2.5
					Retrieve syste	m information		25 (2.475 GHz)
					Change radio Change EAC J Change physi Switch to Mar	channels Address cal location name nufacturer Mode Number of paired Device Status	e locks and sensors	11, 16, 25 4521 Legacy addre 1 [DIP Switch] : 3 EAC offline
						Lock/sensor [01: MAC Address Assigned Address EAC Address Radio protocol ver	3542]	00:17:7a:01:02: 0x1230 1 22
USB Radio (COM 10))						May 14, 2	013 11:21:24 AM

2) Click Confirm to start the transfer.



3) Wait for the transfer to finish.



4) Hold the credential at the lock, or engage the magnet for the sensor, to accept the configuration. (This will not be required when downloading configuration to a communication hub.)



5) The result is shown. The settings that could not be transferred to the specific hardware are ignored. Click *Close* to finish.



6) Repeat all the steps from the beginning of this section for every lock/sensor you want to configure with a saved configuration.

Change physical location name – communication hub/lock/sensor

This function applies to both communication hubs and locks/sensors. In the example below the physical location name is changed for a lock/sensor.

1) Right click and select Lock/sensor – Change physical location name...

le Aperio Progr	ramming A	pplication - [New_instal	lation]						- • ×
<u>File Scan Setti</u>	ngs <u>H</u> elp								
Lock/sensor		Communication Hub	EAC Ad	ddress	UHF Link		Communica	tion Hub [024521]	
011C43		0216F1		1		8	M0C 0ddres		00:47:7-:04:03:
013542		024521		1			I INING MODICS	tion	00.11.14.01.02.
0148E8	LOCK	/sensor [U13542]		Apply confi	guration		,	vor	DC 495 Multipl
0148ED	Com	imunication Hub (02452	1] '	Configure				rian	R5465, Mulupi
	Upgr	rade Firmware		Retrieve sys	tem inform	ation		SIGH	6.0.22795
				Get Event L	og			arsion	1.2.5
				Get Audit T	rail			pi version	23
									25 (2.475 GHz)
				Change rad	io channels			45	11, 16, 25
				Switch to M	lanufacture	Mode			4521
				Change phy	/sical locatio	on name		ng mode	Legacy addre
				Unpair lock	/sensor fror	n commun	ication hub	ilue	1
									[DIP Switch]
							Remote ope	n is activated	
							Number of p	aired locks and sensors	3
							Device Statu	15	EAC offline
							Lock/senso	r [013542]	
							MAC Addres	s	00:17:7a:01:02:
							Assigned Ad	dress	0x1230
							EAC Addres	s	1
							Radio proto	col version	22
							•	III	÷.
💙 USB Radio (0	COM 10)							May 14, 2	013 11:48:02 AM

2) Enter a description that clearly identifies the lock position and click OK.



3) For a communication hub the information is updated immediately. If you change the physical location name for a lock/sensor you will be prompted to hold the credential at the lock, or engage the magnet for the sensor.

left waiting for user to Show card/Engage sensor	×
Show card/Engage sensor	
onon caraizingago sonsor	
Time remaining until timeout: 15 seconds	
Li.	

Result: After successful reading a progress bar shows the download. After update the new location name can be found in the Lock/sensor section on the lower right side of the installation view.

Aperio Programming A <u>File</u> Scan Settings <u>H</u> elp	pplication - [New_insta	llation]			
Lock/sensor	Communication Hub	EAC Address	UHF Link	Communication Hub [024521] -	
011C43	0216F1	1		MAC Address	00 47 7 04 00 00 45 04
013542	024521	1		MAC Address	00:17:78:01:02:02:45:21
0148E8	024521	2		Physical Location	Office A
0148ED	024521	3		Firmware Flavor	RS485, Multiple Lock [Aper
				Firmware Version	6.0.22795
				Bootloader Version	1.2.5
				Radio protocol version	23
				Channel	25 (2.475 GHz)
				Radio channels	11, 16, 25
				PAN ID	4521
				EAC addressing mode	Legacy address offset
				DIP switch value	1
				EAC Address	[DIP Switch]
				Remote open is activated	
				Number of paired locks and sensors	3
				Device Status	EAC offline
				Lock/sensor [0148E8]	
				MAC Address	00:17:7a:01:02:01:48:e8
				Physical Location	Floor 1 - Door A14
				Assigned Address	0x11fd
				EAC Address	2
				Radio protocol version	23
				· · · · · · · · · · · · · · · · · · ·	4
Signal Comparison (Comparison of the second					May 14, 2013 11:49:10 AM

Get Event Log

This function displays the event log for a particular lock (not available for sensor), where you can find all system events performed on the lock.

1) Right click and select Lock/sensor – Get Event Log...



2) Hold the credential at the lock,.



Result: Successful reading initiates the download of the event log.



3) In the event log window, click *Save As...* to save the information to a txt file or click *Close* to exit without saving.

14ê	×
Fuent log for Lock/geneor [0]/49F9]	_
Created: May 14 2013 11:50:34 AM CEST	
orcacca. May 14, 2015 11.00.04 An orbit	
Number Date	Code
1. January 1. 2007 1:00:00 AM CET	Power-On-Reset [Ox9c02]
2. January 1, 2007 1:00:00 AM CET	New battery detected [0x001e]
3. January 1, 2007 1:00:07 AM CET	Flash content errors in NVM seg
4. January 1, 2007 1:00:08 AM CET	Power On Self Test (POST) perfor-
5. January 1, 2007 1:00:00 AM CET	Power-On-Reset [0x9c02]
 January 1, 2007 1:00:00 AM CET 	New battery detected [0x001f]
 January 1, 2007 1:00:08 AM CET 	Power On Self Test (POST) perfo:
 January 1, 2007 1:00:22 AM CET 	Power-On-Reset [0x9c02]
 January 1, 2007 1:00:22 AM CET 	New battery detected [0x001f]
10. January 1, 2007 1:00:30 AM CET	Power On Self Test (POST) perfo:
11. January 1, 2007 1:00:00 AM CET	Power-On-Reset [0x9c02]
 January 1, 2007 1:00:00 AM CET 	New battery detected [0x0020]
 January 1, 2007 1:00:08 AM CET 	Power On Self Test (POST) perfo:
14. January 1, 2007 1:00:00 AM CET	Power-On-Reset [Ox9c02]
15. January 1, 2007 1:00:00 AM CET	New battery detected [0x001f]
16. January 1, 2007 1:00:08 AM CET	Power On Self Test (POST) perfo:
17. January 1, 2007 1:00:00 AM CET	Power-On-Reset [0x9c02]
 January 1, 2007 1:00:00 AM CET 	New battery detected [0x001f]
19. January 1, 2007 1:00:07 AM CET	Power On Self Test (POST) perfo:
20. January 7, 2007 1:50:07 AM CET	Soft reset
21. January 7, 2007 1:51:01 AM CET	New Main Application Firmware p:
 January 7, 2007 1:51:01 AM CET 	System reset [0x8f02]
 January 7, 2007 1:51:10 AM CET 	Debug event [FATAL, 513]
 January 7, 2007 1:51:13 AM CET 	System reset [0x8f02]
 March 22, 2007 12:37:46 AM CET 	The RTC is about to be updated -
	•
Save ac	
Jave ds	

The window contains information of system events including consecutive number, date, and what type of system event that was performed. (If the number of events exceeds 200 older events are overwritten.)

Get Audit Trail

This function displays a complete list of all access attempts for a particular lock (not available for sensor).

1) Right click and select Lock/sensor – Get Audit Trail.

Aperio Programming File Scan Settings He	g Application - [New_insta Ip	llation]				
Lock/sensor	Communication Hub	EAC Address	UHF Link	Comm	unication Hub [024521] _	
011C43	0216F1	1		MAG	Addross	00.47.7.04.03.03.45.34
013542	024521	1		MAC	al Lesstine	00:17:78:01:02:02:40:21
0148E8 Lock/ser	nsor [013542]	Apply configuration	n	•		
0148ED Commu	inication Hub [024521]	Configure			are Havor	R5485, MURIPIE LOCK [Aper
Upgrade	e Firmware	Retrieve system inf	formation		are version	6.0.22795
		Get Event Log			ader version	1.2.5
	(Get Audit Trail			protocol version	23
	C C C C C C C C C C C C C C C C C C C				iel	25 (2.475 GHz)
		Change radio char	nnels		channels	11, 16, 25
		Switch to Manufac	turer Mode:		þ	4521
		Change physical lo	ocation name		ddressing mode	Legacy address offset
		Unnair lock/sensor	r from communication	huh	vitch value	1
					ddress	[DIP Switch]
				Remo	te open is activated	
				Numb	er of paired locks and sensors	3
				Devic	e Status	EAC offline
				Lock/s	sensor [013542]	
				MAC	0 ddraese	0047-7
				0.ccim	nadi oss	00.11.14.01.02.01.33.42
				EAC /	lida Adal ess	0x1230
				Dada		1
				Raulu	protocol version	22
				•	III	۱.
Signal Communication (Communication)						May 14, 2013 12:30:14 PM

2) Hold the credential at the lock.

left Waiting for user to Show card/Engage sensor	×
Show card/Engage sensor	
Time remaining until timeout: 13 seconds	

Result: Successful reading initiates the download of the audit trail.



3) In the audit trail window, click *Save As...* to save the information to a txt file or click *Close* to exit without saving.

÷			×
Audit 7	rail for Lock/sensor [013542]		
Created	: May 14, 2013 12:30:35 PM CEST		
Number	Date	Code	WTD100 01 045
1.	March 14, 2013 10:17:40 AM CEI	Access denied	MIFARE Classic: 04/
2.	March 14, 2013 10:24:26 AM CEI	Access denied	MIFARE Classic: 04)
J.	May 14, 2013 10:49:30 MM CEST	Access denied	MIFARE Classic: 047
5	May 14, 2013 10:40:35 AM CEST May 14, 2013 10:40:21 AM CEST	Access denied	MIFARE Classic: 047
6	May 14, 2013 10:50:29 AM CEST	Access denied	MIFARE Classic: 047
7.	May 14, 2013 11:48:40 AM CEST	Access denied	MIFARE Classic: 047
8.	May 14, 2013 11:49:42 AM CEST	Access denied	MIFARE Classic: 047
9.	May 14, 2013 11:50:09 AM CEST	Access denied	MIFARE Classic: 047
10.	May 14, 2013 11:52:11 AM CEST	Access denied	MIFARE Classic: 047
•			
	Save as Clo	ise	

The window contains information on the total number of access attempts including consecutive number, date, access decision and what type of credential that was used at each attempt.

Retrieve system information

This function is available for both communication hub and lock/sensors.

Communication Hub 0216F1	EAC Addres	s UHFLink	Communication Hub [024521]	
0216F1	[Unknow	പ്രക്ഷം		
			MAC Address	00:17:7a:01
Lock/sensor [0148ED]	+ 1		Physical Location	Office A
Communication Hub [02	4521] 🕨	Apply configuration	In Flavor	RS485, Mul
		Configure	e Version	6.0.22795
Upgrade Firmware		Pair with lock or sensor	der Version	1.2.5
	_	D.1.	rotocol version	23
		neurieve system informati	l l	11 (2.485 G
		Change radio channels	hannels	11, 16, 25
		Change EAC Address		4521
		Change physical location	name dressing mode	Legacy ad
		Switch to Manufacturer M	tode ch value	1
			EAC Address	[DIP Switcl
			Number of paired locks and senso	rs 2
			Device Status	EAC offline
			Lock/sensor [0148ED]	
			MAC Address	00:17:7a:01
			Assigned Address	0x12b9
			EAC Address	1
			Radio protocol version	23
			Device Status	
	Upgrade Firmware	Upgrade Firmware	Upgrade Firmware Pair with lock or sensor Pair with lock or sensor Change radio channels Change Physical location Switch to Manufacturer M	Upgrade Firmware Pair with lock or sensor Pair with lock or sensor Pair with lock or sensor Change radio channels Change radio channels Change radio channels Switch to Manufacturer Mode give value EAC Address Device Status Lock/sensor [01:48E0] MAC Address EAC Address Radio protocol version Device Status

1) Right click and select Lock/sensor or Communication Hub – Retrieve system information to access the unit.

@ Retrieving system inform	ation from Co	mmunica 💌
Please wait		
	0%	

Result: The Programming Application connects to the unit.

2) Click *Save as...* to save the system information to a local storage, Click *Reset diagnostic counters...* to reset the diagnostic counters in the device or click *Close* to exit.



Change EAC address



It is recommended to use the DIP Switch for setting the EAC address of communication hubs. However, if needed the Change EAC address function allows you to digitally assign an EAC address in the range of 1-63 (1-15 for communication hubs with several locks/sensors paired and 1-63 for communication hubs with one lock/sensor paired).



If the Programming Application is used to set RS 485 addresses, it will override the address set by the DIP switch on the communication hub.

1) Right click and select Communication hub-Change EAC Address.

~ ~
RS-485 Settings Select the EAC Address for this Communication Hub
EAC Address
[DIP Switch]
1 2
3
4 ⊑
6
7
9
10 Select the EAC Address for this Communication Hub
11
OK Cancel

2) Select the address and click OK.

Changing the Security Mode

Secure communication is normally set during first configuration of locks/sensors and communication hubs with the configure wizard. Security mode is also accessible through the right click menu. During normal operation the security mode should not be altered. However, if the hardware must be sent to the factory for service or repair purposes, the security mode must be set to manufacturer mode before service.

Explanation of symbols:

8	Customer mode	Door is using secure radio communication with the customer encryption key.
Ê	Manufacturer mode	Door is using insecure radio communication with the default encryption key.
\bigotimes	Conflicting mode	The modes in the lock/sensor and the communication hub are not the same.

Aperio Programming App File Scan Settings Help	lication - [N	lew_installation]				
Lock/sensor	Commun	ication Hub	EAC Address	UHF Link	Communication Hub [0216F1]	
011C43 013542 0148E8	0216F1 02452 02452	Apply configur Configure	ation 🕨		MAC Address Firmware Flavor	00:17:7a:01:02: RS485 [Aperio
0148ED	0245	Lock/sensor [0:	11C43]	Retrieve system informat	ion	6.0.22795 1.2.5
		Upgrade Firmw	are	Get Event Log Get Audit Trail		23 19 (2.445 GHz)
				Change radio channels Switch to Manufacturer M Change physical location	Node name	14, 19, 25 16F1 Normal addre:
				Unpair lock/sensor from	communication hub	1 [DIP Switch]
					Device Status	1 EAC offline
					Lock/sensor [011C43]	
					MAC Address Assigned Address	00:17:7a:01:02: 0x115e
					EAC Address Radio protocol version	1
					Device Status	Lock/sensor (
					<	4
Signal COM 10 (COM 10)					May 14, 2	013 12:50:23 PM

1) Right click the lock/sensor and select Switch to Customer Mode/Switch to Manufacturer mode.

2) Hold the credential at the lock, or engage the magnet for the sensor.



- 3) A progress bar shows that the transfer is being performed.
- 4) If the encryption key is successfully loaded you get a message that states "Successfully updated security mode". Click OK.



Result: Check the lock symbol at the right side of the door to see that the door has been set to Customer mode/Manufacturer mode.

Lock	Communication Hub	EAC Address	UHF Link	
000001	024521	1		8
0148E8	024521	17		8
0148ED	024521	33		8

Changing the radio channels

Changing the radio channels can be necessary if you experience interference between communication hubs, which can occur if many hubs are installed close to each other.



To use this function, you must have the Show advanced settings checkbox checked in User Settings, see section "User settings" on page 6. Follow these steps to change the radio channel for the communication hub and lock/sensor:



Always change the radio channel in the locks/sensors before changing in the communication hub!

1) Select the lock/sensor in the scan result table. Right click and select Lock/sensor – Change radio channels.

011C43 0226F1 1 MAC Address Bert 72rdaff Oldsda Oldsda Oldsda Communication Hub [024521 Apply configuration Oldsda Oldsda Communication Hub [024521 Configure Better a system information Get Event Log Get Event Log Get Event Log Get Event Log Get Audit Trail Pail Connels 11, 64, 25 Oldsda Change radio channels Change radio channels Unpair lock/sensor form communication hub Redies ops in activated Munber of paired bods and sensors 3 Device Status EAC officin Lock/sensor [013542] MAC Address Bet 72rdaff MAC Address Bet 72rdaff Mac Address Bet 72rdaff Device Status Bet 87rdaff Device St	011C43 0216F1 1 0106C 0016F1 013642 013642 013642 0 013642 0 016F1 0 000F1 0 000F1 0 00F1 0 00	Lock/sensor	Communication Hub	EAC /	Address	UHF Link		Comm	nunication Hub [024521]	
01556 Concest 0417172 > Apply configuration > All coation Office A 014820 Communication Hub [024521] Configure are Floor R5486, MA 014820 Upgrade Firmware Configure are Floor R5486, MA 014820 Upgrade Firmware Configure are Floor R5486, MA 014820 Communication Hub [024521] Configure are Floor R5486, MA 014820 Upgrade Firmware Get Event log protocol version 23 014820 Change radio channels othoreds 11, 2485 G Othoreds 11, 2485 G 014820 Change radio channels othoreds 11, 2485 G Othoreds 11, 2485 G 014820 Change radio channels othoreds 11, 2485 G Othoreds 11, 2485 G 014821 Uppair lock/rensor from communication nub addressing mode Legary ad 1 01492 Uppair lock/rensor from communication nub Machasing other is activated Nuberor 3 01492	01556 00000 Unc. Addess 0001774 01562 00000 Apply configuration are favor Restaur 016825 Communication Hub (024521) Configure are Version Restaur 016825 Communication Hub (024521) Configure are Version Restaur 016825 Get Audit Trail are Version 1.2.5 016825 Get Audit Trail and Version 1.2.6 016825 Change radio channels damets 11 (2.486 016825 Change radio channels ddressing mode Legaxyu 016826 Change radio channels ddressing mode Legaxyu 016826 Unpair lock/sensor from communication hub witch value 1 016826 Unpair lock/sensor from communication hub Mach value 1 016826 Device Status EAC off 016827 Mach value EAC off 016828 EAC off EAC off	011C43	0216F1		1		8	MAG	Address	00.47.704.0
Assigned Address 0x1230 EAC Address 1	CHC HOURDS	019492	Lock/sensor[015542] Communication Hub [024521] Upgrade Firmware		Apply configurat Configura. Retrieve system ii Get Event Log Get Audit Trail Change radio change radio change radio Switch to Manufi Change physical Unpair lock/sens	innels innels icturer Mode location nam or from comr	e	MAC	Address jal Location ware Version addre Version protocol version protocol version protocol version protocol version protocol version protocol version protocol version didressing mode witch value value set open is activated or of paired clocks and sensors te Status sensor [013542] Address Address	00:17:7a:01:0 Office A RS485, Multi 6.0.22795 1.2.5 23 11 (2.405 GH 11, 16, 25 4521 Legacy add/ 1 [DIP Switch] 3 EAC offline 00:17:7a:01:0 0x1230 1

2) Uncheck any of the three currently used channels to be able to select other radio channels. Click OK.



For the US market channel 26 is disabled.

@ X
Change radio channels in Communication Hub [IQ24521] At mostyou are able to set 3 separate radio channels. To consider: When changing radio channels, all connected devices MUST be changed before the Communication hub is updated.
V 11 (2.405 GHz)
12 (2.410 GHz)
13 (2.415 GHz)
14 (2.420 GHz)
15 (2.425 GHz)
✓ 16 (2.430 GHz)
17 (2.435 GHz)
18 (2.440 GHz)
19 (2.445 GHz)
20 (2.450 GHz)
21 (2.455 GHz)
22 (2.460 GHz)
23 (2.465 GHz)
24 (2.470 GHz)
20 (2.400 GHZ)
Set preferred mask OK Cancel

3) Hold the credential at the lock, or engage the magnet for the sensor to perform the update.



Result: A progress bar shows that the update is being performed. The Device update result dialog box shows the result of the update when it has been performed.

Device update result	×
Successfully updated radio chan	nels.
OK	

4) Repeat this procedure for all locks/sensors connected to the current communication hub.

Recommendation: Although it is possible to set different channels to locks/sensors paired with one hub, it is preferable to use the same three channels for all locks/sensors on that communication hub in order to create a more stable radio connection. Communication problems occur more likely between closely installed hubs than between closely installed locks/sensors paired with one hub.

- line and the second sec - • • <u>F</u>ile S<u>c</u>an <u>S</u>ettings <u>H</u>elp Lock/sensor Communication Hub EAC Address UHF Link Communication Hub [024521] 011C43 0216F1 MAC Address 00:17:7a:01:02 Lock/sensor [013542] Physical Location Office A 0148E8 2 Communication Hub [024521] 🔸 Apply configuration Firmware Flavor RS485, Multipl 0148ED 6.0.22795 Configure... Firmware Version Upgrade Firmware... Pair with lock or sensor Bootloader Version 1.2.5 Radio protocol version 23 Retrieve system information... Channel 11 (2.405 GHz) Change radio channels... Radio channels 11, 16, 25 Change EAC Address PAN ID 4521 Change physical location name.. EAC addressing mode Legacy addre Switch to Manufacturer Mode DIP switch value EAC Address [DIP Switch] Remote open is activated Number of paired locks and sensors 3 Device Status EAC offline Lock/sensor [013542] MAC Address 00:17:7a:01:02: Assigned Address 0x1230 EAC Address Radio protocol version 22 Ш Signal Communication (Communication) May 14, 2013 12:54:54 PM
- 5) Finally, change the radio channel for the communication hub: Right click and select *Communication Hub Change radio channels*.

6) Uncheck any of the three currently used channels to be able to select the same radio channels as for the lock/sensor. Click OK.

Result: A progress bar shows that the update is being performed. The Device update result dialog box shows the result of the update when it has been performed.

	Device update result
🐵 Change radio channels	Successfully updated radio channels.
Please wait	
0%	ОК

Setting the time of a lock Follow these steps to set the time of a lock:

- 1) Select a lock in the installation view.
- 2) On the menu bar select Settings Installation Settings and check that the Update device time during door *configuration* checkbox is checked.

🐵 Installation Settings 📃							
MIFARE UID format							
Select how the MIFARE UID shall be formatted in Audit Trails and when configuring Override Credentials.							
Hexadecimal format (i.e. 25A78FA4)							
Decimal format (i.e. 631738276)							
Hexadecimal format, reverse byte order (i.e. A48FA725)							
Decimal format, reverse byte order (i.e. 2760877861)							
Configuration wizard settings							
Vpdate device time during door configuration							
OK Cancel							

3) Close the Installation Settings view. Right click and select Lock/sensor-Configure. Click Next repeatedly until you reach the Device Update window.

Configure Lock/sensor [013542]
Device Update The settings are now ready to be transmitted to Lock/sensor. You might need to Show card/Engage sensor to Lock/sensor. Click "Next".
The following updates will be transmitted to the Aperio™ Lock/sensor:
Time and date - Current system time
Save Configuration
A Back Next Cancel

4) Click Next.



5) Hold the credential at the lock, to update the time.

The time of the lock will now be automatically set each time you configure and update the device.

6) Click *Close* to exit the device update configuration.

Configure Lock/sensor [013542]
Device update result The result of the device update will be presented below.
Successfully updated time and date.
Back Cose Cancel

Change IP address (Communication hub AH40)

1) Right click and select Communication hub – Change IP Address.

Aperio Programming App	olication -	[New_installation	n]					
File Scan Settings Help								
Lock/sensor	Communica	ition Hub	EAC Address	UHFI	Link			
0	0295EB		El Inknown]		≥● 🗳 🔺	Not paire	d wi	ith any device
		Apply configu	ration	•			ion H	lub [0295EB] not paired with a
		Configure						accept
		Communicati	on Hub (0295EB)	•	Pair with lock o	1 I OMMUNICATION H	μοι	UZA2ER]
				T				00:17:7a:01:02:02:95:eb
		Upgrade Firm	ware		Retrieve systen	n information		Office A2
					Change radio d	channels		IP, Multiple Lock [Aperio
					Change FAC A	ddress		1.0.1895
					Change physic	al location name		1.0.1835
					Switch to Cust	omer Mode	on	23
					Switch to Case	omernvioue		11 (2.405 GHz)
					Get Event Log.			11, 16, 26
					Change IP Add	lress		95EB
					Restart			10.63.251.201
						ACO Address		10.63.251.202
						ACU port		9999
						TLS Encryption		Enabled
						•	111	Þ
SB Radio (COM 7)							A	ugust 12, 2013 10:06:16 AM

2) Fill in the IP address of the communication hub. Click OK and the new IP address will be applied in the communication hub, and the IP communication will be restarted using the new IP address.

40		x
IP Addres Specify IP format (XXXI0-25	s address of the IP Hub following IPV4 51,XXX(10-2551,XXX(10-2551,XXX(10-2551)).	4 11 >
IP Address	192 . 168 . 0 . 10	
	OK Cancel	

Importing and exporting configurations

General

The stored configurations made in the configuration wizard, can be exported to a file so that more than one Aperio Programming Application can share the same configuration information. When you import an exported configuration you add it to the local configuration storage and then you can apply that configuration to a lock/sensor or communication hub.



When you export a configuration, you cannot change the name of the configuration, only the file name holding the configuration information. Since configurations can be shared between different Aperio Programming Applications, it is preferable that a shared configuration (identified by its unique name) also has the same meaning on all Aperio Programming Applications. It is therefore advisable that you choose the name of the configuration wisely when you store the configuration.

Exporting Configuration

1) On the File menu, select Export/Import Configurations.

Export/Import Configuration	s
Available configurations	Configuration Content
Standard lock configuration	Adding one override credentials - "Admin" MIFARE Classic: 25a78fa4 Security mode - Customer Mode Time and date - Current system time
Export	Done
	Done

- 2) Select the configuration that should be exported to file and click *Export*.
- 3) Select the folder where you want to store the configuration, select a filename and click Save.

4) Choose a password that will be used when importing the particular configuration, confirm it and click OK.

🖗 Enter Password	×			
Password Enter a password that will be used to save the configuration securely.				
Password		Export Re	lesult	2
Confirm password		i	Configuration successfully exported	to fil
OK Cancel			ОК	

Note that the password must contain at least 8 characters.

Importing Configuration

Importing a configuration takes a previously exported configuration and adds it to the local configuration storage.

1) On the File menu, select Export/Import Configurations View and click Import.

Export/Import Configuration	s
Available configurations	Configuration Content
Standard lock configuration	
Import Export	
	Done
	Done

- 2) Select a valid configuration XML-file and click Open.
- 3) Enter the password and click OK.

😔 Enter Password	×
Password Enter the password	for the configuration.
Password ••••••	
OK	Cancel



The configuration is identified by its name, not the name of the export file. When importing a configuration that already exists in the Programming Application you will be prompted if you want to replace the existing configuration.

Import R	esult 💌
?	Configuration already exist in storage. Would you like to overwrite the existing configuration?
	Yes

Deleting configuration

In the *Export/Import Configurations* view you can also delete existing configurations: Right click the configuration and select *Delete*.

Export/Import Configuration	15
Available configurations	Configura
Standard lock coefficientian	Adding o - "Admin Security - Custom Time and - Current

Upgrade of communication hub/lock/sensor firmware

This chapter describes how to upgrade communication hubs and locks/sensors with a new firmware. The upgrade procedure will be executed only for the selected communication hub or lock/sensor, depending on the content of the firmware. The firmware file only contains firmware applicable to either a communication hub or a lock/sensor.



Always upgrade the communication hub before upgrading the locks/sensors. The reason is that communication hubs should always support older lock/sensor firmware but the opposite may not always be possible.



When upgrading AH30 communication hubs to the latest firmware, when using the DIP switches for EAC addressing, always check that the DIP switch is set to the correct EAC address. If DIP 5 is active by mistake, an upgrade will result in the communication hub starting to use another EAC address.

When upgrading AH40 communication hubs to the latest firmware, Ethernet can be used to download the new firmware, provided that the AH40 communication hub IP address and other network settings has been correctly set up.

Upgrading

- 1) Ensure that you are using the latest version of the Aperio Programming Application. If not install the latest version.
- 2) Check on the UHF Link indicator that the signal strength indicator is good enough to be able to perform an upgrade (green or yellow). If you have bad signal strength (red) the Programming Application will not enable the upgrade function.

Lock	Communication Hub	EAC Address	UHF Link	
000001	024521	1		8
0148E8	024521	17		8
0148ED	024521	33		8

3) Right click on the communication hub/lock/sensor in the Installation view and select Upgrade Firmware.

Lock/sensor		Communication Hub		EAC
011C43		0216F1		
		024521	_	
0148E8 0148ED	Lock/se Comm	nsor [013542] unication Hub [024521]	•	
	Upgrad	e Firmware		

4) Select the firmware file (.afw/.fw file) and click Open.

🤏 Select firmwar	e image file				×
Look in:	🕕 Aperio firm	nware	•	🤌 📂 🛄 -	
Tidigare	Aperio2_c	:100_mifareDesfire-2.6.4.1344.a :100_mifarePlus-2.6.4.1344.afw .F_SDR-3.09.afw >100_LF_SDR-2.6.4.1199.afw	afuv K		
Skrivbord	build_c10	0_aperio2_mifarePlus-8.1.2235	7.afw		
Mina dokument					
Dator					
Nätverk	File name: Files of type:	Aperio2_c100_mifareDesfire-2.	.6.4.1344.afw .fw)		Open Cancel

5) Enter the password supplied with the firmware.

🖗 Enter i	Password 💌
Lösen Ange li	ord ösenord för filen
Lösenord	••••••
	Ok Avbryt

Result: The firmware upgrade window is shown, with a list of the units that may be upgraded. Depending on the firmware file, the list of firmware may vary. Two examples are shown below.

Weight and the second secon	
Firmware	😔 Upgrading Lock/sensor [0148E8]
Lock - Main Application Lock - Main Applic G.1.19489 Firmware Version	cation Firmware Lock - SDR
Lock - UHF 2.3.18976	Lock - SDR V Firmware Version 3.8.0
	Not started
Release Info Close	Start Release Info Close Start

6) Click on *Release Info* to get more information about the selected .afw file.

🐵 Release Info	X
Aperio Version	
2.6.1	
Description	
Lock FW file for release 2.6.1, automatically generated for devices of type 2x_c100_mifareDesfire	

The Programming Application performs a check of firmware and lock so that the firmware always match the hardware. A C100 afw file will only be used with cylinder locks. An E100 afw file will only be used with escutcheon locks etc.

7) Close the Release Info window.

8) Check that the new firmware version is higher than the firmware version currently loaded on the hardware.

🐵 Upgrading Lock/sensor [0135	42]	×
Firmware		
Lock - Main Application		Lock - Main Application
6.1.19489		Firmware Version 6.1.19489
👝 Lock - UHF	V	Progress Information
2.3.18976		Not started
Lock - Secure Area 2.6.18976	V	0%
Release Info		Close Start

No sanity check is done by the Programming Application before the firmware download starts. Applying an older firmware than installed can cause the hardware to malfunction.

9) All firmware is selected to be downloaded by default. Uncheck firmware that you do not wish to download.

rmware		
Lock - Main Application		Lock - Main Application
6.1.19489		Firmware Version 6.1.19489
Lock - UHF		Progress Information
2.3.18976		Not started
Lock - Secure Area		0%
2.6.18976	V	

10) Click Start to initiate the upgrade process.

11) If you are upgrading a lock/sensor you will be prompted to hold a credential at the lock/engage sensor before the download starts.

The Upgrading Lock/sensor [0148E8]	×
Waiting for user to Show card/Engage sensor	
Show card/Engage sensor	
Time remaining until timeout: 14 seconds	

Result: The upgrade will start with the first selected firmware in the list. A green arrow to the left of the selected firmware will indicate the firmware is being upgraded and the firmware is downloaded.

😔 Upgrading Lock/sensor [0148	E8]	×
Firmware		
👃 Lock - Main Application		Lock - Main Application
6.1.19489		Firmware Version 6.1.19489
👝 Lock - UHF		Progress Information
2.3.18976		Loading firmware
Cock - Secure Area 2.6.18976	1	4 %
Release Info		Close Start

After finished download, the device resets.



12) Click *Next* to continue with the next firmware in the list. Or click *Close* to cancel the rest of the firmware upgrade process.

Lock - Main Application 6.1.19489 Lock - UHF 2.3.18976 Lock - Secure Area 2.6.18976	✓	Lock - Main Application Firmware Version 6.1.19489 Progress Information Done 100 %
---	---------------------	--

13) After all firmware is downloaded, click Done.

The second secon				
Firmware Lock - Main Application 6.1.19489	1	Lock - Secure Area		
Lock - UHF 2.3.18976		Progress Information		
Lock - Secure Area 2.6.18976	\checkmark	100 %		
Release Info		Close Done		

Upgrade failure

A failed update is typically due to bad radio conditions. The work around is to move the USB Radio closer to the communication hub and try update again.

1) Click Save support information to file if desired and click OK to close the error message.

🐵 Upgrading Lock/sensor [01488	E8]	×		
Firmware				
Lock - Main Application		Lock - Main Application		
6.1.19489		Firmware Version 6.1.19489	6	
Lock - UHF		Progress Information		Tror occurred
2.3.18976		Not started		
☐ Lock - Secure Area 2.6.18976		0%		No response was received from the device. This could be caused by radio disturbances, please try again.
Release Info		Close Start		Save support information to file

2) Click *Retry* to try the upgrade again.

Firmware Lock - Main Application 6.1.19489		Lock - Secure Area Firmware Version 2.6.18976
☐ Lock - UHF 2.3.18976		Progress Information
Lock - Secure Area 2.6.18976	$\overline{\checkmark}$	0%
Release Info		Close Retry

Note on certificate handling in AH40 communication hub

In order to establish a secure communication between the AH40 communication hub and the ACU, TLS is used. The sequence for connecting when in manufacturer mode is the following:

- 1) The communication hub makes a TCP connection to the ACU.
- 2) ACU and communication hub will try to establish a TLS session. During TLS handshake, the ACU sends its certificate to the communication hub.
- 3) The communication hub validates and stores the certificate.

TLS specifies a number of possible cipher suites, but currently only TLS_RSA_WITH_AES_128_CBC_ SHA is supported by the communication hub. If a certificate using another cipher suite is used by the ACU, the communication hub disconnects the TCP connection.

When in customer mode, The communication hub will only accept a TLS session where the previously stored certificate is presented. If any other certificate is presented, the communication hub will disconnect the TCP connection.

Computer specifications

The Aperio Online Programming Application should be installed on a computer with the following specifications:

- Laptop
- · 32/64-bit version of Windows 7, Windows 8, Vista or XP
- USB 2.0

Files needed for the installation

- Aperio Programming Application software version 2.6.4.X
- Drivers for USB radio dongle

The software is delivered from your local ASSA ABLOY company.

Installing the Programming Application

Follow these steps to install the Programming Application and the drivers necessary for installation of the Radio dongle:

- 1) Unpack the Aperio distribution file (i.e. Aperio_Online_PAP-x.y.z.zip/Aperio_Online_PAP_US-x.y.z.zip) in a temporary folder.
- 2) Run the setup-progapp-x.y.z.exe file.

Result: The Aperio Programming Application is installed and necessary drivers for the Radio dongle are copied to the computer.



The Aperio Programming Application is bundled with Java, so no separate Java installation is required.

Installing the USB Radio Dongle Drivers Follow these steps to install the USB radio dongle driver in Windows 7. This installation procedure also works in Windows 8, Vista and XP, with identical workflow.

1) Run the TriBee_USB_Install.exe file.

Device Driver Installation Wizar	d
	Welcome to the Device Driver Installation Wizard! This wizard helps you install the software drivers that some computers devices need in order to work.
	< <u>B</u> ack <u>Next</u> ≻ Cancel

2) Verify that two USB devices has been installed.

Device Driver Installation Wizar	d		
	Completing the De Installation Wizard	vice Driver 1	
	The drivers were successfully in	stalled on this computer.	
	You can now connect your device to this computer. If your device came with instructions, please read them first.		
	Driver Name	Status	
	✓ Tritech Tritech TriBee U ✓ Tritech TriBee Driver Pa	Ready to use Ready to use	
	< <u>B</u> ack	Finish Cancel	

3) Connect the Aperio USB radio dongle device to a USB port on your laptop.



Other USB devices containing a radio (like WLAN/WiFi) connected to the laptop should be placed as far away from the USB Radio dongle as possible. If the radio link is weak, use an USB extension cable or an external USB HUB. However, wireless keyboards and mice using USB does not disturb the communication and can be used.

A check mark will appear in the left bottom corner after startup of the Programming Application, showing the connection status with the USB Radio dongle.



Updating the USB Radio drivers

To update an existing Tritech TriBee USB Driver, perform the update according to the installation section above.

If you have an older driver that works fine, you do not need to upgrade, but if you experience problems with the driver or if you are running the Aperio Programming Application on Windows 7 or Vista, you are encouraged to ensure that you are using the latest driver.

6 Regulatory Information Regarding the Aperio USB Radio Dongle

Compliance

This device complies with Part 15 of the FCC Rules and with RSS-210 of Industry Canada. Operation is subject to the following two conditions:

- this device may not cause harmful interference, and
- this device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications madeto this equipment not expressly approved by Tritech Technology AB may void the FCC authorization to operate this equipment.

According to FCC15.247

To comply with RF exposure compliance requirements, the device must not be co-located or operating in conjunction with any other antenna or transmitter.

According to FCC15.105 (b) Information to the user

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- · Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Security Statement

The following security measures are applicable to Aperio:

Authentication	3-pass mutual authentication (challenge-response protocol) based on AES128. Standard Aperio authentication scheme.
Confidentiality in communication	The communication is encrypted by a unique session key.
Confidentiality of information in the lock	Secret information such as encryption keys is never visible outside the protected flash of the microcontroller.
Encryption key	Unique encryption key seed for each installation.
Database	The encrypted database in Programming Application is password protected. The computer must also be physically protected.
Applicable tests	AES and RNG tested according to NIST (National Institute of Standards and Technology) test vectors. http://csrc.nist.gov/groups/STM/cavp/documents/rng/RNGVS.pdf http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

ASSA ABLOY is the global leader in door opening solutions, dedicated to satisfying end-user needs for security, safety and convenience

assaabloy.com/aperio

Contact

www.assaabloy.com/aperio



