# Table of Contents

1 Introduction .................................................. 4
   Purpose .................................................. 4
   Scope .................................................. 4
   Applicable Products .................................. 4
   Aperio support in the EAC system .............. 4
   Abbreviations and Definitions ................... 4
   References ............................................. 4

2 System Overview .......................................... 5
   The Aperio system ..................................... 5
   The Aperio programming application .......... 5
   Communication hub versions and EAC interface ........................................... 9

3 The Programming Application Overview ................. 6
   About the Programming Application .......... 6
   Information of encryption key ................... 6
   Main view ............................................ 7
   Status bar ............................................ 7
   Online Installation settings .................... 8
   Offline Installation Settings ................. 8
   User setting ....................................... 9
   Software version .................................. 9
   USB radio indication .............................. 9
   Installation View overview for Aperio Online ............................................. 10
   Installation View overview for Aperio Online ............................................. 11

4 Programming Application Online Functions .......... 12
   Opening/creating installations .................. 12
   Scanning and adding communication hubs 12
   Pairing locks/sensors with communication hub ........................................... 14
   Configure function - Wizard .................. 15
   RFID configuration (Lock/sensor) ............. 16
   Configure RFID Search order for V2 SE locks
   (Lock) ............................................... 19
   Escape and return configuration (Lock) ....... 29
   EAC and Network settings (AH40
   communication hub) ......................... 30
   Advanced settings - Keypad configuration (Lock). 32
   Override credential (Lock) ...................... 33
   Security Mode Settings (Communication hub
   and Lock/sensor) ............................... 38

5 Programming Application Offline Functions .......... 70
   Opening/creating installations ................. 70
   Connecting to an offline lock ................. 70
   Configure function – Wizard ................. 71
   RFID configuration .................................. 72
   DESFire Configuration .............................. 74
   General settings ................................... 75
   Schedule Open & Schedule Data ............. 76
   Security Mode Settings ....................... 79
   Change the radio channels ................... 79
   Advanced Lock Settings ....................... 81
   Device update page – Saving Configuration ... 84
   Applying a stored configuration to a lock ... 84
   System information ................................. 88
   Retrieve Event Log ................................ 90
   Retrieve Audit Trail ............................... 91
   Change lock identification details ........... 93
   Change Radio Channels ....................... 95
   Change the Security Mode .................. 96
   Factory reset .................................... 97
   Reconfiguration of lock after factory reset 98

Electronic Access Controller settings
   (Communication hub) ........................... 39
Advanced setting - Radio channel settings
   (Communication hub or Lock/sensor) ...... 41
Advanced Lock/sensor Settings - Online .... 42
Applying a stored configuration to a communication hub/lock/sensor ........ 46
Retrieve system information .................... 48
Retrieve Event Log ............................... 49
Retrieve Audit Trail ............................... 51
Change EAC address ............................ 52
Change physical location name – communication hub/lock/sensor .......... 53
Change the Security Mode .................. 55
Change the radio channels ................... 56
Setting the time of a lock ..................... 59
Change IP address (Communication hub
AH40) ............................................. 61
Import Existing Installations ................... 62
Managing configurations ....................... 62
Exporting Configuration ....................... 62
Importing Configuration ....................... 64
Deleting configuration ....................... 65
Upgrade of communication hub/lock/
sensor firmware .................................. 65
Upgrading .............................................. 66
Upgrade failure ...................................... 69


Importing and exporting configurations ..... 99
Manage Offline Lock Identification Data ...... 99
  Importing lock identification data ................. 99
Exporting lock identification data ............. 100
  Lock Identification Data XML format .......... 101
Upgrade of lock firmware .................. 101

6 Installation of Programming
Application and USB Radio dongle
firmware ...................................................... 102
  Computer specifications .................. 102
  Files needed for the installation .......... 102
  Installing the Programming Application .... 102
  USB Radio dongle firmware upgrade .... 102

7 Regulatory Information Regarding the
Aperio USB Radio Dongle ................. 103
  Compliance ........................................... 103
  According to FCC15.247 ......................... 103
  According to FCC15.105 (b) Information
to the user .............................................. 103
  Security Statement ................................ 103
1 Introduction

Purpose
The main purpose of this manual is to provide information for installation and configuration of Aperio Online/Offline based products using the Aperio 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 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. For a standard Offline system, refer to ref [3], Aperio Offline Quick Installation Guide.

This manual is applicable to version 2.6.5 of the Aperio Programming Application.

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.

Abbreviations and Definitions

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>EA</td>
<td>Electronic Access Control. The system controlling the access rules which is then conveyed to user cards through the Offline Updater.</td>
</tr>
<tr>
<td>DIP</td>
<td>Dual in-line Package. A manual electric switch used for settings on the communication hub.</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio Frequency Identification. The credential technology used.</td>
</tr>
<tr>
<td>ACU</td>
<td>Access Control Unit. The device within the EAC system that communicates with the communication hub</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security. Cryptographic protocol that provides secure communication over TCP/IP connections</td>
</tr>
</tbody>
</table>

References

2 System Overview

The Aperio system
The Aperio system is used in the following way: The user holds an RFID credential in front of an online or offline lock.
- **Aperio Online**: An online lock sends card credentials wirelessly to the communication hub which in turn communicates with an EAC (Electronic Access Control) system (wired through RS-485, Wiegand or TCP/IP). The EAC system makes the access decision. The decision is sent via the communication hub to the lock and access is granted or denied.
- **Aperio Offline**: Access decision is taken locally by lock. Result of decision depends on access rights stored on the card and also on lock configuration received from the EAC through offline updaters with setup- or user cards.

Regulatory and security information
See section 7 “Regulatory Information Regarding the Aperio USB Radio Dongle” on page 103.

The Aperio programming application
The Programming Application is used for the configuration of a door installation. It is normally installed on a laptop and is used with an Aperio USB radio dongle connected to one of the USB ports. The USB radio dongle enables the application to connect via a Communication hub to the door lock or directly to an offline lock. Online locks communicate via the Communication Hub either with the EAC or with the Programming Application.

Communication hub versions and EAC interface
There are four communication hub types according to the table below:

<table>
<thead>
<tr>
<th>Version</th>
<th>Interface</th>
<th>Maximum number of locks/sensors</th>
</tr>
</thead>
<tbody>
<tr>
<td>AH15</td>
<td>Wiegand/RS 485*</td>
<td>1</td>
</tr>
<tr>
<td>AH20</td>
<td>Wiegand</td>
<td>1</td>
</tr>
<tr>
<td>AH30</td>
<td>RS-485</td>
<td>8</td>
</tr>
<tr>
<td>AH40</td>
<td>IP (Ethernet)</td>
<td>8</td>
</tr>
</tbody>
</table>

* 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.
- Multi-language installation management tool.
- Encrypted installation database.

Refer to section "6 Installation of Programming Application and USB Radio dongle firmware" on page 102 for installation and upgrade from earlier versions.

Information of encryption key
To obtain secure communication between communication hubs and locks/sensors an Encryption key is used. This Encryption key should be handled with the same care as the Master Key in a traditional Master Key System. A person with access to the Encryption key can gain unauthorized access to any Aperio door in the system. Once loaded into the Programming Application, it will be stored encrypted in a local database and any copy should be erased from the hard drive or e-mail. It is however recommended that a copy of the encryption key is stored in safe.

The encryption key file is delivered from your local ASSA ABLOY company and should be requested on a customer/site basis.

Proper handling of encryption keys is essential to lock/sensor security!

It is absolutely necessary to use the customer encryption key by setting all communication hubs and locks/sensors in Customer mode to ensure a secure and encrypted communication with the lock/sensor.
Main view
The main view of the Programming Application consists of three areas:
- Menu bar: The buttons are used to connect to either Aperio Online communication hubs or Offline locks.
- Installation view: Displays the Aperio devices in the installation.
- Status bar

Status bar
The status bar contains the following information:
- USB Radio indication
- Date label
Online Installation settings
The Online Installation Settings (on the Settings menu) contains settings that are applicable to the current installation:

- MIFARE Classic UID format: Selected format will be used for displaying MIFARE Classic Credentials (for example in the Audit trail and Override credential dialogs).
- Configuration wizard settings: Select if the communication hub/lock/sensor should be updated with correct time during configuration.

Offline Installation Settings
The Offline Installation Settings (on the Settings menu) contains settings that are applicable to the current installation:

- USB radio channels: The radio channels that will be used when connecting to the lock.
- MIFARE Classic UID format: Selected format will be used for displaying MIFARE Classic Credentials (for example in the Audit trail and Override credential dialogs).
**User settings**

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

- **Language**: Select the language used by the Programming Application. For the language changes to take effect, restart the Programming Application.
- **USB Radio Port**: 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.

**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 dongle is ready to transmit data.

USB Radio together with a red dot indicates that the serial port or the USB radio dongle is not ok.
Installation View overview for Aperio Online

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.

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 dongle) 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.
  - Customer mode: Lock is using secure radio communication with the customer encryption key.
  - Manufacturer mode: Lock 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.
- For example: Security mode for communication hub is undefined.
- For example: The communication hub firmware (rfif) version is older than Aperio Programming Application.
- For example: The communication hub is not paired with any lock.
- For example: The security modes in communication hub and lock are not equal and should be changed, see section 'Change EAC address' on page 52.

- 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 Online Functions” on page 12 for an overview of all functions.

Installation View overview for Aperio® Offline

The installation view is the main window when working with door installations. This window is displayed after logging in to an installation and after connecting to a lock.

The following information is shown:

- **Lock**: The MAC address of the lock.
- **Lock Id**: The lock id is a unique identification number assigned to the lock.
- **Lock Group**: Lock group is a number used for managing access rights for the lock. Several locks can have the same lock group number.
- **Assigned Address**: The address the USB Radio dongle use when communicating with a lock.
- **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.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer mode</td>
<td>Lock is using secure radio communication with the customer encryption key.</td>
</tr>
<tr>
<td>Manufacturer mode</td>
<td>Lock is using insecure radio communication with the default encryption key.</td>
</tr>
</tbody>
</table>
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 via encrypted e-mail or on a USB memory stick.)

1) Insert the USB Radio dongle and start the Aperio Programming application.

2) Select File - New installation... or Open Installation... in the Programming Application.

3) For a new installation, enter a name for the installation, a password matching the requirements and finally click the button in the key file field to add the encryption key.

Proper handling of encryption keys is essential to lock/sensor security!

It is absolutely necessary to use the customer encryption key by setting all communication hubs and locks/sensors in Customer mode to ensure a secure and encrypted communication with the lock/sensor.

4) Click Create.

Scanning and adding communication hubs
1) To scan for communication hubs, click Quick Scan (F7). (If your communication hub is not found on the default channels, retry and click Scan (Ctrl+F7), which searches on all channels.)
Result: All communication hubs within reach of the USB Radio dongle of your computer are displayed in the scan result table.

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 in the window above to view detailed information.

Result: Selected communication hub(s) are displayed 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.

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/sensor and communication hub 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.

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.

- **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 byte 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:
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 UID**

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

- **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 byte 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 byte, in this particular case: 00112233445566778899AABBCCDDEEFF. The configuration should look like this:
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*.
Select DESFire in the RFID Card Type drop down list.

- **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 byte. Minimum length is 1 and the maximum length supported by the Aperio lock is 30 byte (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 byte keys, 3K3DES is a 24 byte 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**:

```
KEY AES-128 nr: 0
AUD: 1235 0bf1232040567899aabbccccddee
FID: 1
FID: 2 Encrypted
    17101234
FID: 3
```

The configuration should look like this:
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.
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

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 of characters. 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 byte: Specifies the number of byte 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 byte 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 byte  
Checksum: CRC 16 byte 0-5  
Checksum address: 6
Segment 1:
Search String: 30 03 00 09
Segment type: Access
Data length: 24 byte
Checksum 1: CRC 16 byte 0-10
Checksum 1 address: 11
Checksum 2: CRC 16 byte 13-21
Checksum 2 address: 22

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 byte
Checksum: CRC 8 byte 0-6
Checksum address: 7
Configure RFID Search order for V2 SE locks (Lock)

When using V2 SE locks the search order of used RFID protocols can be specified. By enabling only the protocols used, energy consumption and user waiting time can be reduced.

V2 locks does not support this setting.

1) To enable and/or change search order of RFID protocols click Change...

2) Select the protocols used and/or use the arrows to set the order the lock will perform a reading of a credential.

Important about RFID Search Configuration

If the RFID Search Configuration is done wrong, the lock may become inoperable. Be careful before changing these values. This configuration is supported by V2SE locks only.

The lock search for credentials using different RFID protocols (14443A, 14443B, 15693). This panel is used to change the default search order and to enable/disable specific protocols. Follow these guidelines:

- In installations where only one credential is used: Only enable corresponding RFID protocol.
- In installations with credentials using different RFID protocols: Change order so the most frequent RFID protocol is searched first.
- In installations where credential use may change over time: Do not change default configuration.

The mapping between RFID protocols and credentials are as follows:

- ISO/IEC 14443A: MIFARE Classic, MIFARE DESFire, MIFARE Plus, iCLASS SEOS
- ISO/IEC 14443B: UID only
- ISO/IEC 15693: iCLASS
Escape and return configuration (Lock)
This function allows the lock to remain unlocked a certain time after the door have been opened from the inside.

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

1) To set Escape and return configuration, click Change...

2) Select desired settings:

- **Enable handle detection**: Enables the lock to register which handle was used to open the door, the inside or outside handle (lock side).
- **Escape and return**: Activate this function to either be Disabled or Enabled (in lock).
- **Default unlock time (seconds)**: The time the lock is unlocked. Default is 240 seconds.
EAC and Network settings (AH40 communication hub)
This window only applies for AH40 communication hub (IP) in order to set the network and ACU settings for the installation site. This will allow maintenance such as firmware upgrade of the communication hub through the local network, instead of using the USB radio dongle.

Network settings

For correct settings contact your network administrator:
- **Network Mask**: Network mask for the local network in IPV4 format, normally 255.255.255.0.
- **Default Gateway**: Default gateway for the local network in IPV4 format.
ACU settings

For correct settings contact your network/EAC administrator:

- **Address**: Network address for the EAC/ACU on the network: For example 192.168.0.155.
- **Port**: The TCP port of the EAC used for communication. Default value is 9990.
- **Enable TLS**: This setting provides secure communication between the EAC/ACU and the IP AH40 communication hub. The default value is enabled. Note that TLS must be enabled to allow customer mode to be set in the IP AH40 communication hub.

In order to establish a secure communication between the 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 Hub will try to establish a TLS session. During TLS handshake, the ACU sends its certificate to the Hub.

3) 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 Hub. If a certificate using another cipher suite is used by the ACU, the 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.
Advanced settings - Keypad configuration (Lock)

This window is only visible if Show advanced settings is activated in User Settings window, see section “Online installation settings” on page 8.

1) Click Change to enter specific Keypad configuration.

2) Choose between two reading modes:

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

- **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 lock.

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

- When adding an override credentials in the lock all existing override credentials are removed from the lock.

**Tip:** You do not have to enter the override credential data manually for every lock 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**.

Set 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.

**Configure Lock/minor (003142)**

![Override Credential](image)

Add and replace override credentials. If no changes are made, the credits that are in the lock will be left unchanged. Note that the list below does not show override credentials currently loaded into the lock. If you load new cards into the lock, the old cards are replaced. Click **Next** to continue.
**MIFARE UID**

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

**MIFARE Sector**

- **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

- **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

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

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

**iCLASS**

- **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.

**HiQ prox and EM prox**
- **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**

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

**Seos**

- **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**

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

- **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.

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**.
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. Note that for IP AH40 communication hubs, TLS must also be enabled to allow customer mode to be set.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer mode</td>
<td>Lock is using secure radio communication with the customer encryption key.</td>
</tr>
<tr>
<td>Manufacturer mode</td>
<td>Lock is using insecure radio communication with the default encryption key.</td>
</tr>
</tbody>
</table>

Electronic Access Controller settings (Communication hub)
The following options apply for both RS-485 and Wiegand unless specified. Click Change... for each option, to enter the settings.

**EAC Addressing Mode (RS-485 only)**

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, 2, 3, 4, 5, 6, 7, 8 (communication hub 1), (9-16 for communication hub 2, 17-24 for communication hub 3 and so on).
**Lock Access Decision Timeout**

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

**Remote unlock**

This function enables the Remote unlock functionality in the communication hub.

- **Default unlock duration for Wiegand**: Enter the time the lock will be unlocked after the lock performs a status report. To deactivate Remote Unlock, set the time to 0. This setting only applies for Wiegand communication hubs. (Unlock duration is set in the EAC for RS-485 communication hubs.)
- **Time to live**: The time for how long the Remote unlock command will be present in the communication hub. (This setting must always be longer than the Status Report interval set in the lock. This setting only applies for RS-485 communication hubs. The maximum value is 17 hours and 59 minutes.

**RS-485 communication hubs (firmware version 2.6.5 or later)**: Remote unlock is by default enabled in the communication hub.

**RS-485 communication hubs (firmware version earlier than 2.6.5)**: Activate Remote unlock by clicking OK, since this is disabled in the firmware by default.

**Enable EAC Address via DIP Switch (RS-485 only)**

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 - Online

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 Battery Check Interval

The battery power check 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 adjust the time interval for this check depending on the type of battery used and the surrounding temperature, e.g. in cold surroundings the battery runs out faster. Default value is 60 (minutes).

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**

This setting applies to both lock/sensor and communication hub.

The interval setting is normally set to 60 minutes. If Remote Unlock functionality is used, this parameter should be set to a shorter interval such somewhere in between 5 and 15 minutes or depending on the time the remote unlock command is present in the communication hub.

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

As the status report 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. If one lock is paired with the communication hub, this is done automatically.

If more than one lock is paired with the communication hub (AH30 and AH40) the status report interval must be set through the communication hub right-click menu to a value equal or higher then the longest interval of the locks paired.

**Locking Parameters**

This dialog allows you to 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, 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**

Configure the way in which the lock indicates a card read. Please note that you must know what card read indication capabilities the selected lock has since not all options are applicable to every type of lock. Initial values shown here are just default values. The

<table>
<thead>
<tr>
<th>Card Read Indication</th>
<th>LED</th>
<th>Buzzer</th>
<th>LED and buzzer</th>
</tr>
</thead>
</table>

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 Events**

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**

The following updates will be transmitted to the Aperio Lock (sensor):

- Keypad
  - Disable
- Adding one override credentials
  - "User" "MIC600" Class: 1:23:56:78
- Card read indication
  - LED
- Time and date
  - Current system time

Save Configuration...
The Device Update dialog 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. Exclude configuration tasks by clicking the check boxes.

   ![Save Configuration dialog box](image)

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.

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.

   ![Configuration name field](image)

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.

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.
2) Click **Confirm** to download the selected configuration to the unit.

![Device update confirmation](image)

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

![Show card/engage sensor](image)

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

![Device update result](image)

5) Repeat all the steps from the beginning of this section for every lock/sensor you want to configure with a saved configuration. Click **Close** to finish.
Retrieve system information
This function is available for both communication hub and lock/sensors.

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

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.
Retrieve 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 – Retrieve 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.
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.)
Retrieve 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 – Retrieve Audit Trail.

2) Hold the credential at the lock.

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.

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.

**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*.

![](image1)

2) Select the address and click *OK*.

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

![Description entry screen]

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.

![Show card/Engage sensor message]

**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.
Change 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:

- **Customer mode**: Lock is using secure radio communication with the customer encryption key.
- **Manufacturer mode**: Lock is using insecure radio communication with the default encryption key.
- **Conflicting mode**: The modes in the lock/sensor and the communication hub are not the same.

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.

![Device update result](image)

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

AH40 communication hubs must be connected to an EAC system to accept change of security mode. If not so, the following error message is shown:

![Device update result](image)

### Change 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 check box checked in User Settings, see section "Online Installation settings" on page 8. 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.

![Change radio channels](image)
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.

3) Hold the credential at the lock, or engage the magnet for the sensor to change radio channels.

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.

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.
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.
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 – Online Installation Settings... and check that the Update device time during configuration checkbox is checked.

3) Close the Online Installation Settings view. Right-click and select Lock/sensor-Configure. Click Next repeatedly until you reach the Device Update window.
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.
Change IP address (Communication hub AH40)

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

2) Fill in the IP address of the IP 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.
Import Existing Installations

1) To import an existing Aperio installation including security keys and configurations, select File-Import Installations...

2) Select the location by clicking the button. Your current installations will not be deleted.

Managing configurations
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 Manage Configurations...
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 file name and click Save.

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

**Result:**

- The password must contain at least 8 characters of which at least one upper and lower case character and a number.
Importing Configuration

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

1) On the File menu, select Manage Configurations...

2) Click Import...

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

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.

Deleting configuration
In the Manage Configurations view you can also delete existing configurations: Right-click the configuration and select Delete.

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 that use the DIP switch for EAC addressing, always check that the DIP switch is set to the correct EAC address. If DIP 5 (Pairing mode) is active by mistake, an upgrade will result in that the communication hub starts using a different 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.

After firmware upgrade of all communication hubs versions always perform a Rescan to ensure that the Aperio Programming Application is sync with any new feature in the upgraded communication hub.
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.

<table>
<thead>
<tr>
<th>Lock</th>
<th>Communication Hub</th>
<th>EAC Address</th>
<th>UHF Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>000001</td>
<td>024521</td>
<td>1</td>
<td>green</td>
</tr>
<tr>
<td>01 RED</td>
<td>024521</td>
<td>17</td>
<td>yellow</td>
</tr>
<tr>
<td>02 RED</td>
<td>024521</td>
<td></td>
<td>red</td>
</tr>
</tbody>
</table>

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

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

5) Enter the password supplied with the firmware.
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.

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

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.

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.
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.

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.

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.

13) After all firmware is downloaded, click 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.

2) Click Retry to try the upgrade again.
5 Programming Application Offline Functions

Opening/creating installations
An installation is a password protected set of settings you need when you want to communicate with 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.)

1) Insert the USB Radio dongle and start the Aperio Programming application.

2) Select File - New installation... or Open Installation... in the Programming Application.

3) Enter a name for the installation, a password matching the requirements and finally click the button in the Key file field to add the Encryption key.

4) Click Create.

Connecting to an offline lock
Follow these steps to connect to an offline lock:

1) Click Connect in the Offline section of the menu bar.
2) Hold the radio activation card at the lock (or remove and reinsert the battery).

**Result:** Detailed information is downloaded and the Programming application connects to the lock.

Configure function – Wizard

1) Select a lock in the scan result table, right-click and select Configure...

2) Click Next after completion of each dialog in the Configuration Wizard.

The following sections describe each window in the wizard.
RFID configuration

Select the tab depending upon the lock type. Only one type of configuration can be sent to the Lock. Click Add/Change... to enter the settings for each card format.

MIFARE Classic configuration

MIFARE Classic configurations is a part of the Lock-Unit setup information that describes which MIFARE sectors are to be used by the Aperio Offline application. This configuration screen allows the user to specify a MIFARE ‘B’ key and configure the MIFARE-sector usage (system sector, alarm sector, schedule open sector).

If MIFARE RFID configuration is done wrong, the lock may become inoperable.
Key configuration:
- **MIFARE key B**: Enter the 6 byte long hexadecimal MIFARE Classic Key B that applies for the user cards in your installation. Example: AABBCC112233.

Sector configuration:
- **Total number of sectors**: Enter the total number of sectors to be used on the card.
- **Number of alarm sectors**: Enter the number of alarm sectors reserved on access cards used on the particular site.
- **Number of scheduled open sectors**: Enter number of scheduled open sectors reserved on access cards used on the particular site.

After adding the number of sector used, click the *Physical number* drop down menu to select/change a physical number for each sector.

Physical numbers not used are free to be used by other applications.
System limitation

The sector configuration settings affect the number of lock groups that can be used (see section “Change lock identification details” on page 93).

Plan your sector configuration with the following limitations in mind:

<table>
<thead>
<tr>
<th></th>
<th>MIFARE Classic 1K</th>
<th>MIFARE Classic 4K</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max lock units</td>
<td>65536</td>
<td>65536</td>
</tr>
<tr>
<td>Max lock groups</td>
<td>1344</td>
<td>5088</td>
</tr>
<tr>
<td>Max alarms</td>
<td>84</td>
<td>420</td>
</tr>
</tbody>
</table>

Having max lock groups means no alarms and vice versa since they share the same storage space on the credential.

It is up to the system owner to ensure that the appropriate number of sectors needed to represent all doors is reserved on all user credentials in the system.

It is recommended to reserve extra sectors not reserved for alarms/schedules, in order to obtain space for lock group addressing. Each free sector allows 96 lock groups (MIFARE Classic 1K card).

DESFire Configuration

- **Application ID:** Identification number for the Aperio Offline application on the MIFARE DESFire cards used in the system. A MIFARE DESFire card can have up to 32 applications. Application IDs range from 0 to 16777215.
- **File Data Protection Level:** Security level for the communication between lock and card. Choose one of the two options (Data Authenticity by MAC, Full Encryption) depending on how the cards used in the system are configured.
- **Number of alarm slots:** Numeric value representing number of alarm slots on access cards used in the system.
- **Number of scheduled open slots:** Numeric value representing number of scheduled open slots on access cards used in the system.
- **Number of lock groups:** Numeric value representing maximum number of allowed lock groups on access cards used in the system.
- **Key Type:** Choose one of the three options (2K3DES, 3K3DES, AES-128) depending on the cryptographic algorithm used to read/write data from/to the card. Type the key value in hexadecimal. 2K3DES and AES-128 are 16 byte keys. 3K3DES is a 24 byte key.
- **Key:** MIFARE DESFire key that applies for the user cards in your installation in HEX format. Example: 011234456677889aabbccddeeff
- **Key Number:** Each application can use up to 14 keys. Key 0 is always the Application's Master Key. Type here which key number that is used for the Aperio Offline application on the MIFARE DESFire cards. Key numbers range from 0 to 13.

**System limitation**

It is up to the system owner to assure that there is space enough on the access cards used for the actual system configuration. Possible configurations are dependent on the size of the MIFARE DESFire EV1 cards used in the system and if they are used for other applications than Aperio Offline.

Plan your sector configuration with the following limitations in mind:

<table>
<thead>
<tr>
<th></th>
<th>MIFARE DESFire 2K</th>
<th>MIFARE DESFire 4K</th>
<th>MIFARE DESFire 8K</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max lock groups</td>
<td>4000</td>
<td>8096</td>
<td>16288</td>
</tr>
<tr>
<td>Max alarm slots</td>
<td>250</td>
<td>506</td>
<td>1018</td>
</tr>
<tr>
<td>Max scheduled open slots</td>
<td>500</td>
<td>1012</td>
<td>2036</td>
</tr>
</tbody>
</table>

Having max lock groups means no alarms and vice versa since they share the same storage space on the credential.

**General settings**

- **Site code settings:** Each site has a unique code number that all credentials within the system share. It is a mandatory field on the screen where the user is allowed to enter only 12 (max) digit numeric values.
- **Time zone settings:** Select the time zone where the access system is located.
Schedule Open & Schedule Data

Configure Scheduled open settings & schedules
Provide start and end internal time for scheduled open settings. Uploading schedule end data to the lock will set schedule on the lock.

Change scheduled open settings

- **Start time**: Start time for when the lock can be activated for scheduled open (For when access cards with scheduled open functionality can set the lock to be open).
- **End time**: End time for when the lock responds to scheduled open attempts. It is also the time when the lock goes back to locked state after being scheduled open unlocked.

The schedule open function has several options, please refer to the Aperio Offline System Description manual for more details.
Upload schedule data
With this function schedules are enabled in the lock. The schedules for the specific access system are specified in an XML-file.

1) Click Select and then open to select XML with schedule data from your system/network to be uploaded.

Schedule file selected should have data in correct format according to specified XML structure, see below.

2) Check that the schedule data is correct.
Schedule Data XML format

Follow these guidelines when creating XML file for defining schedule data:

- File containing schedule data should be in XML format.
- Schedule data file should have xml extension (ex. schedule_data.xml).

Rules for Schedule data

<table>
<thead>
<tr>
<th>Tag/Attribute Name</th>
<th>Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;year&gt;(Exceptions)</td>
<td>Value should be greater than or equal to the current year.</td>
</tr>
<tr>
<td>&lt;daytype&gt;(Exceptions&gt;&gt;Year&gt;&gt;Entry)</td>
<td>Value should be in the range 0-63 (inclusive).</td>
</tr>
<tr>
<td>&lt;startdate&gt;&amp; &lt;enddate&gt;(Exceptions&gt;&gt;Year&gt;&gt;Entry)</td>
<td>Values specified should be in YYYY-MM-DD format. &lt;startdate&gt; value should be less than or equal (in case of a single day exception) to &lt;enddate&gt; value. Year specified in &lt;startdate&gt; &amp; &lt;enddate&gt; tags should always be same as the above &lt;year&gt; tag value.</td>
</tr>
<tr>
<td>daynumber(Weekdays&gt;&gt;Day)</td>
<td>Value specified should be in the range 0 (Mon) - 6 (Sun) inclusive.</td>
</tr>
<tr>
<td>daytype(Weekdays&gt;&gt;Day)</td>
<td>Value specified should be in the range 0-63 (inclusive).</td>
</tr>
<tr>
<td>&lt;schedule&gt;(Schedules)</td>
<td>Number value specified should be in the range 2-15 (inclusive). Type value should only be a numeric value.</td>
</tr>
<tr>
<td>&lt;type&gt;(Schedules&gt;&gt;schedule)</td>
<td>Only two types of schedules are allowed 0 (Default access schedule), 1 (Schedule open). There can be only one type=&quot;1&quot; (Schedule open) schedule in the XML. There can be any number of type=&quot;0&quot; (default Access) schedule in the XML.</td>
</tr>
<tr>
<td>&lt;daytype&gt;(Schedules&gt;&gt;schedule)</td>
<td>Value specified should be in the range 0-63 (inclusive).</td>
</tr>
<tr>
<td>&lt;start-interval&gt; &amp; &lt;end-interval&gt;(Schedules&gt;&gt;schedule&gt;</td>
<td>Time should be specified in HH:MM 24 hour format. Data should always be entered in terms of quarter of the day. &lt;start-interval&gt; should signify start of the quarter time hence MM value should be one of these values (0,15,30,45). &lt;end-interval&gt; should signify end of the quarter time hence MM value should be one of these values (14,29,44,59).</td>
</tr>
</tbody>
</table>

The Aperio Programming Application F1-help contains a complete example of a Schedule data XML-file.
Security Mode Settings

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, click the check box and click OK.

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

Change the radio channels

Changing the radio channel can be necessary if you experience interference between lock and USB Radio dongle.

To use this function, you must have the Show advanced settings checkbox checked in User Settings, see section "Online Installation settings" on page 8. Follow these steps to change the radio channel for the communication hub and lock/sensor:
1) Select the lock in the scan result table. Right-click and select Change radio channels...

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.
3) Hold the radio activation card at the lock (or remove and reinser t the battery) 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.

To change radio channel in USB Radio Dongle, see section “Offline Installation Settings” on page 8.

**Advanced Lock Settings**

On this page you will be able to configure **Battery Check Interval**, **Status Report Interval**, **Locking Parameters**, **Card Read Indication** and **Configure Toggle Mode**.
Battery Check Interval

The battery power check 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 adjust the time interval for this check depending on the type of battery used and the surrounding temperature, e.g. in cold surroundings the battery runs out faster. Default value is 60 (minutes).

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.

Locking Parameters

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 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

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.

Configure Toggle mode

If a lock is set in toggle mode then it will work exactly like a normal mechanical lock. Showing an access card will open the lock until the user shows the card again to close it. Toggle mode is by default turned off.
Device update page – Saving Configuration

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 the lock. 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. Exclude configuration tasks by clicking the check boxes.

2) Recommended tasks to save could be:
   a) RFID configuration
   b) Change security mode
   c) Device time update
   d) 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.

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.

4) Click OK.

Result: The configuration is saved in the local storage, and you are back in the Configuration Wizard. Choosing Cancel on the Device Update page does not affect the locally stored configuration.

5) Click Next to download the configuration to the lock.
6) Hold the radio card at the lock (or remove and reinset battery).

7) Click Close to exit the wizard.
Applying a stored configuration to a lock

If you saved a configuration in the configuration wizard, you can apply it to numerous locks. Follow these steps to download a saved configuration to a lock:

1) Connect to another lock that you want to apply a saved configuration on. In the installation view, right-click the new lock and select Apply configuration and choose an earlier stored configuration.

2) Click Confirm to start the transfer.

3) Hold the radio activation card at the lock (or remove and reinsert the battery) to download the configuration.
4) After download the result is shown. The settings that could not be downloaded to the specific hardware are ignored. Click OK to finish.

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

Retrieve system information

1) Right-click and select Retrieve system information to access the unit.
2) Hold the radio activation card at the lock (or remove and reinsert the battery) to access the unit.

Result: The Programming Application connects to the unit.

3) Click Save as... to save the system information to a local storage or click Close to exit.
Retrieve 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-Retrive Event Log

2) Hold the radio activation card at the lock (or remove and reinset the battery).

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

4) In the event log window, click Save As to save the information to a txt file or click Close to exit without saving.
This window contains a listing of the recent system events along with the date when it was observed. (If the number of events exceeds 200, older events are overwritten.)

Retrieve Audit Trail
This function displays a complete list of all access attempts for a particular lock.

1) Right-click and select Retrieve Audit Trail.
2) Hold the radio activation card at the lock (or remove and reinsert the battery).

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.

This window contains a listing of the total number of access attempts showing date, access decision and credential type.
Change lock identification details
This menu option will allow the user to change Lock ID, Group & Physical location. Lock ID is used as an identifier for each lock. Lock Group is used to cluster several locks for example in order to create access areas, where all the locks in one group will use the same access settings. Physical location is just a logical name for the lock.

The maximum number of lock groups is decided by the sector configuration done in the configure lock function, see section RFID configuration.

1) Select the lock, right-click and select Change Lock Identification Details.

2) User should always set RFID configurations (see section RFID configuration) before changing/adding lock identification details. However if a user tries to set lock identification details before setting RFID configurations then following screen will be shown to the user.
3) Set lock identification details either **Manually** or through **Imported data** by selecting one of the radio buttons.

   a) **Manually:** Enter **Physical Location** (max 20 alpha numeric characters), **Lock Id** (max 5 numeric characters), **Lock Group** (max 5 numeric characters & max value decided by RFID configurations).

   b) **Imported data:** This option can be used if lock identification details have been imported using the function File-Manage Offline Lock Identification Data, see section "Manage Offline Lock Identification Data" on page 99. After import, lock identification details will automatically be displayed here. Select lock identification details in the list by clicking the desired row.
4) Hold the radio card at the lock (or remove and reinsert battery) to download the Physical location data.

Change Radio Channels
Changing the radio channel can be necessary if you experience interference between lock and USB Radio dongle.

To use this function, you must have the Show advanced settings check box checked in User Settings, see section User settings. Follow these steps to change the radio channel for the lock.

1) Select the lock in the scan result table. Right-click and select Change Radio Channels....
2) Uncheck any of the three currently used channels to be able to select other radio channels. Click OK.

3) Hold the radio activation card at the lock (or remove and reinsert the battery) 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.

To change radio channel in USB Radio Dongle, see section "Offline Installation Settings" on page 8.

Change the Security Mode
This procedure is equal as for Aperio Online. See section "Change the Security Mode" on page 55.
Factory reset

When a factory reset is performed, lock id, lock group, site code, sector information, logs and the RFID Key(s) are erased from the lock. To reconnect and configure a lock that have been reset, you need to remove and reinstall the battery to activate the UHF transceiver in the lock.

1) Select lock, right-click and select Factory reset.

2) Confirm the reset by clicking Yes.

3) Hold the radio activation card at the lock (or remove and reinser t the battery) to download the change.

Result: The lock is reset and disappears from the installation view.
Reconfiguration of lock after factory reset
To reconfigure a lock that has been reset without use of a factory default radio activation card:

1) Dismantle the lock cover and remove the battery from the lock.

2) Reinstall the same battery.
   **Result:** The lock performs a power on self test, one red and one green flash. After that the UHF transceiver is activated - yellow blinking during 20 s.

3) When the lock starts blinking yellow, click Connect in the menu bar.

4) When the lock is visible in the installation view, select the lock, right-click and select Configure. (Or Apply configuration [your configuration] if it contains your MIFARE Classic/DESFire Key configuration.)

5) On the first page in the Wizard, in the Change RFID Key configuration section, click Change and add the MIFARE Classic/DESFire configuration (see section “RFID configuration (Lock/sensor)” on page 16), depending upon the type of lock that you have.

6) Repeatedly, click Next on the rest of the pages in the Wizard until the download starts.

7) Hold the radio activation card at the lock (or remove and reinset the battery) to download the change.

After this the lock is updated with the MIFARE Classic/DESFire key that applies for your system.

Reconfigure the lock with the settings needed. Lock identification details must also always be reconfigured after a factory reset, see section ‘Change lock identification details’ on page 93.
Importing and exporting configurations
This procedure is equal as for Aperio Online, see section "Managing configurations" on page 62.

Manage Offline Lock Identification Data
This function allows import of lock identification data from an EAC system in the form of an XML. After installation, the lock identification data (changes made during installation on the site) is exported back for use in the EAC system.

Importing lock identification data

1) Select File-Manage Offline Lock Identification Data.

2) Click the Import... button to open the XML-file created by the EAC or manually (according to specified XML structure, see section "Lock Identification Data XML format" on page 101).
Result: The lock identification data is displayed. Exit the dialog by clicking OK.

Exporting lock identification data

1) Select File-Manage Offline Lock Identification data.

2) Click the Export... button to save the installation performed.
Lock Identification Data XML format

Follow these guidelines when creating XML-file for defining lock identification data:

- Data file to be uploaded should contain list of lock identification data which will be imported into the system and can further be used to assign to different locks.
- File containing data should be in XML format.
- Data file should have xml extension (e.g., door_data.xml)

Description of data

<table>
<thead>
<tr>
<th>Tag/Attribute Name</th>
<th>Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;number&gt;</td>
<td>A unique numeric value that is used to identify the lock on the site.</td>
</tr>
<tr>
<td>&lt;group&gt;</td>
<td>A numeric value representing the group that the lock belongs to. There can be multiple locks in a group.</td>
</tr>
<tr>
<td>&lt;description&gt;</td>
<td>A logical description for the lock.</td>
</tr>
<tr>
<td>&lt;mac&gt;</td>
<td>Represents the Mac address of the lock that has this identification data (number/group). An empty value for this tag will signify that this lock identification data can be assigned to a lock.</td>
</tr>
</tbody>
</table>

Sample data file content

See the F1-help in the Aperio Programming application for an example.

Lock Identification Data Import XSD

See the F1-help in the Aperio Programming application for XSD content.

Upgrade of lock firmware

This procedure is equal as for Aperio Online, see section "Upgrade of communication hub/lock/sensor firmware" on page 65.
6 Installation of Programming Application and USB Radio dongle firmware

Computer specifications
The Aperio 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 2.6.5.X
- Encryption key file

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.

USB Radio dongle firmware upgrade
The USB radio dongle firmware version is checked both during installation of the Aperio Programming Application and when starting the application. An upgrade is automatically initiated if the USB radio dongle has an older firmware version than the current Programming application:

1) Click OK to perform firmware upgrade (or Cancel to close the application).
2) The USB radio dongle is upgraded with the latest firmware.
3) Click OK after successful upgrade, to start the Programming application.
### 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 made to 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.

### Security Statement

The following security measures are applicable to Aperio:

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality in communication</td>
<td>The communication is encrypted by a unique session key.</td>
</tr>
<tr>
<td>Confidentiality of information in the lock</td>
<td>Secret information such as encryption keys is never visible outside the protected flash of the micro controller.</td>
</tr>
<tr>
<td>Encryption key</td>
<td>Unique encryption key seed for each installation.</td>
</tr>
<tr>
<td>Database</td>
<td>The encrypted database in Programming Application is password protected. The computer must also be physically protected.</td>
</tr>
<tr>
<td>Applicable tests</td>
<td>AES and RNG tested according to NIST (National Institute of Standards and Technology) test vectors.</td>
</tr>
</tbody>
</table>
ASSA ABLOY is the global leader in door opening solutions, dedicated to satisfying end-user needs for security, safety and convenience.

assaabloy.com/aperio