ASSA ABLOY

Aperio® Programming Application Manual

Document No: D000732077 rev 12 Date: 2022-02-04

aperio®

The global leader in door opening solutions

Table of Contents

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 possible 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 27.0 of the Aperio Programming Application.

Applicable Products

The Aperio Program Application can be used for all versions of communication hubs, locks and sensors.

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

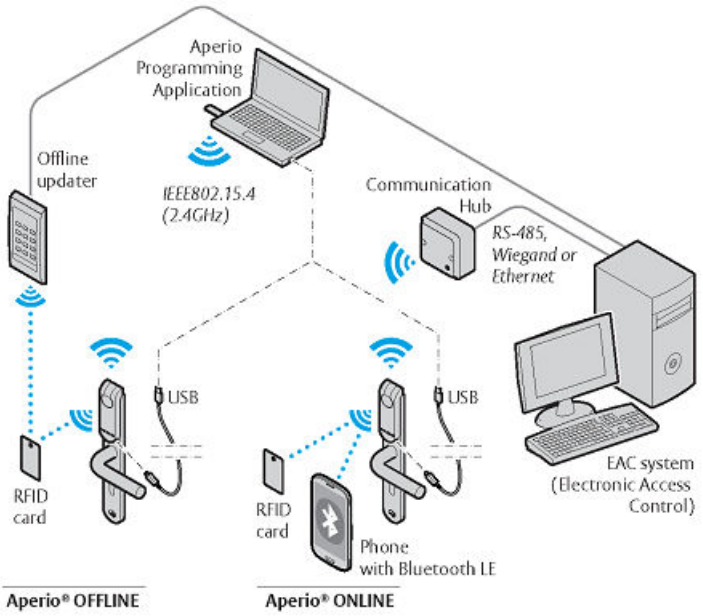
Abbreviation	Definition
EAC	Electronic Access Control. The system controlling the access rules which is then conveyed to user cards through the Offline Updater.
DIP switch	Dual in-line Package. A manual electric switch used for settings on the communication hub.
RFID	Radio Frequency Identification. The 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.
OSS	Open Security Standard. Credential standard for offline locks.
V2	Generation 2 of the Aperio platform.
V2SE	Generation 2 of the Aperio platform using HID SE.
V3	Generation 3 of the Aperio platform.

References

Ref [1]	D000732079-Aperio Online Mechanical Installation Guide
Ref [2]	D000732078-Aperio Online Quick Installation Guide
Ref [3]	ST-001802-Aperio Offline Quick Installation Guide

2 Aperio System Overview

Figure 1: Aperio technology 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 System**: 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 System**: Access decision is made locally by the lock. Result of decision depends on access rights stored on the card and also on lock configuration transferred from the EAC through offline updaters with setup- or user cards.

The Aperio programming application

The Aperio 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 Aperio programming application uses the USB radio dongle to connect to a communication hub and an online lock (via the communication hub) or directly to an offline lock. V3 locks also supports a USB cable connection.

Communication Hub Versions and EAC interface

There are four communication hub types:

Version	Interface	Maximum number of locks/ sensors
AH15	Wiegand/RS 485 [1]	1
AH20	Wiegand (Adv., Std.)	1
AH30	RS-485	8/16[3]
AH40	IP (Ethernet)	8/16[2]/64[3]

[1] The firmware type loaded into the communication hub controls what interface is enabled.
[2] Applicable for release 3.0.0 and onwards.
[3] Applicable for GEN5 communication hubs.

3 The Aperio Programming Application Overview

About the Aperio Programming Application

- Software running under 32-bit or 64-bit versions of Windows 8, Windows 8.1, or Windows 10.
- Multi-language installation management tool.
- Encrypted installation database.

All testing is done on desktop and laptop PC:s, no validation is made on mobile phones, tablets etc.

Regular Offline Classic or Offine Desfire products follows the layout of user card that is specified by ASSA ABLOY where as OSS Classic, OSS Desfire and OSS Legic products are based on OSS standard.

Refer to section *Installation of Aperio Programming Application and USB Radio Dongle Firmware* on page 148 for installation and upgrade from earlier versions.

Encryption Key

To obtain secure communication for an Aperio system (communication hubs, locks/sensors and Aperio Programming Application) 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 Aperio 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 a safe.

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

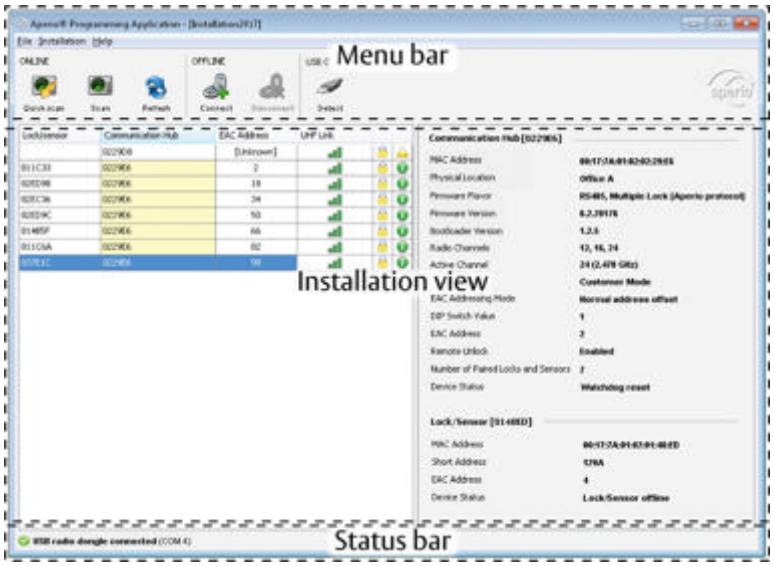
Proper handling of encryption keys is essential to lock/sensor security!

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 Aperio 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:** Information of USB radio dongle connection.



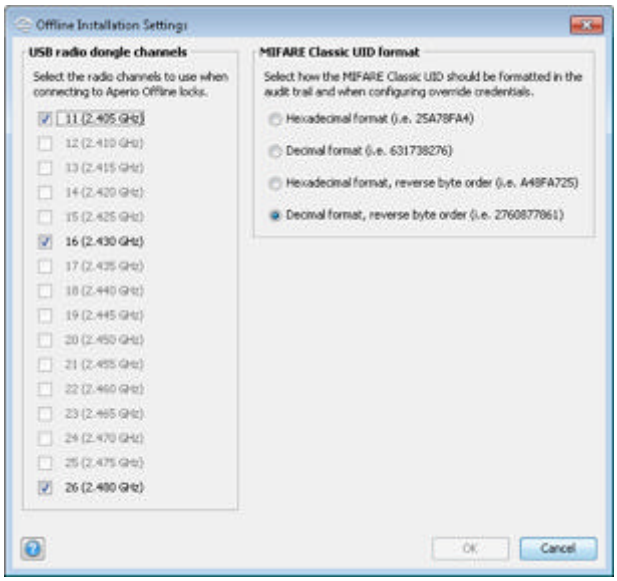
Online Installation Settings

The Online Installation Settings contains settings that are applicable to the current installation. In the menu bar, select ***Installation*** → ***Online*** → ***Settings...***:

- **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 contains settings that are applicable to the current installation. In the menu bar, select ***Installation*** → ***Offline*** → ***Settings...***:



- **USB radio dongle 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).

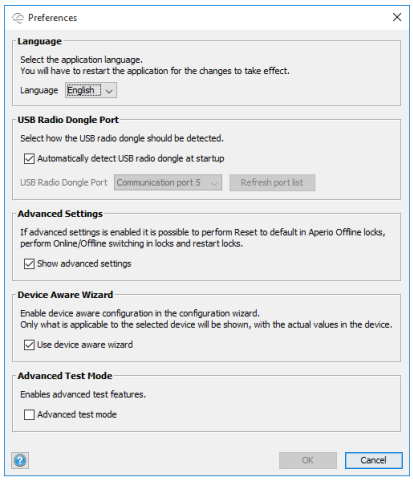
Change Password

To change password for the current installation, select ***Installation*** → ***Change Password...*** in the menu bar:

The password must contain at least 8 characters of which at least one upper and lower case character and a number. The installation name can not be used as password.

Preferences

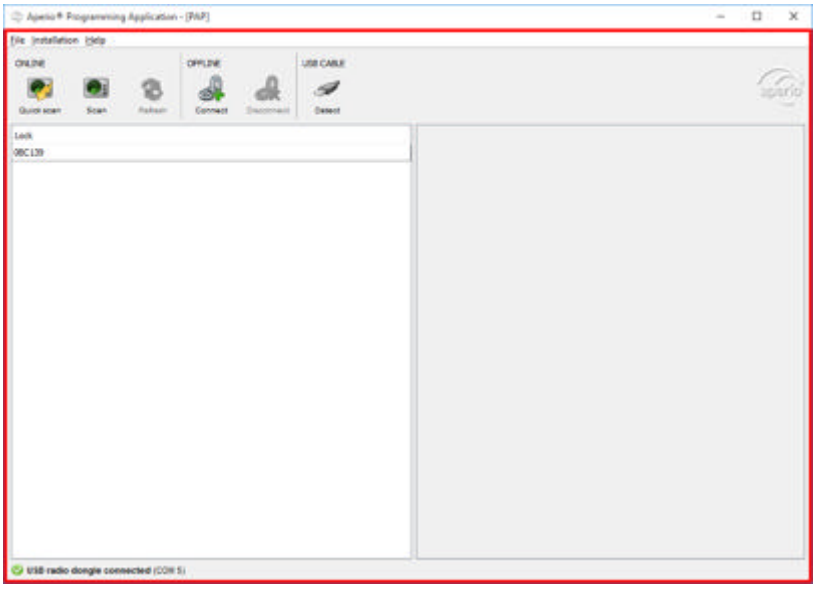
The preferences dialog contains settings that are applicable to all the installations. In the menu bar, select ***File*** → ***Preferences...***:



- ***Language***: Select the language used by the Aperio Programming Application. For the language changes to take effect, restart the Aperio Programming Application.
- ***USB Radio Dongle Port***: The Aperio Programming Application automatically detects USB radio at start up: Unselect this option to manually specify the port used by the USB radio dongle, in case of a hardware conflict.
- ***Advanced Settings***: Activate the advanced menu functions, factory reset for offline locks, and switching between online and offline operating mode for Aperio locks.
- ***Device Aware Wizard***: Detects the applicable features for the connected device and their current settings.

  The ***Device Aware Wizard*** function is enabled by default after installing the application.

- ***Advanced test mode***: Activates special test functions such as the test function ***Set Energy Counter***. See *Set Energy Counter* on page 79. ***Advanced test mode*** is indicated by a red frame in the main application window.



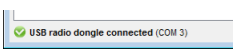
Software Version

To check the version of installed software, in the menu bar select ***Help*** → ***About Aperio Programming Application***:

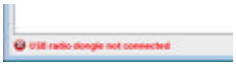
To view the open source licenses used by the Aperio Programming Application, click ***View open source licenses***.

USB Radio Indication

USB radio together with a green check mark indicates that the serial port used is working correctly and the USB radio dongle is ready to transmit data.

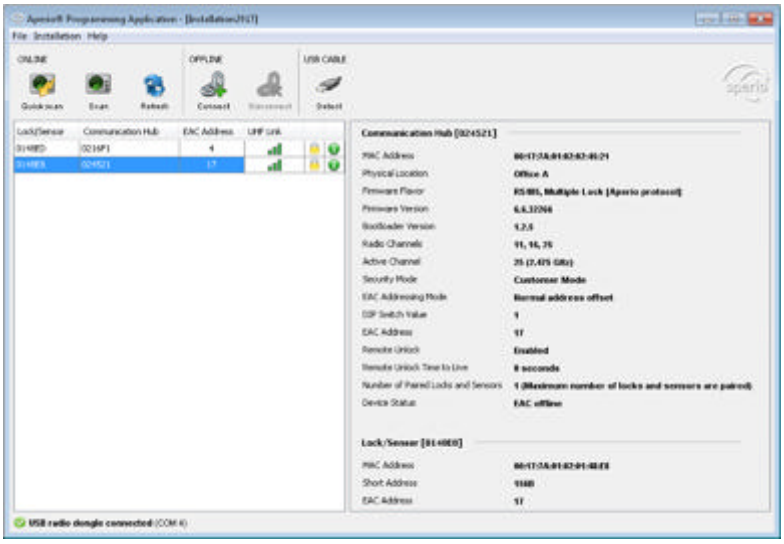


USB radio together with a red dot indicates that the serial port or the USB radio dongle is not connected or not working correctly. (Refer to section *Preferences* on page 8 to verify that correct settings are used.)



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 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.

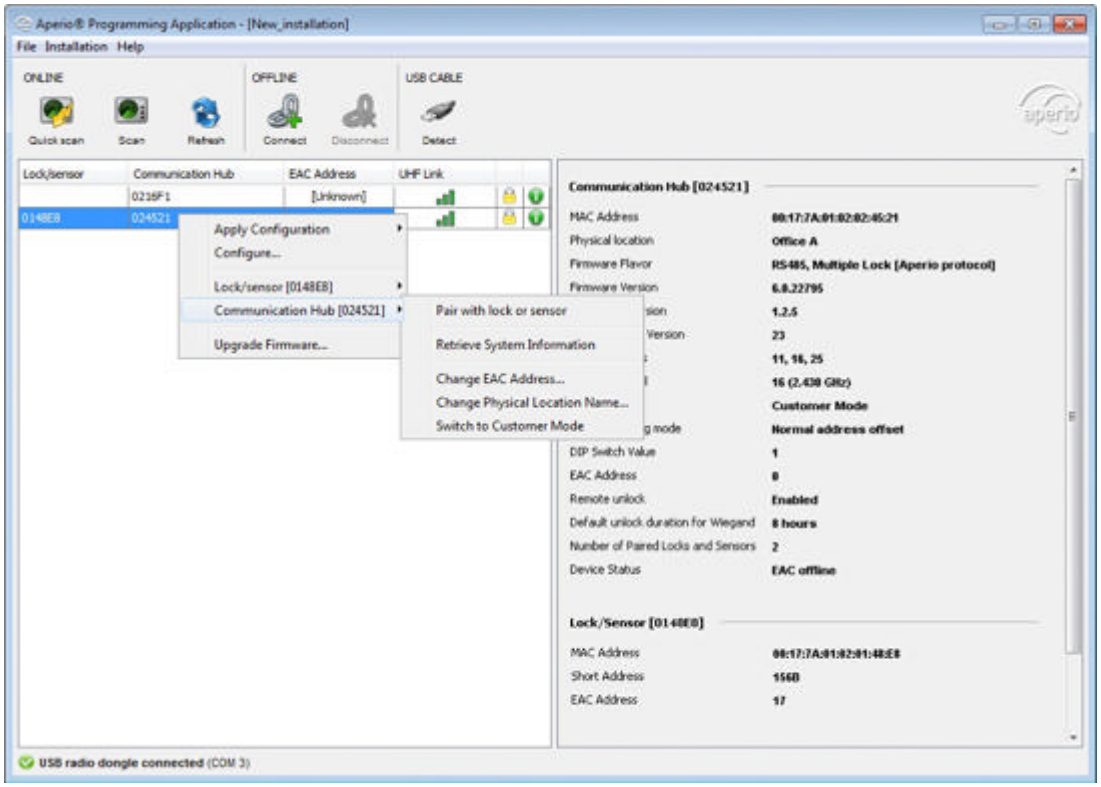
	Customer mode	Lock is using secure radio communication with the customer encryption key.
	Manufacturer mode	Lock is using insecure radio communication with the default encryption key.

- **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/lock/sensor firmware version (Aperio radio protocol version) is older than Aperio Programming Application.
	For example: The Aperio Programming Application is older than communication hub firmware version (Aperio radio protocol version).
	For example: The security modes in communication hub and lock are not equal and should be changed, see section *Change EAC Address* on page 75.

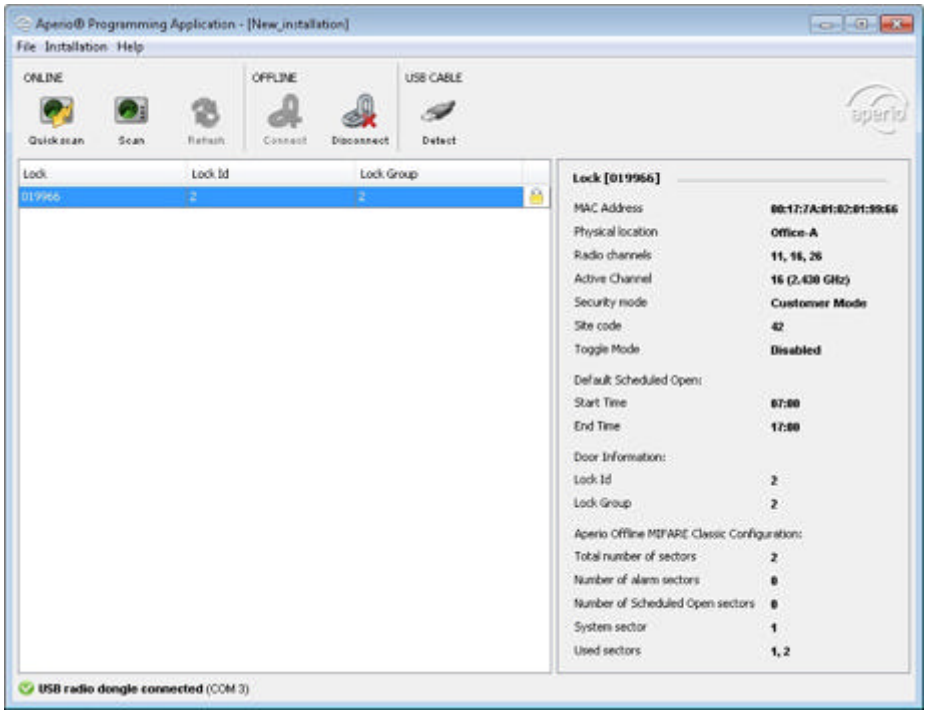
- Detailed information about the selected hub and lock/sensor is shown on the right side of the window.

Right-clicking a communication hub or lock/sensor will give access to the functions available in the Aperio Programming Application. See section *Aperio Programming Application Online Functions* on page 13 for an overview of all functions.



Installation View Overview for Aperio Offline

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



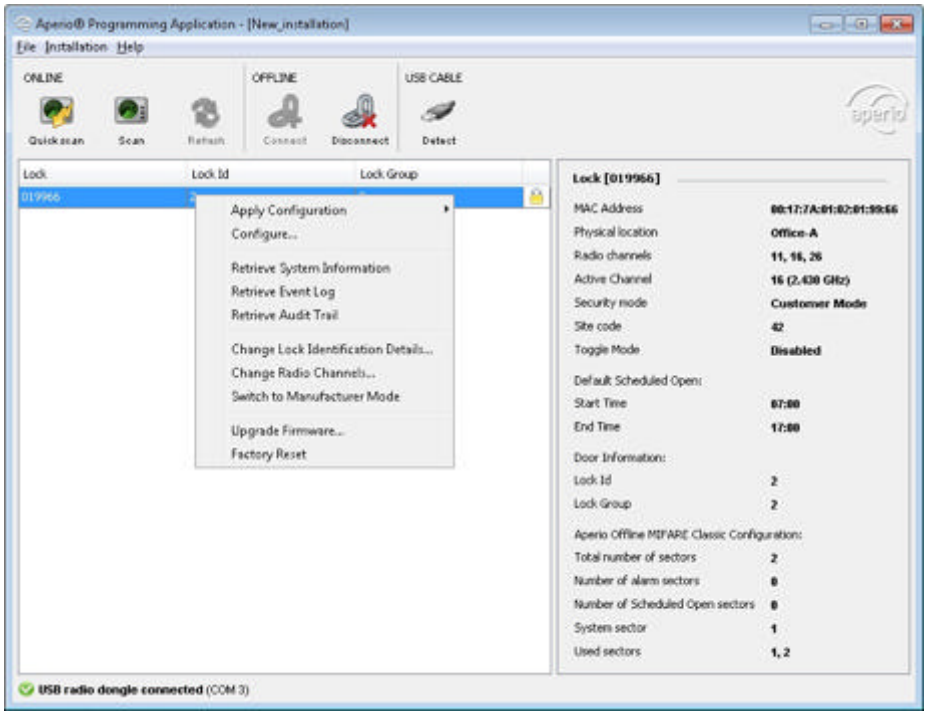
The following information is shown:

- **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.
- **Security Mode:** Indicates the security mode of the lock. During final installation all locks 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.

- Detailed information about selected lock is shown on the right side of the window.

Right-clicking a lock will give access to the functions available in the Aperio Programming Application. See section *Aperio Programming Application Offline Functions* on page 95 for an overview of all functions.

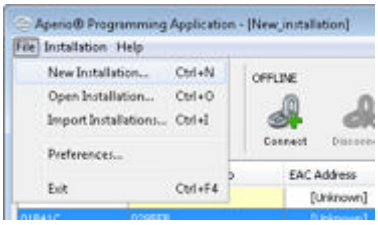


4 Aperio Programming Application Online Functions

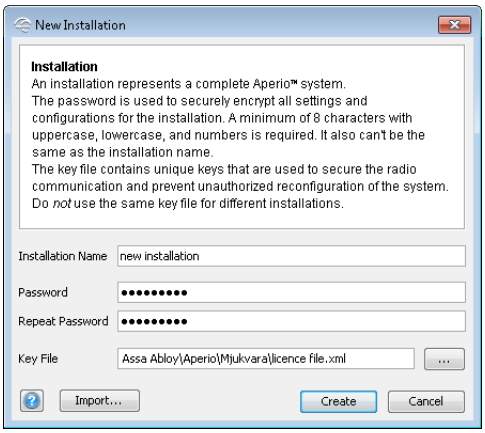
Creating Installations

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*** in the Aperio programming application menu.



3. Enter a name for the installation, a password containing at least 8 characters of which at least one upper and lower case character and a number. Finally click the browse button in the Key file field to add the encryption key (site_name-xxxxx.xml).



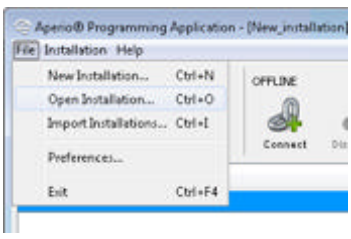
Proper handling of encryption keys is essential to lock/sensor security! It is absolutely necessary to use the customer encryption key by setting all communication hubs and locks/sensors in Customer mode to ensure a secure and encrypted communication.

4. Click ***Create***.

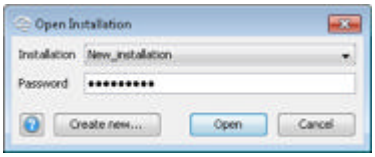
Opening Installations

The login window is automatically opened at start up if stored installations exist.

1. To open a stored installation select ***File*** → ***Open Installation...***

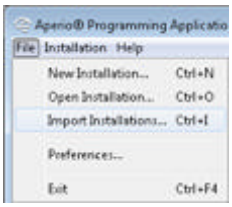


2. Select the Installation and enter the password. Click ***Open*** to proceed.

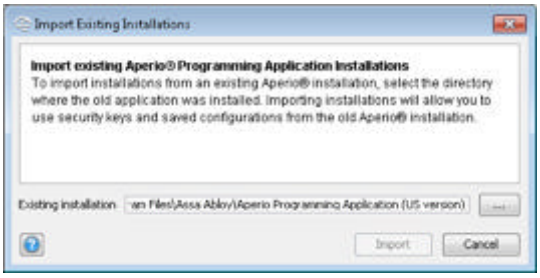


Import Existing Installations

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



2. Click the button and select the location for the old installation of the Aperio Programming Application. Your current installations will not be deleted. If you want to import installations from another computer, see section *Managing Existing Installations* on page 14.



3. Finish by clicking ***Import***.

Managing Existing Installations

Taking backup of existing installation

1. Locate the application directory of the Aperio Programming Application, `C:\Program Files\Assa Abloy\Aperio Programming Application\` (or `C:\Program Files (x86)\Assa Abloy\Aperio Programming Application\` for a 64-bit computer)
2. All installations are located in the `aperioinstallations` folder for backup. Encryption key including configurations are included in each installation.

Move installations to a new computer

1. Take a backup of the desired installation, according to *Taking backup of existing installation* on page 14, or backup the complete `aperioinstallations` folder.
2. Transfer the backup to the corresponding folder in the Aperio Programming Application folder on the new computer. If the `aperioinstallations` folder does not exists, it needs to be created.

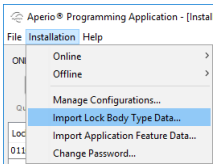
Remove installation

1. Locate the `aperioinstallations` folder in the application folder for the Aperio Programming Application, according to above and delete the entire folder for the desired installation.

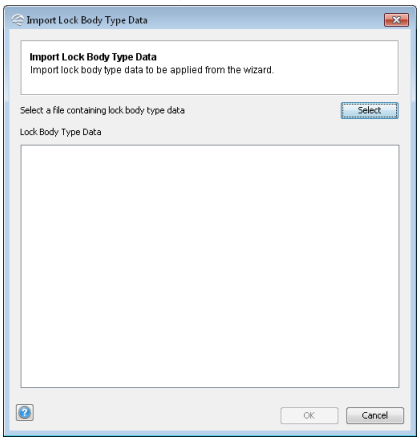
Import Lock Body Type Data

The ***Import Lock Body Type Data*** is used to simplify the configuration of the locks of a certain type in an installation. The XML-file that is imported contains a complete set of parameters applicable for each of the locks that are supported.

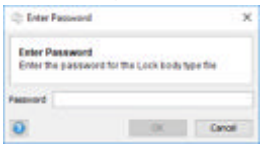
1. In the menu bar, select ***Installation*** → ***Import Lock Body Type Data***.



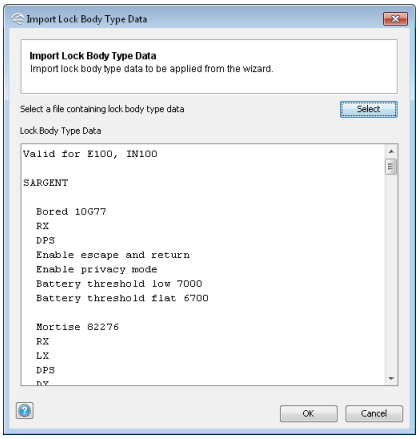
2. Click ***Select*** to open the file browser dialog and choose the XML-file.



3. Enter the password for the lock body type file to add it to Aperio Programming Application.



The settings for the locks supported are displayed in the dialog.



The PCB id of the lock used in the installation must match one of the products listed in the XML-file. The PCB id of the lock can be determined by using ***Retrieve System Information***.

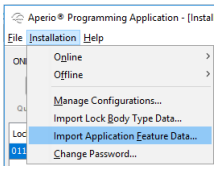
To apply the lock body type settings on a lock, use the ***Configure*** function and browse to the ***Lock Body Type Configuration*** page.

Device Aware Wizard must also be activated.

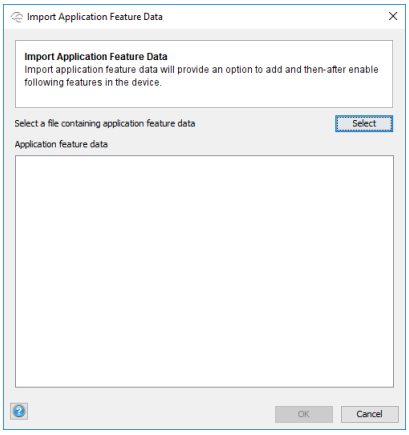
Import Application Feature Data

The ***Import Application Feature Data*** is used to add application dependent features to the Aperio Programming Application configuration wizard, in which they can be activated and configured for the lock. The XML-file that is imported contains a complete set of parameters applicable for each of the locks that are supported.

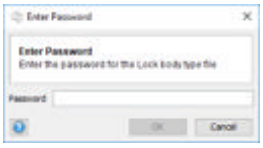
1. In the menu bar, select ***Installation*** → ***Import Application Feature Data***.



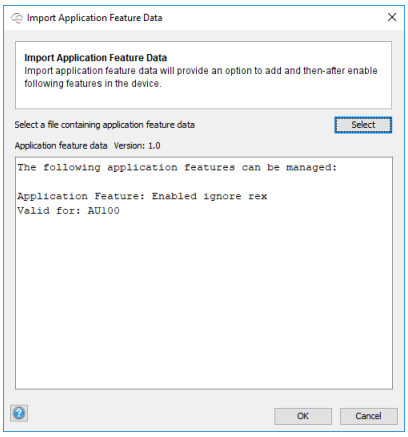
2. Click ***Select*** to open the file browser dialog and choose the XML-file.



3. Enter the password for the lock application feature data file to add it to Aperio Programming Application.



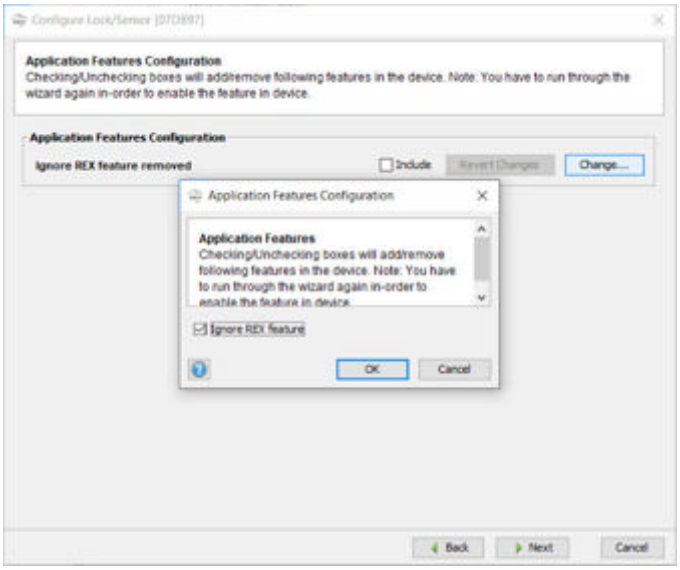
The settings for the locks supported are displayed in the dialog.



Add application feature to the device

Before an imported application feature can be used, it must be added to the device using the configuring wizard.

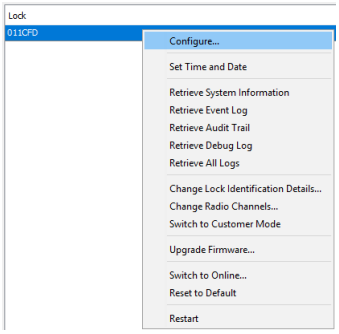
1. Right-click on the device and select ***Configure***.
2. Go through the wizard to the ***Application Features Configuration*** page.
3. Click ***Change*** and select the checkbox to add the feature to the device.



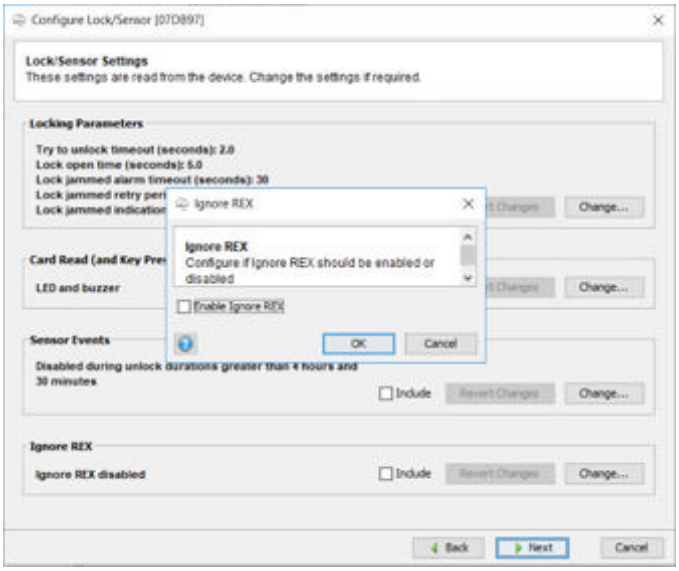
4. Click ***OK*** and then ***Next*** repeatedly to finish the wizard.

Enable application feature in the device

1. Right-click on the device and select ***Configure***.



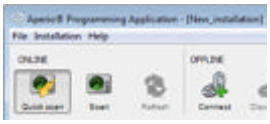
2. Go through the wizard to the ***Lock/Sensor Settings*** page.
3. Click ***Change*** and select the checkbox to enable the feature in the device.



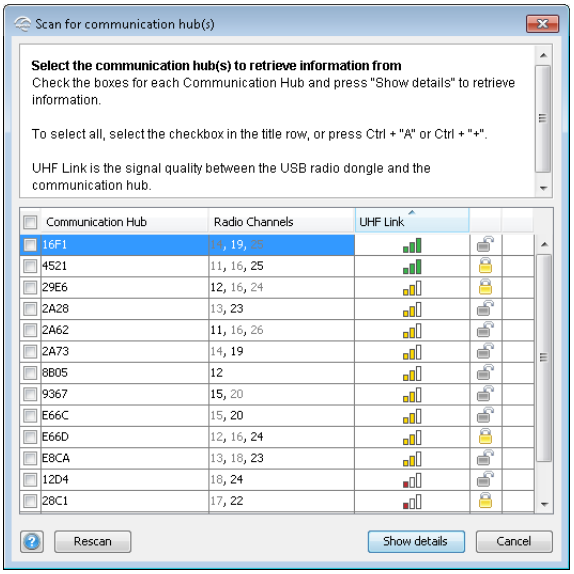
4. Click ***OK*** and then ***Next*** repeatedly to finish the wizard.

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.)

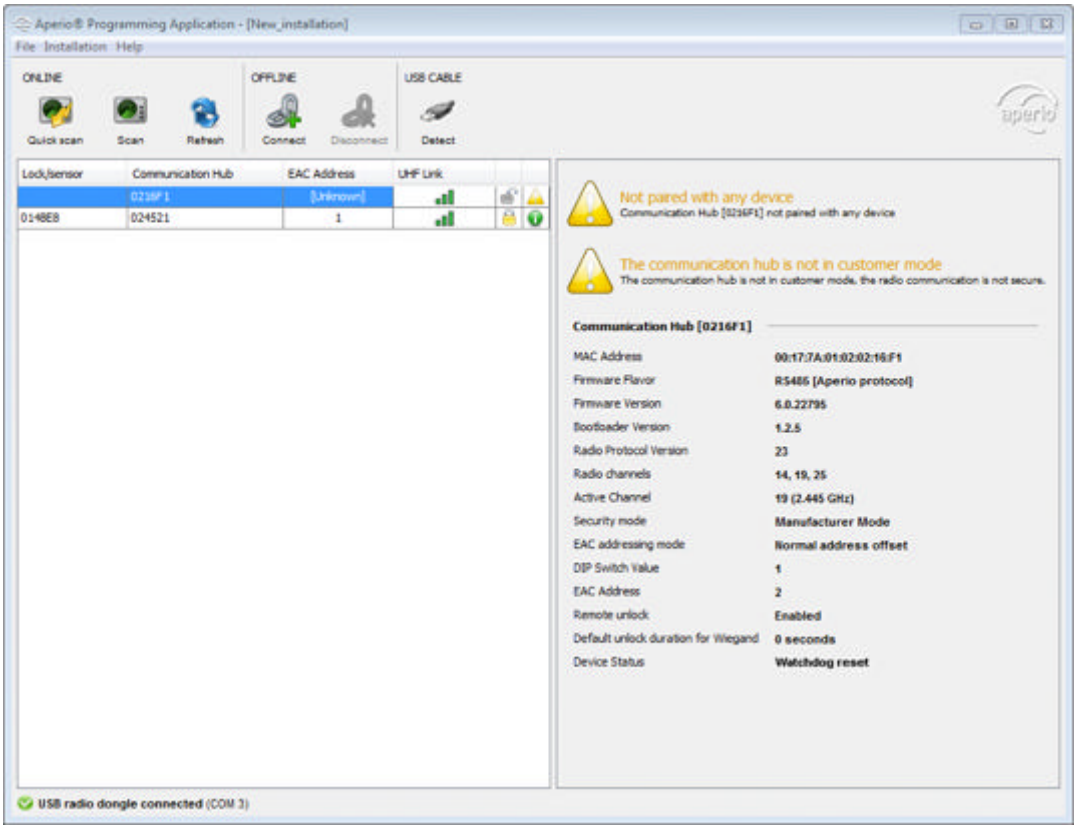


Result: The Aperio Programming Application starts scanning. All communication hubs within reach of the USB radio dongle of your computer are displayed in the scan result table.



2. Locate a communication hub by the last four characters of the communication hub MAC address (ex. 16F1) 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.

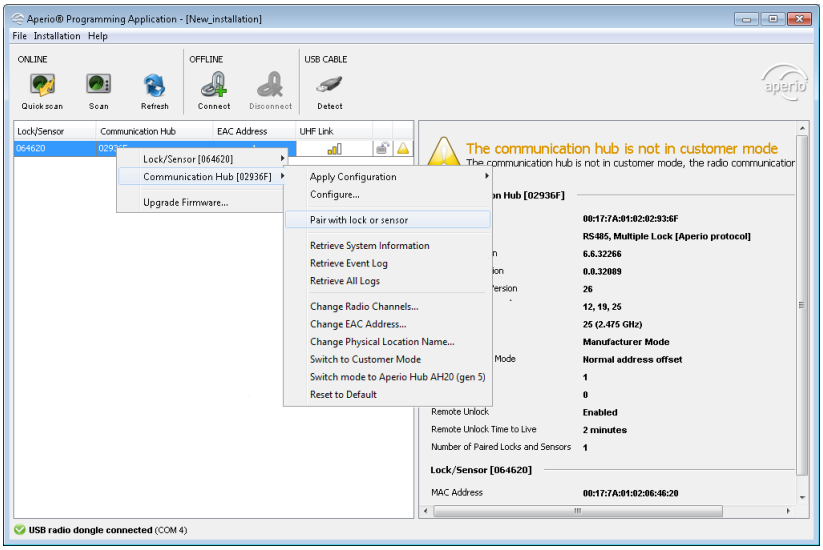
3. Select the communication hub(s) to be included in your installation. Click ***Show Details*** to view detailed information.
   Result: Selected communication hub(s) are displayed in the installation view.



Pairing Locks/Sensors with Communication Hub

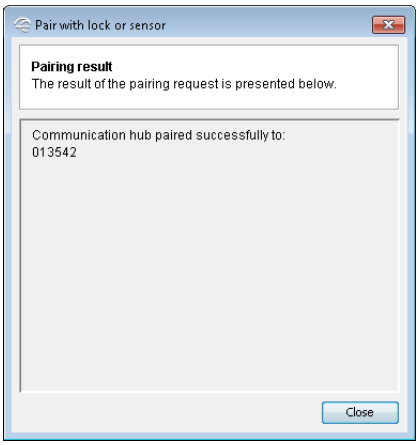
AH30 version of the communication hub can be paired with a combination of up to 8 locks/sensors. AH40 can manage 16 locks/sensors. AH15/AH20 can manage one lock/sensor.

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.

3. When the communication hub's LED indicates successful pairing with alternating green and yellow light, you can click ***Done*** to see the pairing result.



Result: The result is displayed. If the pairing result could not be retrieved from the communication hub, close dialog and press ***F5*** to see if pairing was successful.

Connecting to V3 Locks with USB Cable

For V3 locks equipped with USB cable connection, configuration can be made without performing the pairing process.

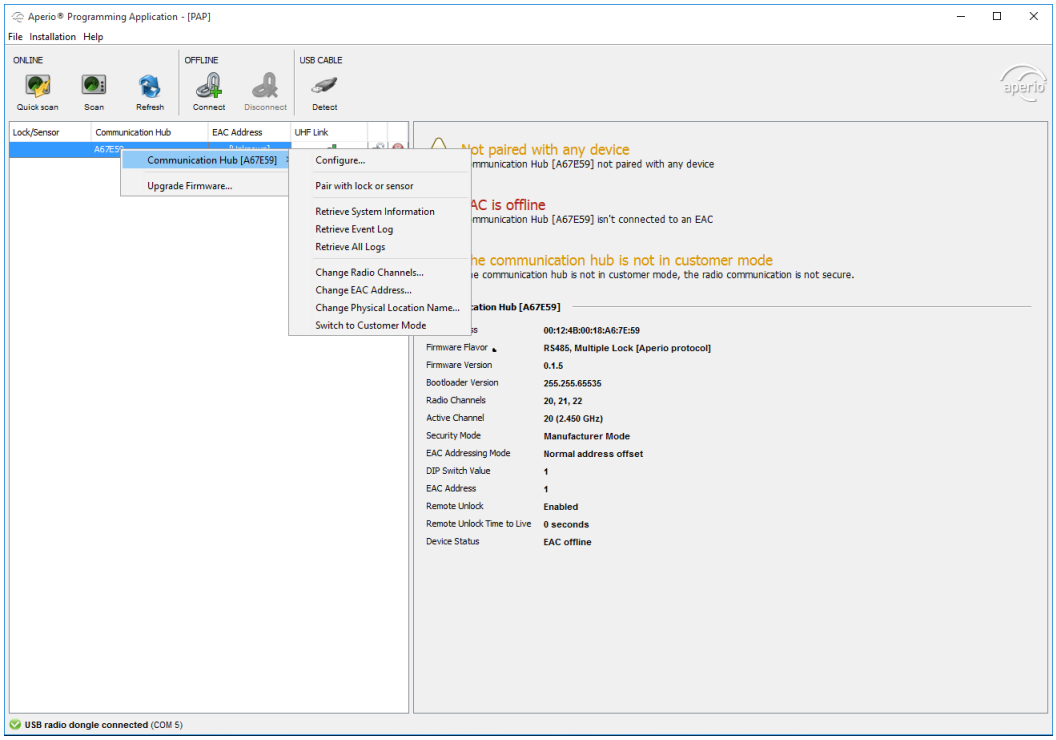
Before using this function, perform the installation of drivers according to section *Recommended Procedure when Using the V3 Lock USB Cable* on page 148.

1. Connect the cable to the lock.
2. Click ***Detect*** to connect to the lock.

The lock indicates correct connection with 5 yellow flashes and the lock is listed in the main view.

Configure Function – Wizard

Open the configure function by right-clicking a communication hub/lock/sensor and selecting either ***Lock/Sensor*** or ***Communication Hub***, and then ***Configure...*** on the sub-menu.



Depending on the hardware, different windows appears in the wizard.

The following sections describe each window in the wizard.

Device Aware Configuration Wizard

When enabled, the Device Aware Configuration Wizard will detect the applicable features for the connected device and their current settings.

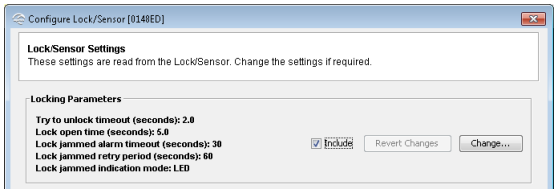
To enable the Device Aware Configuration Wizard: select ***File*** >***Preferences...*** and check the option ***Device Aware Wizard***.

Device Aware Wizard is enabled by default after installing the application.

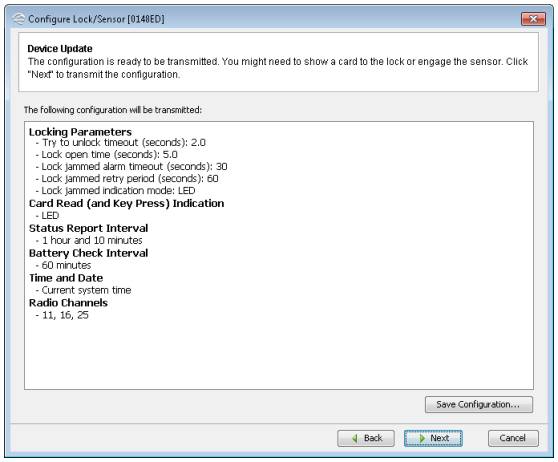
About the Include option

When the ***Device Aware Wizard*** function is enabled, the ***Include*** checkbox is available for all settings in the configuration wizard.

This checkbox must be selected in order to transfer the setting to the device on the last page in the wizard. Changed settings during the configuration process will be automatically selected.



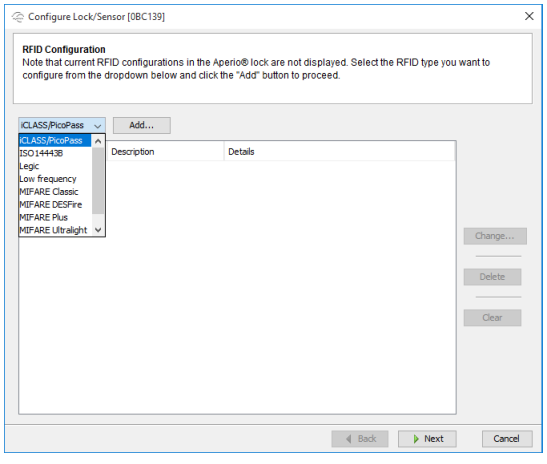
The ***Save Configuration*** function on the last page also depends on the ***Include*** status. Only the selected settings will also be available for saving.



RFID Configuration (Lock/sensor)

A corresponding firmware for the given RFID type must be installed on the locks/sensors.

Select the RFID type in the list and click ***Add...*** to enter the settings for each credential type. It is possible to add one configuration per RFID type, except for MIFARE DESFire and MIFARE Classic, for which 3 configurations each can be added.



Seos RFID format is also supported by the hardware. However, no settings are necessary.

Once a credential format has been added, use the buttons to the right to edit or delete each RFID setting. Click ***Clear*** to remove all added credential formats.

iCLASS/PicoPass

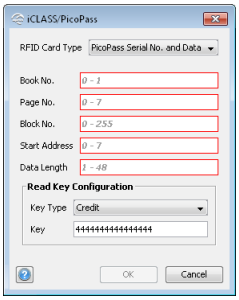
iCLASS

No settings are made to ***iCLASS***.

PicoPass Serial Number

No settings are made to ***PicoPass Serial Number***.

PicoPass Serial No. and Data



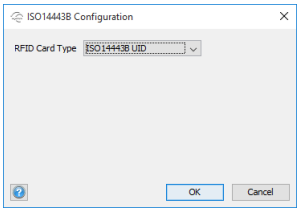
- ***Book No.***: The book number used for the credentials. 0 or 1.
- ***Page No.***: The page number used for the credentials. 0 - 7.
- ***Block No.***: The block number used for the credentials. 0 - 255.
- ***Start address***: The start address for the credential data. 0 - 7.
- ***Data length*** The data length for the credential data.

Read Key Configuration:

- ***Key Type***: Select the cryptographic algorithm used to read/write data from/to the card, ***Credit***, ***Debit*** or disable Read key configuration with the option ***None***.
- ***Key***: The picopass key that applies for the user cards in the installation in HEX format.

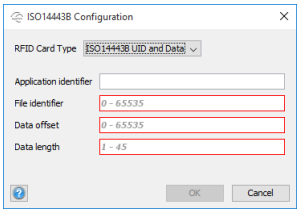
ISO14443B

ISO14443B UID



No settings are made to ***ISO14443B UID***.

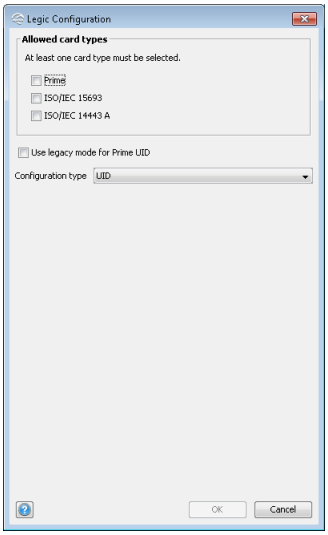
ISO14443B UID and Data



- ***Application identifier***: To configure the lock for file credential reading, you need to set first the Application Identifier of the application which contains the file. Application Ids range from 3 byte hex to 16 byte hex.
- ***File identifier***: You need to type the File Identifier of the file you want to read. File Ids range is 0 to 65535
- ***Data offset***: 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.
- ***Data length***: 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 is 45 byte.

Legic

Legic UID



In the list, select the card type to use:

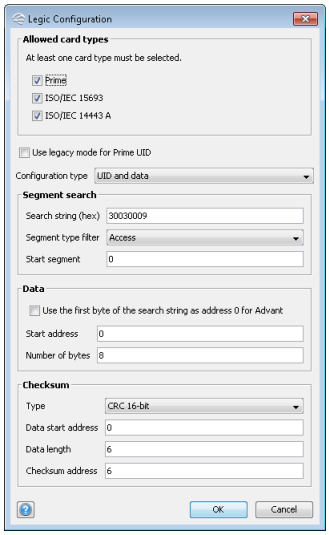
- Prime
- ISO 15693 (Advant)

- ISO 14443 A (Advant)

Check the check box ***Use legacy mode for Prime UID*** if applicable. This mode is used for older types of EACs, where the 2nd and 4th bytes of the UID are swapped. For example, if the original Prime UID is "AA11BB22", selecting this option will result in that "AA22BB11" is sent to the EAC instead.

No other settings are made to Legic UID.

Legic UID and Data



In the list, select the card type to use:

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

Check the check box ***Use legacy mode for Prime UID*** if applicable. This mode is used for older types of EACs, where the 2nd and 4th bytes of the UID are swapped. For example, if the original Prime UID is "AA11BB22", selecting this option will result in that "AA22BB11" is sent to the EAC instead.

Select UID and Data in the drop down list ***Configuration type***.

Segment search:

- ***Search string (hex)***: Max 24 characters hexadecimal, even number och 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.

Field name	Mandatory	Supported data type	Data range	Example data	Comments
Search string	No	Hexadecimal	Max 24 characters	0123456789aabbccdd	Must be an even number of characters.
Segment type filter	No	Select any value from the dropdown list (None, Data or Access)		Data	Only one value from the dropdown can be selected.

Field name	Mandatory	Supported data type	Data range	Example data	Comments
Start segment	Yes	Number (positive integer)	0 to 255	1	Specifies the segment from which to start the search. It is useful in cases where more than one similar search string exists.

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.

Field name	Mandatory	Supported data type	Data range	Example data	Comments
Data: Start address	Yes	Number (positive integer)	0 to 255	0	Specifies the start address of the data.
Data: Number of byte	Yes	Number (positive integer)	1 to 45	32	Specifies the number of byte of data to be read.

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.

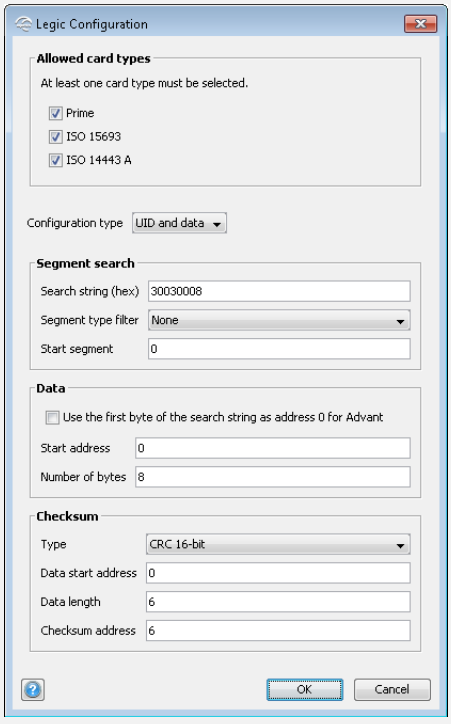
Field name	Mandatory	Supported data type	Data range	Example data	Comments
Checksum: Type	No	Select any value from the dropdown list (None, CRC 8-bit, CRC 16-bit)		CRC 8-bit	"None" does not require any of the checksum related fields to be specified, but CRC 8-bit and 16-bit does.
Checksum: Data start address	Yes, if other than "None"	Number (positive integer)	0 to 255	0	Specifies the address where the data which checksum is to be calculated starts.
Checksum: Data length	Yes, if other than "None"	Number (positive integer)	0 to 255	64	Specifies the length of the data in number of byte to be read.

Field name	Mandatory	Supported data type	Data range	Example data	Comments
Checksum: Address	Yes, if other than "None"	Number (positive integer)	0 to 255	2	Specifies the address where the checksum is located.

Example
Legic Advant Card

Segment 0:

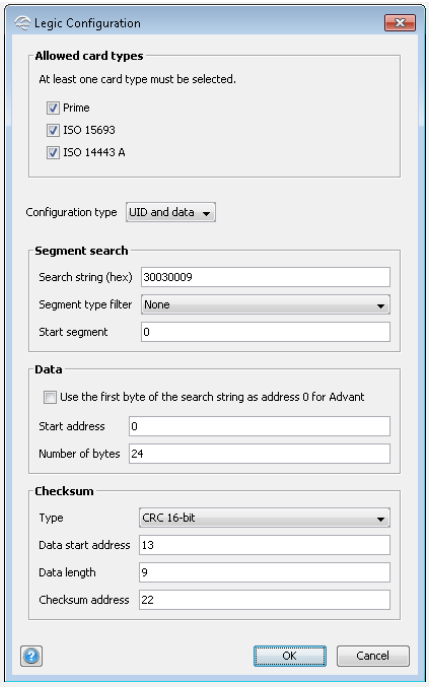
- Search String: 30 03 00 08
- Segment type: Data
- Data length: 8 byte
- Checksum: CRC 16 byte 0-5
- Checksum address: 6



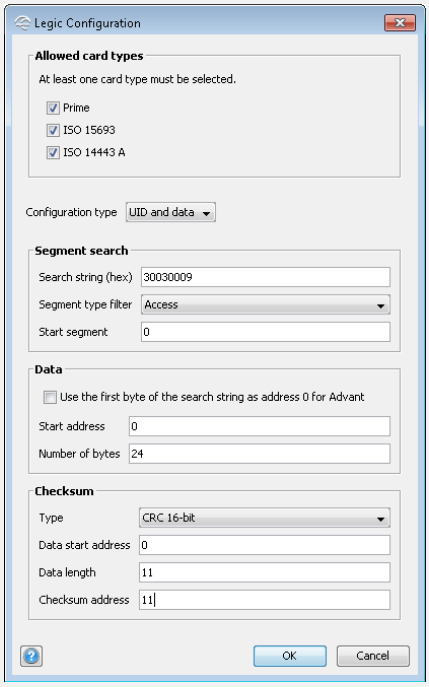
Segment 1:

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



or



Only one checksum can be selected.

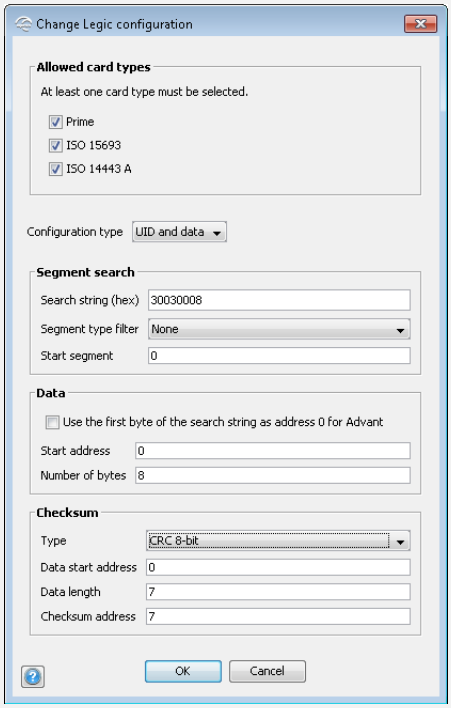
To include the search string in the first data byte, check the Use the first byte of the search string as address 0 for Advant.

Example

Legic Prime Card

Segment 0: (only segment)

- Search String: 30 03 00 08
- Segment type: Data
- Data length: 8 byte
- Checksum: CRC 8 byte 0-6
- Checksum address: 7



How to Include Advant Search String in Credential Data:

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 of Legic Advant and Prime segment, each with a search string/stamp of 4 byte:

	Data Address	
Member	**Legic Advant:**	**Legic Prime:**
STAMP0	n/a	0
STAMP1	n/a	1
STAMP2	n/a	2
STAMP3	n/a	3
DATA0	0	4
DATA1	1	5
DATA2	2	6
DATA3	3	7
DATA4	4	8
DATA5	5	9

	Data Address	
Member	Legic Advant:	Legic Prime:
...	...	...
DATAn	n	n+STAMP_LENGTH

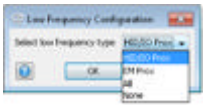
Using the check box ***Use the first byte of the search string as address 0 for Advant***, the data addressing of Advant is changed. The first data byte will then be the first search string/stamp byte as shown in example bellow.

Legic Advant using STAMP0 as address 0:

Member	Data Address
STAMP0	0
STAMP1	1
STAMP2	2
STAMP3	3
DATA0	4
DATA1	5
DATA2	6
DATA3	7
DATA4	8
DATA5	9
...	...
DATAn	n+STAMP_LENGTH

- It's mandatory to select at least one card type for the configuration.
- All selected card types will share the same settings.
- Card types which are not selected will lose their configurations and be disabled in the lock. For example, if you select "Prime" and "ISO 15693" as allowed card types, then "ISO 14443 A" cards would automatically be considered as not allowed card types and will not be supported in the lock.

Low Frequency



Select the low frequency credential type to use from the list:
- ***HID/IO Prox***
- ***EM Prox***
- ***All***
- ***None***: Low frequency RFID will be disabled in lock. Only visible by Multiclass locks.

Not all products are available in Low Frequency.

This credential type cannot be used together with any other credential types. V3 Multiclass locks are though an exception. Before the lock has been configured with the Aperio Programming Application, the lock will accept any Low Frequency credential technology.

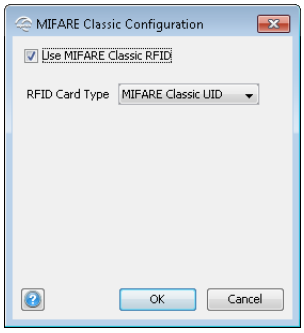
The following information is applicable for V2 low frequency locks only:
Once the lock has read any credential technology 3 times the lock will only accept this technology. If the power is toggled the lock will return to the initial state of accepting any credential.

The following information is applicable for V2 & V3 low frequency locks as well as V3 Multiclass locks:
Once a specific credential technology has been configured via the Aperio Programming Application, this will be the only accepted type of credential. The lock will remain in this condition after the power has been toggled as well.

MIFARE Classic

MIFARE Classic UID (Default)

It is possible to add 3 configurations for MIFARE Classic RFID.



No settings are made to ***MIFARE Classic UID***.

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

MIFARE Classic SE

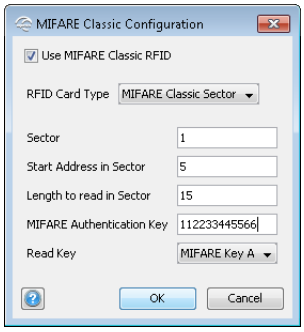
No settings are made to MIFARE Classic SE.

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

MIFARE Classic Sector

It is possible to add 3 configurations for MIFARE Classic RFID.

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

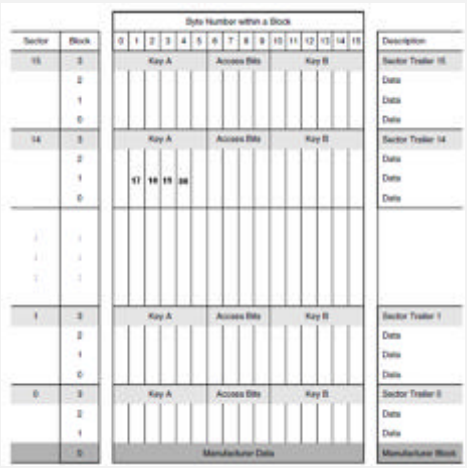


- ***Sector***: The sector used for the credentials.
- ***Start Address in Sector***: Parts of blocks within a sector can be used for credential data: 0 to 47 for 1K MIFARE Classic credentials. For 4K MIFARE Classic credential 0-47 (Start sector 0 to 31) and 0 – 239 (Start sector above 31).
- ***Length to read in Sector***: Length of the credential data: 1 - 48 (Start sector above 31 cannot be used in the current release of the Aperio 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.

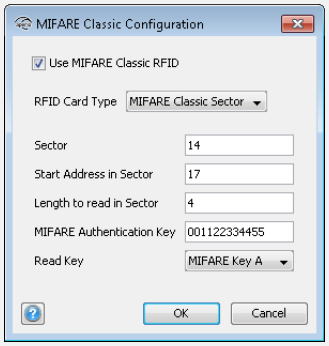
If key B is selected as sector data read key, make sure that the access bits on the credential prevent reading of key B. If key B is readable on the credential, key B cannot be used to read the credential data.

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.



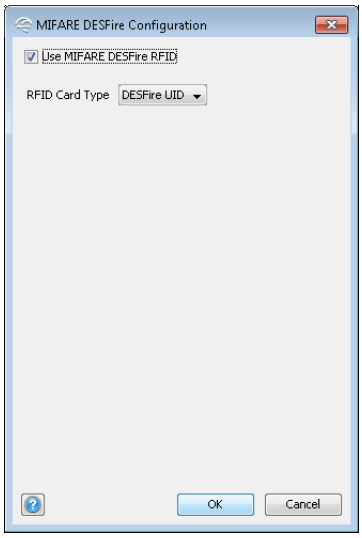
The configuration should look like this:



MIFARE DESFire

MIFARE DESFire UID

It is possible to add 3 configurations for MIFARE DESFire RFID.



No settings are made to MIFARE DESFire UID.

If you want to prevent MIFARE DESFire from being read by the lock, unselect ***Use MIFARE DESFire RFID***.

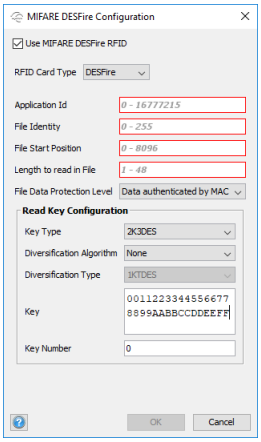
MIFARE DESFire SE

No settings are made to ***MIFARE DESFire*** SE.

If you want to prevent ***MIFARE DESFire*** UID from being read at all by the lock, unselect ***Use MIFARE DESFire RFID***.

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

It is possible to add 3 configurations for MIFARE DESFire RFID.

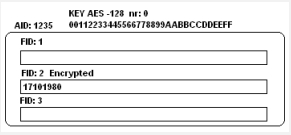


- ***Application Id***: To configure the lock for file credential reading, you need to set first the Application Id of the application which contains the file. A credential can have up to 32 applications. Application Ids range from 0 to 16777215.
- ***File Identity***: You need to type the File Id of 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. 8096 is the highest start position.
- ***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 48 byte.
- ***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.

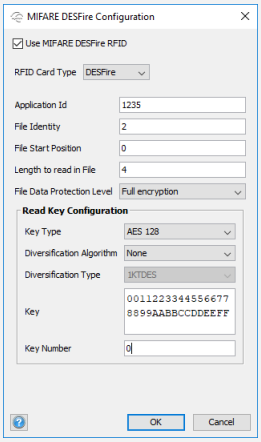
Read Key Configuration:

- ***Key Type*** Select one of the options (2K3DES, 3K3DES, AES 128, FREE ACCESS) depending on the crypto used by your application's key. Free access will disable the read key and card will be without encryption.
- ***Diversification Algorithm***: Algorithm used to determine the diversified key used by the credential. None, NXP or smartMAX. When smartMAX is selected, the application id and file settings are set automatically.
- ***Diversification Type***: Applicable for the diversification algorithm, select 1KTDES, 2KTDES, 3KTDES, AES 128 and CMAC (CMAC requires ***Diversification Algorithm*** NXP and ***Key Type*** AES 128).
- ***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

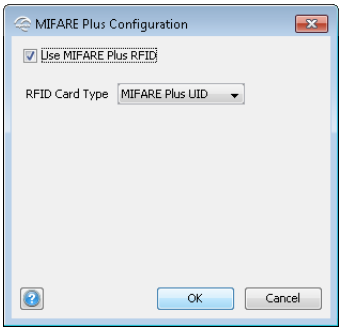


The configuration should look like this:



MIFARE Plus

MIFARE Plus UID

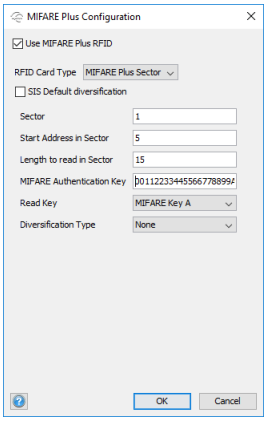


No settings are made to MIFARE Plus UID.

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

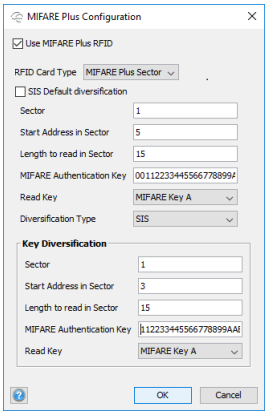
MIFARE Plus Sector

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



- ***SIS Default diversification***: Select to use the default configuration for key diversification for ***SIS*** (SeaWing Integrated Solution).
- ***Sector***: The sector used for the credentials.
- ***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 Aperio 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.

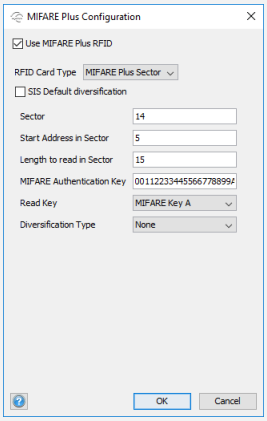
  If key B is selected as sector data read key, make sure that the access bits on the credential prevent reading of key B. If key B is readable on the credential, key B cannot be used to read the credential data.
- ***Diversification Type***: Select ***SIS*** in the list to add key diversification from a master key.



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:

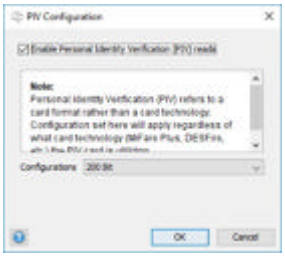


MIFARE Ultralight

No settings are made to MIFARE Ultralight.

If you want to prevent MIFARE Ultralight from being read at all by the lock, unselect ***Use MIFARE Ultralight RFID***.

PIV Configuration

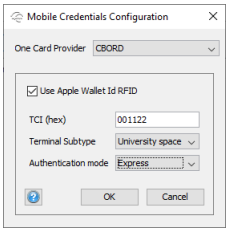


- ***Configurations***: Select the setting associated with the RFID technology to be used with PIV (Personal Identity Verification).

Mobile Credentials

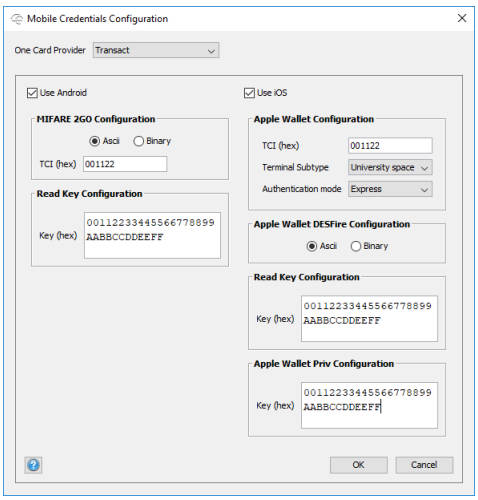
CBORD

This feature is only available to select customers in the US market.



- ***Use Apple Wallet Id RFID***: Enables the use of Apple Wallet Credentials.
- ***TCI (hex)***: Customer specific identifier for Apple Wallet.
- ***Terminal Subtype***: Sets the customer group for the Apple Wallet installation.
- ***Authentication mode***: Sets if 1 factor (Express - without faceid or passcode) or 2 factor (TRA) authentication should be used.

Transact



Android configuration

- ***TCI (hex)***: Customer specific identifier for ***MIFARE 2GO Configuration***.
- ***Key (hex)***: Select the read key that the credential is configured to use for sector reading. The lock will give access only for this key.

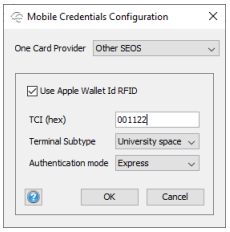
iOS configuration

This feature is only available to select customers in the US market.

- ***TCI (hex)***: Customer specific identifier for Apple Wallet.
- ***Terminal Subtype***: Sets the customer group for the Apple Wallet installation.
- ***Authentication mode***: Sets if 1 factor (Express - without faceid or passcode) or 2 factor (TRA) authentication should be used.
- ***Apple Wallet DESFire Configuration***: Select the valid format.
- ***Read Key Configuration***:
  Key (hex): Select the read key that the credential is configured to use for sector reading. The lock will give access only for this key.
- ***Apple Wallet Priv Configuration***:
  Key (hex): Select the apple wallet priv configuration key.

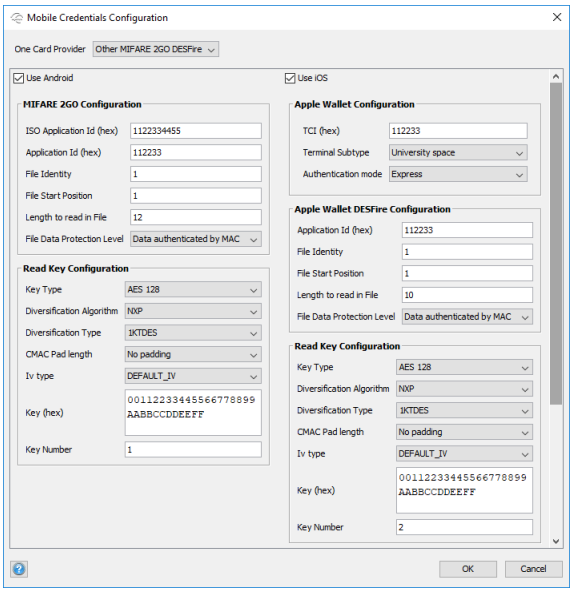
Other SEOS

This feature is only available to select customers in the US market.



- ***Use Apple Wallet Id RFID***: Enables the use of Apple Wallet Credentials.
- ***TCI (hex)***: Customer specific identifier for Apple Wallet.
- ***Terminal Subtype***: Sets the customer group for the Apple Wallet installation.
- ***Authentication mode***: Sets if 1 factor (Express - without faceid or passcode) or 2 factor (TRA) authentication should be used.

Other MIFARE 2GO DESFire



Android configuration

MIFARE 2GO Configuration

- ***ISO Application Id (hex)***: Enter the ISO Application id.
- ***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. 8096 is the highest start position.
- ***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 48 byte.

- ***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.

Read Key Configuration

- ***Key Type*** Select one of the options (2K3DES, 3K3DES, AES 128, FREE ACCESS) depending on the crypto used by your application's key. Free access will disable the read key and card will be without encryption.
- ***Diversification Algorithm***: Algorithm used to determine the diversified key used by the credential. None, NXP or smartMAX. When smartMAX is selected, the application id and file settings are set automatically.
- ***Diversification Type***: Applicable for the diversification algorithm, select 1KTDES, 2KTDES, 3KTDES, AES 128 and CMAC (CMAC requires ***Diversification Algorithm*** NXP and ***Key Type*** AES 128).
- ***CMAC Pad length***: Select the applicable paddning, no padding, one block padding (16 bytes) or two block padding (32 bytes).
- ***Iv type***: Select the applicable type, DEFAULT_IV, NXP_UID_AID_IV, NXP_MF2GO_IV.
- ***Key (hex)***: 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.

iOS configuration

This feature is only available to select customers in the US market.

Apple Wallet Configuration

- ***Use Apple Wallet Id RFID***: Enables the use of Apple Wallet Credentials.
- ***TCI (hex)***: Customer specific identifier for Apple Wallet.
- ***Terminal Subtype***: Sets the customer group for the Apple Wallet installation.
- ***Authentication mode***: Sets if 1 factor (Express - without faceid or passcode) or 2 factor (TRA) authentication should be used.

Apple Wallet DESFire Configuration

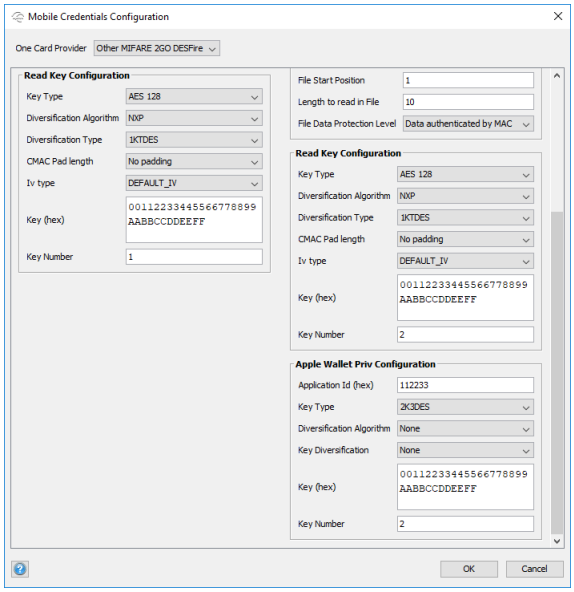
- ***Application Id***: To configure the lock for file credential reading, you need to set first the Application Id of the application which contains the file. A credential can have up to 32 applications. Application Ids range from 0 to 16777215.
- ***File Identity***: You need to type the File Id of 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. 8096 is the highest start position.
- ***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 48 byte.
- ***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.

Read Key Configuration

- ***Key Type*** Select one of the options (2K3DES, 3K3DES, AES 128, FREE ACCESS) depending on the crypto used by your application's key. Free access will disable the read key and card will be without encryption.
- ***Diversification Algorithm***: Algorithm used to determine the diversified key used by the credential. None, NXP or smartMAX. When smartMAX is selected, the application id and file settings are set automatically.

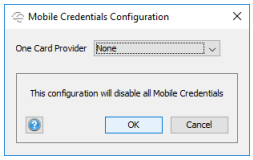
- ***Diversification Type***: Applicable for the diversification algorithm, select 1KTDES, 2KTDES, 3KTDES, AES 128 and CMAC (CMAC requires ***Diversification Algorithm*** NXP and ***Key Type*** AES 128).
- ***CMAC Pad length***: Select the applicable paddning, no padding, one block padding (16 bytes) or two block padding (32 bytes).
- ***Iv type***: Select the applicable type, DEFAULT_IV, NXP_UID_AID_IV, NXP_MF2GO_IV.
- ***Key (hex)***: 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.

Mobile Apple Wallet Priv DESFire



- ***Key Type*** Select one of the options (2K3DES, 3K3DES, AES 128, FREE ACCESS) depending on the crypto used by your application's key. Free access will disable the read key and card will be without encryption.
- ***Diversification Algorithm***: Algorithm used to determine the diversified key used by the credential. None, NXP or smartMAX. When smartMAX is selected, the application id and file settings are set automatically.
- ***Key Diversification***: Applicable for the diversification algorithm, select 1KTDES, 2KTDES, 3KTDES, AES 128 and CMAC (CMAC requires ***Diversification Algorithm*** NXP and ***Key Type*** AES 128).
- ***Key (hex)***: 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.

None

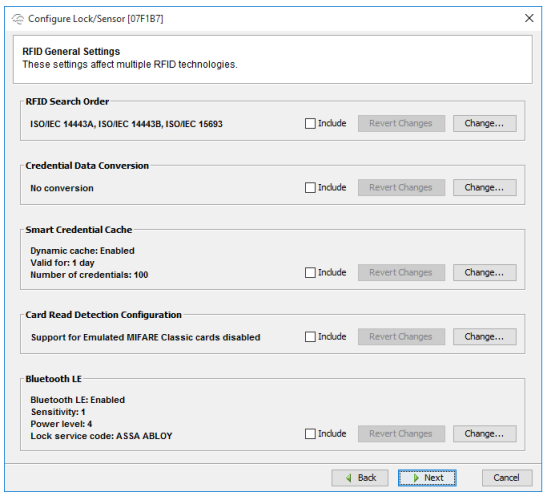


Select ***None*** to disable mobile credentials in the device.

RFID General Settings (Lock)

These settings affect multiple RFID technologies.

RFID Search Order only applies to V2SE and V3 locks. ***Credential Data Conversion***, ***Smart Credential Cache***, ***Card Read Detection Configuration*** and ***Bluetooth LE*** only applies for V3 locks.



RFID Search Order

When using **V2 SE** or **V3** locks the search order of used RFID protocols can be specified. By changing the search order and/or disabling protocols not used, energy consumption and user waiting time can be reduced.

V2 locks does **not** support this setting.

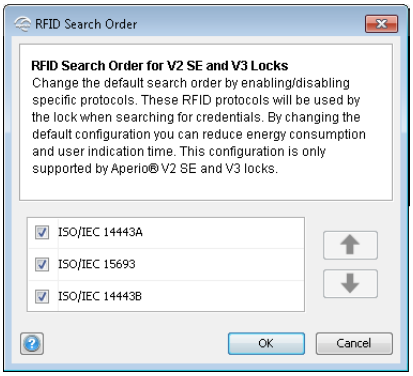
Important about *RFID Search Order* Configuration

If the RFID Search ***Configuration*** is done wrong, the lock may become inoperable. Be careful before changing these values.

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.

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

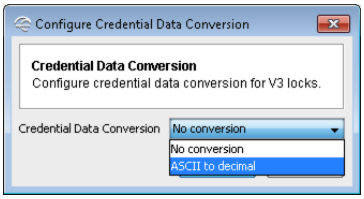


Credential Data Conversion (V3 locks)

This function is only supported by V3 locks, using the Aperio programming application 3.2.0 and onwards.

This function activates conversion of the credential data.

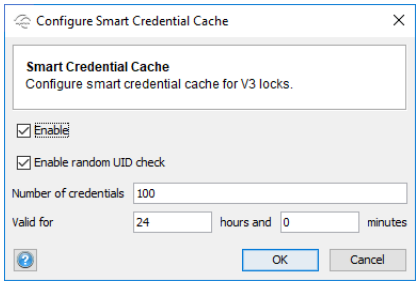
1. Select ***ASCII to Decimal*** to activate credential data conversion.



Smart Credential Cache (V3 locks)

This function is only supported by V3 locks, using the Aperio programming application 3.2.0 and onwards.

This is a function that saves granted credentials locally in the lock memory. If the lock is offline from the communication hub or the EAC, all credentials stored in the cache will be granted access.

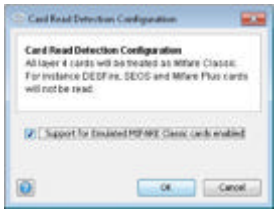


- ***Enable***: Click to enable the function.
- ***Enable random UID check***: Enables/disables the ability to detect if a credential has random UID or not. When this function is enabled, the random UID will be removed from the credential, that is, only the data is stored in the cache. Credentials with random UID only, will not be saved in the cache.
- ***Number of credentials***: Select the maximum number of grant access credentials that can be saved in the cache. Maximum cache size is 200 credentials. For products with firmware V3.4 or later, the maximum cache size is 1000 credentials.
- ***Valid for***: Select for how long time the credential is stored in the cache from the point when access is granted. Maximum 720 hours (30 days) and minimum 1 minute.

Card Read Detection Configuration (V3 locks)

This function is only supported by V3 locks, using the Aperio programming application 3.2.0 and onwards.

This is a function enables layer 4 cards, such as java cards emulating MIFARE Classic, to be read.

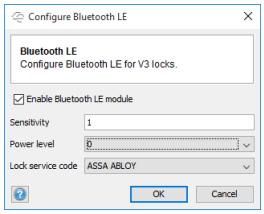


- ***Support for Emulated MIFARE Classic cards enabled*** / ***disable***: Click to enable/disable the function.

Bluetooth LE

This function is only supported by V3 locks, equipped with bluetooth LE module.

This function enables lock communication with compatible bluetooth LE (low emitter) devices for use as credentials, such as mobile phones.

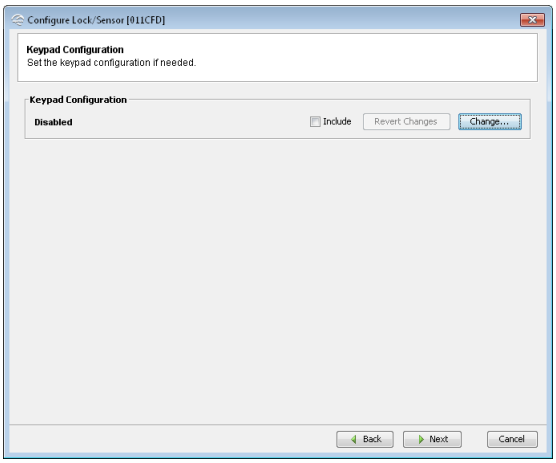


- ***Enable Bluetooth LE module***: Click to enable the bluetooth communication module in the lock.
- ***Sensitivity***: Sets the lock sensitivity to detect a bluetooth LE credential. A value from -128 to 127 (dBm), where a lower number increases the read distance to bluetooth device. Default 1.
- ***Power level***: Sets the bluetooth module's communication power level. Ranges from -21 to +2 (dBm) (+4 for single ended antenna). This setting interacts with the ***Sensitivity*** setting. Default 0.
- ***Lock service code***: Select the mobile app to be used for access in EAC. ***HID*** or ***ASSA ABLOY***.

Sensitivity and ***Power level*** differs between bluetooth device manufacturers. Adjustments may be required for optimal usability.

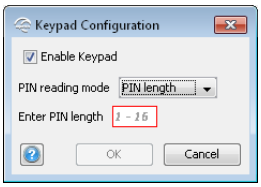
Keypad Configuration (Lock)

1. Click ***Change...*** to enter specific Keypad configuration.

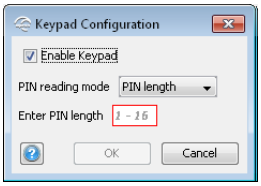


2. Choose between two PIN reading modes:

- ***PIN length***: PIN is set to use a fixed length.

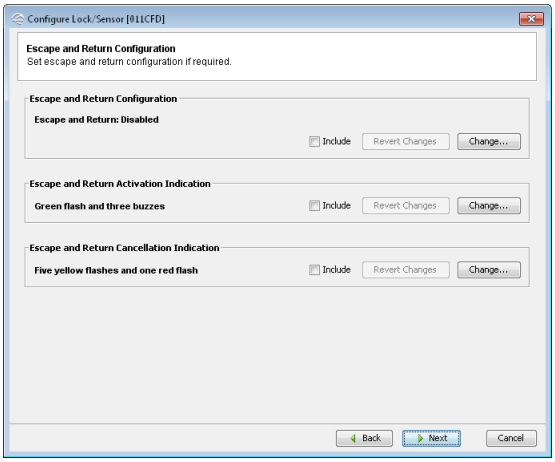


  - ***Enter PIN length***: A value between 1 and 16, as specified by the EAC.
- ***End character***: PIN is sent to the EAC after an end character is pressed. The end character is decided by lock configuration during production.



Escape and Return Configuration (Lock)

This function allows the lock to remain unlocked a certain time after the door has been opened from the inside. The Privacy mode function provides a method for an occupant of a room to lock the door and change access rights to the room. The privacy mode function can be enabled on locks equipped with privacy mode button or a monitored deadbolt.



Escape and Return and Privacy Mode Configuration

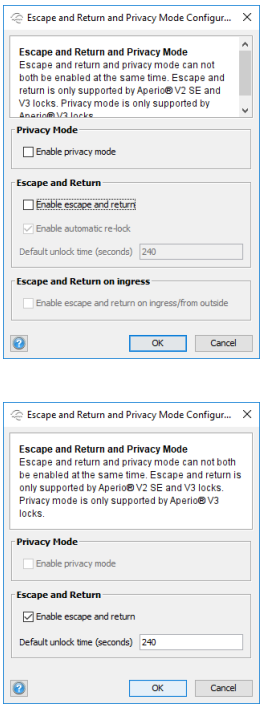


Figure 2: First image: V3 lock with firmware version 3.2 or later. Second image: V2SE/V3 lock with firmware version less than 3.2.

- ***Privacy Mode***: Enables the possibility to use the privacy mode button or deadbolt, to change access rights to the room. If the lock is offline, only override credentials can open the lock. This function is supported by V3 locks only.
- ***Escape and Return***: Activate the function to allow the lock to remain unlocked after the door has been opened from the inside.

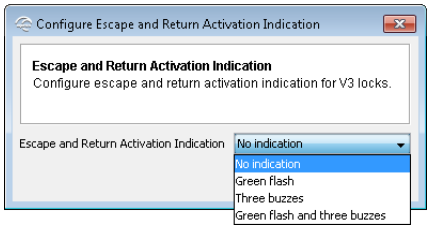
Escape and Return and ***Privacy Mode*** can not be enabled at the same time.

- ***Enable automatic re-lock***: Activate the function to automatically re-lock the lock after the default unlock time specified. If this function is not activated, the door will remain unlocked until the user manually locks the door, or the EAC issues a lock command. This function is only supported by V3 locks with firmware version 3.2 or later.
- ***Default unlock time (seconds)***: The time the lock is unlocked. Default is 240 seconds.
- ***Enable escape and return on ingress/from outside***: Enables the lock to remain unlocked after the door has been opened from the outside.

Escape and Return Activation Indication (V3 locks)

Different locks can have a different mechanism for audio-visual indication to show that the escape and return function is activated in the lock. This setting only applies for V3 locks.

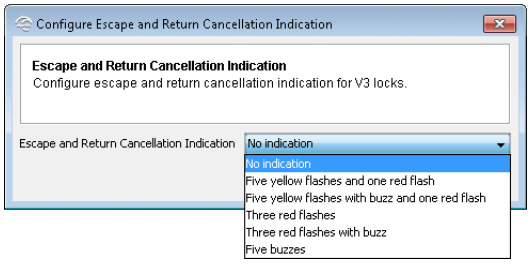
To enable, select the indication pattern in the drop down list.



Escape and Return Cancellation Indication (V3 locks)

Different locks can have a different mechanism for audio-visual indication to show that the escape and return function is deactivated in the lock. This setting only applies for V3 locks.

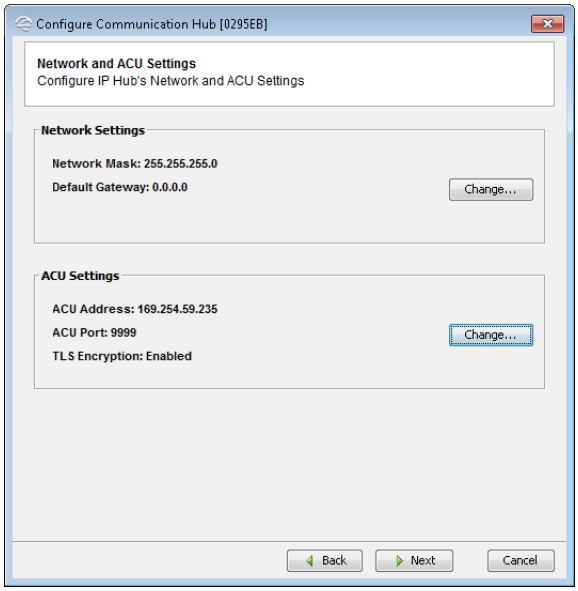
To enable, select the indication pattern in the drop down list.



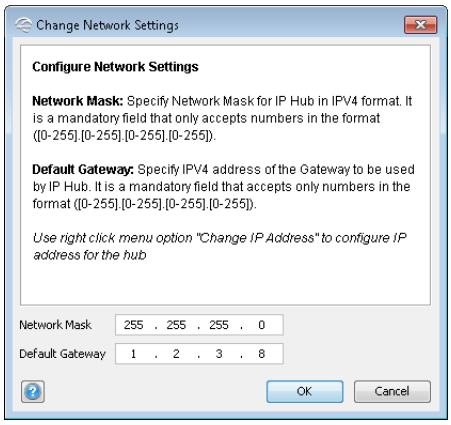
Network and ACU Settings (only AH40 Communication Hub)

This window only applies for AH40 communication hub in order to set the network and ACU settings for the installation site.

To download firmware, a correct IP-address must be set for the AH40 communication hub and the Aperio Programming Application must be connected to the same network.



Network Settings

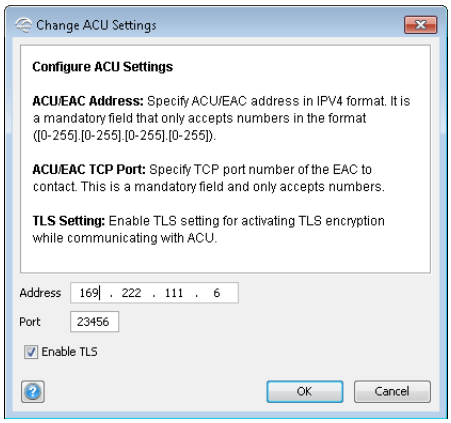


For correct settings contact your network administrator:

- **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.

To configure the IP address, use the right-click option in the installation view, see section *Change IP Address (Communication Hub AH40)* on page 84.

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 use for communication. Default value is 9999.
- Enable TLS: This setting provides secure communication between the EAC/ACU and the communication hub. The default value is enabled. Note that TLS must be enabled to allow customer mode to be set on the 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 communication 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 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.

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.

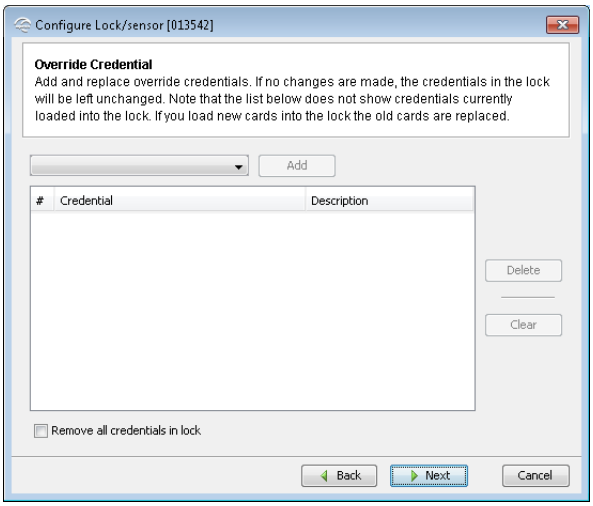
Use of override credentials when using a Wiegand hub requires that DIP switch 1 is set to position ON.

When adding an override credentials in the lock all existing override credentials are removed from the lock. It can therefore be convenient to include this when saving a configuration.

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.

To open the Escape and Return and Privacy Mode Configuration window: right-click on a hub and select ***Lock/Sensor*** > ***Configure...***. Click ***Next*** until the menu appears.

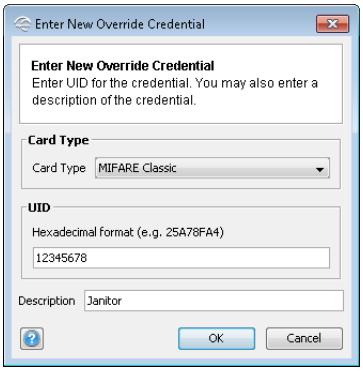
1. To add an override credential, select the desired card type in the drop-down list and click ***Add***.



See subsections for a description of each credential.

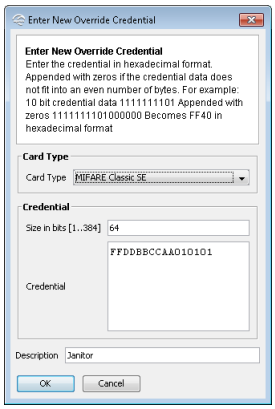
If you check ***Remove all credentials in lock***, all existing override credentials in the lock will be deleted during the configuration process.

MIFARE UID (Classic/Plus/Ultralight)



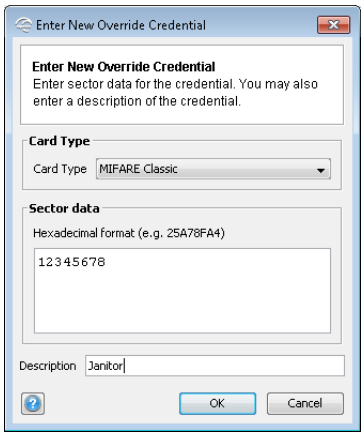
- **Card Type:** MIFARE Classic, MIFARE Plus or MIFARE Ultralight.
- **UID:** Card number.
- **Description:** For example the credential owner.

MIFARE SE (Classic/DESFire)



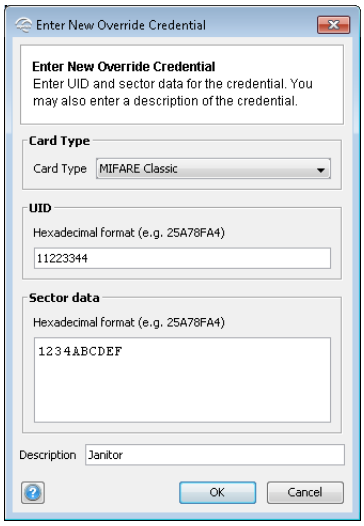
- ***Card Type***: MIFARE Classic SE or MIFARE DESFire SE.
- ***Size in bits [1...384]:***: Number of bits used for credential data on the credential.
- ***Credential***: Card number.
- ***Description***: For example the credential owner.

MIFARE Sector data (Classic/Plus)



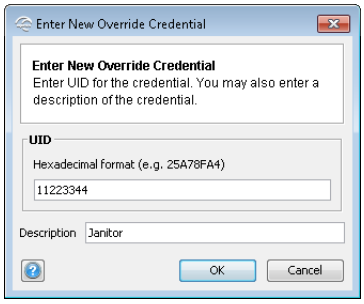
- **Card Type:** MIFARE Classic or MIFARE Plus.
- **Sector data:** Sector data stored on the credential. This value is normally stored in the EAC.
- **Description:** For example the credential owner.

MIFARE UID and Sector data (Classic/Plus)



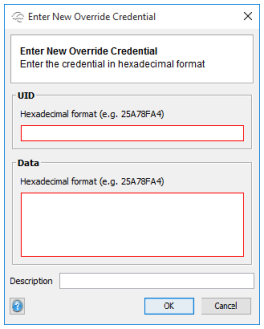
- **Card Type:** MIFARE Classic or MIFARE Plus.
- **UID:** Card number.
- **Sector data:** Sector data stored on the credential. This value is normally stored in the EAC.
- **Description:** For example the credential owner.

ISO 14443B UID



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

ISO 14443B UID and Data



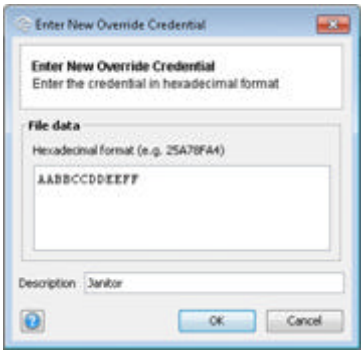
- **UID**: Card number.
- **Data**: The file data stored on the credential.

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

MIFARE DESFire UID

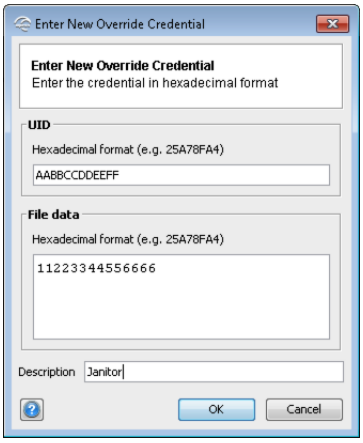
- **UID:** Card number.
- **Description:** For example the credential owner.

MIFARE DESFire Application



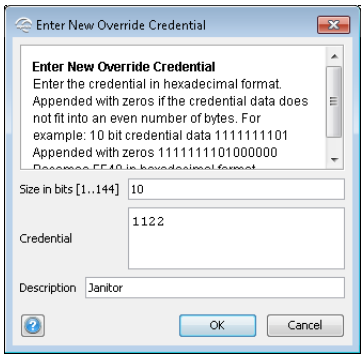
- **File data:** The file data stored on the credential.
- **Description:** For example the credential owner.

MIFARE DESFire UID and Application



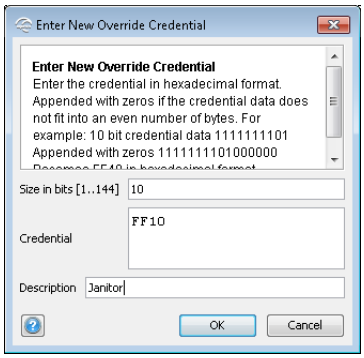
- **UID:** Card number.
- **File data:** The file data stored on the credential.
- **Description:** For example the credential owner.

iCLASS



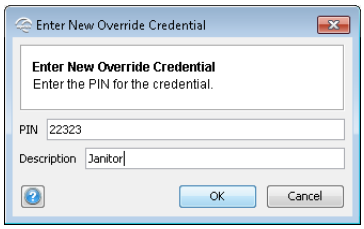
- **Size in bits [1...144]:** Number of bits used for credential data on the iCLASS credential.
- **Credential:** Card credential appended with zeroes on the right side, and translated to hexadecimal format.
- **Description:** For example the credential owner.

Low Frequency



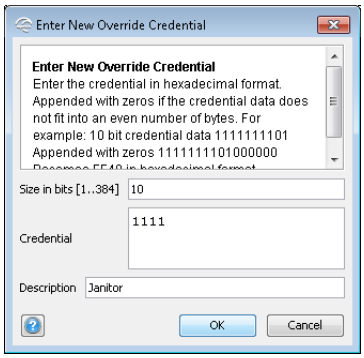
- **Size in bits [1...144]:** Number of bits used for credential data on the credential.
- **Credential:** Card credential appended with zeroes on the right side, and translated to hexadecimal format.
- **Description:** For example the credential owner.

PIN



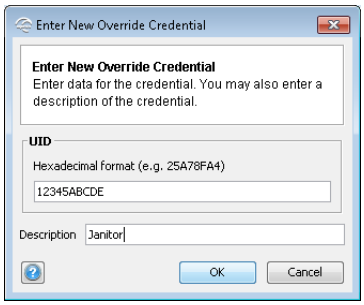
- **PIN:** PIN code
- **Description:** For example the PIN user.

Seos



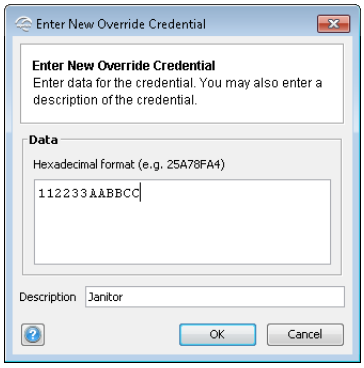
- **Size in bits [1...384]:** Number of bits used for credential data on the credential.
- **Credential:** Card credential appended with zeroes on the right side, and translated to hexadecimal format.
- **Description:** For example the credential owner.

Legic UID



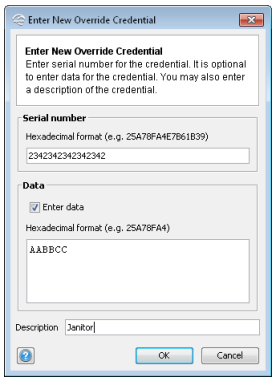
- **UID:** Card number.
- **Description:** For example the credential owner.

Legic Data



- **Data**: Sector data stored on the credential.
- **Description**: For example the credential owner.

PicoPass

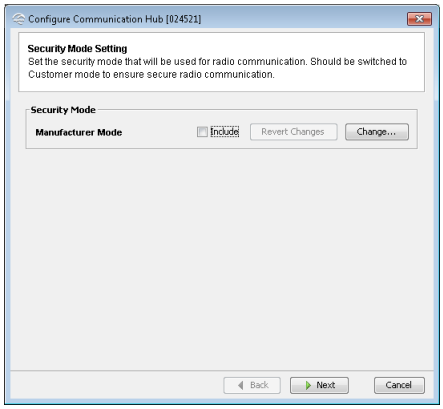


- ***Serial number***: The serial number in HEX format for the credential.
- ***Data***: Select ***Enter data*** to add credential data in HEX format.
- ***Description***: For example the credential owner.

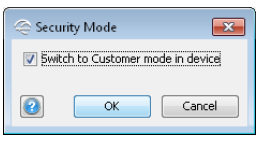
Security Mode Setting (Communication hub and Lock/sensor)

To open the Security Mode Setting window: right-click on a hub and select ***Lock/Sensor*** > ***Configure...***. Click ***Next*** until the menu appears.

This setting will apply for both the communication hub and the lock.



1. Click ***Change*** in the ***Security Mode Setting*** area if you want to change the security mode, or click ***Next***.
2. Check the check box ***Include*** to include the settings changed to the list of settings to be transmitted to the device, or to be saved by clicking ***Save configuration*** in the Update device wizard..
3. To change to customer mode, check the check box and click OK.



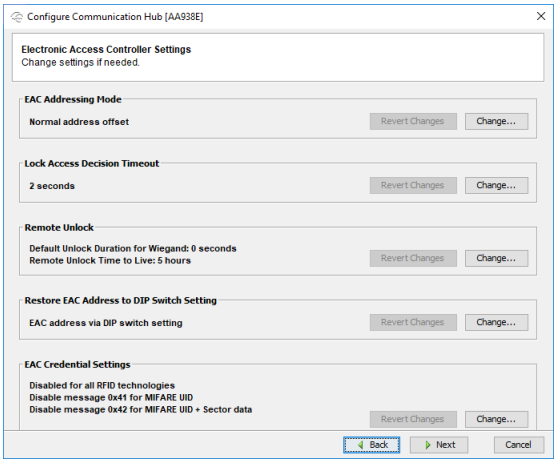
The default mode is Manufacturer mode, but you should always change it to Customer mode. If you change to Manufacturer mode the lock will no longer be using secure radio communication. Note that for AH40 communication hubs, TLS must also be enabled to allow customer mode to be set.

	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.

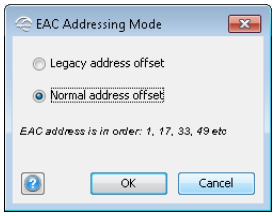
Electronic Access Controller Settings (Communication hub)

The following options apply for both RS-485, Wiegand and IP unless otherwise specified.

To open the Electronic Access Controller Settings window: right-click on a hub and select ***Communication hub*** > ***Configure...***. Click ***Next*** until the menu appears. Click ***Change...*** for each option to enter the settings.



EAC Addressing Mode (RS-485 only)



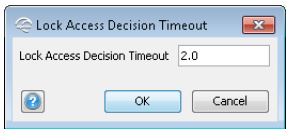
The default EAC addressing mode is Normal address offset, which means that the communication hub assigns the EAC address to the paired locks according to the addressing table, see Ref [1], Aperio Online Mechanical Installation manual. This setting is used when the EAC can handle addresses without limit.

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 and so on.
- **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).

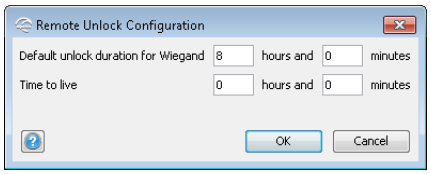
Mercury, Honeywell, and VertX AH30 communication hubs do not support normal address offset, but use addressing mode similar to Legacy mode.

Lock Access Decision Timeout



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

Remote Unlock Configuration



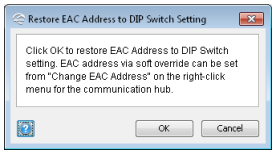
This function enables the Remote unlock functionality in the communication hub.

- **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 (grantAccessSequence) will be present in the communication hub. The maximum value is 17 hours and 59 minutes. (This setting must always be longer than the ***Status Report interval*** set in the lock.) This setting only applies for RS-485 communication hubs.

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.

Restore EAC Address to DIP Switch Setting (RS-485 only)

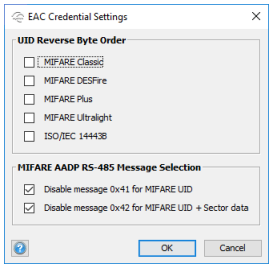


Clicking ***OK*** will restore the EAC addressing to what is configured with the DIP switches on the back of the communication hub.

After applying the change to DIP Switch mode on the last page of the wizard, the communication hub will be rebooted.

To set the EAC address digitally, use the ***Change EAC Address*** function on the right-click menu for the communication hub.

EAC Credential Settings

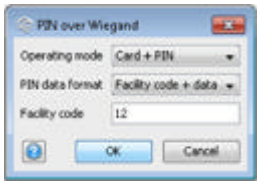


The selected credential types will have reversed byte order when the communication hub sends the UID information to the EAC.

For MIFARE AADP, messages for MIFARE UID and MIFARE UID with sector data can be disabled.

PIN over Wiegand (Communication hub)

This function activates the possibility to use PIN credentials with a Wiegand communication hub.



- ***Operating mode***: Select ***PIN*** or ***Card + PIN*** to activate the function. ***Card*** is the default operating mode. ***Card + PIN*** allows any combination of card and PIN to be used for access in the EAC.
- ***PIN data format***: The PIN format can be set to ***ASCII***, ***Facility code + data***, or ***Binary***.
- ***Facility code***: Each facility has a unique code that all credentials within the system share. This is a mandatory field that applies for the ***Facility code + data*** PIN data format. The maximum value is 255.

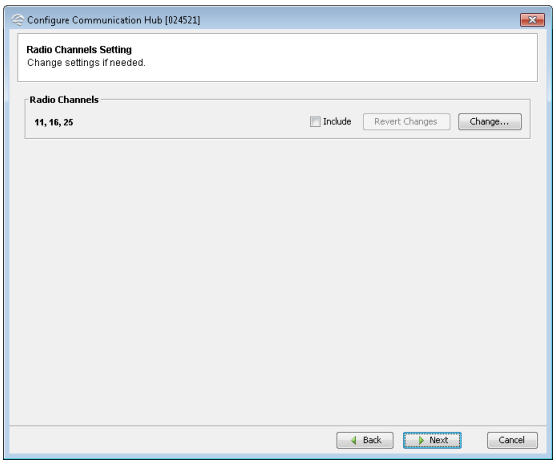
Radio Channels (Communication hub or Lock/sensor)

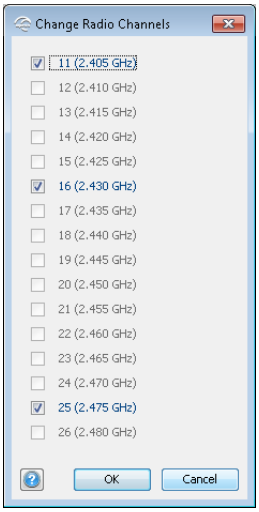
Always change the radio channel on the lock before changing on the communication hub.

This function is also available on the right-click menu in the ***Installation view***.

To open the Radio Channels Setting window: right-click on a hub and select ***Lock/Sensor*** → ***Configure...***. Click ***Next*** until the menu appears.

1. Click ***Change...*** to set the radio channel for the communication hub/lock/sensor.



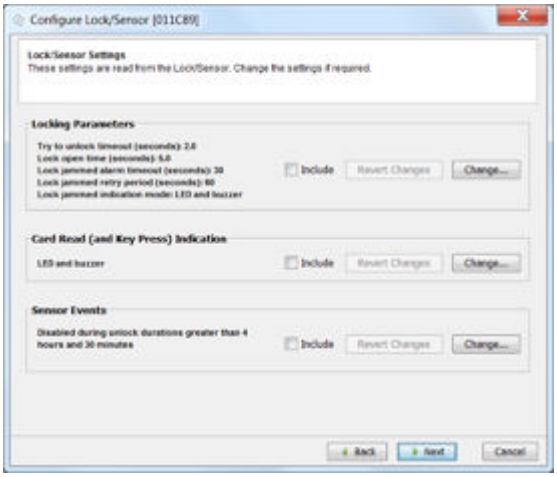


2. Deselect one or several of the used channels to make a new selection of channels.

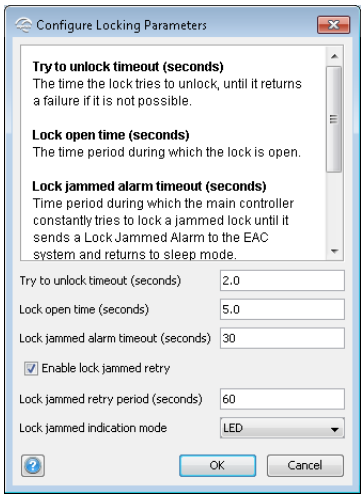
For the US market channel 26 is disabled.

Lock/Sensor Settings - Online

These settings allow configuration of ***Locking Parameters***, ***Card Read (and Key Press) Indication***, and ***Sensor Events***.



Locking Parameters



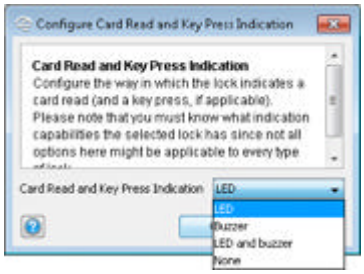
This dialog allows you to configure timing for different operations in the lock:

- ***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 is open, in seconds (default = 5 s).

Mercury and Honeywell AH30 communication hubs do not support this setting. For these type of communication hubs lock open time must be set through the protocol

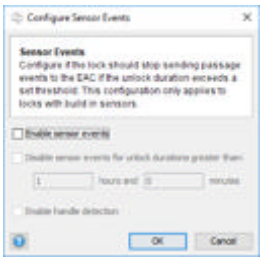
- ***Lock jammed alarm timeout (seconds)***: How long time the system tries to lock the lock before it sends an alarm to the EAC and goes back to idle state.
- ***Enable lock jammed retry***: This enables a periodic retry to lock the lock according the settings under ***Lock jammed retry period (seconds)***.
- ***Lock jammed retry period (seconds)***: How long the lock waits 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.

Card Read (and Key Press) 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.

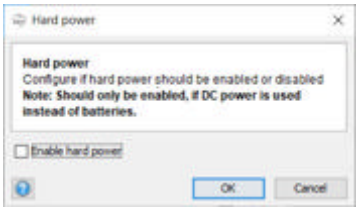
Sensor Events



This setting applies for locks with built in sensor. This setting will save battery life in high traffic doors.

- ***Enable sensor events***: By activating this function sensor events will be sent to the EAC.
- ***Disable sensor events for unlock durations greater than:*** The lock sensor will stop sending passage events to the EAC for unlock durations longer than set here.
- ***Enable handle detection***: Enables the lock to register handle change (inside/outside) and pass it on to the communication hub/EAC.

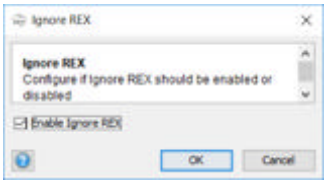
Hard power



This setting is only available after import of device dependent features using the ***Import Application Feature Data*** function, see section *Import Application Feature Data* on page 16.

- ***Enable hard power***: If the lock is equipped with hard power this setting will disable the Aperio platform's state of charge calculation and low battery warnings. Enable this setting to avoid confusion when monitoring a lock with a DC power option installed.

Ignore REX

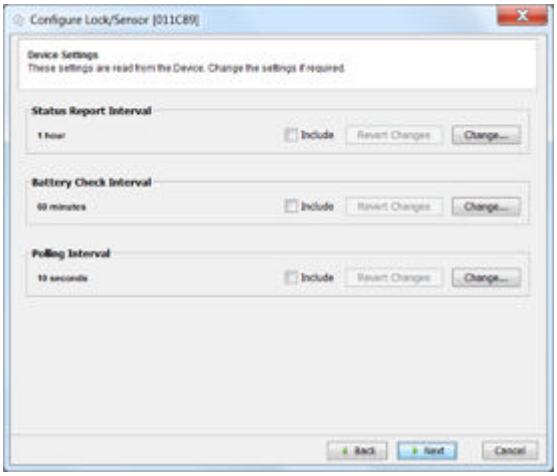


This setting is only available after import of device dependent features using the ***Import Application Feature Data*** function, see section *Import Application Feature Data* on page 16. It only applies for devices that can register REX (Request to exit) events.

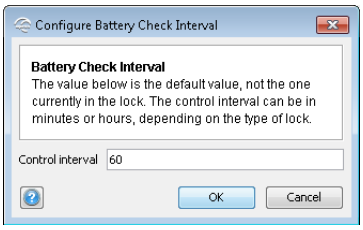
- ***Enable Ignore REX***: When enabled, the lock will ignore handle change, and REX event notification will not be sent to the EAC.
  This function is useful for devices with the inside and outside handle connected together, such as AU100. To avoid a REX message to the EAC every time someone enters the door from the outside the ***Ignore REX*** feature will disable the handle sensor event during access granted.

Device Settings

These settings allow configuration of ***Battery Check Interval***, ***Status Report Interval***, and ***Polling Interval*** and applies for both a communication hub and a lock/sensor.



Battery Check Interval

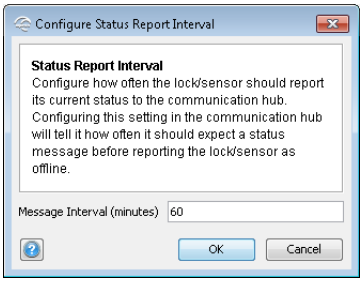


It may be necessary to adjust the control interval for this check depending on the type of battery used, and the surrounding temperature. For example in cold surroundings where the battery runs out faster. Default value is 60 (minutes).

For some products with battery measurement on the secure side (Aperio V2 P100/I100 currently), the interval you set translates into hours, i.e. 6 minutes = 6 hours.

An alarm event is sent to the EAC system when the battery is low.

Status Report Interval



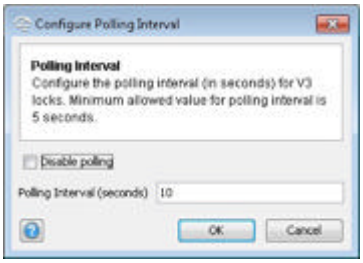
The interval setting is normally set to 60 minutes. If ***Remote unlock*** functionality is used, this parameter should be set to a shorter interval such somewhere in between 5 and 15 minutes.

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 with a value, equal or higher than the longest status report interval for the locks paired.

Polling Interval (V3 locks)



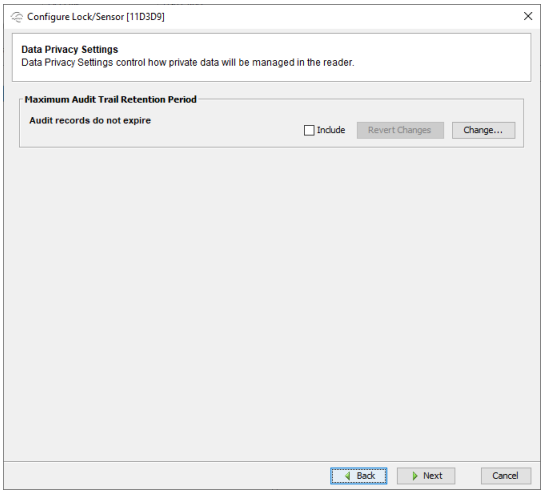
This setting only applies for V3 locks. Polling interval decides how often the lock wakes up and connects to the communication hub to check for information from the EAC. Unlike a status report, where the lock status information is also sent to the EAC, see section *Status Report Interval* on page 63.

Polling also allows the Aperio Programming Application to connect to the lock without the need of activating the radio with a credential (if set to less than 15 seconds). The default polling interval in the lock is 10 seconds.

To change this setting, enter a new polling interval here. Polling is deactivated in the lock by selecting ***Disable polling***. It is recommended to deactivate this function if the Remote unlock functionality is not used, or if the automatic connection to the lock without credential is not wanted.

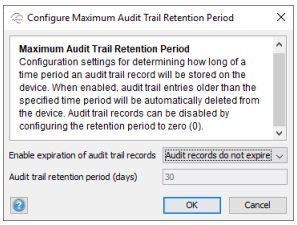
Data Privacy Settings

Data Privacy Settings control how private data will be managed by the device, in order to support local directives such as GDPR.



- ***Maximum Audit Trail Retention Period***: Setting for how long the audit trail is stored in the device.

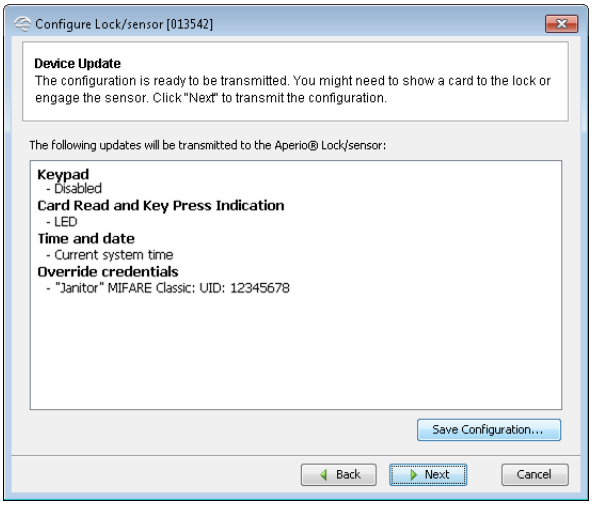
Maximum Audit Trail Retention Period



This function allows you to set how long credential data will be stored in the device:

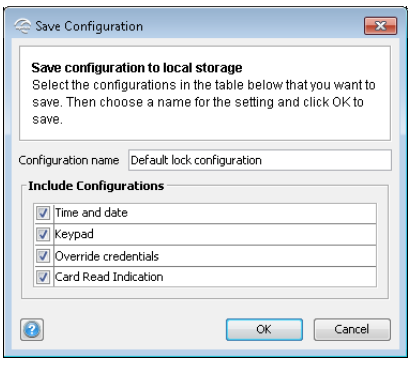
- ***Enable expiration of audit trail records:*** Enable/disable if credentials data will be deleted from the device. (Default: Audit records do not expire).
- ***Audit trail retention period (days)***: Sets the number of days the audit records are stored in the device. (Default: 30 days).

Device Update page – Save Configuration



The Device Update dialog shows a summary of the configuration tasks that will be downloaded to communication hub/lock/sensor. The summary lists all settings for features where the ***Include*** check box has been checked while updating. The configuration may be used later to configure other devices with the same information, by clicking ***Save configuration***:

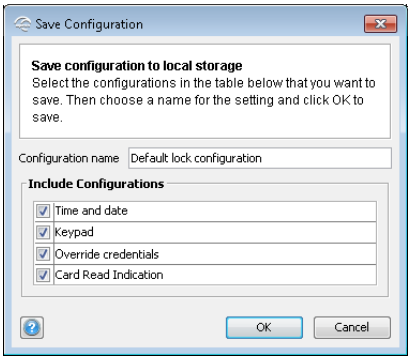
1. The ***Save Configuration*** dialog box shows a summary of the configuration tasks that have been collected during the different steps in the Configuration Wizard. Exclude configuration tasks by clicking the check boxes.



2. Recommended tasks to save could be:
   - RFID configuration
   - Change security mode
   - Override credential
   - Device time update
   - And optionally some advanced features like Battery Alarm, Status configuration and Locking parameters.

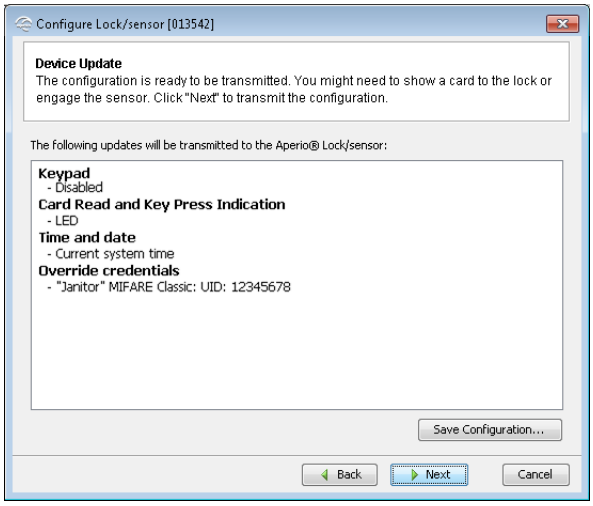
   Create a set of configurations for the most common settings in your system.

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 unit type.

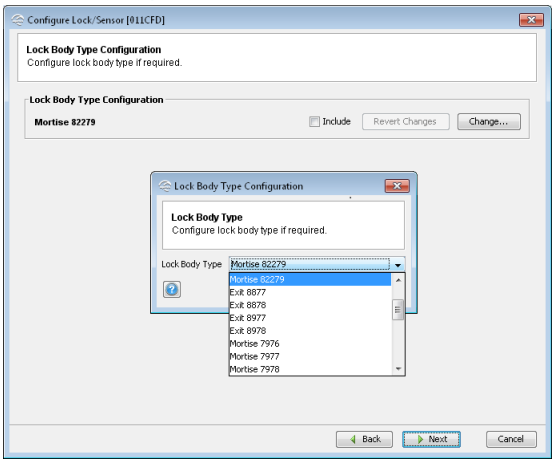


4. Click ***OK***.

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



Lock Body Type Configuration



The ***Lock Body Type Configuration*** page is only visible if (1) an XML-file with lock body type data is imported, (2) the PCB id of the lock matches one of the products in the XML-file, and (3) the ***Device Aware Wizard*** is enabled.

The PCB id of the lock can be determined by using ***Retrieve System Information***.

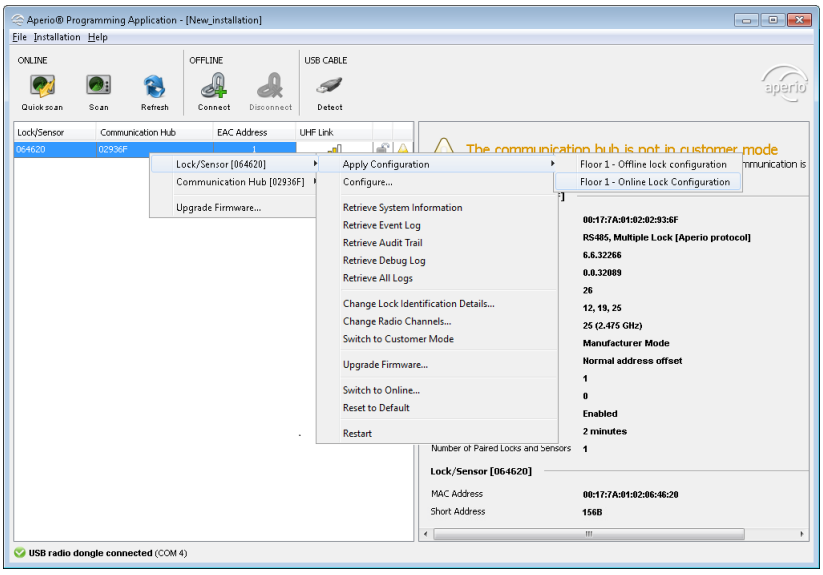
The XML-file is imported in the menu, ***Installation*** → ***Import Lock Body Type Data***.

Applying a Stored Configuration to a Communication Hub/lock/sensor

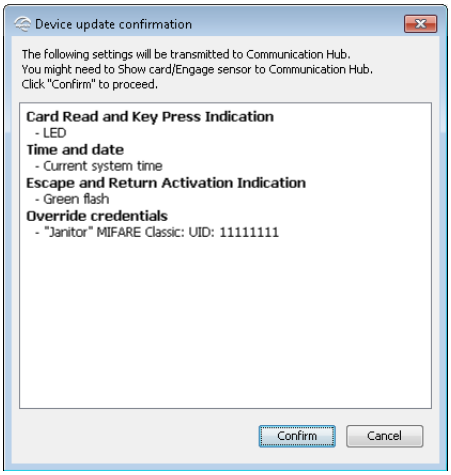
If you saved a configuration in the configuration wizard, you can apply it to numerous locks/sensors. This function is available on the communication hub/lock/sensor sub-menu or directly on the right-click menu for offline locks. Only hardware specific settings are downloaded to the selected unit.

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

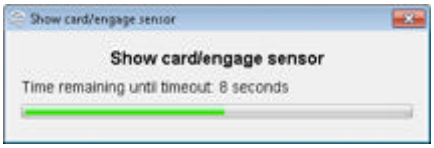
1. In the ***Installation view***, right-click and select communication hub/lock/sensor, on the sub-menu select ***Apply Configuration*** and choose an earlier stored configuration.



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



3. Hold the credential at the lock, or engage the magnet for the sensor. (This step is not necessary for V3 locks that are connected with a USB cable, or online locks that have the polling interval set to less than 15 seconds.) For a communication hub the information is updated immediately.

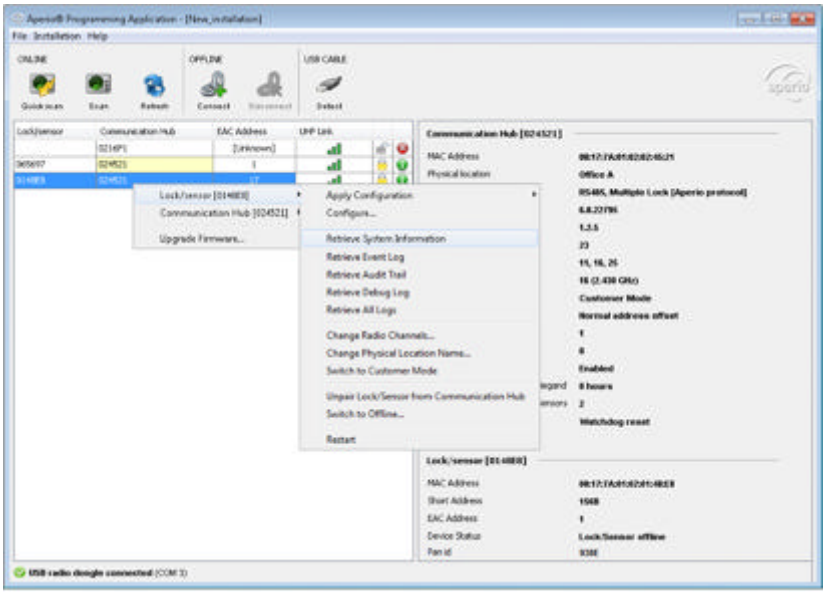


4. After download the result is shown. The settings that could not be transferred to the specific hardware are ignored. Click ***Close*** to finish.

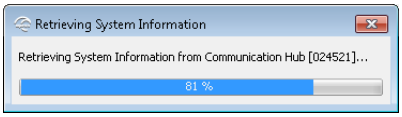
5. Repeat all the steps from the beginning of this section for every lock/sensor you want to configure with a saved configuration.

Retrieve System Information

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

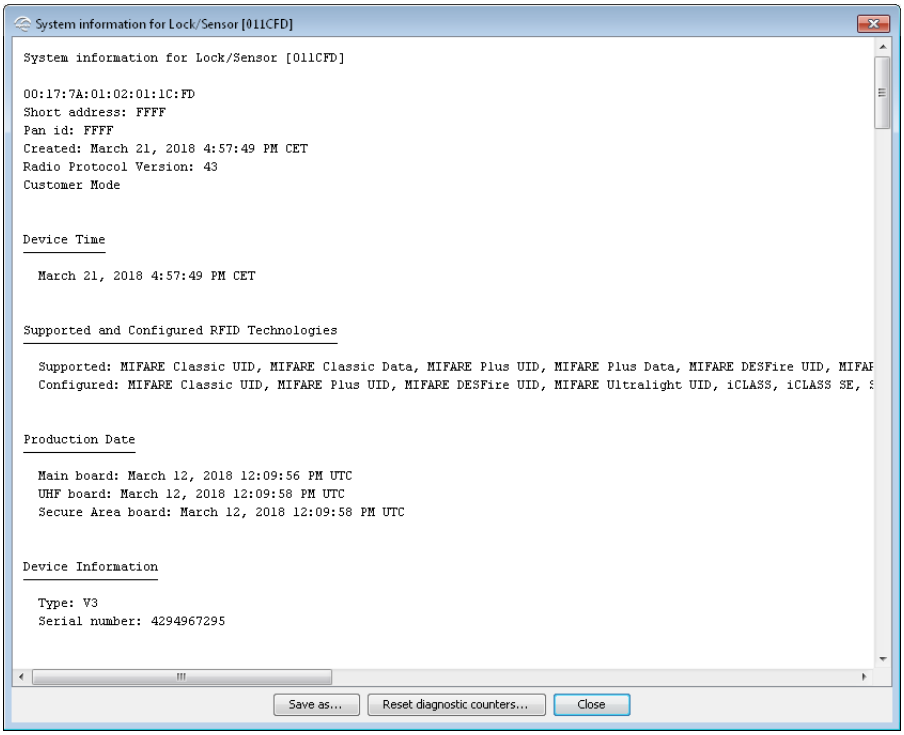


1. Right-click and select ***Lock/Sensor*** or ***Communication Hub*** → ***Retrieve System Information*** to access the unit.



Result: The Aperio Programming Application connects to the unit.

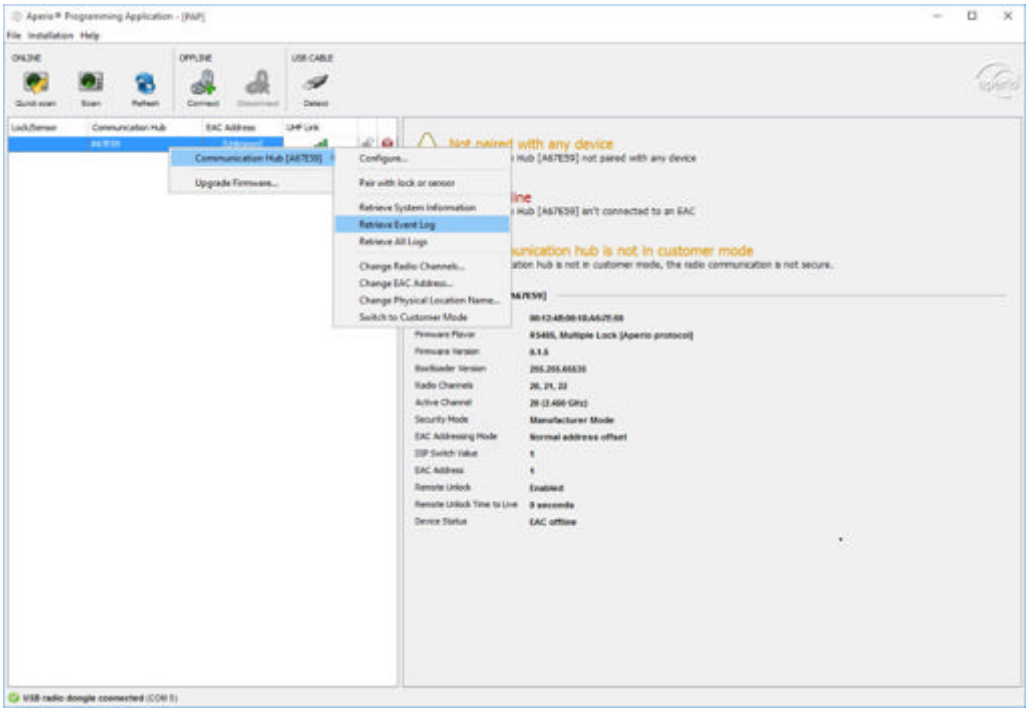
2. Click ***Save as*** to save the system information to a local storage, Click ***Reset diagnostic counters*** to reset the diagnostic counters in the device or click ***Close*** to exit.



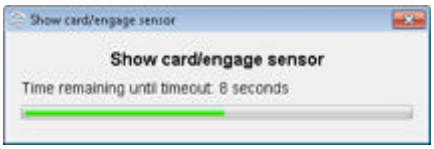
Retrieve Event Log

This function displays the event log for a particular lock or an AH40 or AH20/30 gen 5 communication hub (this function is not available for sensor), where you can find all system events performed on the device. In the example below the event log is retrieved from a lock.

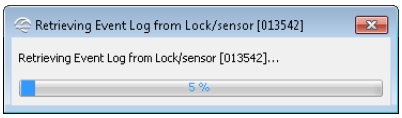
1. Right-click and select ***Lock/Sensor*** → ***Retrieve Event Log*** or ***Communication Hub*** → ***Retrieve Event Log***.



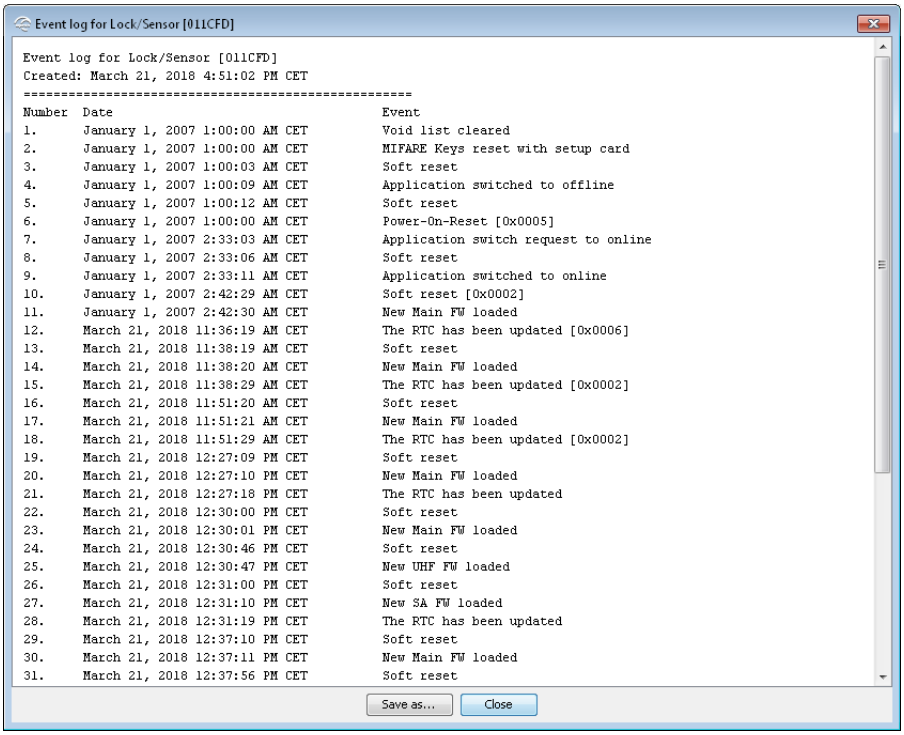
2. Hold the credential at the lock, or engage the magnet for the sensor. (This step is not necessary for V3 locks that are connected with a USB cable, or online locks that have the polling interval set to less than 15 seconds.)



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.



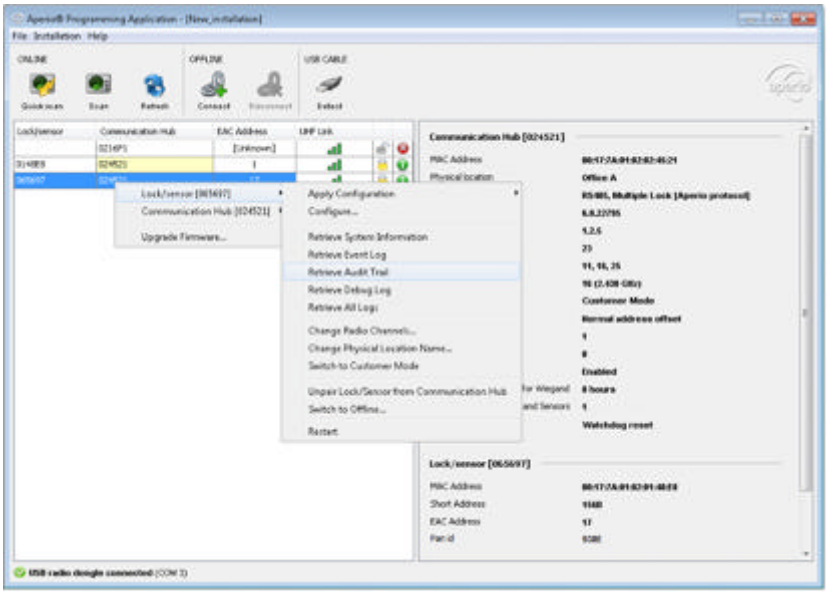
The window contains information about system events including consecutive number, date, and what type of system event that was performed. (If the number of events exceeds 200 older events are overwritten.)

Retrieve Audit Trail

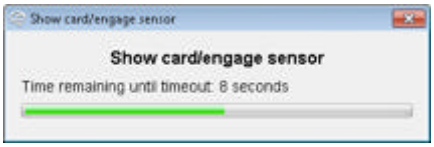
This function displays the list of access attempts for a lock (not available for sensor). It shows the latest 200 records.

Access attempts are stored only when the lock is not in connection with the EAC.

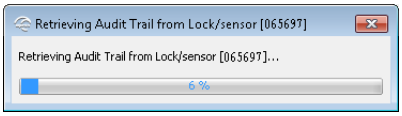
1. Right-click and select ***Lock/Sensor → Retrieve Audit Trail***



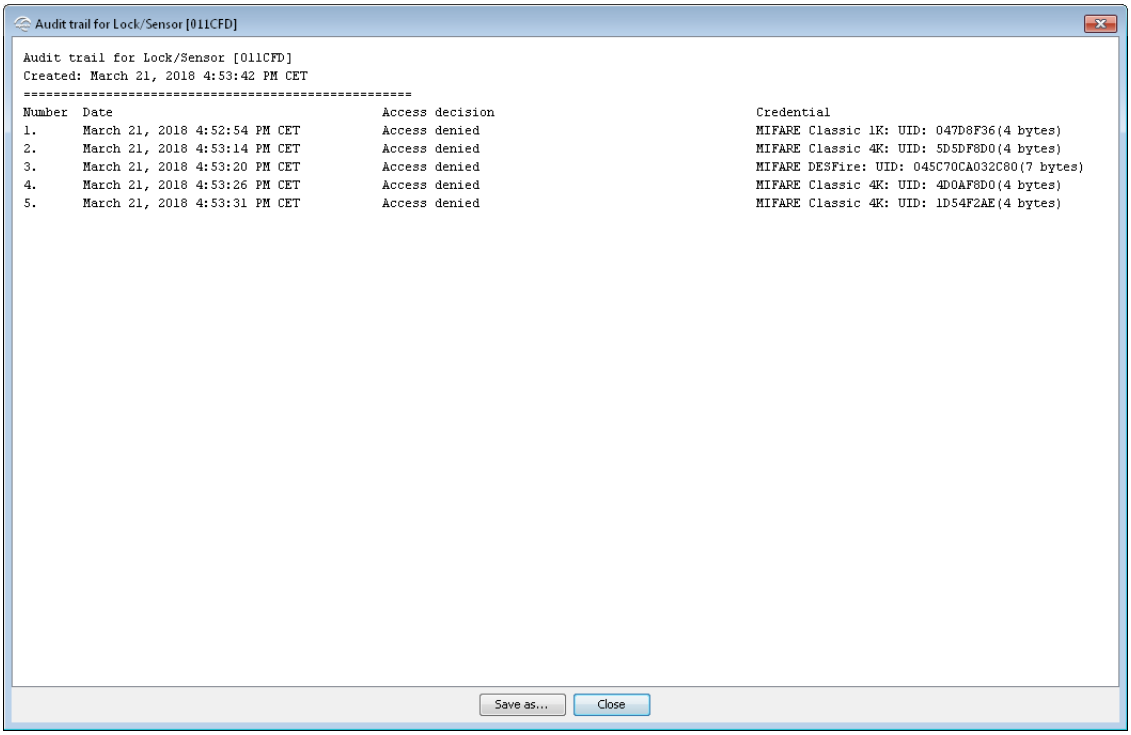
2. Hold the credential at the lock, or engage the magnet for the sensor. (This step is not necessary for V3 locks that are connected with a USB cable, or online locks that have the polling interval set to less than 15 seconds.)



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.

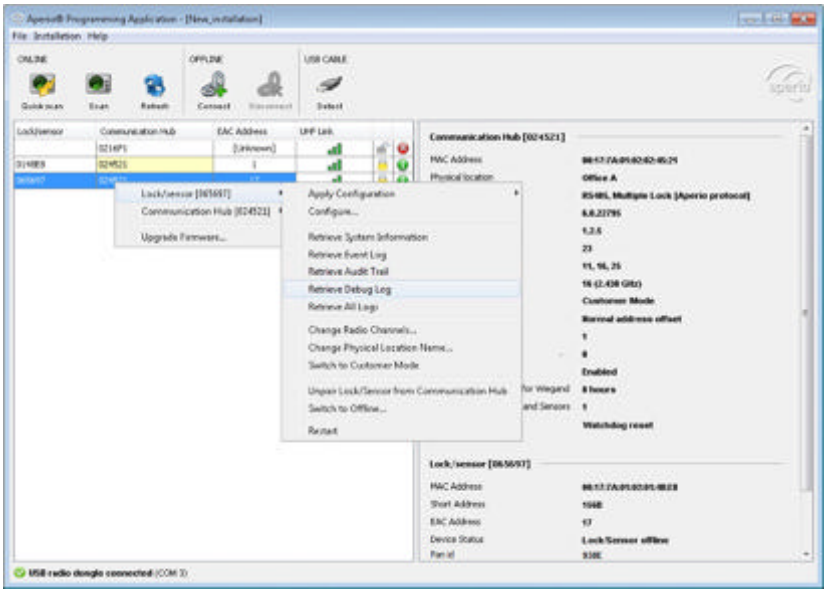


The window contains information about the latest 200 access attempts including consecutive number, date, access decision and what type of credential that was used at each attempt.
The audit trail is encrypted for V3 locks. If the lock is in manufacturer mode when the audit trail is downloaded, it shows `<Encrypted>` instead of the credential, for access attempts that was made in customer mode, and the other way around.

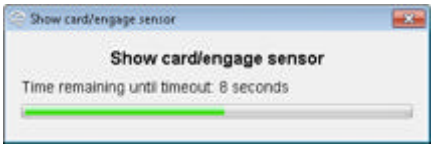
Retrieve Debug Log (V3 locks)

This function displays a debug log, intended for support and maintenance purposes. This menu item is only visible for V3 locks with firmware version 3.2 or higher.

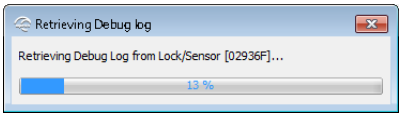
1. Right-click and select ***Lock/Sensor*** → ***Retrieve Debug Log***



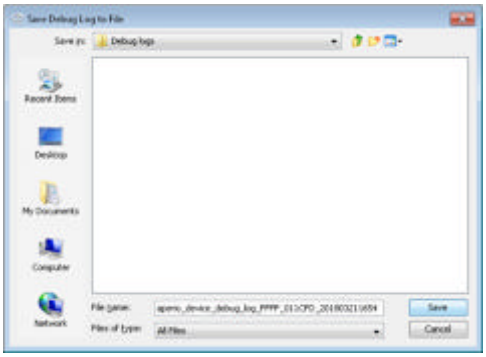
2. Hold the credential at the lock, or engage the magnet for the sensor. (This step is not necessary for V3 locks that are connected with a USB cable, or online locks that have the polling interval set to less than 15 seconds.)



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



3. Edit the name for the generated XML-file if needed, and click ***Save***.

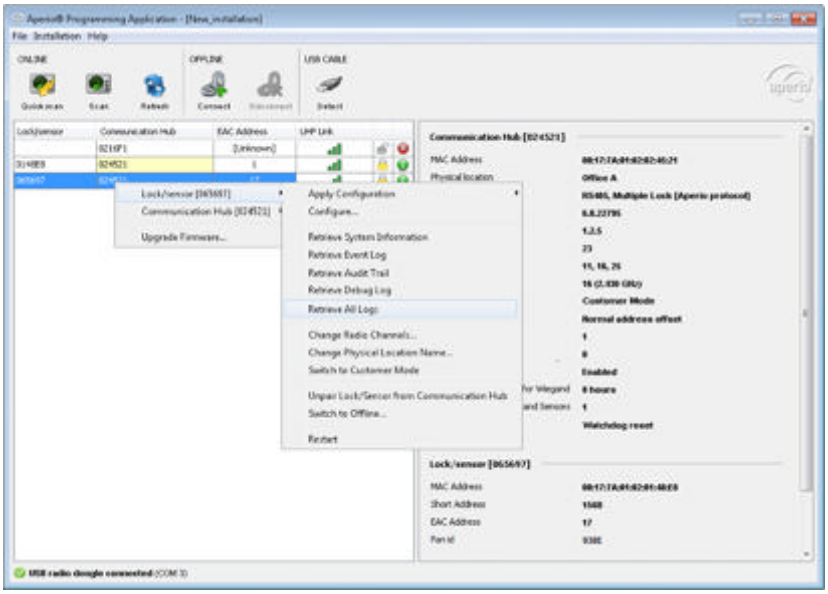


Retrieve All Logs

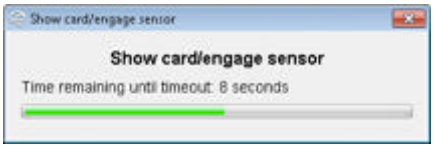
This function displays the list of access attempts for a lock (not available for sensor). It shows the latest 200 records.

Access attempts are stored only when the lock is not in connection with the EAC.

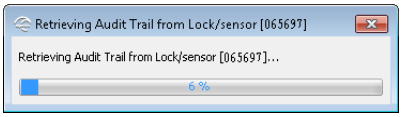
1. Right-click and select ***Lock/Sensor*** → ***Retrieve All Logs*** (or directly on the right-click menu)



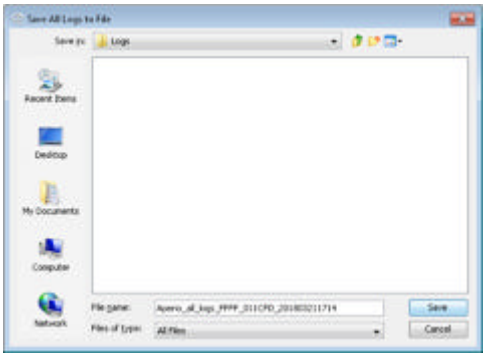
2. Hold the credential at the lock, or engage the magnet for the sensor. (This step is not necessary for V3 locks that are connected with a USB cable, or online locks that have the polling interval set to less than 15 seconds.)



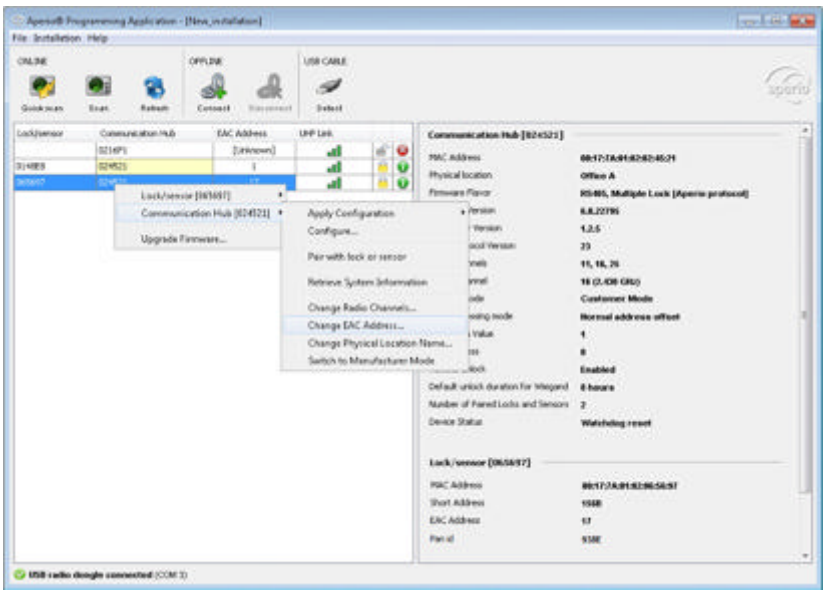
Result: Successful reading initiates the download of all logs.



3. Edit the name for the generated zip-file if needed, and click ***Save***.



Change EAC Address

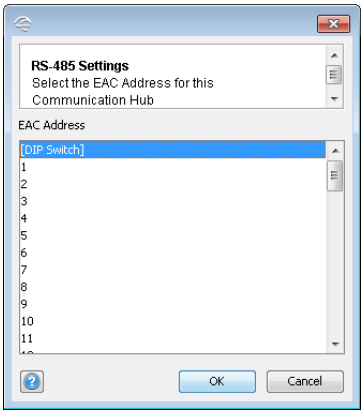


It is recommended to use the DIP Switch for setting the EAC address of communication hubs.

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 Aperio 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***.



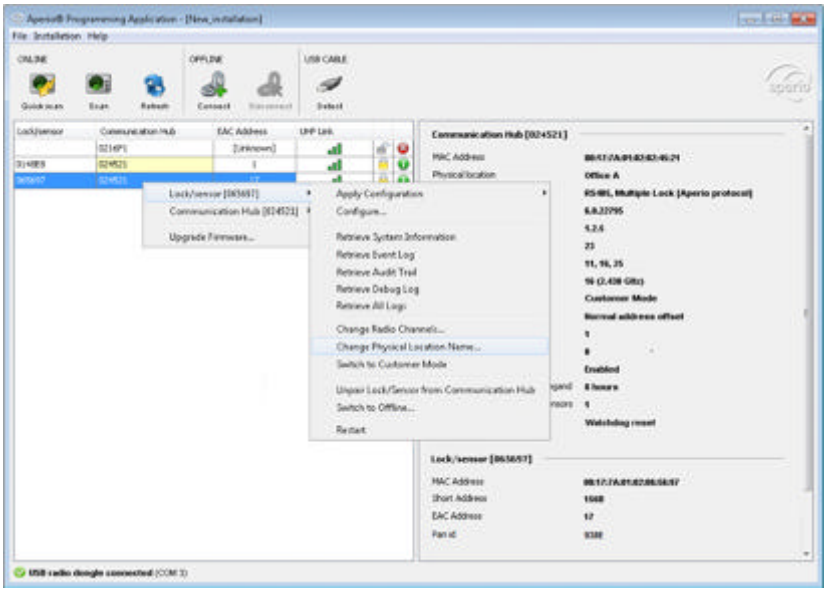
2. Select the address and click ***OK***.

After change of EAC address, hubs will be rebooted.

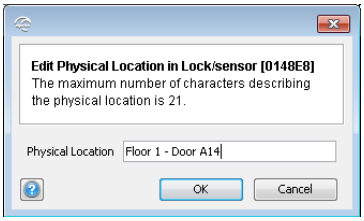
Change Physical Location Name

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

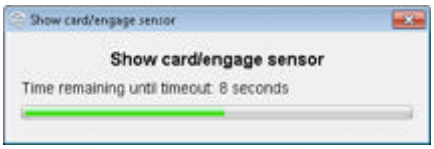
1. Right-click and select ***Lock/Sensor*** → ***Change Physical Location Name....***



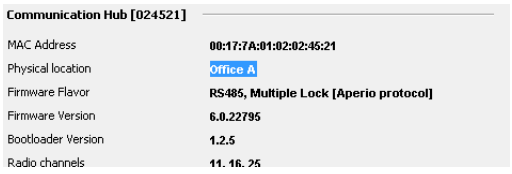
2. Enter a description that clearly identifies the lock position and click ***OK***.



3. Hold the credential at the lock, or engage the magnet for the sensor. (This step is not necessary for V3 locks that are connected with a USB cable, or online locks that have the polling interval set to less than 15 seconds.) For a communication hub the information is updated immediately.



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

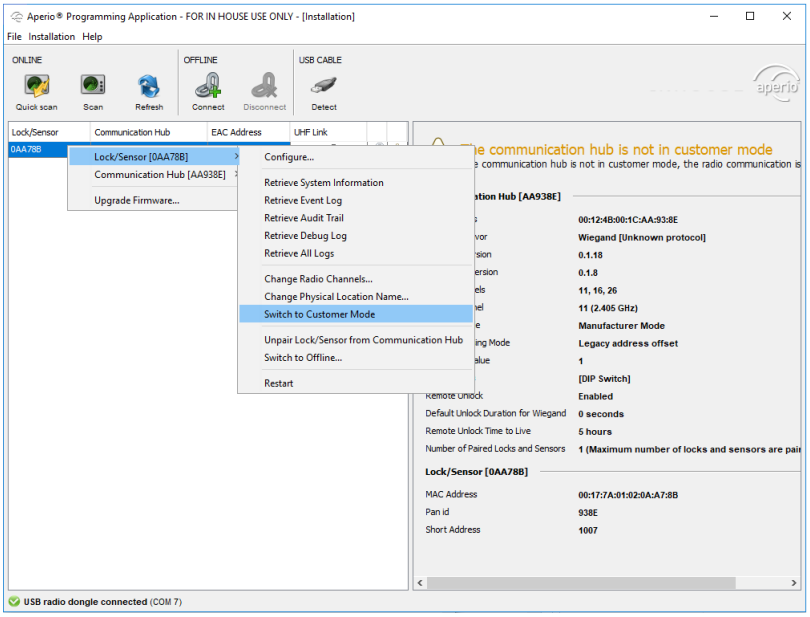
Secure communication is normally set during first configuration of locks/sensors and communication hubs with the configure wizard. Security mode is also accessible through the right-click menu.

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.

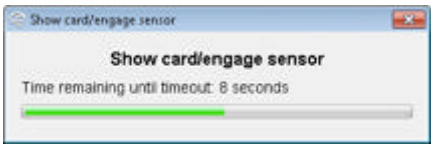
Explanation of symbols:

	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.

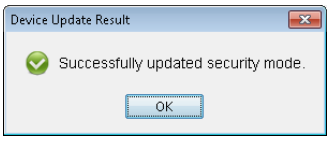
1. Right-click the unit and select ***Switch to Customer Mode/Switch to Manufacturer mode*** (This function is found directly on the right-click menu for offline locks).



2. Hold the credential at the lock, or engage the magnet for the sensor. (This step is not necessary for V3 locks that are connected with a USB cable, or online locks that have the polling interval set to less than 15 seconds.)



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 lock to see that the door has been set to Customer mode/Manufacturer mode.

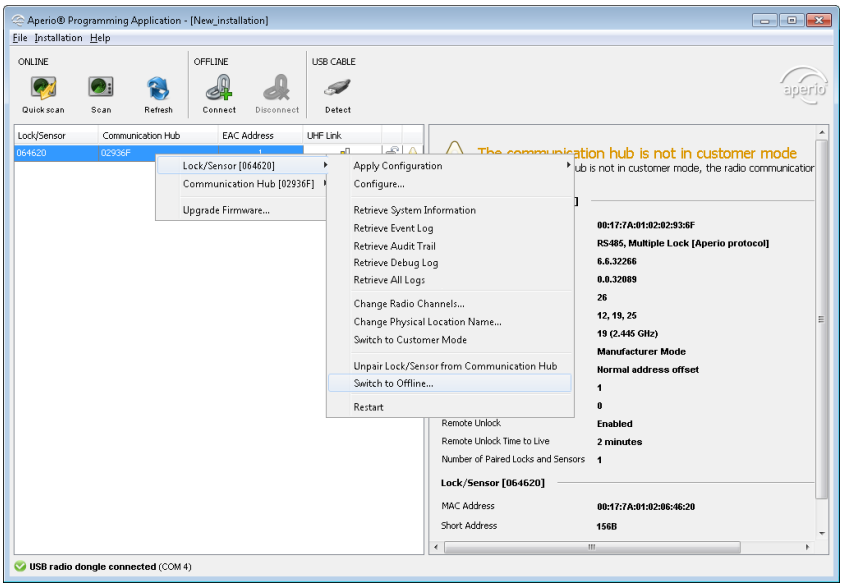
For Aperio online, the AH40 communication hubs must be connected to an EAC system (steady green light on the LED) to accept change of security mode. TLS encryption must also be enabled in the communication hub. If not so, the following error message is shown:

Switch to Offline (V3 locks)

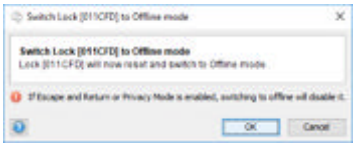
This function is only available if ***Show advanced settings*** is activated in Preferences, see section *Preferences* on page 8.

This function changes the operating mode of the selected V3 lock (V3.3 and higher).

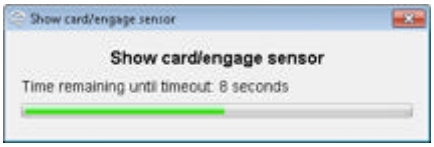
1. Right-click and select ***Lock/Sensor*** → ***Switch to Offline/Online***



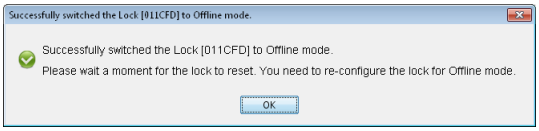
2. Click ***OK*** to change the operating mode for the lock.



3. Hold the credential at the lock. (This step is not necessary for V3 locks that are connected with a USB cable, or that have the polling interval set to less than 15 seconds.)



4. Confirm the change of operating mode.



After switching to **Offline**: Unpair the lock from the communication hub before reconfiguration.

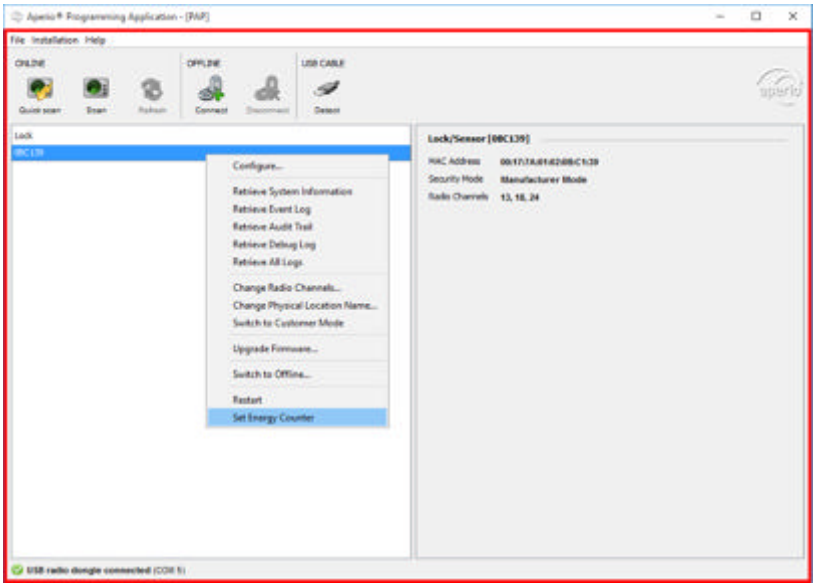
5. Reconnect to the lock, before performing further configuration according to the new operating mode.

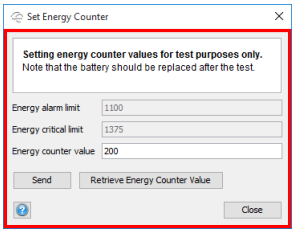
Set Energy Counter

This feature is only available when ***Advanced test mode*** is enabled in the Aperio programming application, see *Preferences* on page 8.

This only applies to products with lithium batteries that are using energy counter such as: C100/E100/L100/H100/R100/K100/KS100.

This function allows for tests of the lock to verify correct operation at low battery levels.





- ***Energy alarm limit***: The value when the lock triggers battery low level.
- ***Energy critical limit***: The value when the lock triggers battery flat level.
- ***Energy counter value***: The battery counter value to be sent to lock.

Click ***Retrieve Energy Counter Value*** to fetch the current value in the lock.

Click ***Send*** to start testing the lock with the entered battery counter value.

When clicking ***Close***, the energy counter in the battery is reset to original value before testing.

Note that the battery should be replaced after the test.

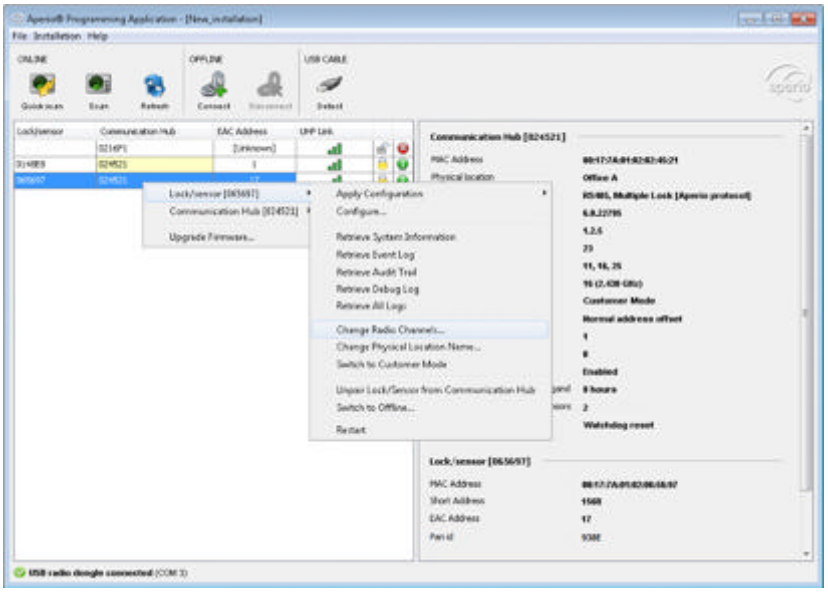
Change Radio Channels

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.

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

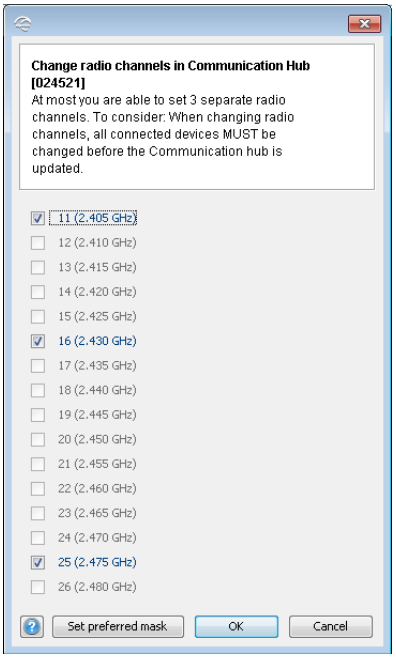
The lock radio channels may be inaccurate if the communication hub details are refreshed when the locks and hubs are on different channels.

1. Select the lock/sensor in the scan result table. Right-click and select ***Lock/Sensor*** → ***Change Radio Channels...***.

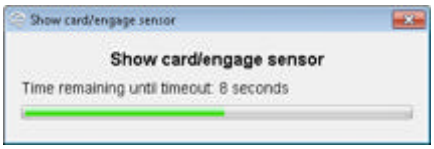


2. Unselect any of the three currently used channels to be able to select other radio channels. Click ***OK***.

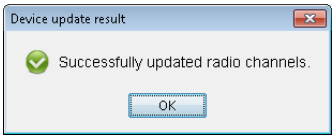
For the US market channel 26 is disabled.



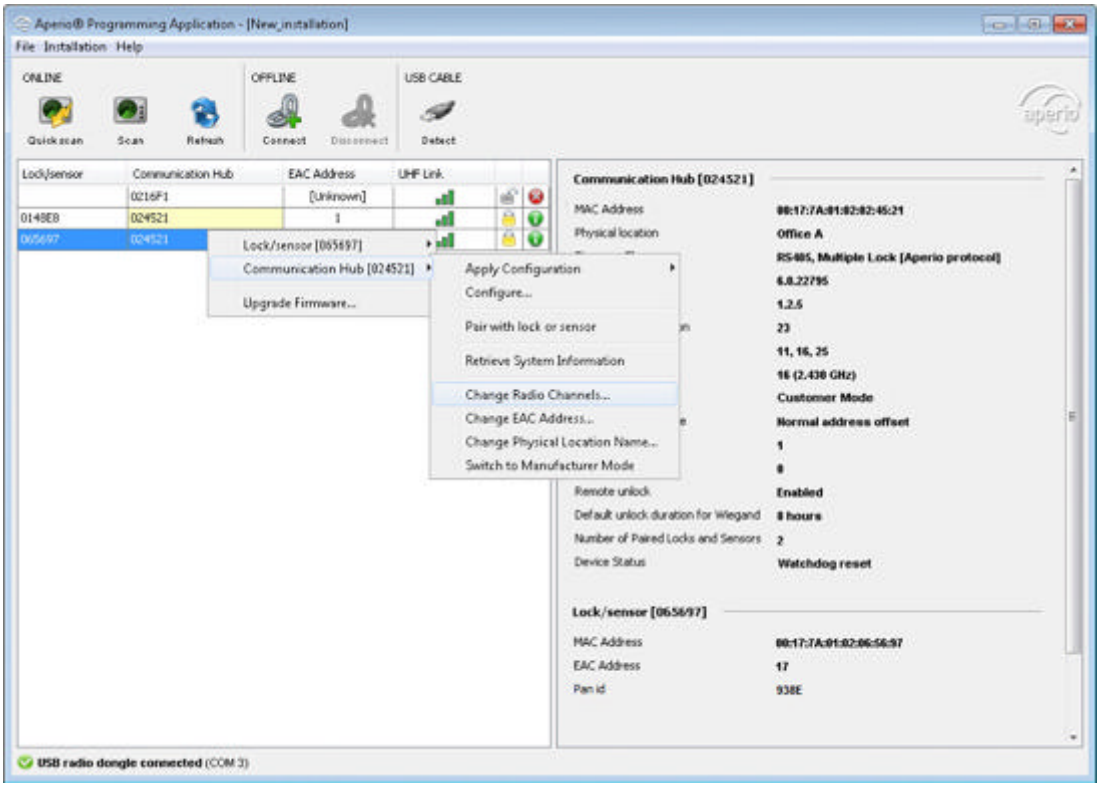
3. Hold the credential at the lock, or engage the magnet for the sensor. (This step is not necessary for V3 locks that are connected with a USB cable, or online locks that have the polling interval set to less than 15 seconds.)



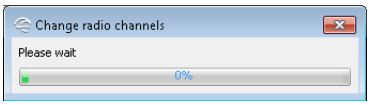
Result: A progress bar shows that the update is being performed. The ***Device Update Result*** dialog box shows the result of the update when it has been performed.

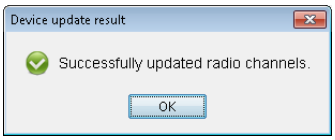


4. Repeat this procedure for all locks/sensors connected to the current communication hub. **Recommendation:** All locks/sensors should use the same three channels in order to create a more stable radio connection. Communication problems occur more likely between closely installed communication hubs 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. Unselect 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.

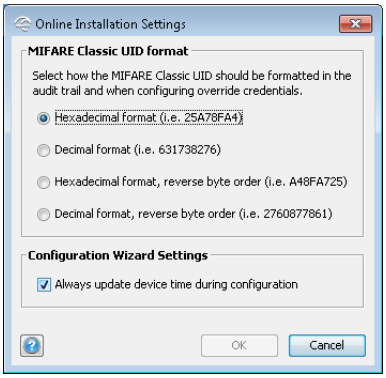




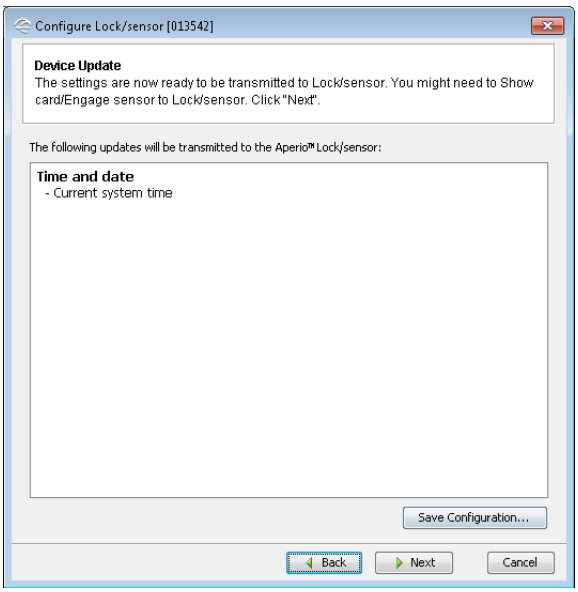
Setting the Time of a Lock

Follow these steps to set the time of a lock:

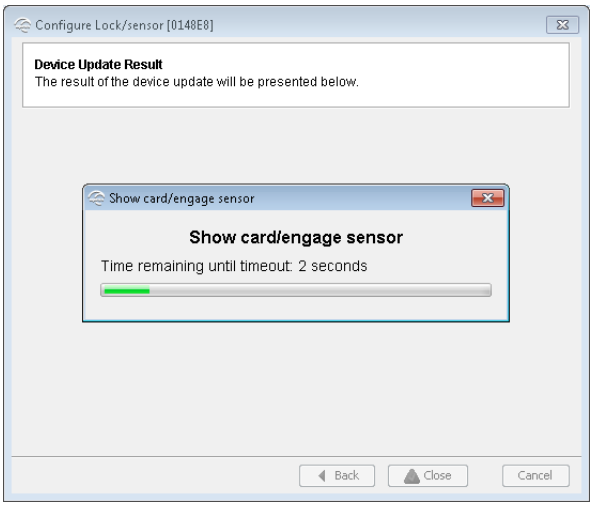
1. Select the lock in the installation view.
2. In the menu bar select ***Installation*** → ***Online*** → ***Settings*** and check that the ***Always update device time during configuration*** check box is checked.



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



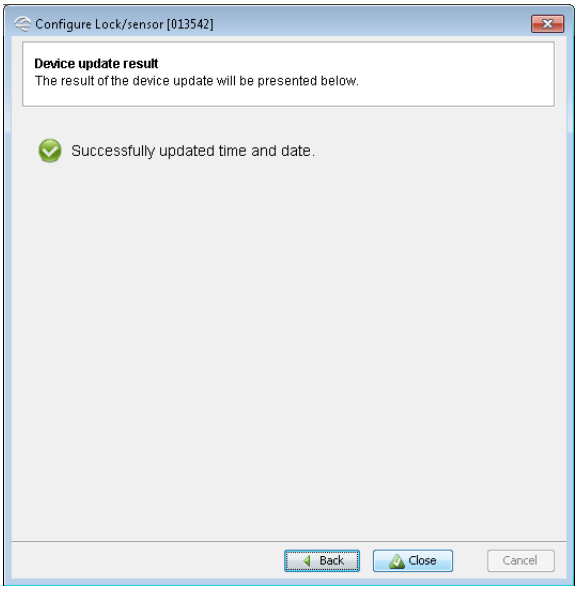
4. Click ***Next***.



5. Hold the credential at the lock. (This step is not necessary for V3 locks that are connected with a USB cable, or that have the polling interval set to less than 15 seconds.)

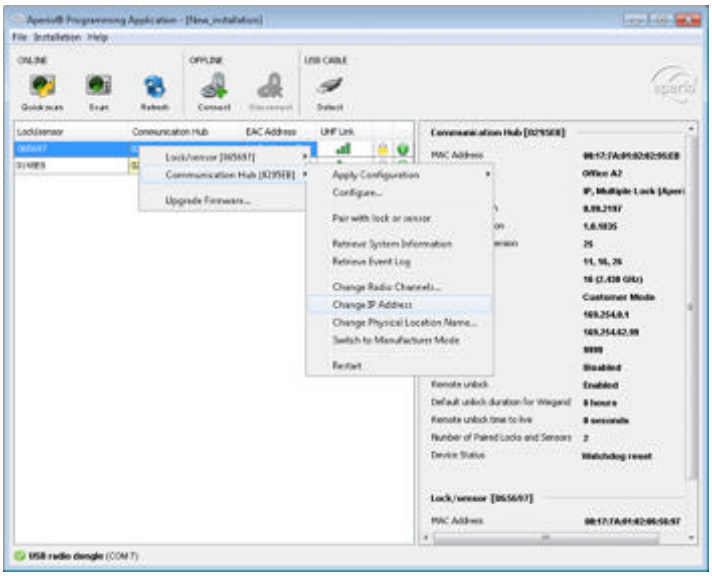
The time of the lock will now be automatically set each time you configure and update the device.

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

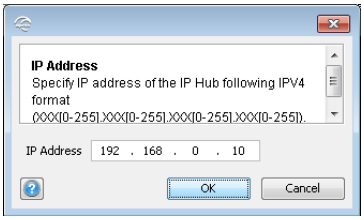


Change IP Address (Communication Hub AH40)

1. Right-click and select ***Communication Hub*** → ***Change IP Address***.

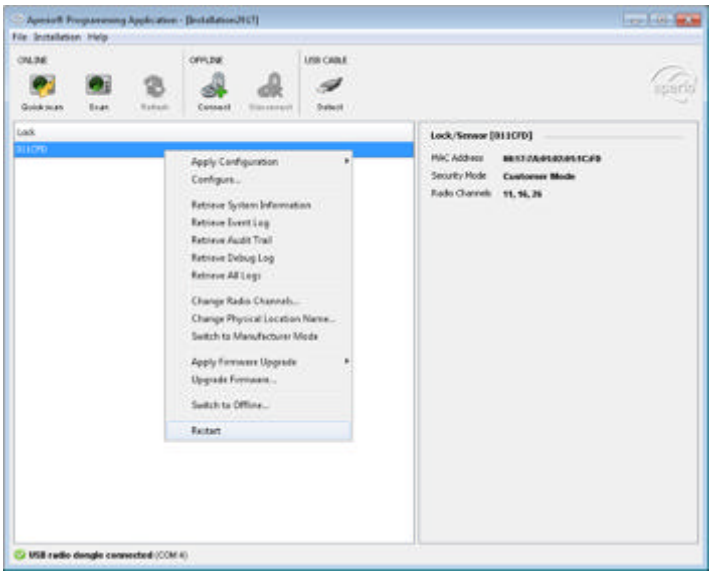


2. Fill in the IP address of the communication hub. Click ***OK*** and the new IP address will be applied in the communication hub, and the IP communication will be restarted using the new IP address.

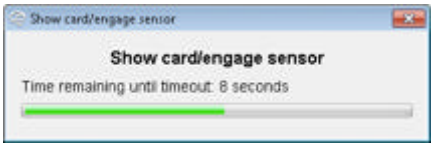


Restart (Communication Hub AH40 / Locks)

1. On the ***Lock/Sensor*** or ***Communication Hub*** right-click sub-menu, select ***Restart***.



2. Hold the credential at the lock, or engage the magnet for the sensor. (This step is not necessary for V3 locks that are connected with a USB cable, or online locks that have the polling interval set to less than 15 seconds.) This step does not apply for communication hubs either.



3. Click ***OK*** to close.

Allow the device to restart for approximately 10 seconds. Reconnect to the device to perform further configuration.

Manage Configurations

General

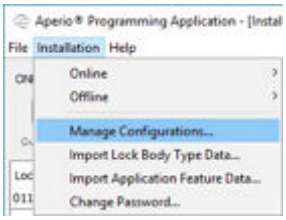
The stored configurations made in the configuration wizard, can be exported to a file so that more than one Aperio Programming Application can share the same configuration information. When you

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.

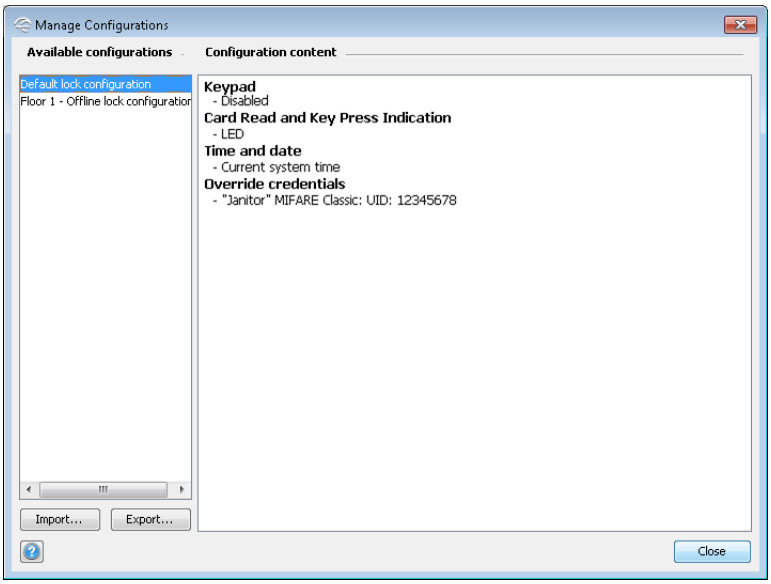
When you export a configuration, you cannot change the name of the configuration, only the file name holding the configuration information. Since configurations can be shared between different Aperio Programming Applications, it is preferable that a shared configuration (identified by its unique name) 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

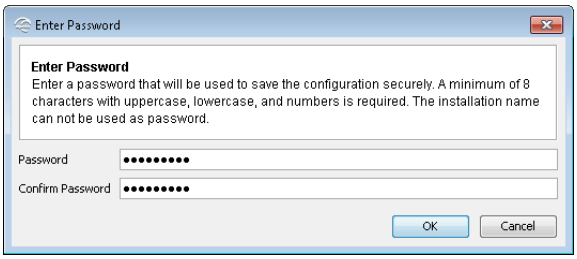
1. In the menu bar, select ***Installation*** → ***Manage Configurations***.



2. Select the configuration that should be exported to file and click ***Export...***.



3. Select the folder where you want to store the configuration, chose a file name and click ***Save***.
4. Choose a password that will be used when importing the particular configuration, confirm it and click ***OK***.



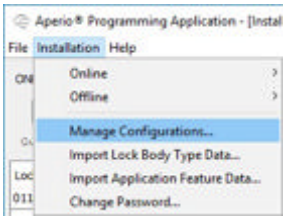
The password must contain at least 8 characters of which at least one upper and lower case character and a number.

Result:

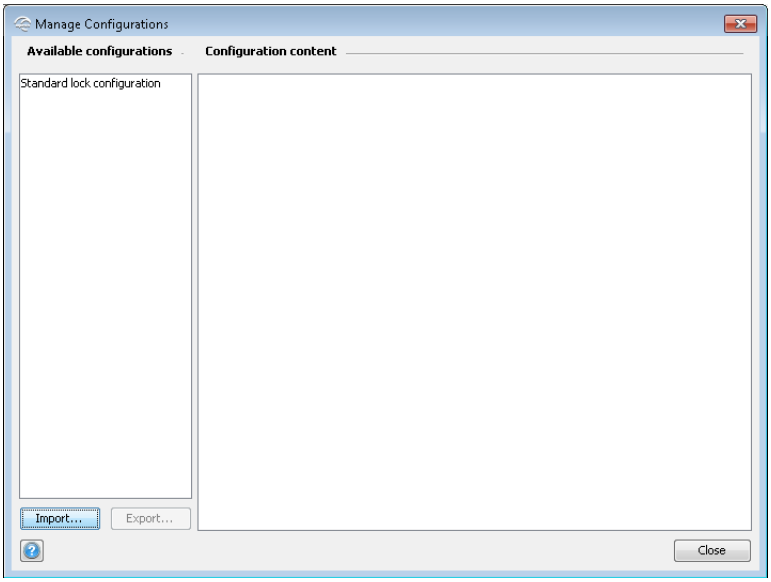
Importing Configuration

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

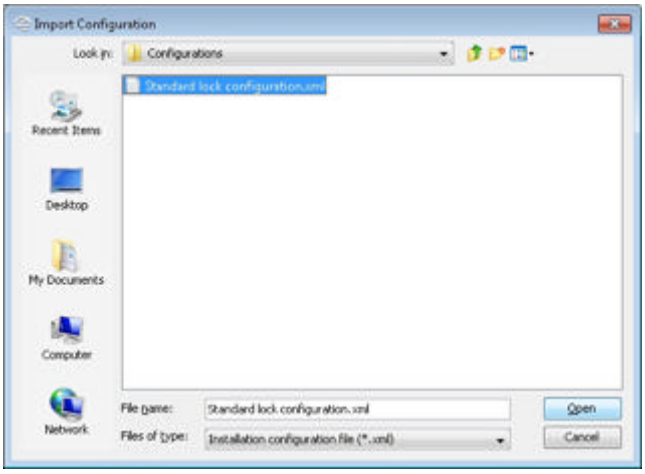
1. In the menu bar, select ***Installation*** → ***Manage Configurations***.



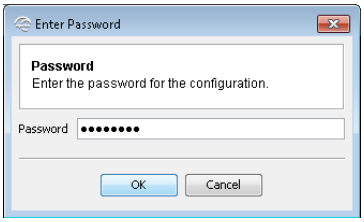
2. Click ***Import***.



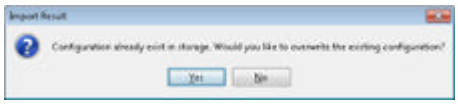
3. Select a valid configuration XML-file and click ***Open***.



4. Enter the password and click ***OK***.

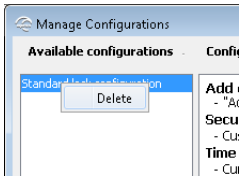


The configuration is identified by its name, not the name of the export file. When importing a configuration that already exists in the Aperio Programming Application you will be prompted if you want to replace the existing configuration.



Deleting Configuration

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



Upgrade of Aperio Hardware Firmware

This chapter describes how to upgrade both online and offline communication hubs and locks/sensors with a new firmware that is contained in the firmware file. 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.

Consider the following notes when upgrading the Aperio online firmware:

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 selecting a device for firmware upgrade the Aperio Programming Application will compare the current device firmware version to the new firmware version in the afw file. In the firmware upgrade window upgrade components for units with firmware older than the version contained in the afw file will be selected by default. The rest will be greyed and not selected.

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 must be used to download the new firmware, which requires that the AH40 communication hub IP address and other network settings has correctly been 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.

Upgrade Firmware

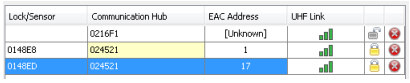
No sanity check is done by the Aperio Programming Application before the firmware download starts. Applying an older firmware than installed can cause the hardware to malfunction.

The Aperio 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.

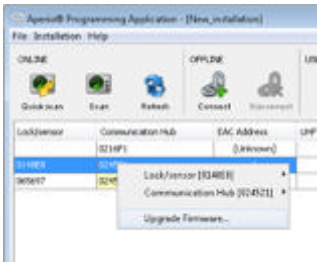
All firmware included in the afw file should be downloaded to hardware. Canceling the upgrade process or partly upgrading the hardware can cause malfunction.

Do not remove the battery or the V3 locks USB cable during the upgrade process. This can cause malfunction.

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 Aperio Programming Application will not enable the upgrade function.

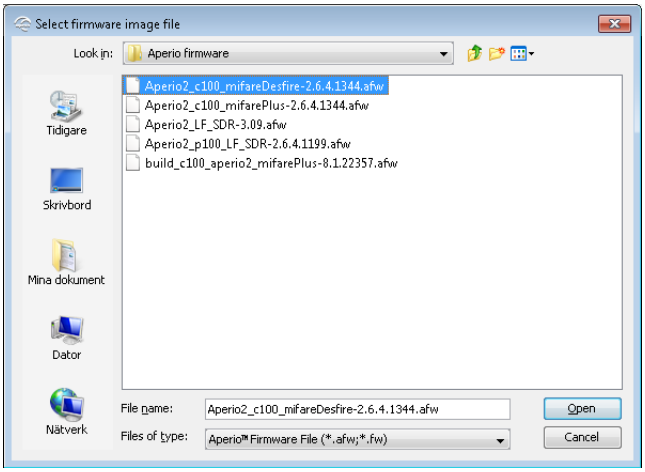


3. Right-click on the communication hub/lock/sensor in the Installation view and select ***Upgrade Firmware***.

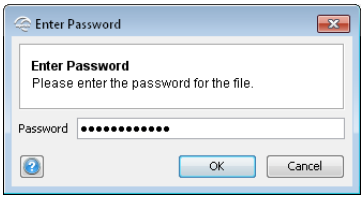


Always upgrade the communication hub before upgrading the locks/sensors. The reason is that communication hubs should always support older lock/sensor firmware but the opposite may not always be possible.

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

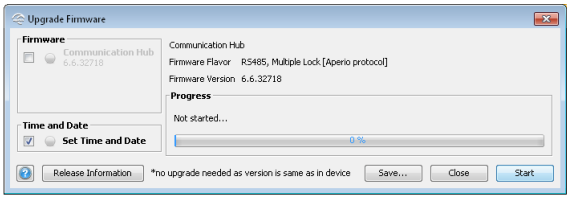


5. Enter the password supplied with the firmware.

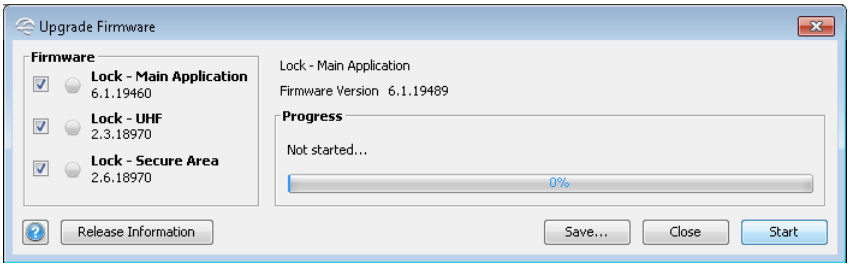


Result: The firmware upgrade window is shown, with a list of the firmware components that may be upgraded. Click ***Release Information*** to get more information about the firmware file.
The firmware list varies, depending on the firmware file and on the firmware version in the devices:

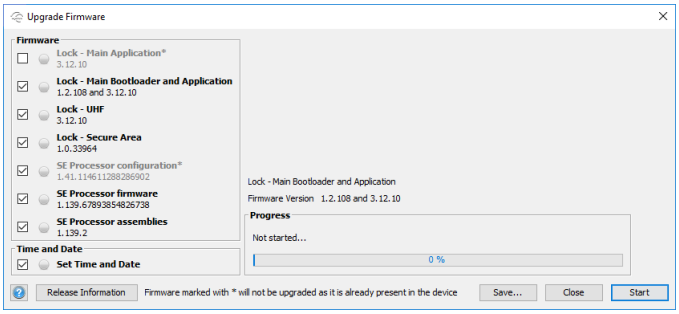
- The first example shows a communication hub which already has the same FW version as the one in the firmware file. Therefore ***Communication Hub*** is greyed out and upgrade is not necessary.



- The next example shows a list of three firmwares for a lock, all with FW versions older than the new FW version in the firmware file. Therefore all three components are checked by default.



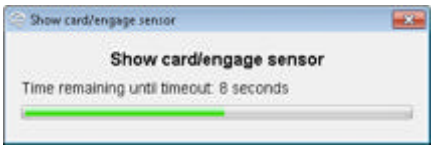
- The third example shows a list of firmwares, where two of them have the same FW versions as in the lock. Therefore only the newer firmwares are checked by default. To reinstall the firmware, although it already has the same version, select the checkbox.



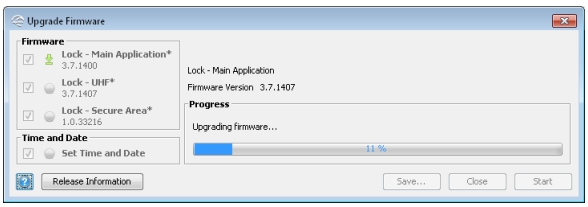
6. Click ***Start*** to run the upgrade process.

Only deselect firmware if site specific settings allow this. Existing old firmware in hardware combined with new firmware can cause malfunction.

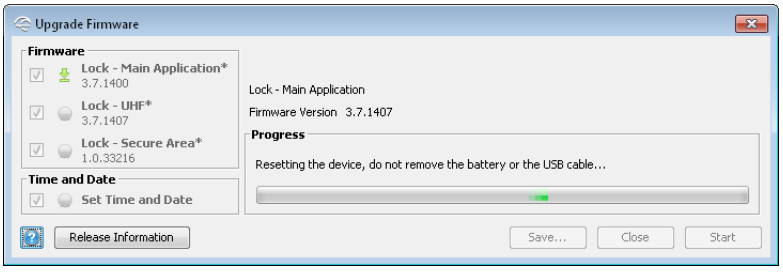
7. If you are upgrading a lock/sensor you will be prompted to connect. Hold the credential at the lock, or engage the magnet for the sensor. (This step is not necessary for V3 locks that are connected with a USB cable, or online locks that have the polling interval set to less than 15 seconds.)



Result: The upgrade will start with the first 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.



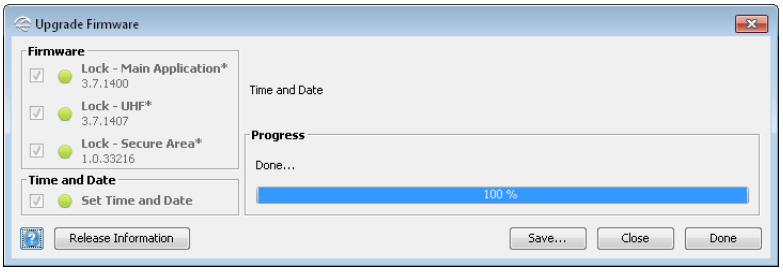
After finished download, the device resets.

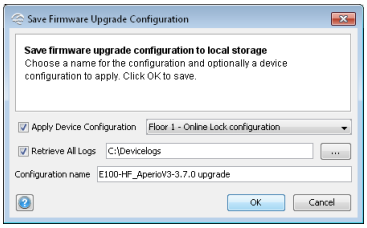


The firmware upgrade continues automatically with the remaining firmwares in the list.

Canceling the firmware upgrade process by clicking ***Close*** should be avoided. Existing old firmware in hardware combined with new firmware can cause malfunction.

8. **Optional**: After all firmware is downloaded, click ***Save...*** to save the settings for firmware upgrade of several devices.





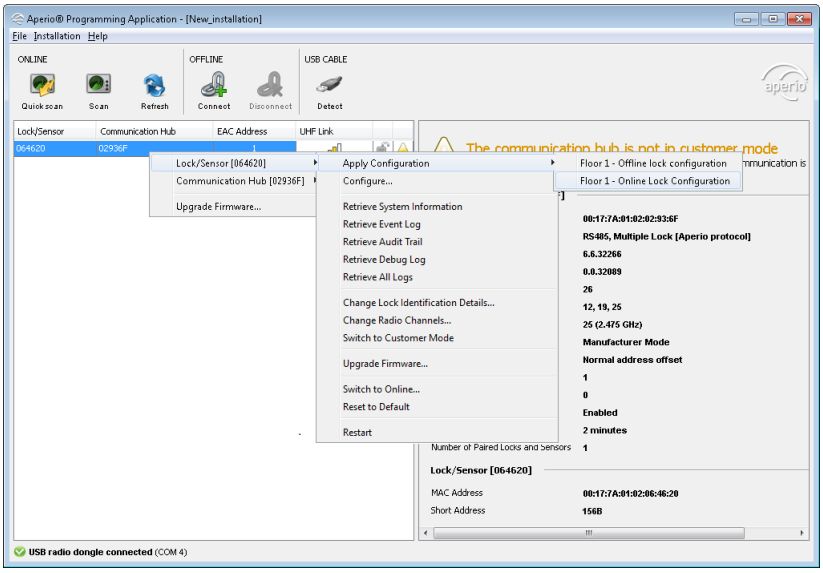
- ***Apply Device Configuration***: Select an existing device configuration, valid for the same device type as the firmware.
- ***Retrieve All Logs***: Downloads all logs of the device, prior of the firmware upgrade.
- ***Configuration name***: The name of the firmware configuration visible in the Aperio programming application.

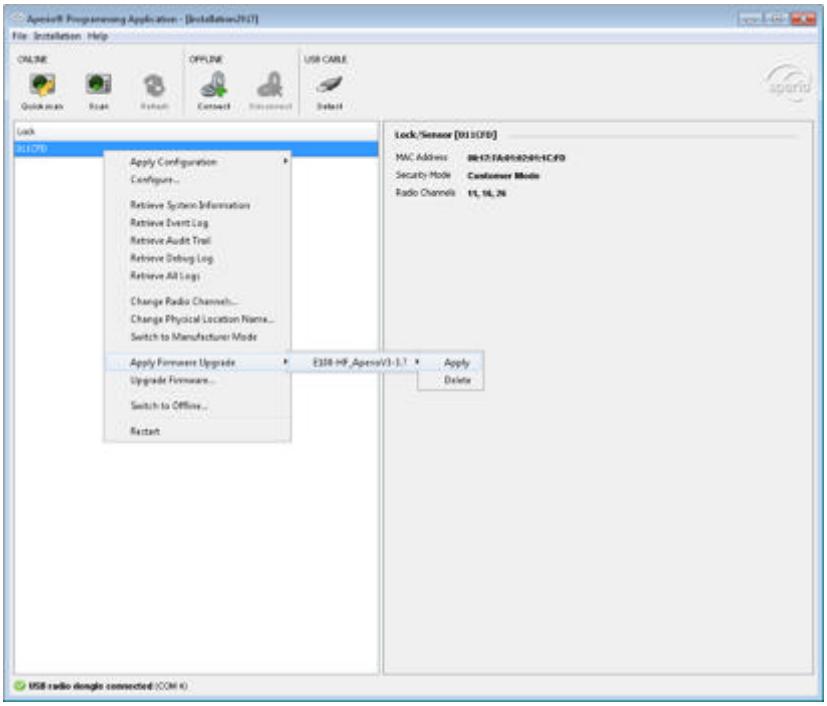
9. Click ***Close***/***Done*** to finish.

Applying a Stored Firmware Configuration to a Communication Hub/lock/sensor

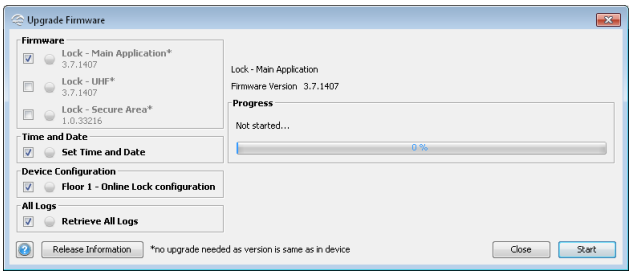
If you saved a firmware upgrade configuration, you can apply it to numerous communication hub/locks/sensors. This function is available on the right-click menu. Only firmware corresponding to the selected device is accepted and downloaded.

1. In the ***Installation view***, right-click and select ***Apply Firmware Upgrade*** → ***[Name of configuration]*** → ***Apply*** and choose an earlier stored configuration.

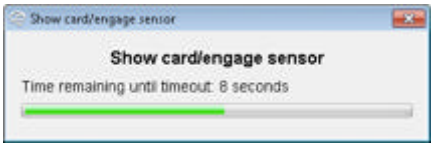




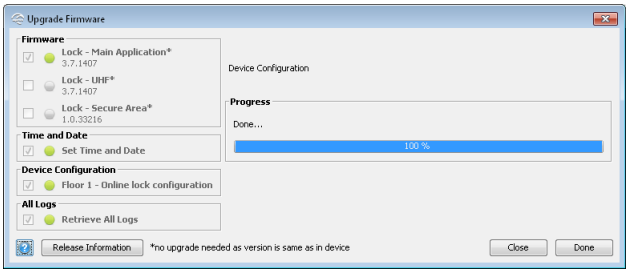
2. Select or deselect the items to alter the saved firmware configuration if needed. Click ***Start*** to run the firmware upgrade.



3. Hold the credential at the lock, or engage the magnet for the sensor. (This step is not necessary for V3 locks that are connected with a USB cable, or online locks that have the polling interval set to less than 15 seconds.) For a communication hub the information is updated immediately.



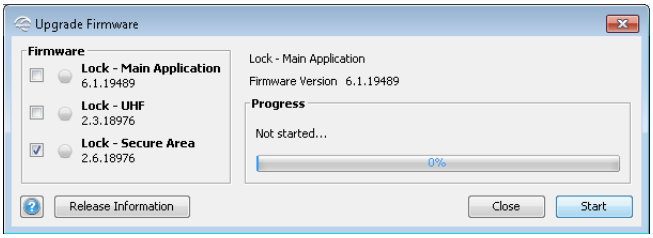
4. After download the result is shown. The settings that could not be transferred to the specific hardware are ignored. Click ***Close*** to finish.

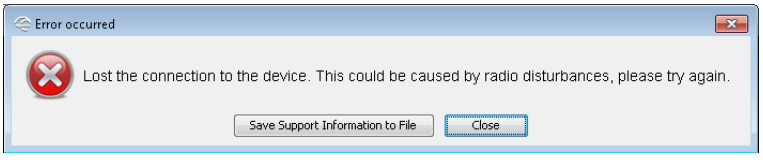


Upgrade Failure

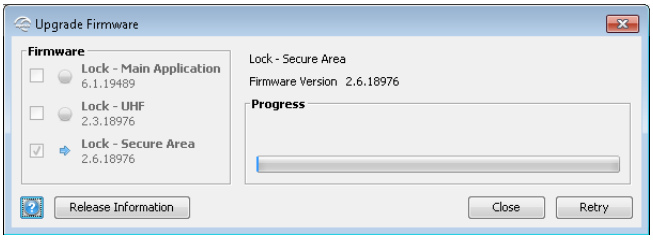
An upgrade failure is typically due to bad radio conditions. The work around is to move closer to the communication hub/offline lock and try upgrading again.

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.

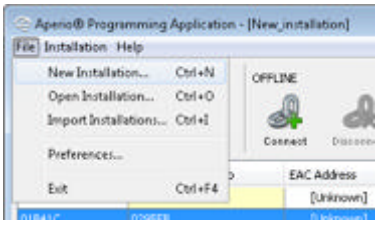


5 Aperio Programming Application Offline Functions

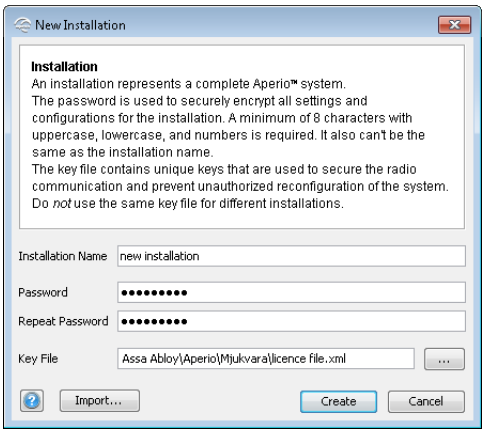
Creating Installations

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*** in the Aperio programming application menu.



3. Enter a name for the installation, a password containing at least 8 characters of which at least one upper and lower case character and a number. Finally click the browse button in the Key file field to add the encryption key (site_name-xxxxx.xml).



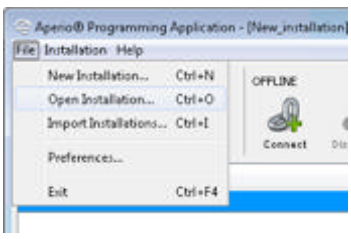
Proper handling of encryption keys is essential to lock/sensor security! It is absolutely necessary to use the customer encryption key by setting all communication hubs and locks/sensors in Customer mode to ensure a secure and encrypted communication.

4. Click ***Create***.

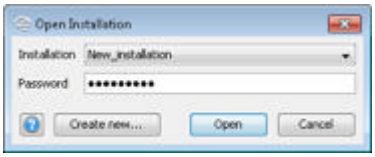
Opening Installations

The login window is automatically opened at start up if stored installations exist.

1. To open a stored installation select ***File*** → ***Open Installation...***

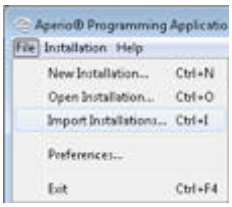


2. Select the Installation and enter the password. Click ***Open*** to proceed.

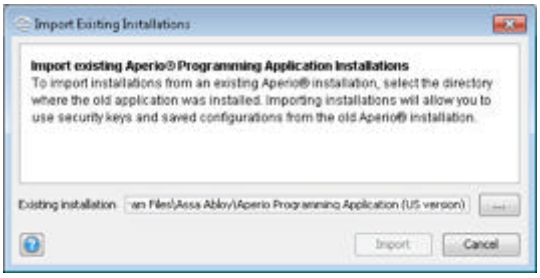


Import Existing Installations

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



2. Click the button and select the location for the old installation of the Aperio Programming Application. Your current installations will not be deleted. If you want to import installations from another computer, see section *Managing Existing Installations* on page 14.



3. Finish by clicking ***Import***.

Managing Existing Installations

Taking backup of existing installation

1. Locate the application directory of the Aperio Programming Application, `C:\Program Files\Assa Abloy\Aperio Programming Application\` (or `C:\Program Files (x86)\Assa Abloy\Aperio Programming Application\` for a 64-bit computer)
2. All installations are located in the `aperioinstallations` folder for backup. Encryption key including configurations are included in each installation.

Move installations to a new computer

1. Take a backup of the desired installation, according to *Taking backup of existing installation* on page 96, or backup the complete `aperioinstallations` folder.
2. Transfer the backup to the corresponding folder in the Aperio Programming Application folder on the new computer. If the `aperioinstallations` folder does not exists, it needs to be created.

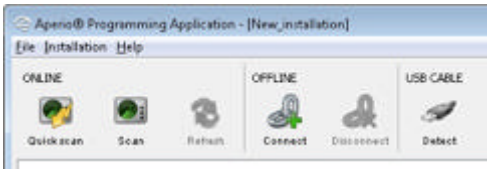
Remove installation

1. Locate the `aperioinstallations` folder in the application folder for the Aperio Programming Application, according to above and delete the entire folder for the desired installation.

Connecting to an Offline Lock

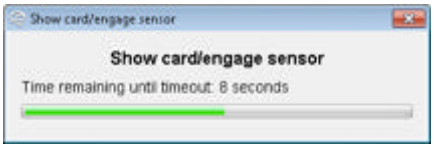
For **V3** locks with USB Cable, before connecting the first time, install the drivers according to section *Recommended Procedure when Using the V3 Lock USB Cable* on page 148.

1. Click ***Connect*** in the Offline section of the menu bar or ***Detect*** for a V3 lock connected with USB cable.

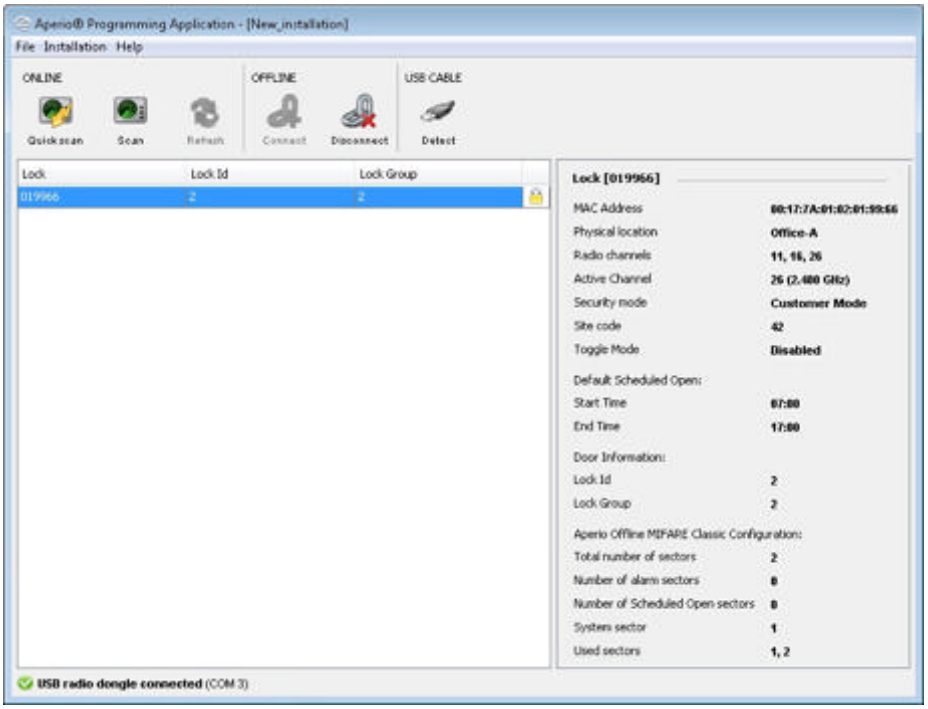


The radio channels used in the Aperio Programming Application must conform with the offline lock channels, if connection problems occur, check the radio channel settings, see section *Offline Installation Settings* on page 7.

2. Hold the radio activation card at the lock, or remove and reinsert the battery (This step is not necessary for V3 locks that are connected with a USB cable.)

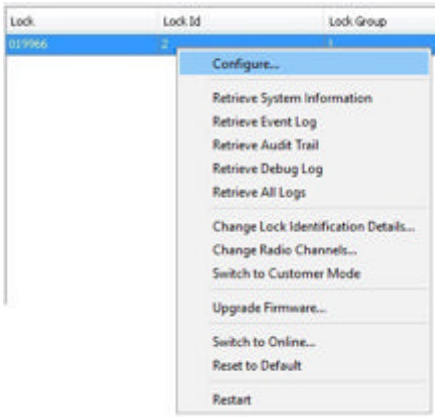


Result: Detailed information is downloaded and the Aperio Programming Application connects to the lock.



Configure Function – Wizard

Open the configure function by right-clicking the lock and selecting ***Configure***.



The following sections describe each window in the wizard.

RFID Configuration

For V2 locks, select the tab depending upon the lock type. Only **one** type of configuration can be sent to the Lock. For V3 locks, the valid RFID type is read from the lock.

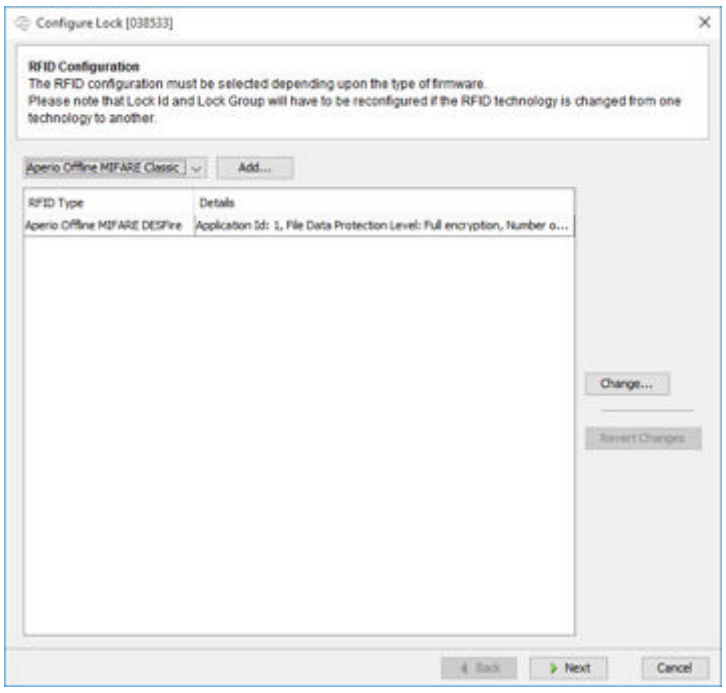


Figure 3: V2 locks: Select the lock type applicable

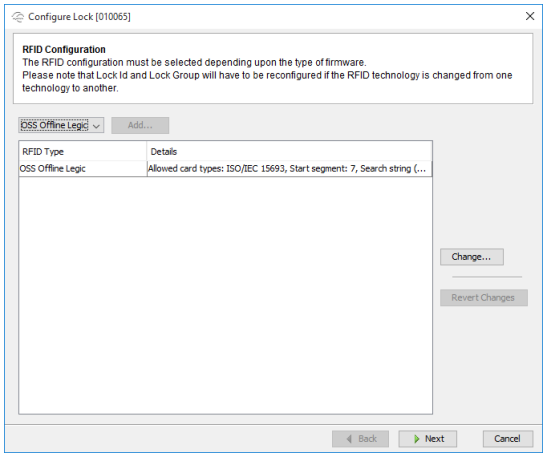


Figure 4: V3 locks: The RFID is read from the OSS Legic lock

Click ***Add*** and/or ***Change*** to enter the settings for the card format.

Offline Card Specifications

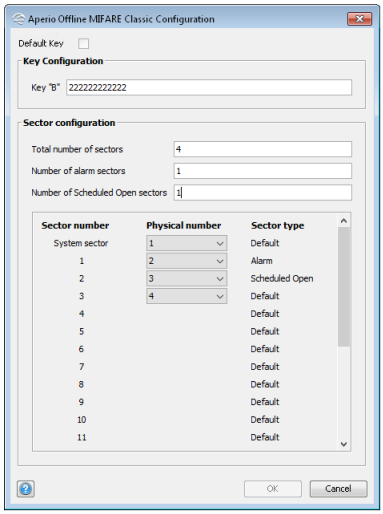
There are two offline card specifications when using Aperio in Offline mode. The first card specification is created by ASSA ABLOY and is called Aperio Offline. Products that follow this specification are Aperio Offline MIFARE Classic and Aperio Offline MIFARE DESFire.

The second specification is called OSS Offline where OSS (Open Security Standard) is an open standard that is specified by the OSS committee. Aperio products supporting this standard are OSS Offline MIFARE Classic, OSS Offline MIFARE DESFire and OSS Offline Legic.

Aperio Offline MIFARE Classic Configuration

Aperio Offline 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 the RFID configuration is done wrong, the lock may become inoperable.



Default Key: If selected, the Key "B" will be set automatically. The information will be sent in the background to obtain increased security.

Key Configuration:

- ***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 setting the sector configuration, 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 124).

Plan your sector configuration from the following limitations:

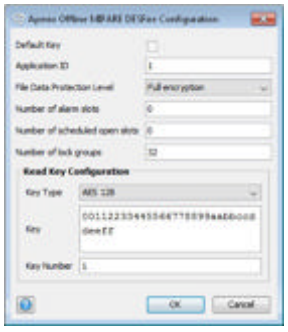
	MIFARE Classic 1K	MIFARE Classic 4K
Max lock units	65536	65536
Max lock groups	1344	5088
Max alarms	84	420

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 add 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).

Aperio Offline MIFARE DESFire Configuration



- ***Default Key***: If selected, the Application ID, File Data Protection level, and Read Key Configuration will be set automatically. The information will be sent in the background to obtain increased security.
- ***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 ID:s 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.

Read Key Configuration:

- ***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: 00112233445566778899aabbccddeeff.
- ***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 credentials 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 configuration from the following limitations:

	MIFARE DESFire 2K	MIFARE DESFire 4K	MIFARE DESFire 8K
Max lock groups	4000	8096	16288
Max alarms slots	250	506	1018
Max scheduled open slots	500	1012	2036

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

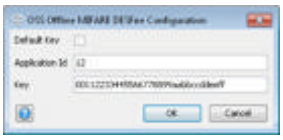
OSS Offline MIFARE Classic Configuration

- ***Default Key***: If selected, the key "B" will be set automatically. The information will be sent in the background to obtain increased security.
- ***Key B***: Enter the 6 byte long hexadecimal MIFARE Classic Key B that applies for the user cards in your installation. Example: AABBCC112233.

Info file location:

- ***Sector number***: Sector used for the OSS Offline information file, in the range of 0-39.
- ***Block number***: Start block for the OSS Offline information file in the used sector. Possible start block depend on sector used: Sector 0: block number 1-2, sector 1-31: block number 0-2 and sector 32-39: block number 0-14.

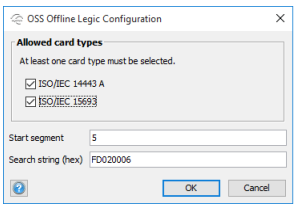
OSS Offline MIFARE DESFire Configuration



- ***Default Key***: If selected, the Application Id and Key will be set automatically. The information will be sent in the background to obtain increased security.
- ***Application Id***: Identification number for the application on the OSS Offline MIFARE DESFire cards used in the system. A MIFARE DESFire card can have up to 32 applications. Application ID:s range from 0 to 16777215.
- ***Key***: MIFARE DESFire key that applies for the user cards in your installation in HEX format. Example: 00112233445566778899aabbccddeeff.

OSS Offline Legic Configuration

This RFID is supported from release 3.3.0 and onwards.



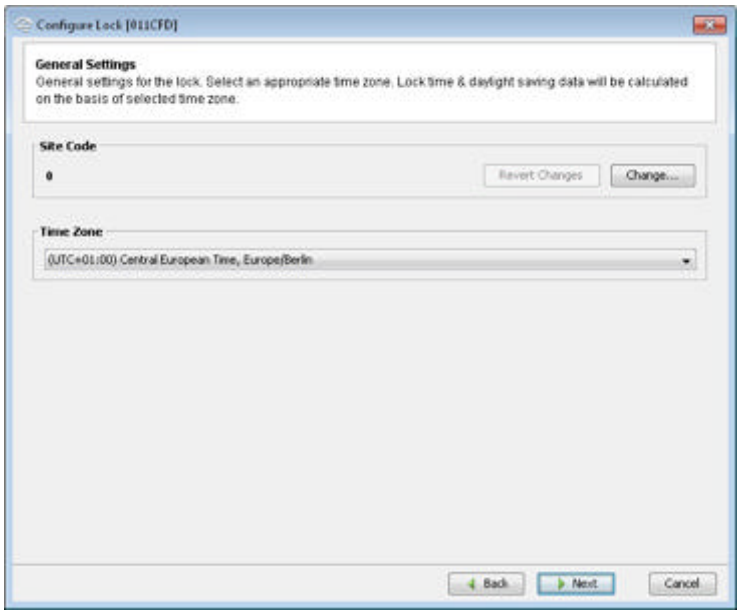
In the list, select the card type to use:

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

- ***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.
- ***Search string (hex)***: Max 24 characters hexadecimal, even number och characters. For example: 30030009.

Field name	Mandatory	Supported data type	Data range	Example data	Comments
Start segment	Yes	Number (positive integer)	0 to 255	1	Specifies the segment from which to start the search. It is useful in cases where more than one similar search string exists.
Search string	No	Hexadecimal	Max 24 characters	0123456789aabbccdd	Must be an even number of characters.

General Settings



Site Code:

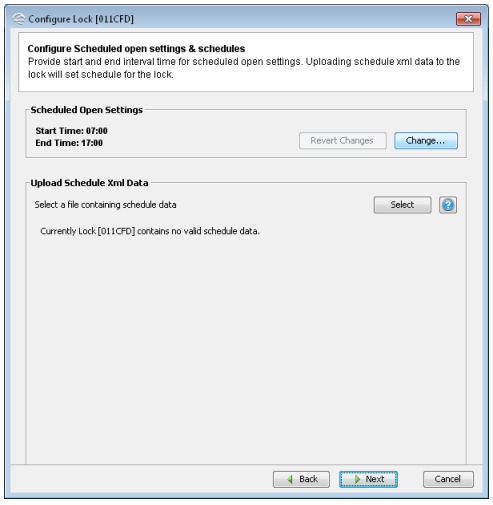
Each site has a unique code that all credentials within the system share. The maximum value is 4294967295.

Time Zone:

Select the time zone where the access system is located.

Scheduled Open & Schedule Data

This function is not applicable for OSS Offline data models.



Change Scheduled Open Settings

This function is not applicable for OSS Offline data models.

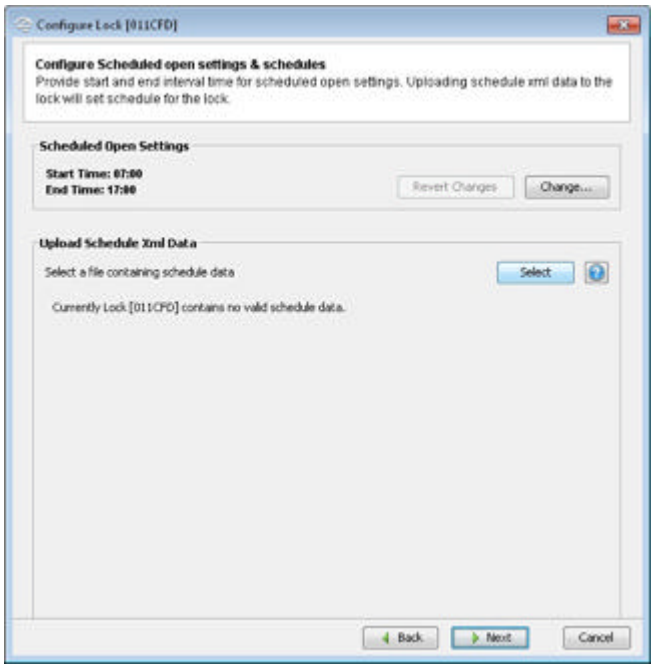
- **Start time:** Start time for when the lock can be activated for scheduled open (For when access cards with scheduled open functionality can set the lock to be open).
- **End time:** End time for when the lock responds to scheduled open attempts. It is also the time when the lock goes back to locked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

The schedule open function has several options, please refer to the Aperio Offline Description manual for more details.

Uploaded Schedule Data

This function is not applicable for OSS Offline data models.

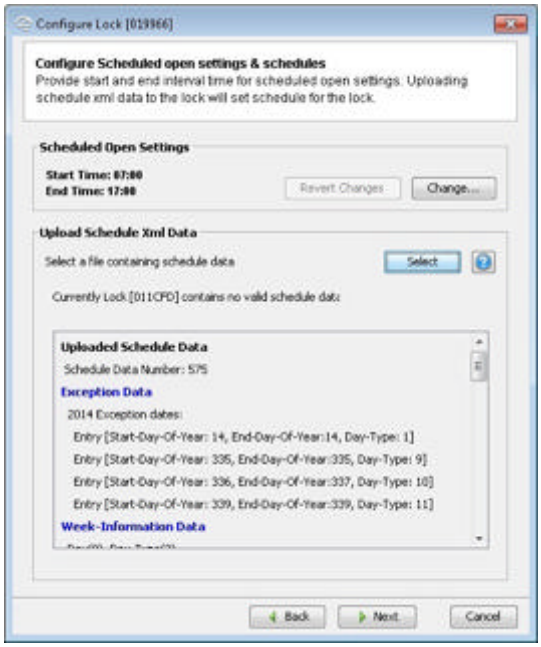
With this function schedules are enabled in the lock. The schedules for the specific access system are specified in an XML-file.



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 section *Schedule Data XML format* on page 105.

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

Tag/Attribute Name	Rules
<year> (Exceptions)	· Value should be greater than or equal to the current year.
<daytype> (Exceptions>>Year>>Entry)	· Value should be in the range 0-63 (inclusive).
<startdate> & <enddate> (Exceptions>>Year>>Entry)	· Values specified should be in YYYY-MM-DD format. · <startdate> value should be less than or equal(in case of a single day exception) to <enddate> value. · Year specified in <startdate> & <enddate> tags should always be same as the above <year> tag value.
daynumber (Weekdays>>Day)	· Value specified should be in the range 0 (Mon) - 6 (Sun) inclusive. Entries for all the days (0-6) are required.
daytype (Weekdays>>Day)	· Value specified should be in the range 0-63 (inclusive).
<schedule> (Schedules)	· Number value specified should be in the range 2-15 (inclusive). · Type value should only be a numeric value.
<type> (Schedules>>schedule)	· Only two type of schedules are allowed 0(Default access schedule), 1 (Schedule open). · There can be only one type="1" (Schedule open) schedule in the XML. · There can be any number of type="0" (default Access) schedule in the XML.
<daytype> (Schedules>>schedule)	· Value specified should be in the range 0-63 (inclusive).

Tag/Attribute Name	Rules
<start-interval> & <end-interval> (Schedules>>schedule>>daytype)	· Time should be specified in HH:MM 24 hour format. · Data should always be entered in terms of quarter of the day. · <start-interval> should signify start of the quarter time hence MM value should be one of these values (00,15,30,45). · <end-interval> should signify end of the quarter time hence MM value should be one of these values (14,29,44,59).

Sample Schedule Data XML file

Example of XML-file for defining schedules:

```
<?xml version="1.0" encoding="utf-8"?>
<scheduledata number="1" version="23" xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="schedule.xsd">

    <exceptions>
        <year value="2020">
            <entry>
                <startdate>2020-01-15</startdate>
                <daytype>1</daytype>
                <enddate>2020-01-15</enddate>
            </entry>
            <entry>
                <startdate>2020-12-02</startdate>
                <daytype>9</daytype>
                <enddate>2020-12-02</enddate>
            </entry>
            <entry>
                <startdate>2020-12-03</startdate>
                <daytype>10</daytype>
                <enddate>2020-12-04</enddate>
            </entry>
            <entry>
                <startdate>2020-12-06</startdate>
                <daytype>11</daytype>
                <enddate>2020-12-06</enddate>
            </entry>
        </year>
    </exceptions>

    <weekdays>
        <day daynumber="0" daytype="2"/>
        <day daynumber="1" daytype="3"/>
        <day daynumber="2" daytype="4"/>
        <day daynumber="3" daytype="5"/>
        <day daynumber="4" daytype="6"/>
        <day daynumber="5" daytype="7"/>
        <day daynumber="6" daytype="8"/>
    </weekdays>

    <schedules>
        <schedule number="2" type="1">
            <daytype value="1">
                <start-interval>15:00</start-interval>
                <end-interval>15:14</end-interval>
            </daytype>
```

```
        </schedule>

        <schedule number="3" type="0">
            <daytype value="1">
                <start-interval>15:15</start-interval>
                <end-interval>15:29</end-interval>
            </daytype>
        </schedule>

        <schedule number="4" type="0">
            <daytype value="1">
                <start-interval>00:00</start-interval>
                <end-interval>14:59</end-interval>
                <start-interval>15:30</start-interval>
                <end-interval>23:59</end-interval>
            </daytype>
        </schedule>

        <schedule number="5" type="0">
            <daytype value="2">
                <start-interval>07:00</start-interval>
                <end-interval>07:59</end-interval>
            </daytype>
            <daytype value="3">
                <start-interval>08:00</start-interval>
                <end-interval>08:59</end-interval>
            </daytype>
            <daytype value="4">
                <start-interval>09:00</start-interval>
                <end-interval>09:59</end-interval>
            </daytype>
            <daytype value="5">
                <start-interval>10:00</start-interval>
                <end-interval>10:59</end-interval>
            </daytype>
            <daytype value="6">
                <start-interval>11:00</start-interval>
                <end-interval>11:59</end-interval>
            </daytype>
            <daytype value="7">
                <start-interval>12:00</start-interval>
                <end-interval>12:59</end-interval>
            </daytype>
            <daytype value="8">
                <start-interval>13:00</start-interval>
                <end-interval>13:59</end-interval>
            </daytype>
        </schedule>

        <schedule number="6" type="0">
            <daytype value="10">
                <start-interval>01:00</start-interval>
                <end-interval>11:59</end-interval>
            </daytype>
            <daytype value="11">
                <start-interval>00:00</start-interval>
                <end-interval>23:59</end-interval>
            </daytype>
        </schedule>
```

```
    </schedules>

</scheduledata>
```

Schedule Data XSD

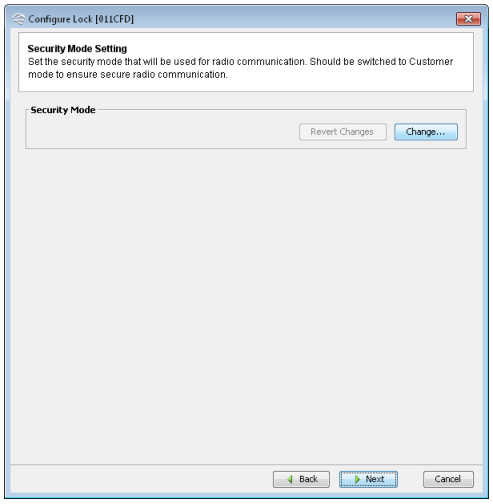
Use the following XML schema definition to validate the XML file produced for Schedule data.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
    <xs:import namespace="http://www.w3.org/XML/1998/namespace"/>
    <xs:element name="scheduledata">
        <xs:complexType>
            <xs:all>
                <xs:element ref="exceptions"/>
                <xs:element ref="weekdays"/>
                <xs:element ref="schedules"/>
            </xs:all>
            <xs:attribute type="xs:integer" name="number"
use="required"/>
            <xs:attribute type="xs:integer" name="version"
use="required"/>
        </xs:complexType>
    </xs:element>

    <xs:element name="exceptions">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="year" maxOccurs="unbounded"
minOccurs="0">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element ref="entry"
maxOccurs="unbounded" minOccurs="0"/>
                        </xs:sequence>
                        <xs:attribute type="xs:integer" name="value"
use="required"/>
                    </xs:complexType>
                </xs:element>
            </xs:sequence>
        </xs:complexType>
    </xs:element>

    <xs:element name="entry">
        <xs:complexType>
            <xs:all>
                <xs:element name="startdate" type="xs:date"
maxOccurs="1" minOccurs="1"/>
                <xs:element name="daytype" type="daytype"
maxOccurs="1" minOccurs="1"/>
                <xs:element name="enddate" type="xs:date"
maxOccurs="1" minOccurs="1"/>
            </xs:all>
        </xs:complexType>
    </xs:element>

    <xs:element name="weekdays">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="day" maxOccurs="7" minOccurs="7">
                    <xs:complexType>
```

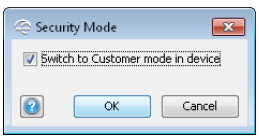
```
                            <xs:attribute name="daytype" type="daytype"
use="required"/>
                            <xs:attribute name="daynumber"
use="required">
                                <xs:simpleType>
                                    <xs:restriction base="xs:integer">
                                        <xs:minInclusive value="0"/>
                                        <xs:maxInclusive value="6"/>
                                    </xs:restriction>
                                </xs:simpleType>
                            </xs:attribute>
                        </xs:complexType>
                    </xs:element>
                </xs:sequence>
            </xs:complexType>
        </xs:element>

        <xs:element name="schedules">
            <xs:complexType>
                <xs:sequence>
                    <xs:element ref="schedule" maxOccurs="unbounded"
minOccurs="0"/>
                </xs:sequence>
            </xs:complexType>
        </xs:element>

        <xs:element name="schedule">
            <xs:complexType>
                <xs:sequence>
                    <xs:element name="daytype" maxOccurs="unbounded"
minOccurs="0">
                        <xs:complexType>
                            <xs:sequence>
                                <xs:group ref="schedule_interval_group"
maxOccurs="unbounded"
                                    minOccurs="1"/>
                            </xs:sequence>
                            <xs:attribute name="value" type="daytype"/>
                        </xs:complexType>
                    </xs:element>
                </xs:sequence>
                <xs:attribute type="xs:integer" name="number"
use="required">
                    <xs:simpleType>
                        <xs:restriction base="xs:integer">
                            <xs:minInclusive value="2"/>
                            <xs:maxInclusive value="15"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:attribute>
                <xs:attribute type="xs:integer" name="type"
use="required">
                    <xs:simpleType>
                        <xs:restriction base="xs:integer">
                            <xs:enumeration value="0"/>
                            <xs:enumeration value="1"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:attribute>
            </xs:complexType>
```

```
    </xs:element>

    <xs:simpleType name="daytype">
        <xs:restriction base="xs:integer">
            <xs:minInclusive value="0"/>
            <xs:maxInclusive value="63"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:group name="schedule_interval_group">
        <xs:sequence>
            <xs:element name="start-interval" type="timeinterval"
maxOccurs="unbounded"
                minOccurs="1"/>
            <xs:element name="end-interval" type="timeinterval"
maxOccurs="unbounded" minOccurs="1"
            />
        </xs:sequence>
    </xs:group>

    <xs:simpleType name="timeinterval">
        <xs:restriction base="xs:string">
            <xs:pattern value="([0-1][0-9]|2[0-3])\:([0-5][0-9])"/>
        </xs:restriction>
    </xs:simpleType>
</xs:schema>
```

Security Mode Setting



1. Click ***Change*** in the ***Security Mode*** 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***.



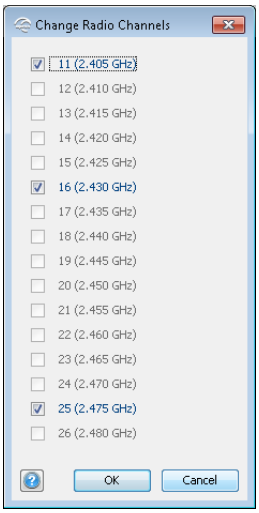
The default mode is Manufacturer mode, but you should always change it to Customer mode. If you change to Manufacturer mode the lock will no longer be using secure radio communication.

	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.

Radio Channels

This function is also available on the right-click menu in the ***Installation view***.

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

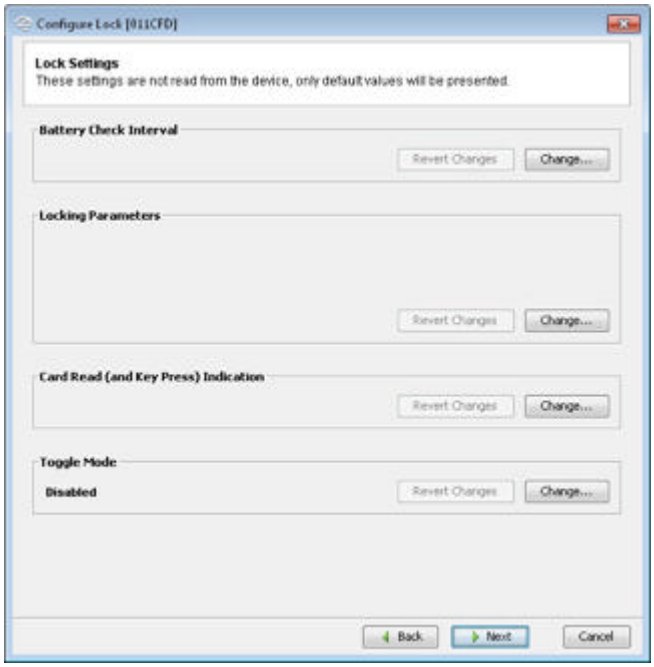


2. Deselect one or several of the used channels to make a new selection of channels.

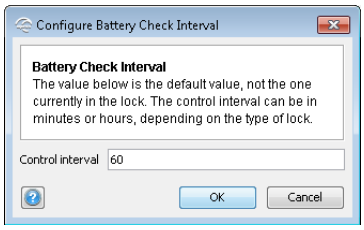
For the US market channel 26 is disabled.

Lock Settings - Offline

On this page you will be able to configure ***Battery Check Interval***, ***Locking Parameters***, ***Card Read (and Key Press) Indication*** and ***Toggle Mode***.



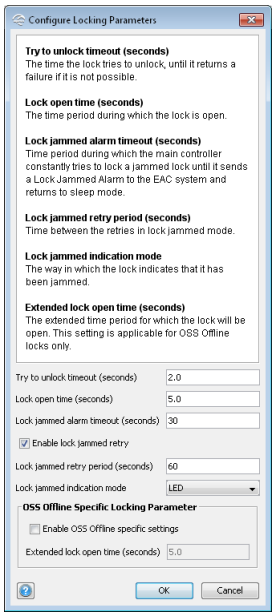
Battery Check Interval



It may be necessary to adjust the control interval for this check depending on the type of battery used, and the surrounding temperature. For example in cold surroundings where the battery runs out faster. Default value is 60 (minutes).

An alarm event is sent to the EAC system for offline locks, via a credential to an Offline updater when the battery is low.

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*** or ***LED and buzzer*** are the different indication modes.

OSS Offline Specific Locking Parameter

- ***Enable OSS Offline specific settings***: Click to enable OSS Offline specific settings.
- **Extended lock open time (seconds)**: This setting enables an extended lock open time to be set for a OSS Offline lock. Default value 5.0 seconds. This setting is used to allow exceptions for certain user credentials to use the extended lock open time instead of the default value set by ***Lock open time (seconds)*** above.

Card Read (and Key Press) Indication

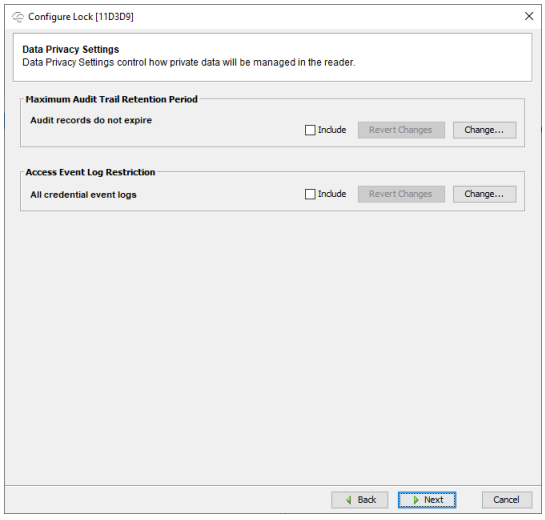
Different locks can have a different mechanism for audio-visual indication of successful credential reading. Here it is possible to disable credential read indication or to set it to LED. Some Aperio locks have support for other mechanisms such as buzzers.

Toggle Mode

If a lock is set in toggle mode it will work exactly like a normal mechanical lock opened with a key. Showing an access card with toggle mode activated will open the lock until the user shows the card again to close it. Toggle mode is by default turned off.

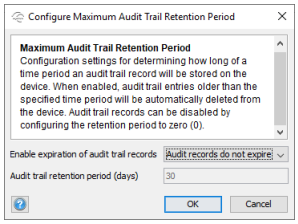
Data Privacy Settings

Data Privacy Settings control how private data will be managed by the device, in order to support local directives such as GDPR.



- ***Maximum Audit Trail Retention Period***: Setting for how long the audit trail is stored in the device.
- ***Access Event Log Restriction***: Setting for which access attempts are stored on the credentials. This function is only supported by SODA locks.

Maximum Audit Trail Retention Period

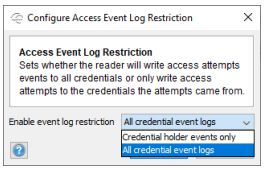


This function allows you to set how long credential data will be stored in the device:

- ***Enable expiration of audit trail records:*** Enable/disable if credentials data will be deleted from the device. (Default: Audit records do not expire).
- ***Audit trail retention period (days)***: Sets the number of days the audit records are stored in the device. (Default: 30 days).

Access Event Log Restriction

This function is only supported by SODA locks.

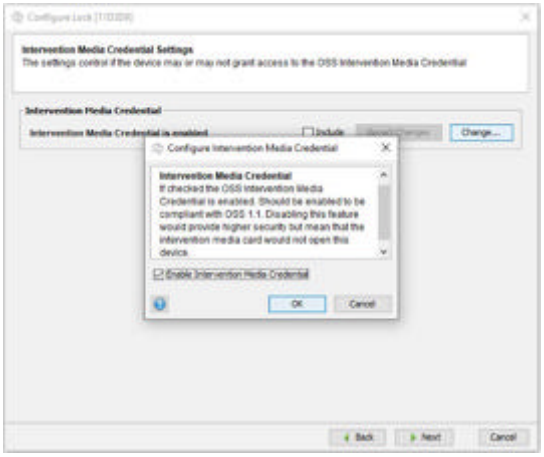


- ***Enable event log restriction:*** Select if access attempts will be stored on all credentials, or only the access attempts made by the current card. (Default: All credential event logs).

Intervention Media Credential Settings

This setting is applicable for OSS offline locks only.

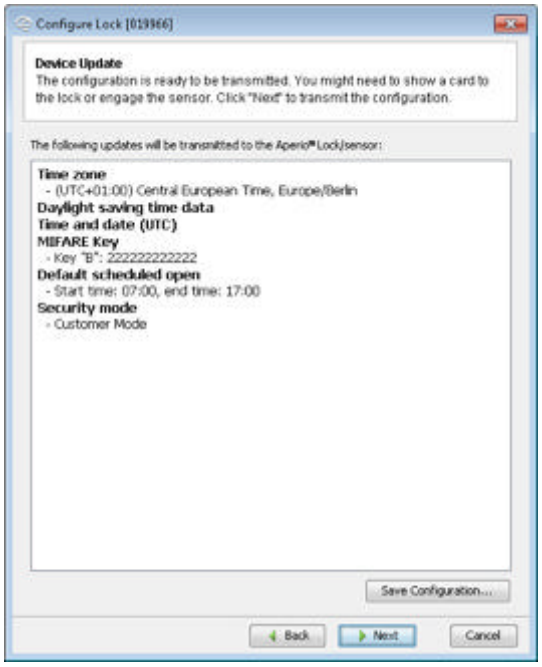
This setting controls if the device may or may not grant access to the OSS ***Intervention Media Credential***. (Default: enabled).



This setting should be enabled to be compliant for OSS 1.1.

Device Update – Save Configuration

This is a summary of the 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:
   - RFID configuration
   - Change security mode
   - Device time update
   - And optionally some advanced features like Battery Alarm, Status configuration and Locking parameters.

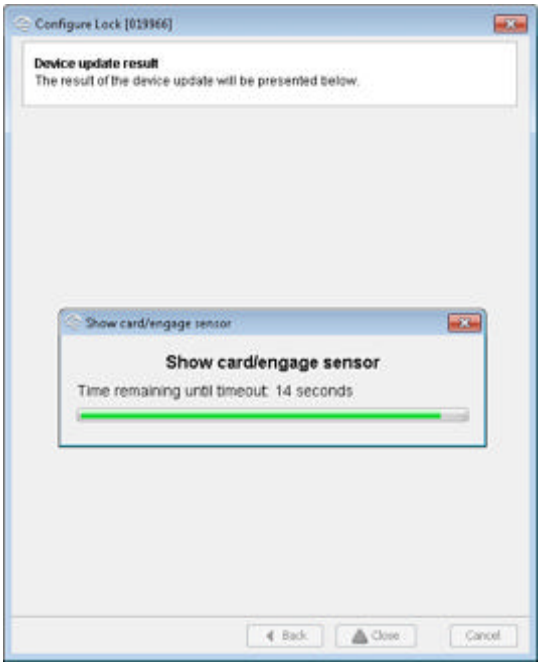
   If you choose to save a configuration, keep in mind that some configuration settings should not be saved. Only save settings that are general for all locks in your installation.

   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 which settings are changed in the lock. You could, for

instance, name it according to the different configuration tasks or, if applicable, use a name that reflects the specific unit type.

4. Click ***OK***.
   Result: The configuration is saved in the local storage, and you are back in the Configuration Wizard. (See section *Applying a Stored Configuration to a Communication Hub/lock/sensor* on page 67 to use the saved configuration) 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 reinsert battery).



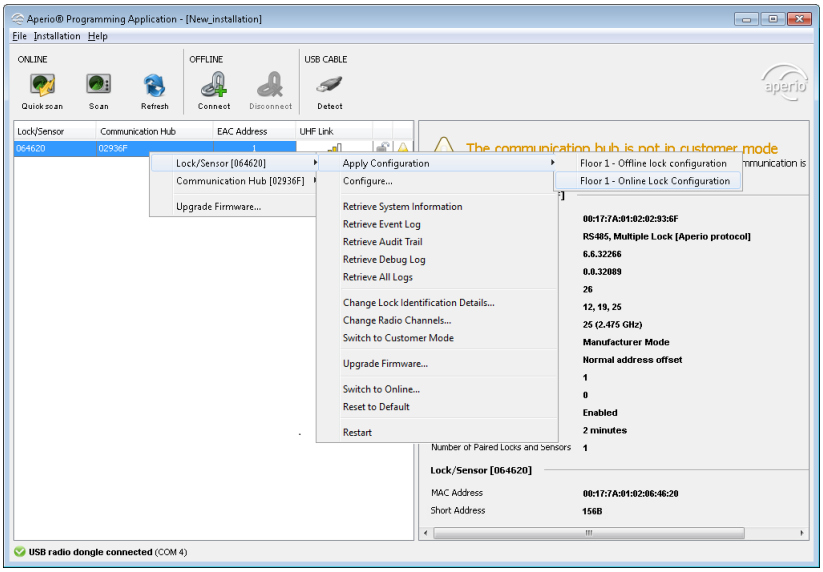
7. Click ***Close*** to exit the wizard.

Applying a Stored Configuration to a Communication Hub/lock/sensor

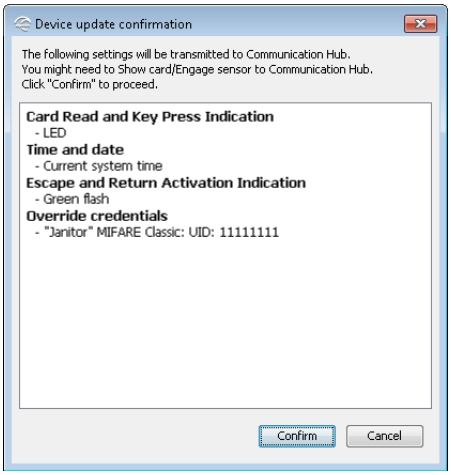
If you saved a configuration in the configuration wizard, you can apply it to numerous locks/sensors. This function is available on the communication hub/lock/sensor sub-menu or directly on the right-click menu for offline locks. Only hardware specific settings are downloaded to the selected unit.

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

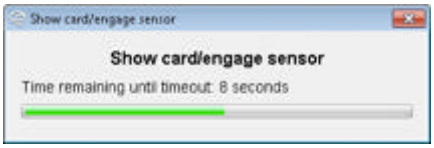
1. In the ***Installation view***, right-click and select communication hub/lock/sensor, on the sub-menu select ***Apply Configuration*** and choose an earlier stored configuration.



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



3. Hold the credential at the lock, or engage the magnet for the sensor. (This step is not necessary for V3 locks that are connected with a USB cable, or online locks that have the polling interval set to less than 15 seconds.) For a communication hub the information is updated immediately.

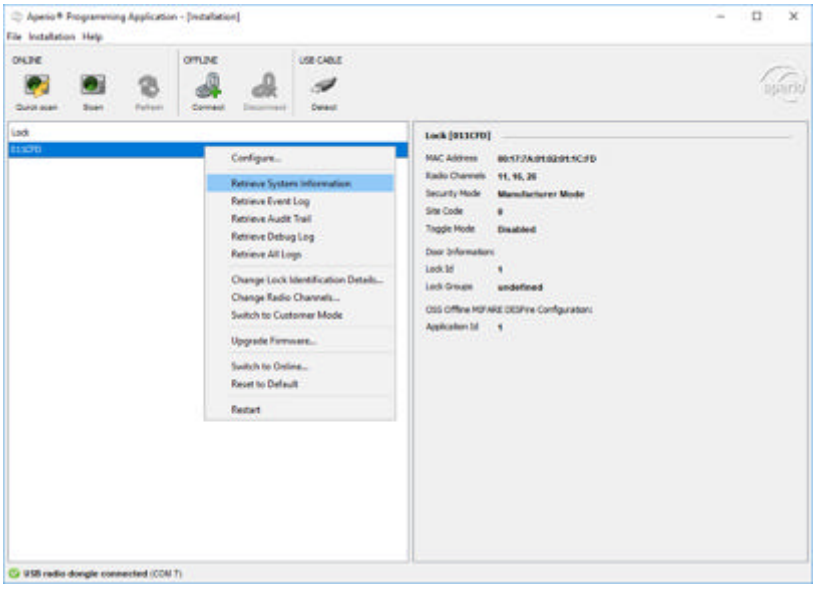


4. After download the result is shown. The settings that could not be transferred to the specific hardware are ignored. Click ***Close*** to finish.

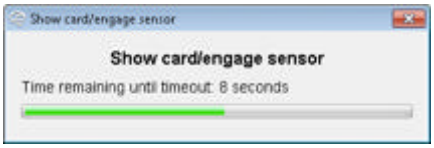
5. Repeat all the steps from the beginning of this section for every lock/sensor you want to configure with a saved configuration.

Retrieve System Information

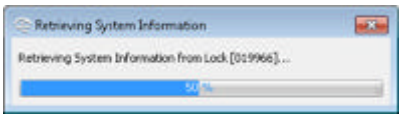
1. Right-click and select ***Retrieve System Information*** to retrieve detailed information about the lock/sensor.



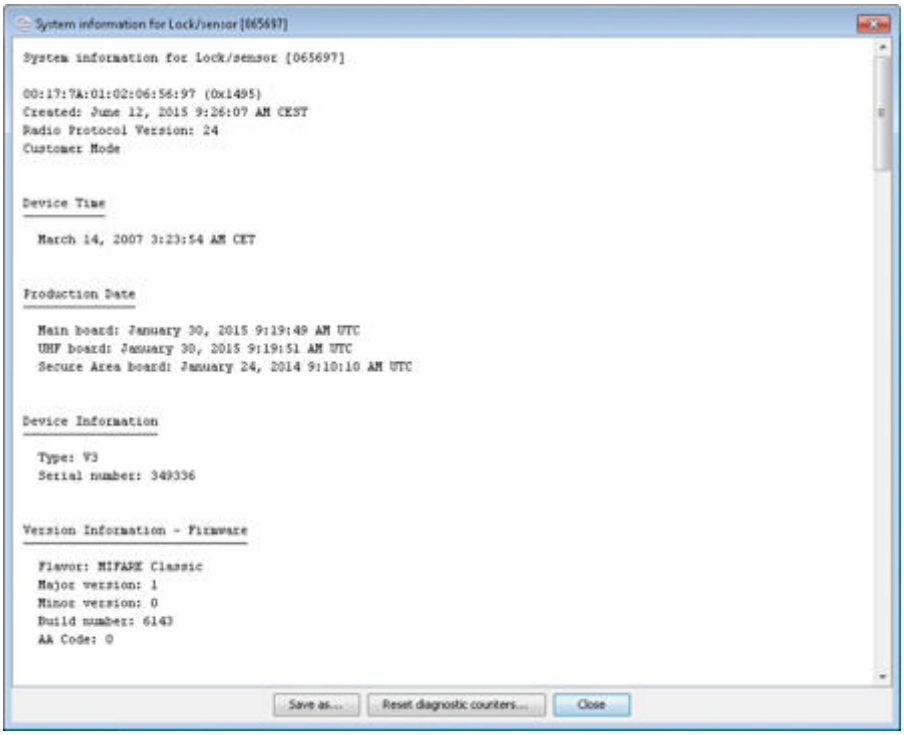
2. Hold the radio activation card at the lock, or remove and reinsert the battery (This step is not necessary for V3 locks that are connected with a USB cable.)



Result: The Aperio Programming Application connects to the unit.



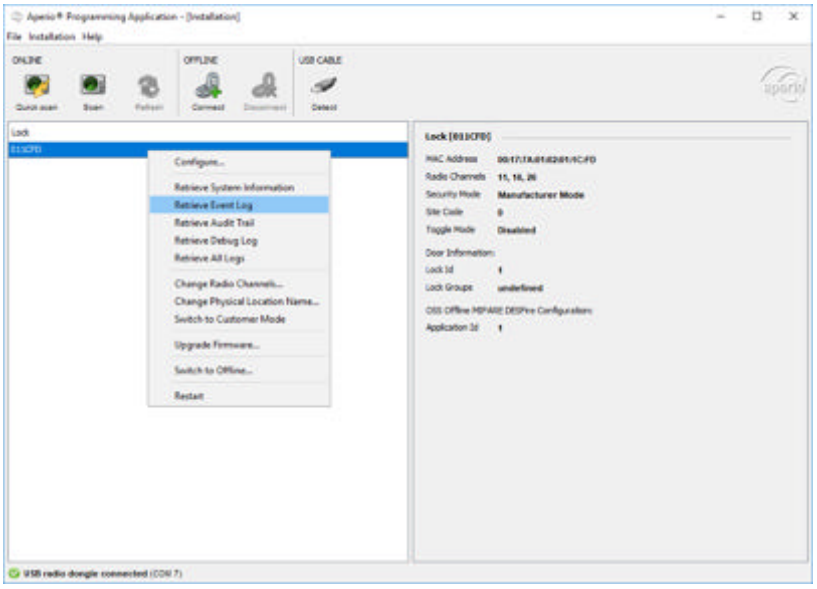
3. Click ***Save as*** to save the system information to a local storage or click ***Close*** to exit.



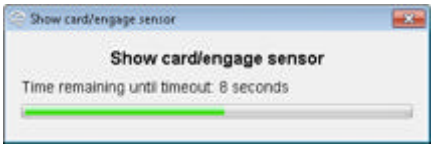
Retrieve Event Log

This function displays the event log for a particular lock, where you can find all system events performed on the lock.

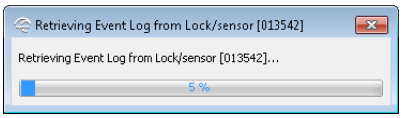
1. Right-click and select ***Lock/Sensor → Retrieve Event Log***



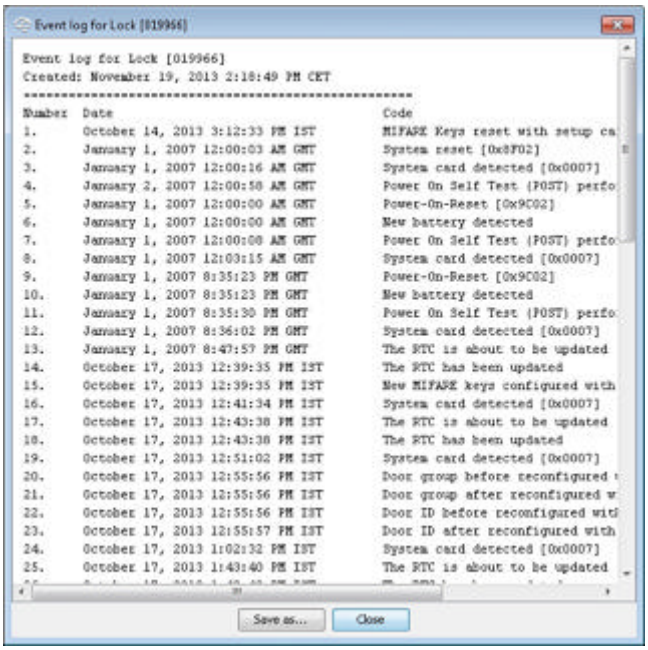
2. Hold the radio activation card at the lock, or remove and reinsert the battery (This step is not necessary for V3 locks that are connected with a USB cable.)



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.

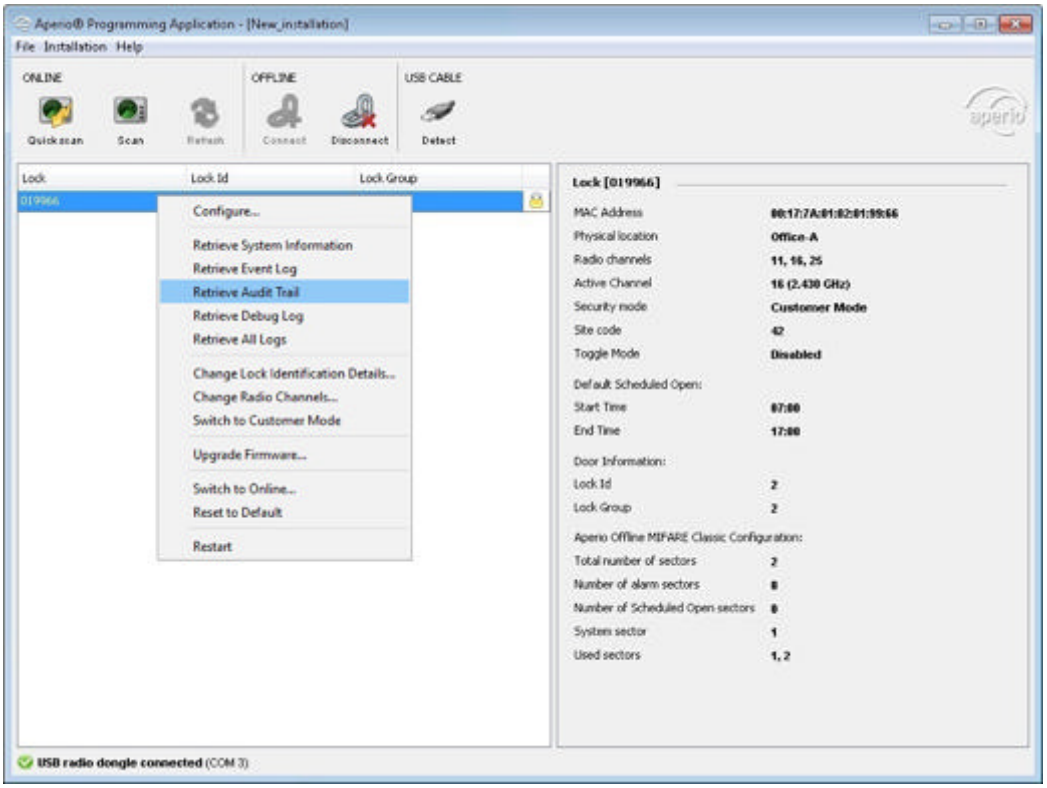


This window contains a listing of the recent system events along with the date when it was observed. (If the number of events exceeds 200, older events are overwritten.)

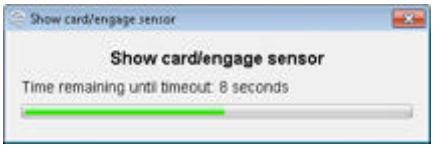
Retrieve Audit Trail

This function displays the list of access attempts for a lock. It shows the latest 200 records.

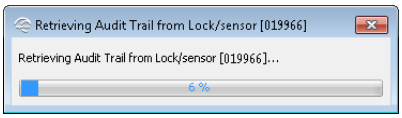
1. Right-click and select ***Retrieve Audit Trail***.



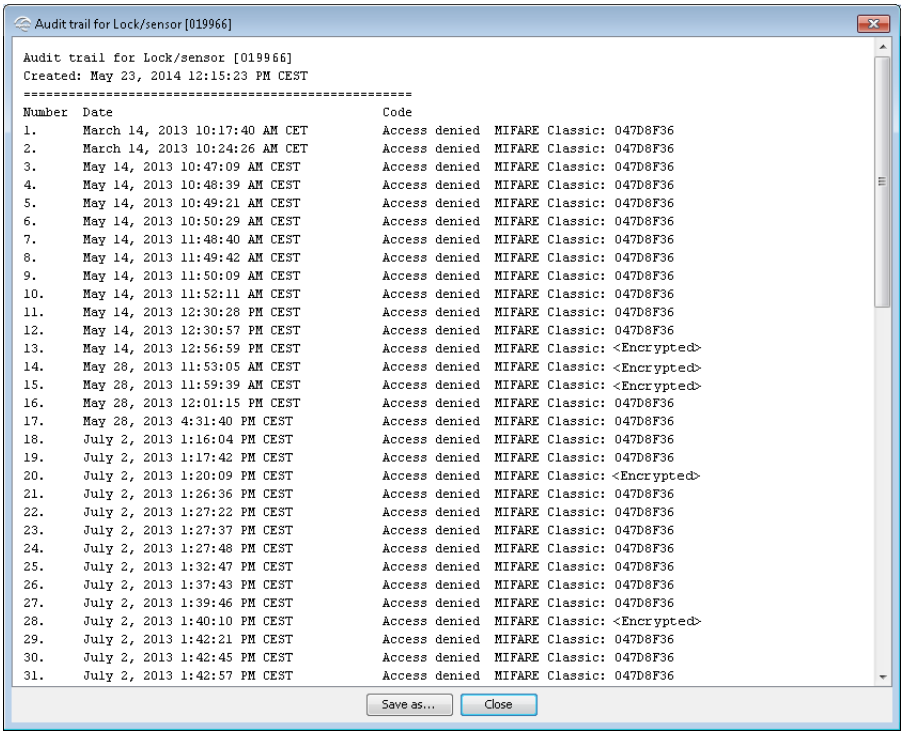
2. Hold the radio activation card at the lock, or remove and reinsert the battery (This step is not necessary for V3 locks that are connected with a USB cable.)



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.



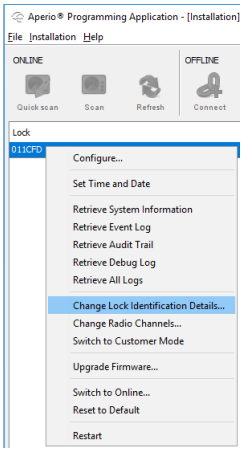
The window contains information about the latest 200 access attempts including consecutive number, date, access decision and what type of credential that was used at each attempt.
The audit trail is encrypted for V3 locks. If the lock is in manufacturer mode when the audit trail is downloaded, it shows <Encrypted> instead of the credential, for access attempts that was made in customer mode, and the other way around.

Change Lock Identification Details

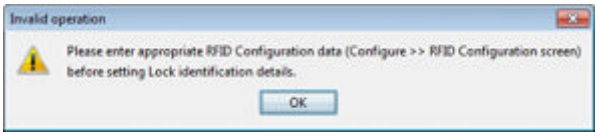
This menu option will allow the user to change Lock ID, Group & Physical location. Lock ID is used as an identifier for each lock. Lock Group is used to cluster several locks for example in order to create access areas, where all the locks in one group will use the same access settings. Physical location 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* on page 98.

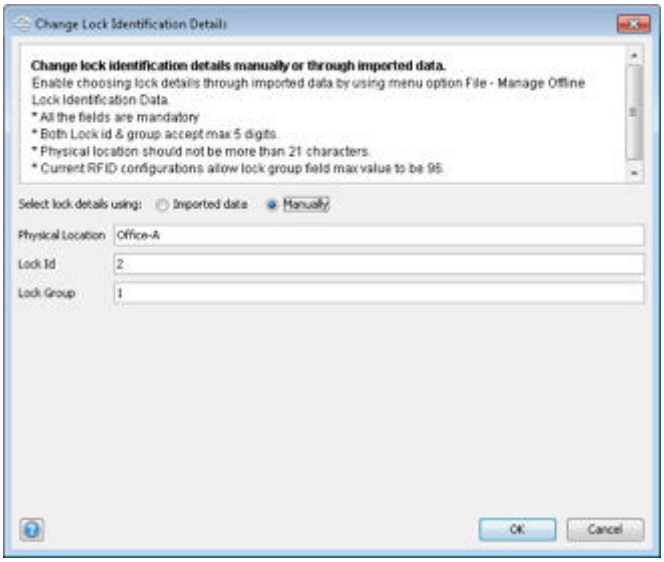
1. Select the lock in the installation view. Right-click and select ***Change Lock Identification Details...***.



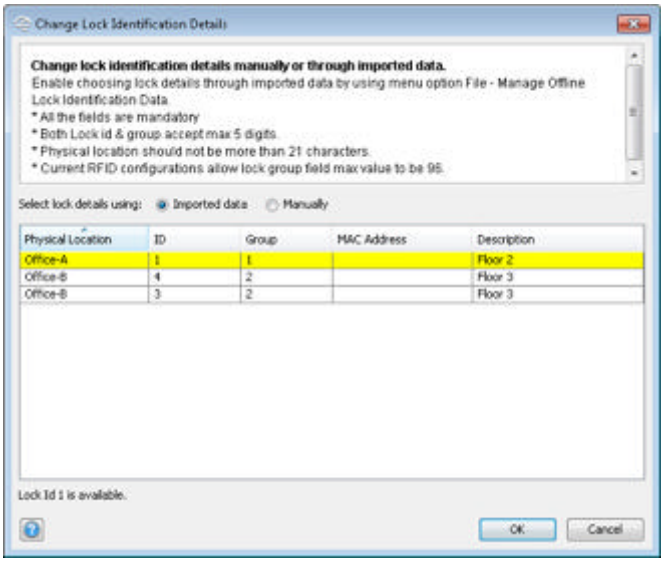
2. User should always set RFID configurations (see section *RFID Configuration* on page 98) before changing/adding lock identification details. However if a user tries to set lock identification details before setting RFID configurations then following screen will be shown to the user



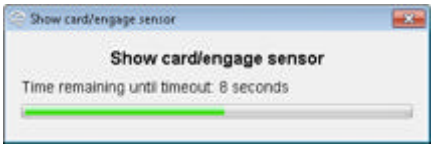
3. Set lock identification details either ***Manually*** or through ***Imported data*** by selecting one of the radio buttons.
   a. **Manually:** Enter ***Physical Location*** (max 20 alpha numeric characters), ***Lock Id*** (max 5 numeric characters), ***Lock Group*** (max 5 numeric characters & max value decided by RFID configurations)



   b. **Imported data:** This option can be used if lock identification details have been imported using the function ***Installation → Offline → Manage Lock Identification Data***. (See section *Manage Offline Lock Identification Data* on page 137). After import, lock identification details will automatically be displayed here. Select lock identification details in the list by clicking the desired row.



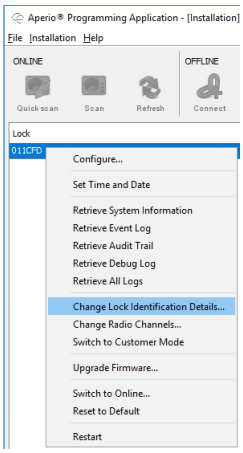
4. Click ***OK***.
5. Hold the radio activation card at the lock, or remove and reinsert the battery (This step is not necessary for V3 locks that are connected with a USB cable.) to change the lock identification details.



Change Lock Identification Details (OSS Offline)

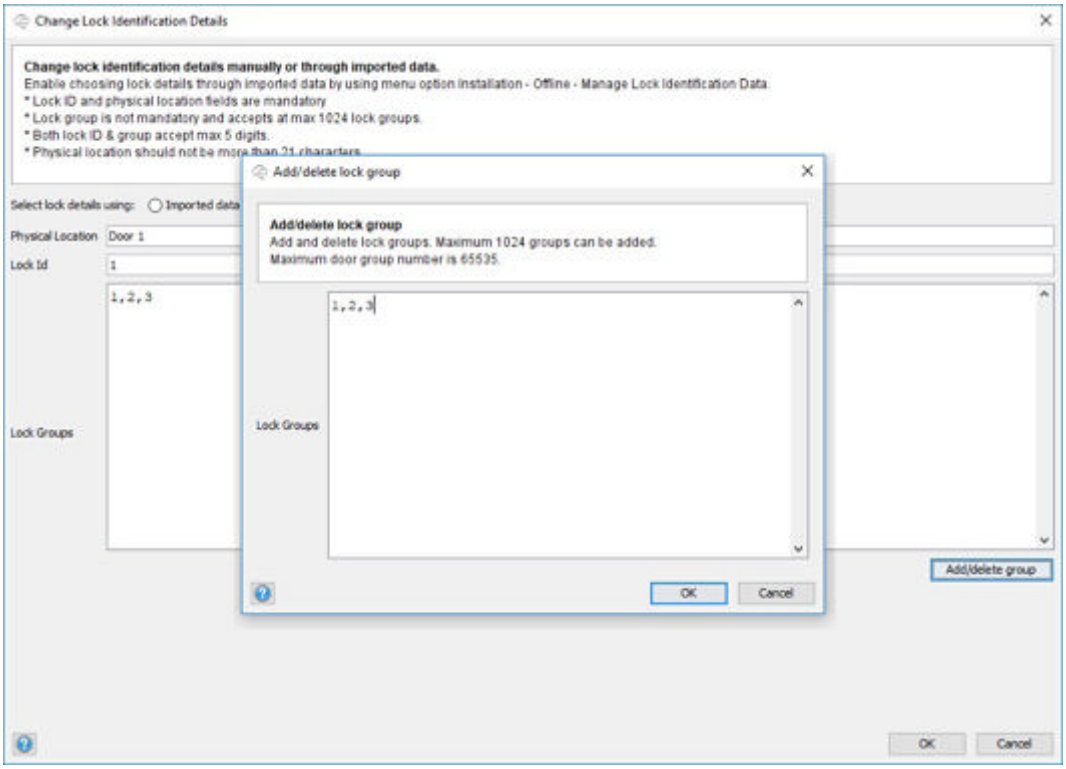
This menu option will allow the user to change Lock ID, Group & Physical location. Lock ID is used as an identifier for each OSS Offline lock. OSS Offline locks can also belong to multiple lock groups or have no lock group belongings at all.

1. Select the lock in the installation view. Right-click and select ***Change Lock Identification Details...***.

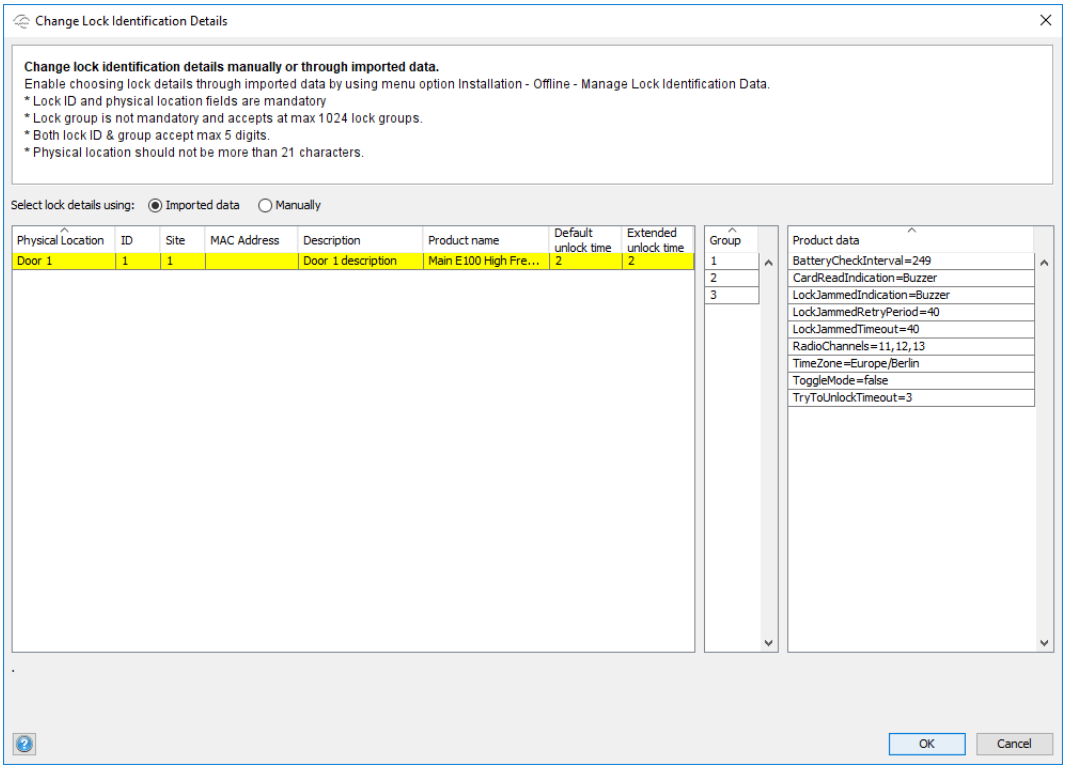


2. Set lock identification details either ***Manually*** or through ***Imported data*** by selecting one of the radio buttons.

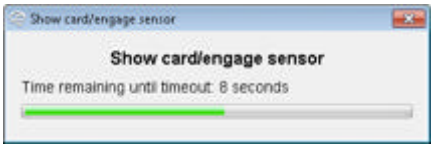
a. **Manually:** Enter ***Physical Location*** (max 20 alpha numeric characters), ***Lock Id*** (max 5 numeric characters), ***Lock Groups*** (max 5 numeric characters). Up to 1024 lock groups can be added. The ***Lock groups*** setting can also be empty.



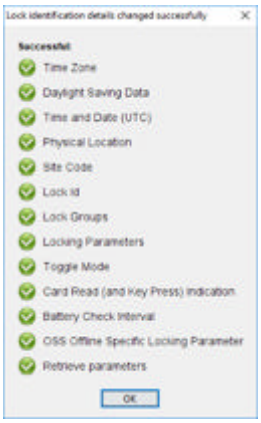
b. **Imported data:** This option can be used if lock identification details have been imported using the function ***Installation*** → ***Offline*** → ***Manage Lock Identification Data***. (See section *Manage Offline Lock Identification Data* on page 137). After import, lock identification details will automatically be displayed here. Select lock identification details in the list by clicking the desired row.



3. Click *OK*.
4. Hold the radio activation card at the lock, or remove and reinsert the battery (This step is not necessary for V3 locks that are connected with a USB cable.) to change the lock identification details.



The result is displayed.



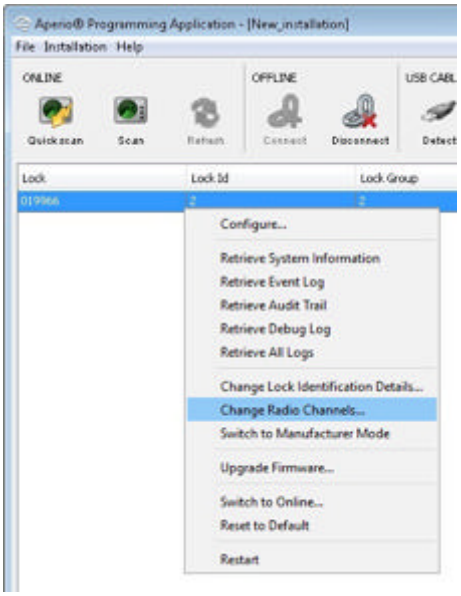
Import of radio channels are not be displayed.

To implement settings for new radio channels, select ***Change Radio Channels*** function on the right-click menu, where the new radio channels will be preselected for download to device. See section *Change Radio Channels* on page 129.

Change Radio Channels

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

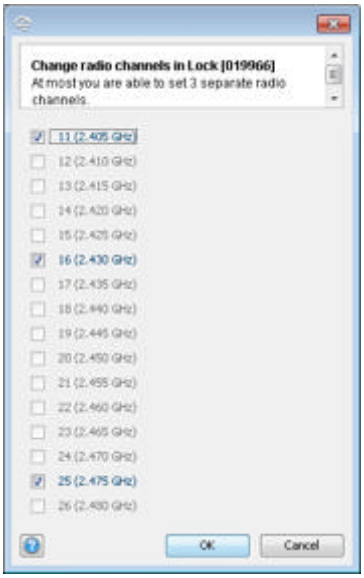
1. Select the lock in the scan result table. Right-click and select ***Change Radio Channels...***.



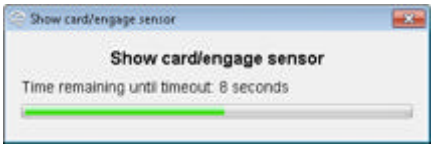
2. Unselect any of the three currently used channels to be able to select other radio channels. Click ***OK***.

For the US market channel 26 is disabled.

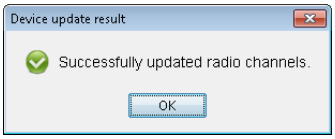
If change lock Identification details where used to import the radio channels, the new channels are preselected for download.



3. Hold the radio activation card at the lock, or remove and reinsert the battery (This step is not necessary for V3 locks that are connected with a USB cable.) to change the 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.



To change radio channel in USB radio dongle, see section *Offline Installation Settings* on page 7.

Change the Security Mode

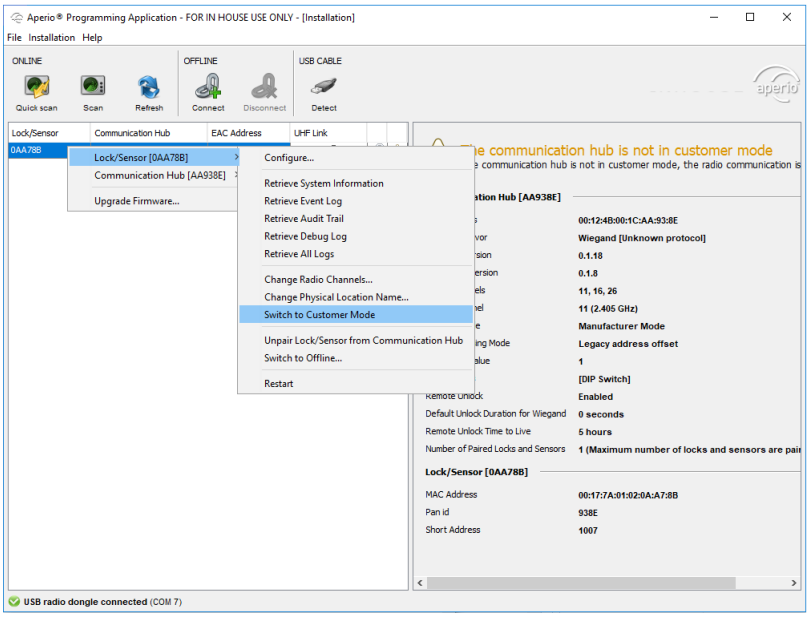
Secure communication is normally set during first configuration of locks/sensors and communication hubs with the configure wizard. Security mode is also accessible through the right-click menu.

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.

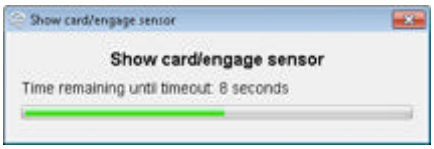
Explanation of symbols:

	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.

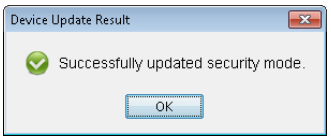
1. Right-click the unit and select ***Switch to Customer Mode/Switch to Manufacturer mode*** (This function is found directly on the right-click menu for offline locks).



2. Hold the credential at the lock, or engage the magnet for the sensor. (This step is not necessary for V3 locks that are connected with a USB cable, or online locks that have the polling interval set to less than 15 seconds.)



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 lock to see that the door has been set to Customer mode/Manufacturer mode.

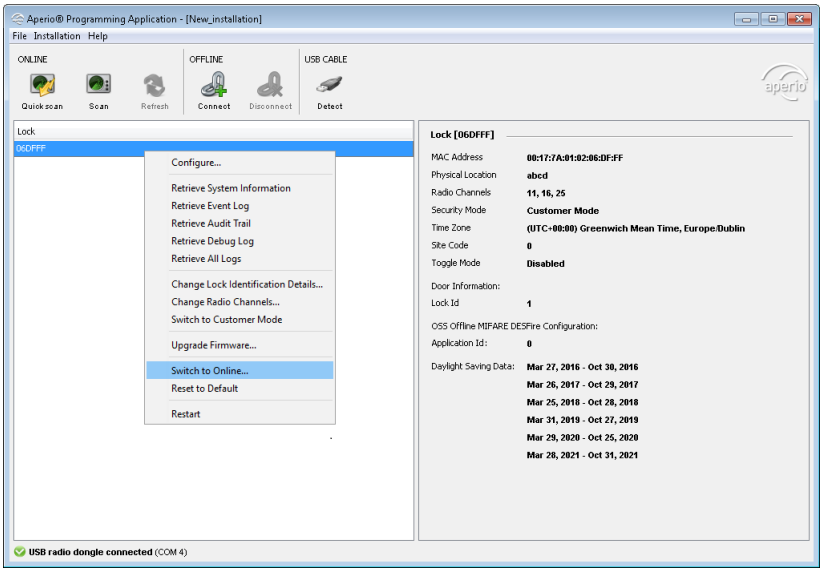
For Aperio online, the AH40 communication hubs must be connected to an EAC system (steady green light on the LED) to accept change of security mode. TLS encryption must also be enabled in the communication hub. If not so, the following error message is shown:

Switch to Online (V3 locks)

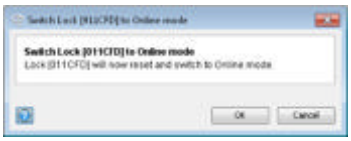
This function is only available if ***Show advanced settings*** is activated in Preferences, see section *Preferences* on page 8.

This function changes the operating mode of the selected V3 lock (V3.3 and higher).

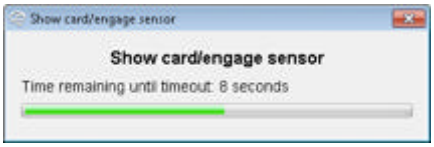
1. Right-click and select ***Lock*** → ***Switch to Online...***.



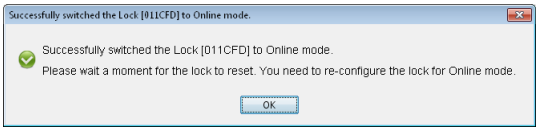
2. Click ***OK*** to change the operating mode for the lock.



3. Hold the radio activation card at the lock, or remove and reinsert the battery (This step is not necessary for V3 locks that are connected with a USB cable.)



4. Confirm the change of operating mode.



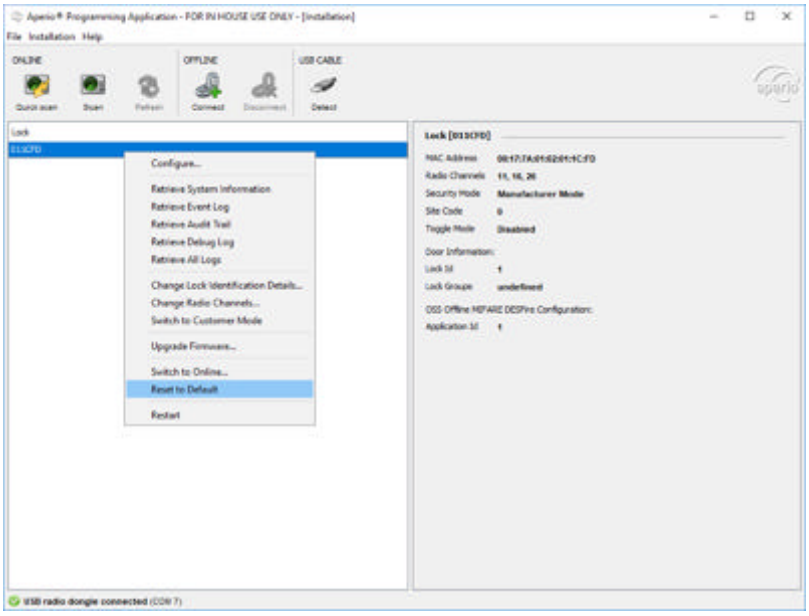
5. Reconnect to the lock, before performing further configuration according to the new operating mode.

Reset to Default

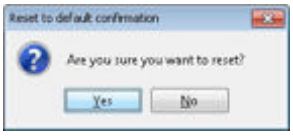
This function is only available if ***Show advanced settings*** is activated in Preferences, see section *Preferences* on page 8.

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.

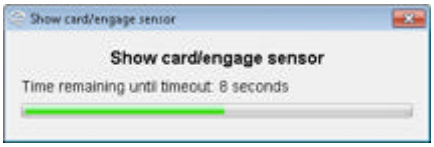
1. Select the lock, right-click and select ***Reset to Default***.



2. Confirm the reset by clicking ***Yes***.



3. Hold the radio activation card at the lock, or remove and reinsert the battery (This step is not necessary for V3 locks that are connected with a USB cable.) to perform a factory reset.



Result: The lock is reset and disappears from the installation view.

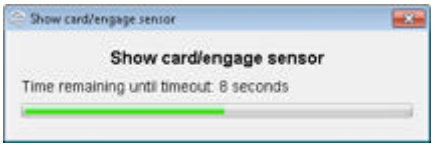
Reconfiguration of Lock after Factory Reset

To reconfigure a lock that has been reset without use of a factory default radio activation card:

1. Dismantle the lock cover.
2. Remove and reinstall the battery.
   Result: The lock performs a power on self test, one red and one green flash. After that the UHF transceiver is activated, yellow flashes during 20 s.

To be able to change the RFID Key in the lock to what is used in your system, you must perform remaining instructions during the 20 s when the UHF transceiver is active.

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* on page 98), 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 reinsert the battery).



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 124.

Manage Configurations

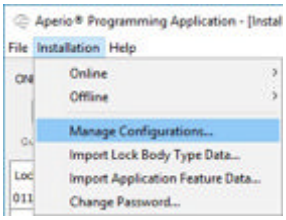
General

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.

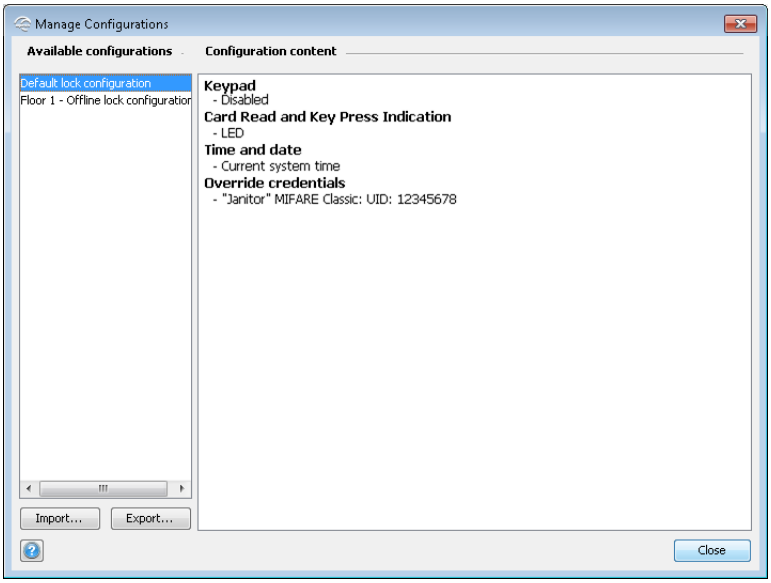
When you export a configuration, you cannot change the name of the configuration, only the file name holding the configuration information. Since configurations can be shared between different Aperio Programming Applications, it is preferable that a shared configuration (identified by its unique name) 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

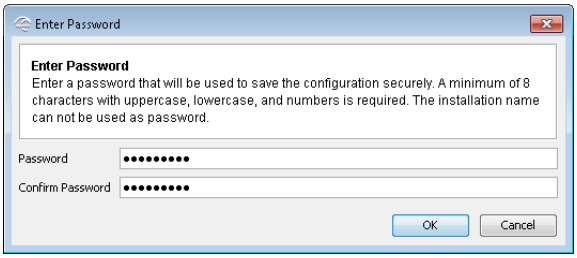
1. In the menu bar, select ***Installation*** → ***Manage Configurations***.



2. Select the configuration that should be exported to file and click ***Export...***.

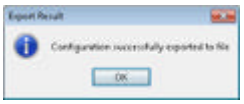


3. Select the folder where you want to store the configuration, chose a file name and click ***Save***.
4. Choose a password that will be used when importing the particular configuration, confirm it and click ***OK***.



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

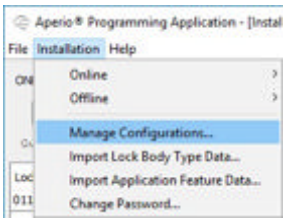
Result:



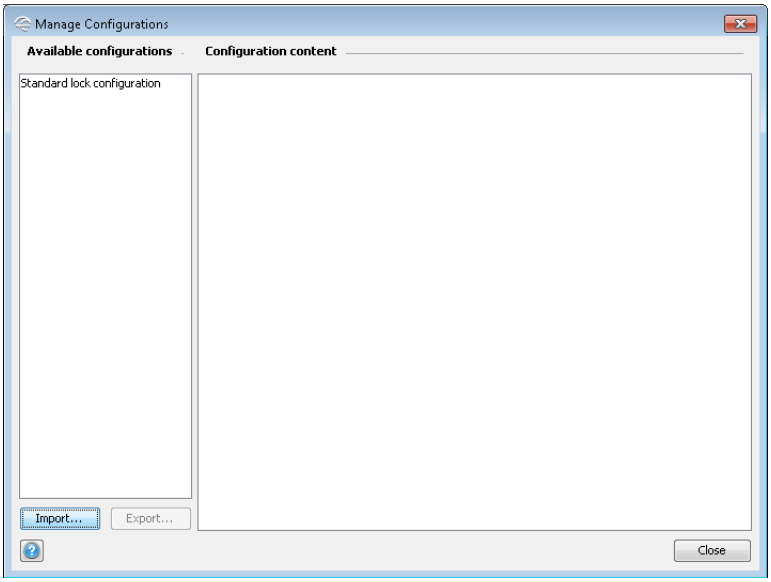
Importing Configuration

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

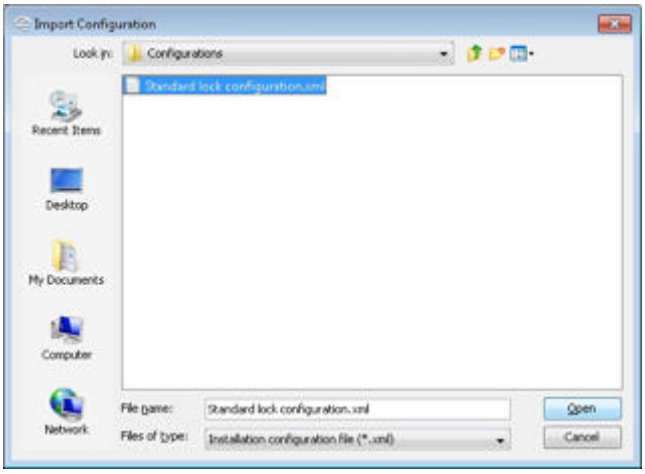
1. In the menu bar, select ***Installation*** → ***Manage Configurations***.



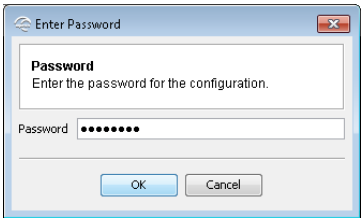
2. Click ***Import***.



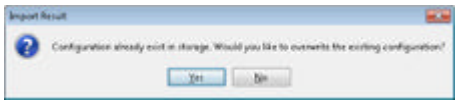
3. Select a valid configuration XML-file and click ***Open***.



4. Enter the password and click ***OK***.

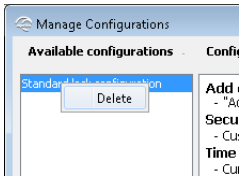


The configuration is identified by its name, not the name of the export file. When importing a configuration that already exists in the Aperio Programming Application you will be prompted if you want to replace the existing configuration.



Deleting Configuration

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



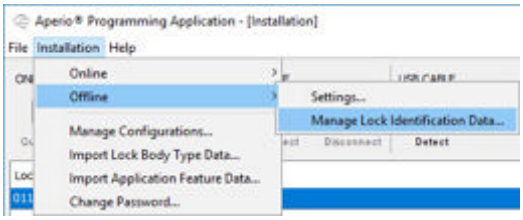
Manage Offline Lock Identification Data

This function allows import of lock identification data from an EAC system in the form of an XML file.

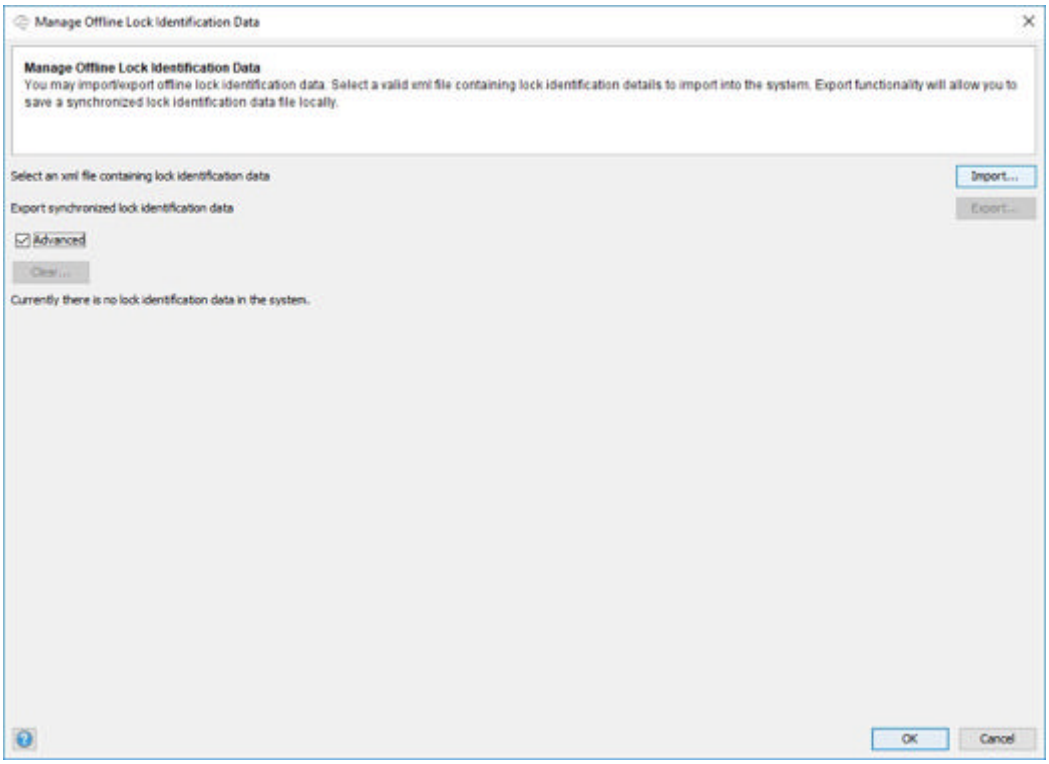
After configuration of the locks on the installation site, the information about the configured locks can be exported back for use in the EAC system.

Importing Lock Identification Data

1. In the menu bar, select ***Installation*** → ***Offline*** → ***Manage Lock Identification Data***.

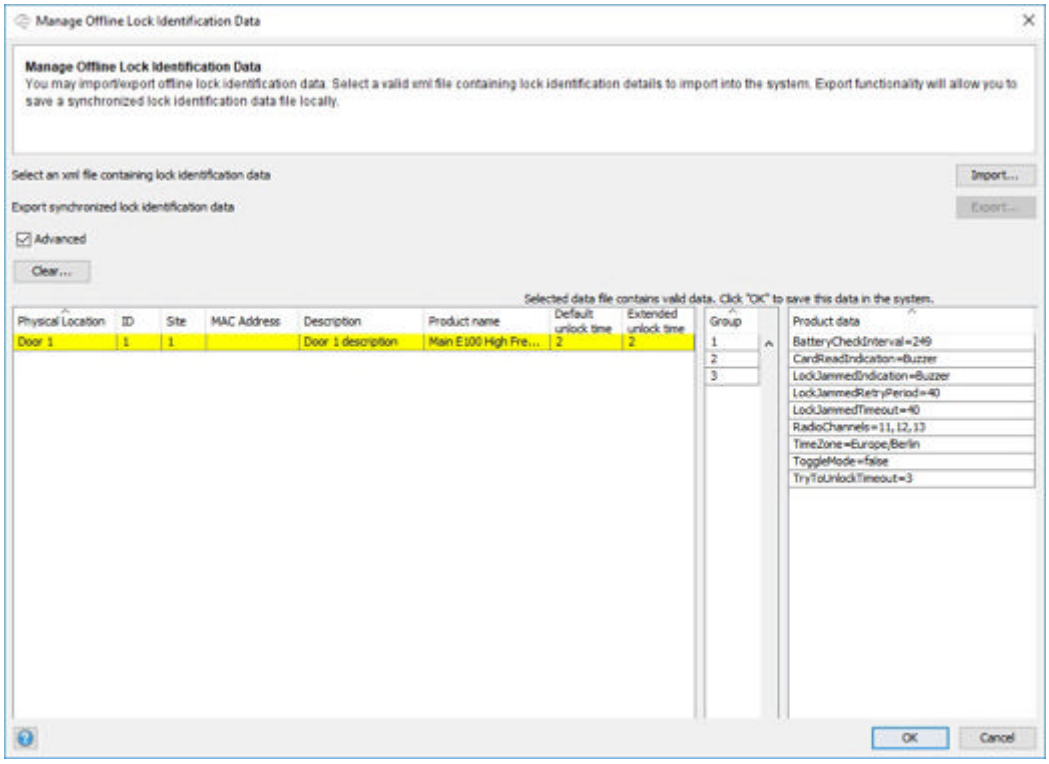


2. Click ***Advanced*** to check if there are any imported lock identification data. Click ***Clear*** to delete these.



3. 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 140).

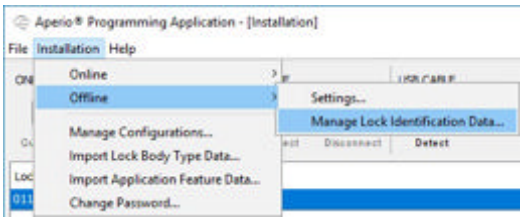
Click the door description to see the group and product data. The lock identification data is displayed. click the Click ***OK*** to save the data to the system.



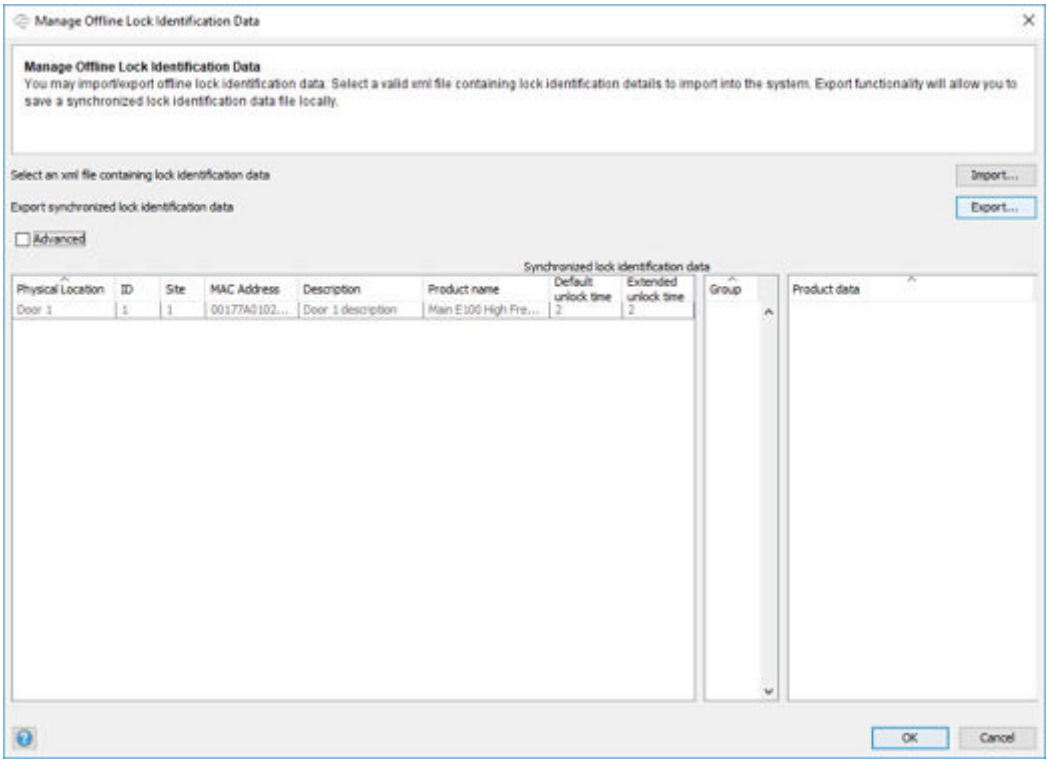
For OSS Offline locks multiple lock groups can be used.

Exporting Lock Identification Data

1. Select ***Installation*** → ***Offline*** → ***Manage Lock Identification Data***.



2. Click the ***Export...*** button to save the installation performed.



3. Click ***OK*** to exit.

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.
- For OSS Offline locks, up to 8 group can be defined per lock. Lock groups can also be omitted for OSS Offline locks
- Data file should have xml extension (ex. door_data.xml).

Configuration

Element name	Description	Mandatory
configName	The configuration name will not be visible in the Aperio Programming Application, but the value will be set when creating a configuration result.	yes
Timestamp	This will be set to the time when user selected to export the data, not when configuration was applied to lock E.g 2020-11-25T14:58:25+00:00	yes
Version	Version currently not used, but this will most likely change in later versions	Yes (due to mandatory in OSS-SO)
DoorAdd	Adds a new door, 0..N If door exists, this information will completely overwrite the previous door without retaining any information	no

Element name	Description	Mandatory
DoorChange	Adds a door if door does not exist, else all information in xml will be overwrite the existing door.	no

ManufacturerData

Element name	Description
ManufacturerId	Will be set to 1 during export
ManufacturerName	Will be set to ASSA ABLOY during export
ManufacturerProductName	Contains the short name of the lock
serial	Contains mac retrieved from lock. When seeding a new door to Aperio Programming Application, this field should not exist in xml or be set to an empty value else Aperio Programming Application will not allow lock with different mac to be configured
batteryState	flat/low/ok or unknown if this functionality is not supported by reader
ASSA_ABLOY_PARAMETERS	Aperio device settings, see below. Example: `<ASSA_ABLOY_PARAMETERS>TimeZone=Europe/Berlin</ASSA_ABLOY_PARAMETERS>`

Parameter name	Description	Min	Max
TimeZone	Sets the timezone (UTC based) in the device (e.g Europe/Berlin)	-	-
RadioChannels	Sets the UHF channels used for wireless communication between the reader and the configuration tool. Sets 1-3 possible channels. (e.g 10,11,12)	11 At least one channel	26 At most three channels specified
BatteryCheckInterval	Sets how often the device should check the battery status outside of the checks that is performed alongside the normal operations. Specified in minutes	1	255
TryToUnlockTimeout	Sets the timeout for how long unlock should be retried before reporting failure. Specified in seconds	1	15
LockJammedTimeout	Sets how long the device should retry to lock before reporting error and going into lower frequency retries. Specified in seconds	10	65535
LockJammedRetryPeriod	Sets how frequent retries should be made after first lock jammed detection. Specified in seconds	1	65535

Parameter name	Description	Min	Max
LockJammedIndication	Sets the indication on the reader for Lock Jammed, set between LED, buzzer and LED/ Buzzer. Note, the support for buzzer is device specific	-	LED Buzzer LED_Buzzer NONE
CardReadIndication	Sets the indication on the reader when a cards is presented, set between LED, buzzer and LED/Buzzer. Note, the support for buzzer is device specific.	-	LED Buzzer LED_Buzzer NONE
ToggleMode	Sets if toggle mode should be used. Boolean true/false	false	true

Sample Lock Identification Data XML file

Example of XML-file that can be used for all types of locks:

```
<?xml version="1.0" encoding="UTF-8"?>
<Configuration xmlns="http://oss-so.com">
    <configName>configurationName</configName>
    <Timestamp>2020-11-25T14:58:25+00:00</Timestamp>
    <Version>Version 1.0</Version>
    <DoorAdd>
        <Door>
            <Id>1</Id>
            <Name>Door 1</Name>
            <Description>Door 1 description</Description>
            <SiteId>1</SiteId>
            <DefaultUnlockTime>2</DefaultUnlockTime>
            <ExtendedUnlockTime>2</ExtendedUnlockTime>
            <manufacturerData>
                <ManufacturerId>1</ManufacturerId>
                <ManufacturerName>ASSA ABLOY</ManufacturerName>
                <ManufacturerProductName>Main E100 High Frequency
V3</ManufacturerProductName>
                <serial></serial>
                <batteryState>ok</batteryState>
                <ASSA_ABLOY_PARAMETERS>TimeZone=Europe/Berlin</
ASSA_ABLOY_PARAMETERS>
                <ASSA_ABLOY_PARAMETERS>TryToUnlockTimeout=3</
ASSA_ABLOY_PARAMETERS>
                <ASSA_ABLOY_PARAMETERS>CardReadIndication=Buzzer</
ASSA_ABLOY_PARAMETERS>
                <ASSA_ABLOY_PARAMETERS>LockJammedRetryPeriod=40</
ASSA_ABLOY_PARAMETERS>
                <ASSA_ABLOY_PARAMETERS>ToggleMode=false</
ASSA_ABLOY_PARAMETERS>
                <ASSA_ABLOY_PARAMETERS>LockJammedTimeout=40</
ASSA_ABLOY_PARAMETERS>
                <ASSA_ABLOY_PARAMETERS>RadioChannels=11,12,13</
ASSA_ABLOY_PARAMETERS>
                <ASSA_ABLOY_PARAMETERS>BatteryCheckInterval=249</
ASSA_ABLOY_PARAMETERS>
                <ASSA_ABLOY_PARAMETERS>LockJammedIndication=Buzzer</
ASSA_ABLOY_PARAMETERS>
            </manufacturerData>
            <doorgroups>
                <int>1</int>
```

```
                <int>2</int>
                <int>3</int>
            </doorgroups>
        </Door>
    </DoorAdd>
</Configuration>
```

Upgrade of Aperio Hardware Firmware

This chapter describes how to upgrade both online and offline communication hubs and locks/sensors with a new firmware that is contained in the firmware file. 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.

Consider the following notes when upgrading the Aperio online firmware:

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 selecting a device for firmware upgrade the Aperio Programming Application will compare the current device firmware version to the new firmware version in the afw file. In the firmware upgrade window upgrade components for units with firmware older than the version contained in the afw file will be selected by default. The rest will be greyed and not selected.

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 must be used to download the new firmware, which requires that the AH40 communication hub IP address and other network settings has correctly been 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.

Upgrade Firmware

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

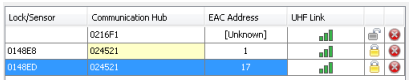
The Aperio Programming Application performs a check of firmware and lock so that the firmware always match the hardware. A C100 afw file will only be used with cylinder locks. An E100 afw file will only be used with escutcheon locks etc.

All firmware included in the afw file should be downloaded to hardware. Canceling the upgrade process or partly upgrading the hardware can cause malfunction.

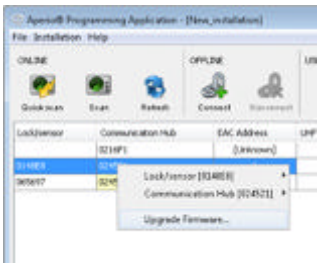
Do not remove the battery or the V3 locks USB cable during the upgrade process. This can cause malfunction.

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 Aperio Programming Application will not enable the upgrade function.

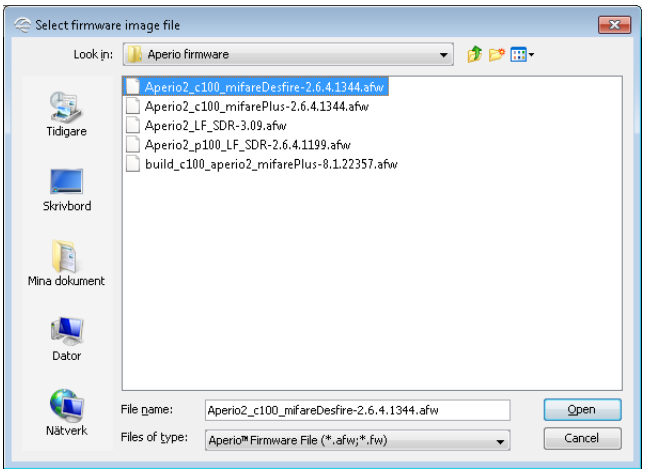


3. Right-click on the communication hub/lock/sensor in the Installation view and select ***Upgrade Firmware***.

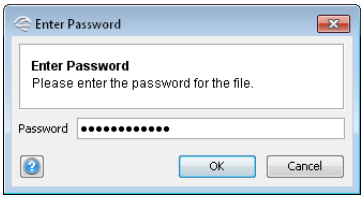


Always upgrade the communication hub before upgrading the locks/sensors. The reason is that communication hubs should always support older lock/sensor firmware but the opposite may not always be possible.

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

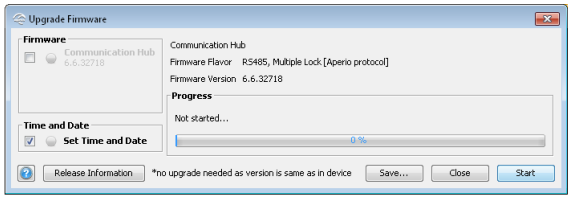


5. Enter the password supplied with the firmware.

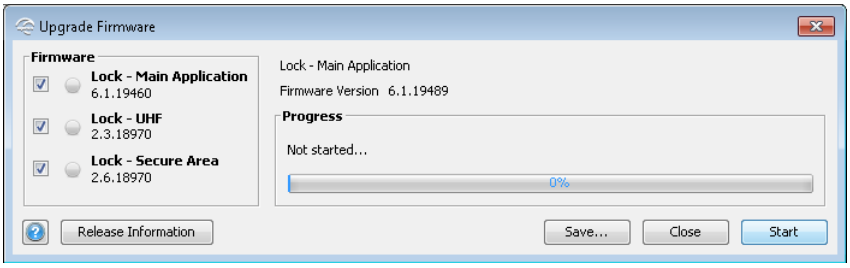


Result: The firmware upgrade window is shown, with a list of the firmware components that may be upgraded. Click ***Release Information*** to get more information about the firmware file.
The firmware list varies, depending on the firmware file and on the firmware version in the devices:

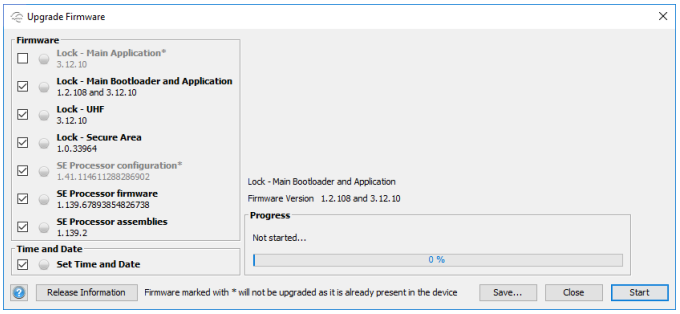
- The first example shows a communication hub which already has the same FW version as the one in the firmware file. Therefore ***Communication Hub*** is greyed out and upgrade is not necessary.



- The next example shows a list of three firmwares for a lock, all with FW versions older than the new FW version in the firmware file. Therefore all three components are checked by default.



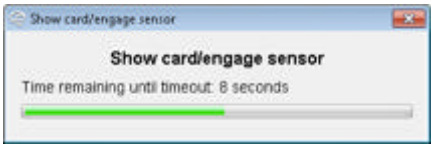
- The third example shows a list of firmwares, where two of them have the same FW versions as in the lock. Therefore only the newer firmwares are checked by default. To reinstall the firmware, although it already has the same version, select the checkbox.



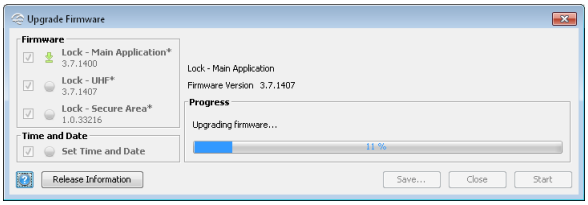
6. Click ***Start*** to run the upgrade process.

Only deselect firmware if site specific settings allow this. Existing old firmware in hardware combined with new firmware can cause malfunction.

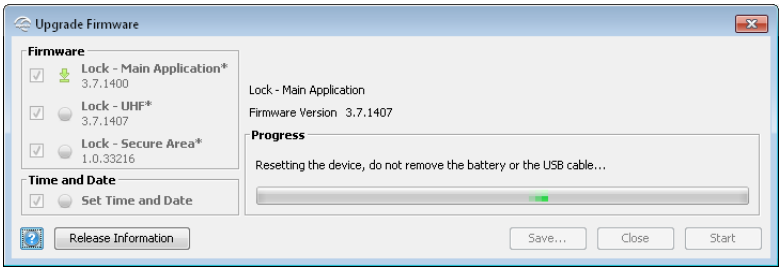
7. If you are upgrading a lock/sensor you will be prompted to connect. Hold the credential at the lock, or engage the magnet for the sensor. (This step is not necessary for V3 locks that are connected with a USB cable, or online locks that have the polling interval set to less than 15 seconds.)



Result: The upgrade will start with the first 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.



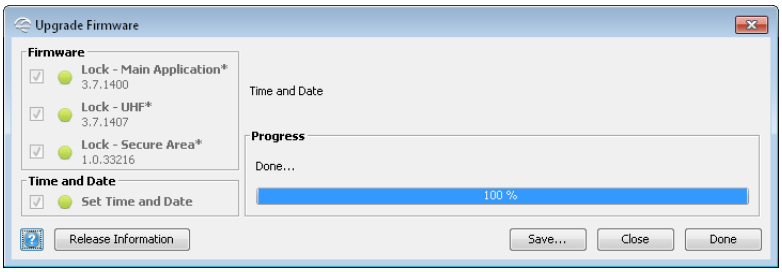
After finished download, the device resets.

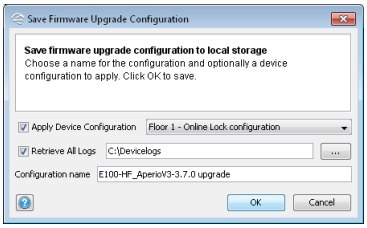


The firmware upgrade continues automatically with the remaining firmwares in the list.

Canceling the firmware upgrade process by clicking ***Close*** should be avoided. Existing old firmware in hardware combined with new firmware can cause malfunction.

8. **Optional**: After all firmware is downloaded, click ***Save...*** to save the settings for firmware upgrade of several devices.





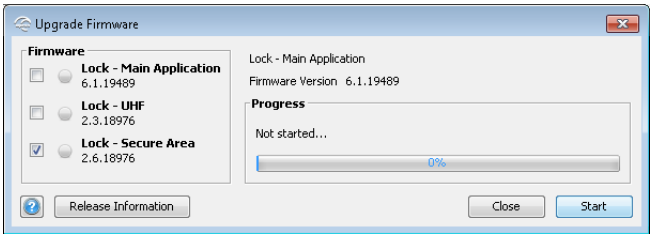
- ***Apply Device Configuration***: Select an existing device configuration, valid for the same device type as the firmware.
- ***Retrieve All Logs***: Downloads all logs of the device, prior of the firmware upgrade.
- ***Configuration name***: The name of the firmware configuration visible in the Aperio programming application.

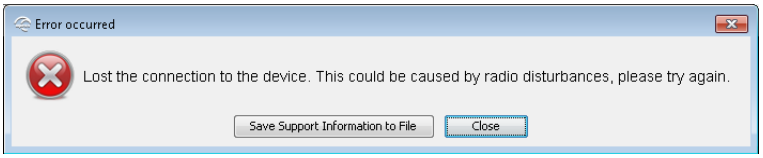
9. Click ***Close***/***Done*** to finish.

Upgrade Failure

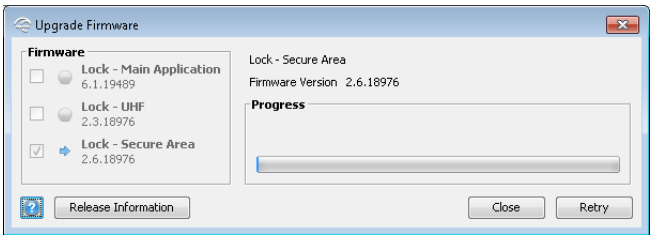
An upgrade failure is typically due to bad radio conditions. The work around is to move closer to the communication hub/offline lock and try upgrading again.

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.



Changing the Battery of the Lock

The exact procedure for changing the battery of the lock is described in the manual for each product. The following are some general issues to consider when changing the battery of an Aperio lock:

1. **Remove old battery:** Always replace the battery with a fresh one. The battery alarm detection algorithm is dependent on that the battery has full capacity when the lock is powered up.
2. **Show a card:** After removing the old battery, show any card to the lock to make sure that all energy is drained from the internal storage capacitors thus ensuring a proper power up.
3. **Insert a new battery:** Prepare for the battery replacement operation. If the lock is left without battery for too many seconds, the time is lost and it is required to use the Aperio Programming Application to set it right again (see section *Setting the Time of a Lock* on page 82).
4. **Check Power on Self test (POST):** After inserting the new battery, check the LED flashing for a successful POST. If the battery is not accepted as new, there will be an error indication (10 red flashes) instead of the POST flashes.

6 Installation of Aperio 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 8, Windows 8.1 or Windows 10
- USB 2.0.

Files Needed for the Installation

- Aperio Programming Application software.
- Encryption key file.

The software is delivered from your local ASSA ABLOY company.

Install the Aperio Programming Application

Follow these steps to install the Aperio Programming Application and the drivers necessary for the usage of the USB radio dongle and the USB cable.

1. Unpack the Aperio distribution file (i.e. progapp-x.y.z.zip/progapp_US-x.y.z.zip), containing the setup.exe file, in a temporary folder.
2. Run the setup.exe file and follow the instructions on screen.
   Result: The Aperio Programming Application and the drivers for the USB radio dongle and the V3 USB cable are installed.

Recommended Procedure when Using the V3 Lock USB Cable

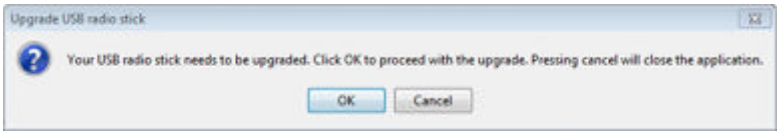
When connecting a V3 lock with a USB cable for the first time, it is recommended to perform the following steps, to successfully install the V3 lock USB cable driver.

1. Make sure that the operating system is upgraded with the latest updates.
2. Before connecting the USB cable, make sure that the computer is connected to the internet.
3. Connect the USB cable to the V3 lock and then to the computer.
   The installation of the driver can take several minutes.

USB Radio Dongle Firmware Upgrade

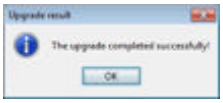
The USB radio dongle firmware version is checked during start-up of the application. An upgrade is automatically initiated if the USB radio dongle has an older firmware version than the current Aperio Programming Application:

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.


Upgrade result
The upgrade completed successfully!
OK

7 Troubleshooting

The tables below shows possible problems when using the Aperio technology, and how to solve them:

Troubleshooting - Online

The tables below shows possible problems when using the Aperio online technology, and how to solve them:

During Scanning

Problem indication	Cause	Action
None or only some of the communication hubs are found when scanning	· All channels are busy or too many communication hubs are using the same channel.. · The communication hub(s) are not working. · The communication hub(s) are out of range. · The communication hub(s) are not powered.	· Repeat the scanning process by selecting Scan /Scan all · Restart the hub. · Temporary reduce the number of powered up Hubs within radio range during configuration. (After configuration, make sure that this communication hub have stable radio communication with paired locks/ sensors.)
Communication error is displayed and no configuration can be done to the communication hub.	· The communication hub belongs to another installation and has another encryption key.	1. Switch installation or create a new installation with the correct encryption key. 2. Repeat the scanning and pairing process.
Unstable communication between communication hub and lock/sensor even though the MAC address is displayed at scan.	· A probable cause is bad radio conditions or limited radio range.	· Try moving the USB radio closer to the communication hub. Either by moving the laptop or by using an A-A USB extension cable to distance the USB radio from the PC.

The Aperio Communication hubs are by default configured to select the best channel out of three possible. If the selected channel is disturbed, a new channel is selected automatically. Communication hubs in an Aperio system normally distribute themselves on different channels but a synchronized power up of all hubs may cause them to initially choose the same channel.

Note that this problem does not affect performance of already installed and paired lock/ cylinders/sensors and communication hubs, only the Aperio Programming Application scan functionality is affected.

During Door Installation and Update

Problem indication	Cause	Action
Not possible to pair communication hub and lock/sensor	· You are using a credential configured as an override credential. · The lock/sensor and the hub are on different radio channels.	· Use a credential that is not on the override credentials list. · Check the radio channel settings for the lock/sensor and the hub so that they match.
Not possible to use override credentials	No default override credentials are configured for the installation.	Add the credentials one by one in the lock configuration wizard.
The device update fails	· You have not shown the credential to the lock within 30 seconds. · The lock and hub might be in different security modes, then communication problems can easily occur.	· Perform device update again and show the credential to the lock within 30 seconds. · Change security mode in the hub and perform device update again. .

During Configuration

Problem indication	Cause	Action
The program application reports an update failure. The device does not support the desired configuration.	· The firmware on the device is outdated. · You are trying to configure something that the device does not support	· Check the current firmware on the device and perform an upgrade if needed. Also check the intended new configuration .
The AH40 communication hub LED is flashing red twice = no connection between the EAC system and the communication hub	· The hub is not properly connected to the IP network. · The hub network parameters are not correctly configured. · The ACU address, port or TLS settings are not properly configured in the communication hub. · The ACU is not properly configured. · The certificate used by the ACU is not supported.	· Check that the Ethernet LED is green. If not, check Ethernet cable and network equipment. · Configure the hub network parameters. · Configure the hub EAC connection. · Make sure that the communication settings in the EAC matches the hub EAC connection settings. · Make sure that a valid certificate type is used.

During Normal Operation

Problem indication	Cause	Action
The communication hub LED is flashing red once = no connection between the lock/sensor and the communication hub	· The lock/sensor and communication hub are not paired. · The lock/sensor and the communication hub have different channel masks. · The battery of the lock/sensor has run out. · The status message intervals differ between the hub and the lock	· Repeat the scanning process by selecting Scan /Scan all. · Pair the lock/sensor and communication hub in the Configure lock wizard of the Aperio Programming Application. · Change the radio channel. See the Aperio Programming Application manual, ref [2]. · Replace the battery of the lock/sensor. See the Aperio Programming Application manual, ref .[1] · Make sure that the lock has the same or a shorter status message interval than the hub
The communication hub LED is flashing red twice = no connection between the EAC system and the communication hub	· The EAC address is not properly configured in the communication hub. · The EAC system is not properly configured.	Configure the EAC address. Refer to the Aperio mechanical installation manual.
Unstable radio communication between lock/sensor and communication hub	· Poor radio link quality. · The lock/sensor and the communication hub have different channel masks.	· Change the radio channel. See the Aperio Programming Application manual, ref .[1]
The V3 lock LED is flashing red.	· The battery has run out.	· Connect the USB cable to provide emergency power, and show credential to open the door. · Replace the battery. See lock installation instructions.

Lock Self Test LED Indication (V2 locks)

After replacing the battery or a power up, a Power on Self Test (POST) is performed.

If the battery is not accepted as new after a power on reset, no POST is performed, instead 10 quick red flashes is used to indicate "Error in lock".

The result is indicated using a series of red and green LED flashes as is described by the figure below:

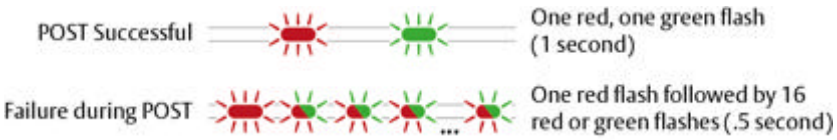


Figure 5: Lock POST LED indication

The first flash is always red. If the POST fails, the color of the 16 trailing flashes indicate the status of each individual test as described by the following table:

Blink	Meaning if red	Code in event log
1	POST initiation flash, always red	-
2	Main board firmware corrupt	0x0001
3	Override list corrupt	0x0002
4	Production data corrupt	0x0004
5	Security data corrupt	0x0008
6	Configuration data corrupt	0x0010
7	Load Circuit Error	0x0020
8	Configuration data corrupt 2	0x0040
9	Secure Area Encryption Key error	0x0080
10	Secure Area Motor error	0x0100
11	Secure area communication error	0x0200
12	Secure area memory corrupt	0x0400
13	Secure area sensor or motor error	0x0800
14	Radio modem communication error	0x1000
15	Radio modem memory corrupt	0x2000
16	Radio modem configuration error	0x4000
17	Radio modem RF circuit error	0x8000

Lock Self Test LED Indication (V3 locks)

After replacing the battery or a power up, a Power on Self Test (POST) is performed.

If the battery is not accepted as new after a power on reset, no POST is performed, instead 10 quick red flashes is used to indicate "Error in lock".

The result is indicated using a series of red and green LED flashes as is described by the figure below:

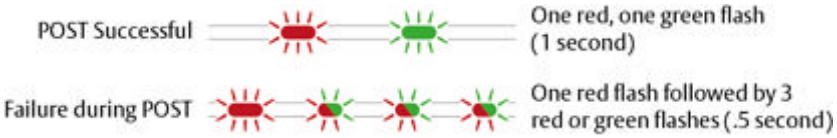


Figure 6: Lock POST LED indication

The first flash is always red. If the POST fail, the color of the 3 trailing flashes indicate the status of each individual test as described by the following table:

Blink	Indication group	Description	Purpose
1	POST initiation flash	Always red	-
2	Fatal error	Tests core functionality. MCUs, memory's and internal communication, etc.	This is a problem that can not be solved on the field.
3	Electrical interconnection error	Tests communication between the different parts in the system, i.e. different boards connected with a wire. Will be different test cases depending on the specific partitioning of a product.	Check that all physical parts are connected together in the right way. If the test fails it is likely a cable/connection problem between the modules. This is a problem that could be solved in the field.
4	Mechanical error	Test related to moving parts of the lock.	If the test fails it is likely due to a mechanical problem. This is a problem that could be solved in the field.

Troubleshooting - Offline

The tables below shows possible problems when using the Aperio offline technology, and how to solve them:

When Connecting to Lock

Problem indication	Cause	Action
The lock is not found when trying to connect = no connection between the programming application/laptop and the lock.	· All channels are busy. · The Aperio Programming Application and the lock have different radio channels. · The lock is not working. · The lock is not powered. · The lock is out of range of the USB dongle.	· Click ***Connect*** again. · Change the radio channel. See the Aperio Programming Application manual, section Change Radio Channels.
Unstable communication between lock and Radio dongle even though the MAC address is displayed after connecting to lock.	· A probable cause is bad radio conditions or limited radio range.	· Try moving the USB radio closer to the lock. Either by moving the laptop or by using an A-A USB extension cable to distance the USB radio from the PC.
The device update fails	· Radio not activated in lock	· Perform device update again and show the radio activation card to the lock.

During Normal Operation

Problem indication	Cause	Action
The lock LED is flashing red.	· Hardware failure/Lock Jam	· Service the lock.

Problem indication	Cause	Action
The V3 lock LED is flashing red.	· The battery has run out.	· Connect the USB cable to provide emergency power, and show credential to open the door. · Replace the battery. See lock installation instructions.

Lock Self Test LED Indication

After replacing the battery or after a power up,, a Power on Self Test (POST) is performed.

If the battery is not accepted as new after a power on reset, no POST is performed, instead 10 quick red flashes is used to indicate "Error in lock".

Battery not fully charged, energy counter not reset, no Power on self-test done.  Ten red flashes (.125 sec. each)

The result is indicated using a series of red and green LED flashes as is described by the figure below:

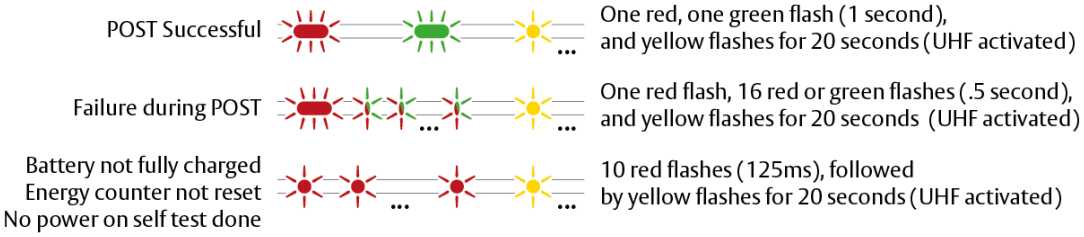


Figure 7: Lock POST LED indication

If the battery is not accepted as new after a power on reset, no POST is performed, instead 10 quick red flashes is used to indicate “Error in lock”.

The first flash is always red. If the POST fail, the color of the 16 trailing flashes indicate the status of each individual test as described by the following table:

Blink	Meaning if red	Code in event log
1	Post initiation flash	-
2	Main board firmware corrupt	0x0001
3	Reserved for future use	0x0002
4	Production data corrupt	0x0004
5	Production data corrupt	0x0008
6	Configuration data corrupt	0x0010
7	Load circuit corrupt	0x0020
8	Configuration data corrupt	0x0040
9	Secure area key error	0x0080
10	Secure area motor error	0x0100
11	Secure area communication error	0x0200
12	Secure area memory error	0x0400
13	Secure area motor sensor error	0x0800
14	Radio modem communication error	0x1000

Blink	Meaning if red	Code in event log
15	Radio modem memory corrupt	0x2000
16	Radio modem EEPROM corrupt	0x4000
17	Radio modem RF error	0x8000

8 Security Statement

The following security measures are applicable to Aperio:

Authentication	3-pass mutual authentication (challenge-response protocol) based on AES 128. 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 micro controller.
Encryption key	Unique encryption key seed for each installation.
Database	The encrypted database in Aperio 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

9 Licenses

The Aperio Programming Application uses a number of open source licenses. For details, see section *Software Version* on page 9.

Assa Abloy

Tribee 2 USB

Compliance

IC

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

To maintain compliance with the RF exposure guidelines, place the product at least 20cm from nearby persons.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

1. L'appareil ne doit pas produire de brouillage;

2. L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Pour rester en conformité avec les consignes d'exposition aux RF, placez le produit à au moins 20 cm des personnes proches.

FCC

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: 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.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) this device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.

RF Exposure

"FCC RF Radiation Exposure Statement Caution: To maintain compliance with the FCC's RF exposure guidelines, place the product at least 20cm from nearby persons."

The ASSA ABLOY Group is the global leader in access solutions. Every day we help people feel safe, secure and experience a more open world.

ASSA ABLOY

Contact

www.assaabloy.com/aperio