



## WHITE PAPER

# How to use Aperio Locks with Access Portal

Information contained in this document is for anyone interested in how to use Aperio in Access Portal. We describe supported features, configuration using the Aperio Programming tool and then configuration and use of Aperio Locks in Access Portal.

#	Revision Date	Revision Author	Comments
1	2016/09/09	Warren Boucher	Initial Revision
2	2016/11/25	Warren Boucher	Remote Unlock
3	2017/01/18	Warren Boucher	Upgrading Firmware, Licensing, Minimum Requirements
4	2017/03/24	Warren Boucher	Added section for FAQ's.
5	2017/07/06	Warren Boucher	Updated Appendix A, Supported Features.

# Table of Content

[1. Minimum Software / Firmware Requirements](#)

[2. Overview](#)

[3. Aperio Hardware Configuration](#)

[4. Access Portal Configuration](#)

[Troubleshooting & FAQ's](#)

[Appendix A - Access Portal Features](#)

[Appendix B - Door Mode Support](#)

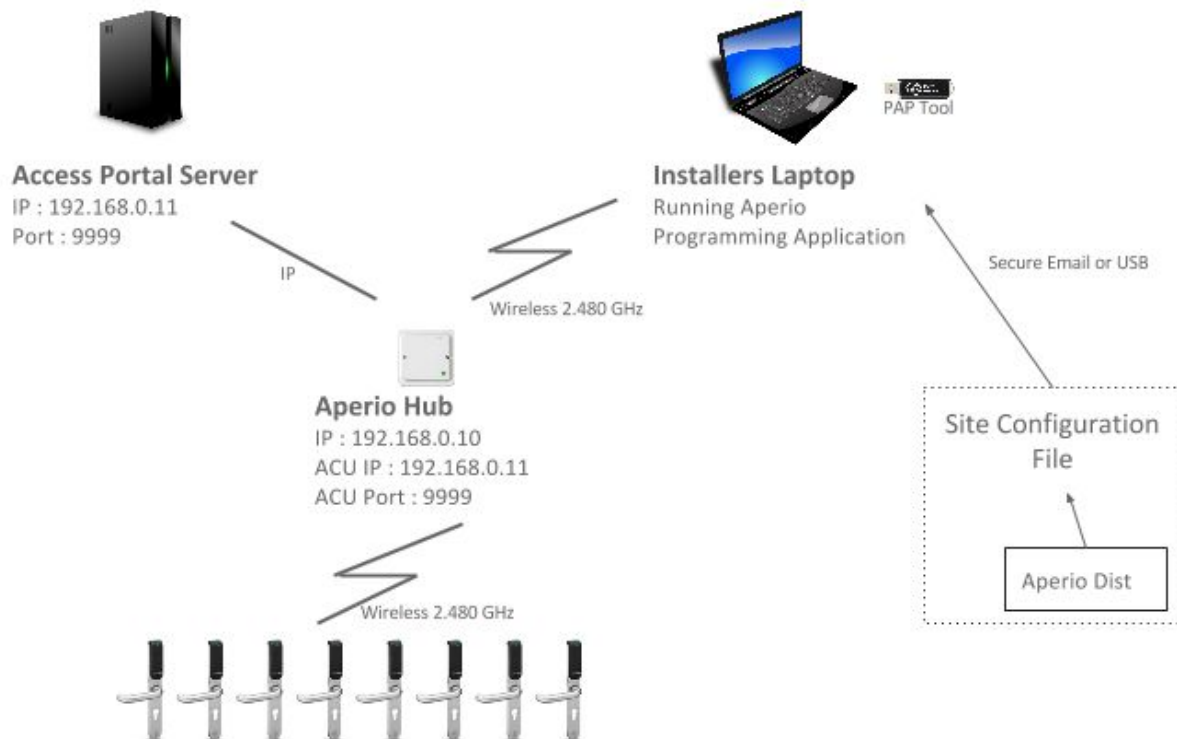
[Appendix C - Firmware Upgrade](#)

# 1. Minimum Software / Firmware Requirements

#	Requirement	Version	Comments
1	Access Portal Software	V2.0	Basic, Pro or Enterprise
2	IP Communication Hub (AH40)	V1.5.2368	FW for communications hub
3	Locks	V3-3.2.x	FW for locks

## 2. Overview

This section gives a brief overview on Aperio Locks and how Aperio Locks get used with Access Portal.



### [Example network diagram & configuration requirements](#)

Aperio is an Assa Abloy technology that enables mechanical locks to be wirelessly linked to a new or existing access control system, while Access Portal is a modern Access Control system that makes use of client server architecture. A typical Access Portal installation consists of proprietary Impro hardware but can also be used with OEM access control hardware such as Aperio Locks.

Aperio locks connect wirelessly to a communications hub which in turn connects via ethernet to the Access Portal server. To achieve this, the Aperio Programming Application needs to be used to pair locks to a communications hub and to configure a communications hub to communicate with Access Portal.

Although Aperio v3 Locks support an offline cache of up to 200 credentials over the last 30 days, we recommend that the offline cache is only used if you are confident the network will only drop in emergencies. Since the offline cache does not follow any authentication rules, a tagholder would be able to access a door after hours, etc if the network dropped or the Access Portal server was down for maintenance.

Communications between Access Portal and the communication hub is encrypted using TLS.

The certificate of which needs to be provided when configuring Access Portal. This can be a self signed certificate.

Aperio communication hubs and locks are installed into Access Portal as system controllers and readers emulating impro hardware. Tagholders are enrolled into Access Portal and granted access to doors as per normal.

#### Steps for using Aperio Locks with Access Portal

1. Physically install locks and communication hubs. *Remember that there is a limit to the number of locks that can be paired with a communication hub and you should plan accordingly.*
2. Configure communication hubs and pair the correct locks to those hubs.
3. Install Access Portal v1.8.6 or later on an access control server.
4. Install Aperio hardware into Access Portal and configure.

## 3. Aperio Hardware Configuration

### Prerequisites for configuring Aperio Communication Hubs and Locks.

1. Communication Hubs and Locks need to be installed.
2. The Installer needs a Laptop with:
  - a. The Aperio Programming Application installed.
  - b. The Aperio PAP tool to communicate wirelessly to an Aperio Communications Hub.
  - c. A site configuration file from Aperio that is unique to the installation.

### Step 1: Launch the Aperio Programming Application and create a new installation

**New Installation**

**Installation**  
An installation represents a complete Aperio® system. The password is used to securely encrypt all settings and configurations for the installation. A minimum of 8 characters with uppercase, lowercase, and numbers is required. The installation name can not be used as password. The key file contains unique keys that are used to secure the radio communication and prevent unauthorized reconfiguration of the system. Do *not* use the same key file for different installations.

Installation Name

Password

Confirm Password

Key File  ...

Aperio Programming Application - New Installation Window

### Fields for the New Installation Window

- The installation name should be a meaningful name that will identify the installation in the future. Possibly consider using a business name or address.
- The password entered here will be required every time you need to later make changes to the configuration of a communication hub or one of its paired locks. The password must be at least 8 characters long and contain at least one uppercase letter, one lowercase letter and one number.
- The Key File is received from Aperio and should be unique per installation to ensure maximum security. Once the Aperio Installation has been locked to Customer mode, only the correct Key File will be able to access the site.

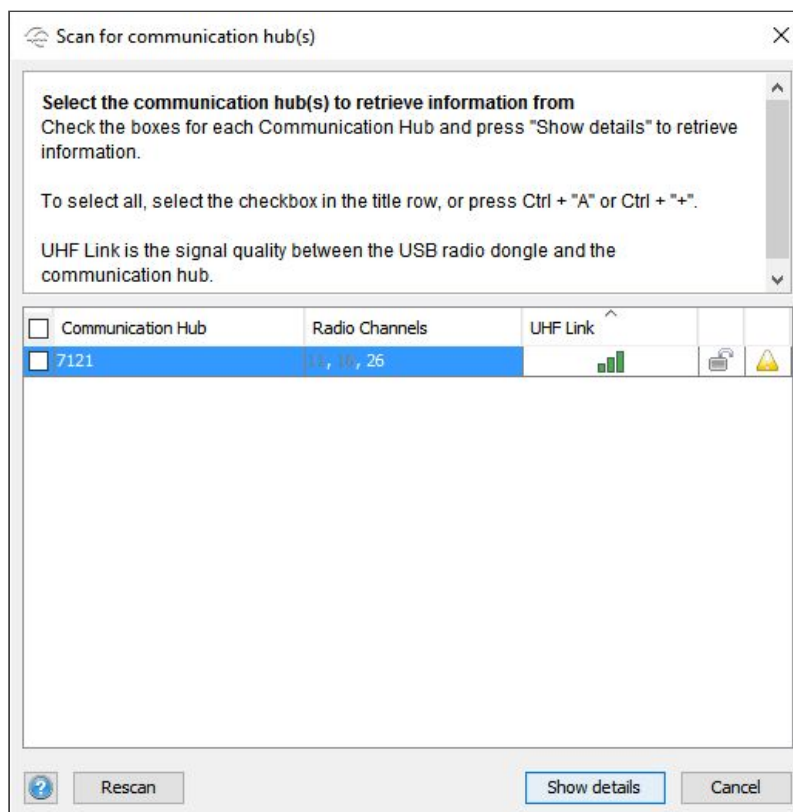
## **Step 2: Use the quick scan button to search for a communication hub to configure**



*Aperio Programming Application - Main installation window*

## **Step 3: Select the communication hub from the scan results**

You need to select a communications hub to configure. The next step is to pair locks with the communication hub.

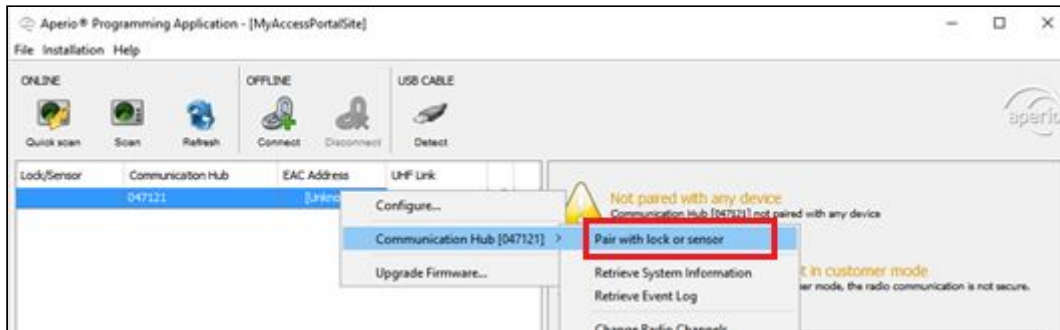


*Aperio Programming Application - Scan for communication hubs result.*

#### **Step 4: Pair the communication hub with locks**

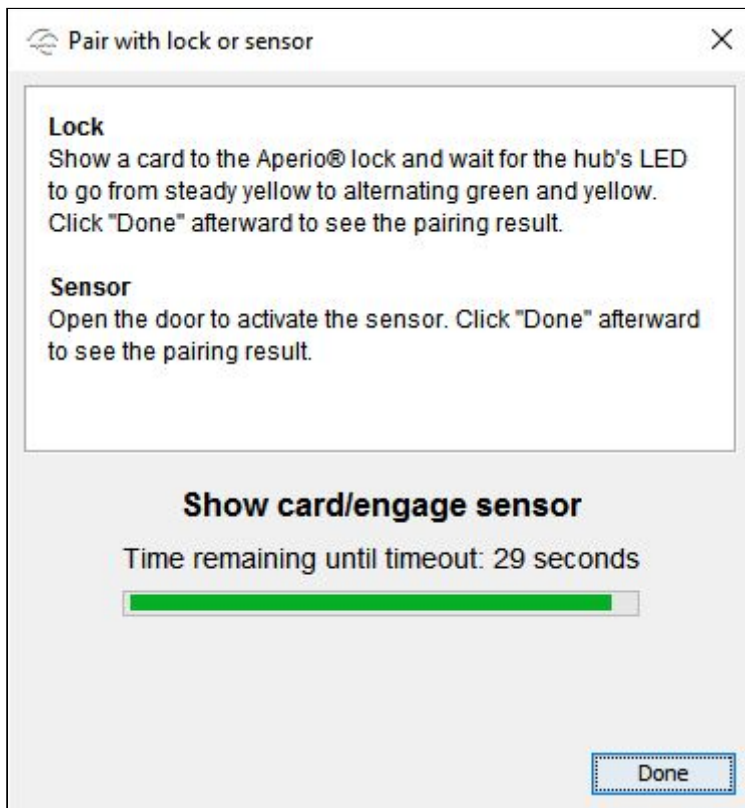
At this step we need to initiate the process of pairing locks to the communication hub that we selected in the previous step.

4.1 Right click the communications hub, select Communication Hub followed by Pair with a lock or sensor.



*Aperi@ Programming Application - Main installation window with selected communications hub*

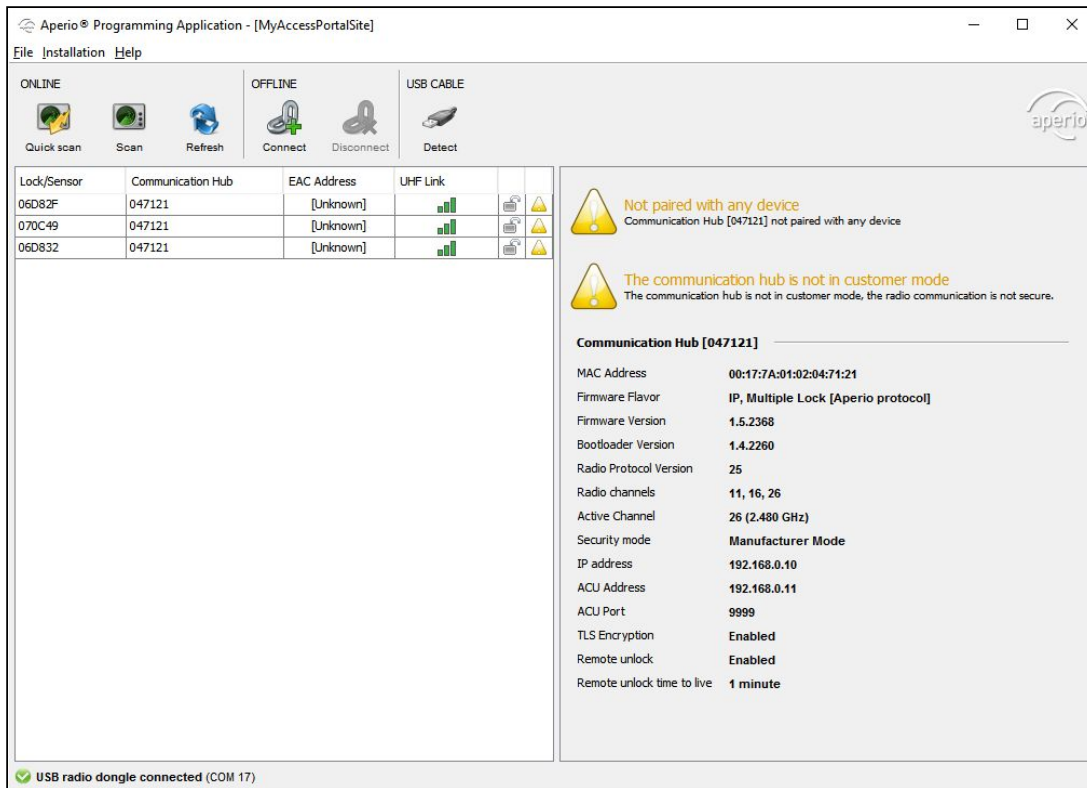
4.2 You should see the below dialog. You now have 30 seconds to present a tag to locks that you want paired to the communication hub. If you don't have enough time, repeat from step 4.1.



*Aperi@ Programming Application - Pairing in progress.*



4.3 Check that all of the locks that were expected to be paired with the communication hub are displayed in the main window. If not, repeat from step 4.1



Aperio Programming Application - Result of pairing locks to a communication hub.

### Site map

It is a good idea to have a site map handy so that you can check that the required devices have been detected. The site map will also be useful later when you need to configure doors in Access Portal. You can use the site map to check what a door should be named and that the correct entry and exit reader are being configured for a door.

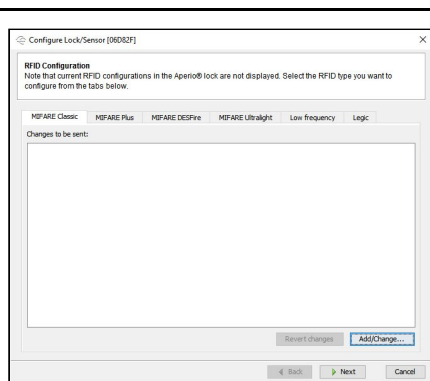
## Step 5: Configure the locks



To configure a lock, right click the lock from the main configuration window, -> select lock sensor -> select configure. This will launch a configuration wizard that will take you through the steps required to configure the locks.

### Current configuration settings are not always displayed

For example, the override credentials section does not show current override credentials. Any changes that you make will be the actual settings used. For example, when loading override credentials, the newly added credentials will replace the old credentials.

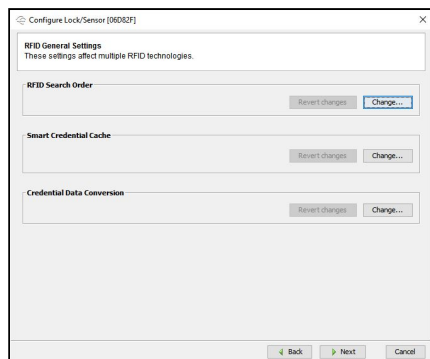


Aperio Programming Application - Lock RFID Configuration

In this section you need to enable the tag / credential technology that the lock will use. Ideally only enable the technology that will be used to save the battery life and improve security.

Access Portal makes use of a tag's UID for authentication so leave tag type configuration on UID.

- MIFARE Classic
- MIFARE Plus
- MIFARE DESFire
- MIFARE Ultralight
- Low Frequency
- Legic



Aperio Programming Application - Lock General RFID Configuration

- Configure RFID Search Order - From here you can specify the order in which the lock should try technologies to read a tag. The most commonly used technology should be at the top of the list to save on battery usage.

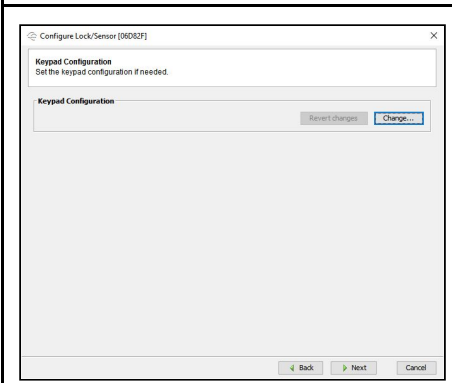


### IMPORTANT NOTE ON SECURITY

- Smart Credential Cache - Although Aperio v3 Locks support an offline cache of up to 200 credentials over the last 30 days, we recommend that the offline cache is only used if you are confident that the network will only drop in emergencies. Otherwise the cache could undermine access decisions made by Access Portal.



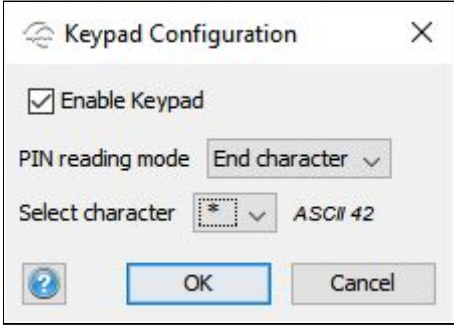
- Credential Data Conversion - Access Portal requires the default setting here “No Conversion”.



Apero Programming Application - Lock Keypad Configuration

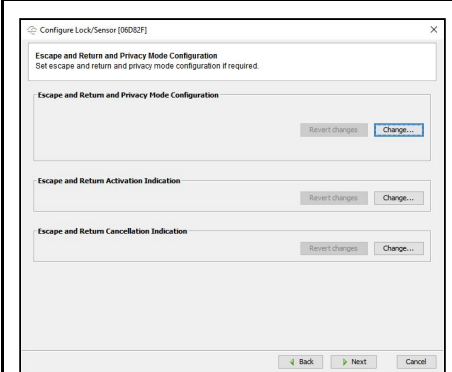
Enable the keypad if the site will need to use any door modes that require a keypad from Access Portal. For example, anything that makes use of Personal Access Code, PIN or Reason Codes.

The PIN reading mode can be set to either a length or to use an End character. For most modes of use in Access Portal we recommend the use of an End Character.



Apero Programming Application - Keypad configuration.

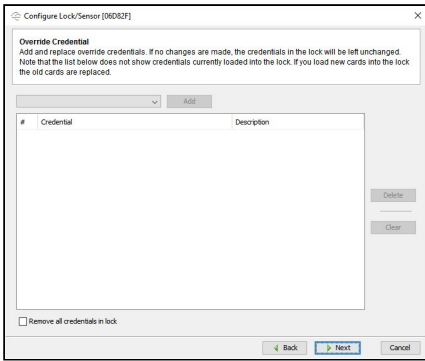
This allows different length values to be entered as well as a combination of values. For example, *Personal Access Code + character + PIN + character + Reason Code*.



Apero Programming Application - Lock Escape and Return and Privacy Mode Configuration

There is nothing in this section that needs to be configured for Access Portal.

- Escape and Return Privacy Mode Configuration.
- Escape and Return Activation Indicator.
- Escape and Return Cancellation Indicator.

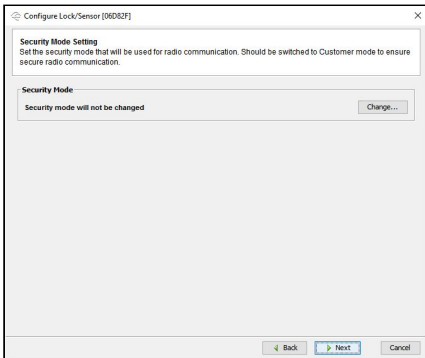


*Aperio Programming Application - Lock Override Credentials*

This section allows the specification of override credentials. Override credentials are useful for accessing a location during an emergency or during maintenance of the network or access control system.

 **IMPORTANT NOTE ON SECURITY**

Always keep override credentials in a safe place.

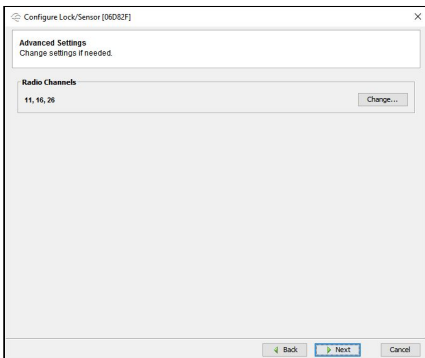


*Aperio Programming Application - Lock Security Mode Settings*

This section should only be configured after the communication hub has been installed into Access Portal.

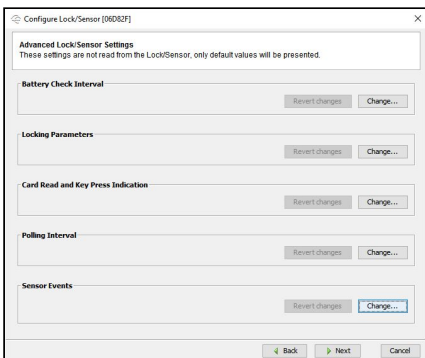
 **IMPORTANT NOTE ON SECURITY**

Once the communication hub has been installed into Access Portal, the communication hub and locks need to be changed to customer mode to secure communications. This is only done once installed into Access Portal because Access Portal specifies the certificate used to secure communications.



*Aperio Programming Application - Lock Advanced Settings*

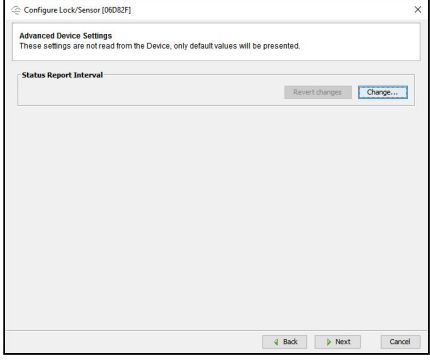
This section is used to configure Radio Channels used by the lock. There is nothing specific that needs to be done here for use with Access Portal.

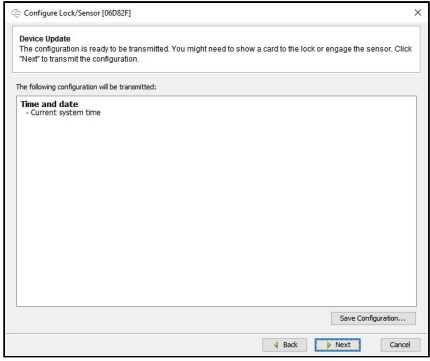


*Aperio Programming Application - Lock Advanced Lock/Sensor Settings.*

- Battery Check Interval - The default value is set to 60 minutes.
- Locking Parameters
  - Try to unlock timeout
  - Lock open time - If a tagholder presents a tag and Access Portal deems that the tagholder is allowed access, this is the time that the lock will be opened for.
  - Lock jammed alarm timeout
  - Enable lock jammed retry

	<ul style="list-style-type: none"> <li>○ Lock jammed retry period</li> <li>○ Lock jammed indication mode</li> <li>● Card Read and Key Press Indicator - Configure the indication for a tag or key press.</li> <li>● Polling Interval - How often should a v3 lock check with the communication hub for new configuration information.</li> <li>● Sensor Events - Do not enable this value.</li> </ul>
--	---

 <p><i>Aperio Programming Application - Lock Advanced Device Settings</i></p>	<p>Used to set the status report interval. (Or how often the lock reports its status to the communications hub and checks for new messages from Access Portal)</p> <p>For newer v3 locks you can usually leave the default time to 60 minutes. The v3 locks support a low powered message (Polling interval configured on the previous tab) to check if there are new messages from Access Portal.</p> <p>For v2 locks, remote open functionality will be delayed by up to the interval configured here.</p> <p>If more than one lock is connected to the communications hub, you need to make this change from the hub configuration wizard instead.</p>
---	---

 <p><i>Aperio Programming Application - Lock Device Update</i></p>	<p>From here, you get a summary of the changes that were made so that you can review the changes before sending the configuration to the lock.</p>
---	--

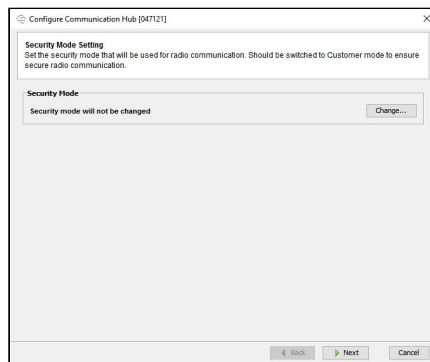
## Step 6: Configure the communications hub



To configure a communication hub, right click the communication hub / lock from the main configuration window -> select communication hub -> select configure. This will launch a configuration wizard that will take you through the steps required to configure the communication hub.

### Current configuration settings are not always displayed

For example, when configuring the status report interval, the current value is not read from the device, instead the default value is displayed.



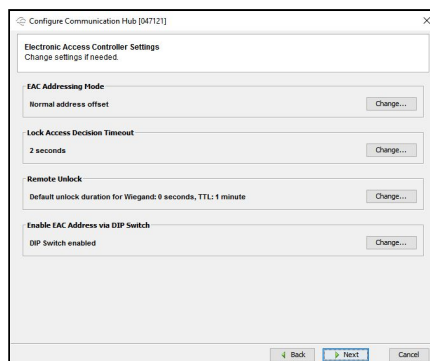
Aperio Programming Application -  
Communication hub security mode settings.

This section should only be configured after the communication hub has been installed into Access Portal.



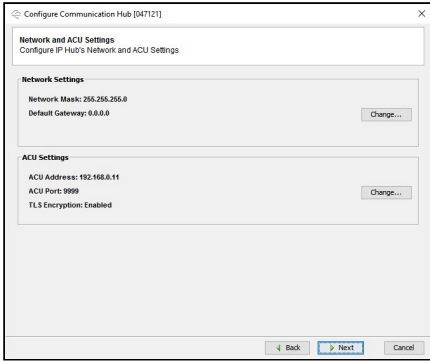
### IMPORTANT NOTE ON SECURITY

Once the communication hub has been installed into Access Portal, the communication hub and locks need to be changed to customer mode to secure communications. This is only done once installed into Access Portal because Access Portal specifies the certificate used to secure communications.



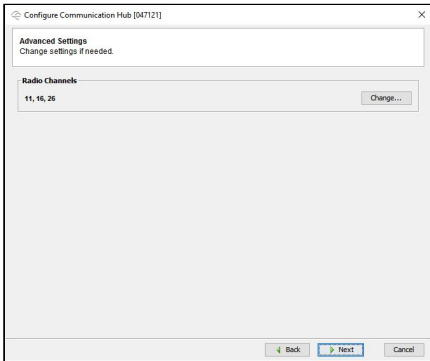
Aperio Programming Application -  
Communication hub Electronic Access Controller  
Settings

- EAC Addressing Mode - Do not change anything.
- Lock Access Decision Timeout - This is the time that Access Portal has to respond with an Access decision. On most networks, the default of 2 will work.
- Remote Unlock - Change Time To Live to 1 minute.
- Enable EAC Address via DIP Switch - Do not change anything.



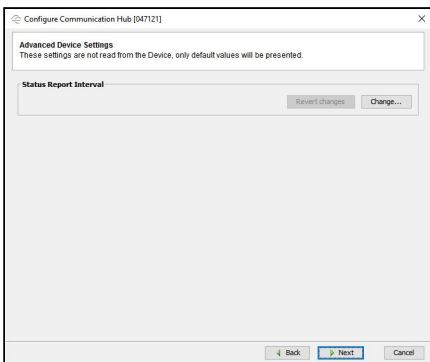
Aperio Programming Application -  
Communication hub Network and ACU Settings

- Network Settings - From here you can change the subnet mask and gateway of the communication hub.
  - To change the IP address, from the main configuration window, right click the hub / lock, click communication hub, click change IP Address.
- ACU Settings
  - ACU Address should be the IP Address of the computer that Access Portal is running on.
  - ACU Port is the port that Access Portal listens on for communication hubs to connect on.
  - TLS Encryption should always be enabled as Access Portal will not communicate to a lock unless over a secure TLS connection.



Aperio Programming Application -  
Communication hub Advanced Settings

This section is used to configure Radio Channels used by the communication hub. There is nothing specific that needs to be done here for use with Access Portal.



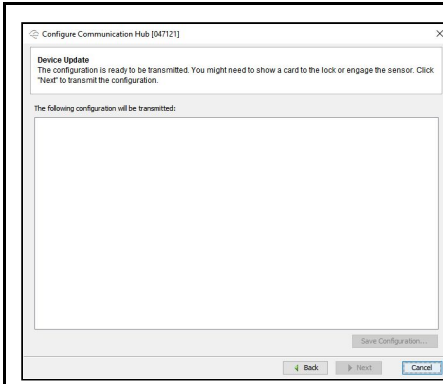
Aperio Programming Application -  
Communication hub Advanced Device Settings

Used to set the status report interval. (Or how often the lock reports its status to the communications hub and checks for new messages from Access Portal)

For newer v3 locks you can usually leave the default time to 60 minutes. The v3 locks support a low powered message (Polling interval configured on the previous tab) to check if there are new messages from Access Portal.

For v2 locks, remote open functionality will be delayed by up to the interval configured here.

If more than one lock is connected to the communications hub, you need to make this change from the hub configuration wizard instead.



*Aperio Programming Application -  
Communication hub Device Update*

From here, you get a summary of the changes that were made so that you can review the changes before sending the configuration to the communication hub.



## 4. Access Portal Configuration

Access Portal configuration consists of :

1. Configuring Aperio Communications.
2. Installing Aperio Locks into Access Portal.
3. Configuring doors
4. Configuring Access Portal features for use with Aperio Locks

### Prerequisites for configuring Aperio locks in Access Portal

1. Communication Hubs and Locks need to be physically installed and configured.
2. You need a certificate to use for encrypting communications between Access Portal and communication hubs.

### **Step 1: Configure Aperio Communications**

For Access Portal (AP) to support Aperio Locks, AP needs to be able to talk to the communication hubs that Aperio Locks are paired with. These communication settings can be found under AADP (Assa Abloy Device Protocol) Settings on the Miscellaneous Settings tab of the AP server.

The screenshot shows the 'Miscellaneous Settings' tab in the 'Portal Server' application. The interface includes a navigation bar with tabs for 'Console', 'Network Discovery', 'Biometric Configuration', 'Biometric Install', and 'Miscellaneous Settings'. The 'Language' section has a dropdown menu set to 'English' and a 'Save Settings' button. The 'AADP Settings' section includes a checkbox for 'Enable Assa Abloy Device Support', a text field for 'AADP Certificate Path' with a 'Browse' button, a text field for 'AADP Certificate Password', and a text field for 'AADP Listening Port' set to '9999'. An 'Actions' panel on the right contains buttons for 'Export', 'Import', 'Import Unlock File', and 'Export Unlock File'. The footer shows 'Open Client Connection : http://DUR1WKS014:82' and a 'Database' indicator.

Access Portal Server Application - Miscellaneous Settings.

## AADP Setting Fields

- Enabled - The enabled check box needs to be checked before any of the other fields will enable.
- Use the browse button to locate the certificate used to encrypt communications between the Aperio Communications Hub and AP. (The certificate is allowed to be self signed. Once the communication hub is switched to customer mode, it will only communicate using this certificate)
- The certificate password is the password used while generating the certificate.
- The listening port is the port number that AP listens on for connections from communication hubs. The default value is 9999. This value should match the ACU Port configured on the communication hub.

Fill in the required fields and then save. Already configured communication hubs will report themselves and the locks connected to them automatically and will show in the install view ready to be installed into Access Portal.

### Step 2: Installing Aperio Locks into Access Portal

Aperio hubs that have been configured will show up in the install view of Access Portal. (Login to Access Portal -> Select Site Menu -> Select Install Sub Menu)

To install a communication hub:

1. Select the hub from the selection list.
2. Click the install button.

A hub can be installed multiple times for the case where additional locks have been paired since the initial install.

The screenshot shows the 'Install' sub-menu in the Access Portal Web Client. The interface is divided into several sections:

- Header:** MENU, DEFAULT SITE, SYSDBA
- Notification:** Showing 3 new Network devices.
- Controllers:** Search bar, displaying 1 to 1 of 1.
- Communication Hub:** \* Communication Hub, VCO47121, 192.168.0.10
- Install Button:** A large blue 'Install' button.
- Gateway:** Site: Default Site, ID No: 00177A01020471210000..., IP: 192.168.0.10
- 3 New Devices:** A table with columns: Device, Group Id, Type, Status.

Device	Group Id	Type	Status
00177A010206D83200000000	00177A010206D83200000000	Lock	
00177A0102070C4900000000	00177A0102070C4900000000	Lock	
00177A010206D82F00000000	00177A010206D82F00000000	Lock	
- 0 Installed Devices:** A table with columns: Device, Type, Fixed Address, Channel, Version, LA, Enabled, Status.

Device	Type	Fixed Address	Channel	Version	LA	Enabled	Status
No devices have been installed yet							

Access Portal Web Client - Site -> Install

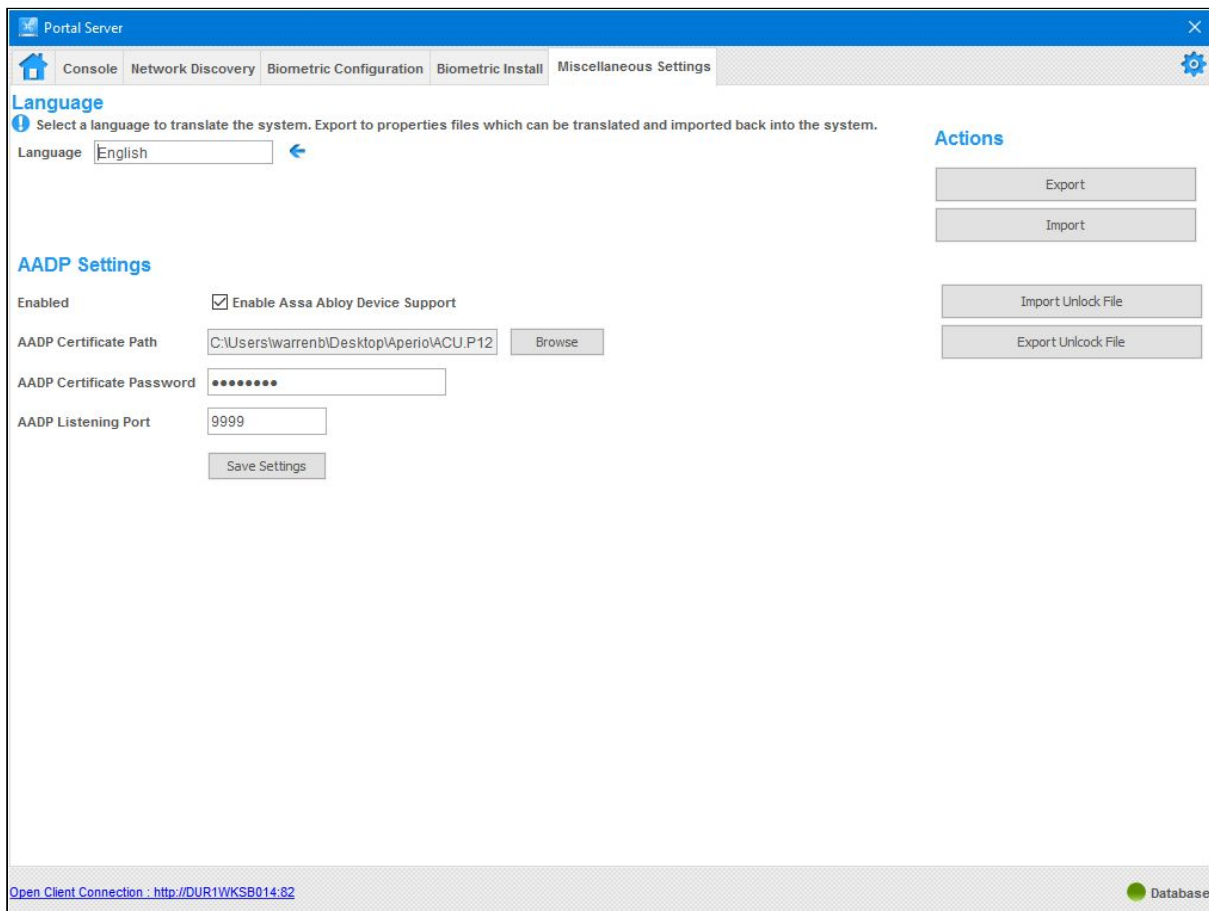
### Tips on using the Install View.

- Installed Aperio Communication hubs are displayed in a searchable list. Search for a hub using its IP Address or Fixed Address. (The fixed address is the hubs 6 character group ID prefixed with VC, e.g. VC047121. VC because the communications hub acts as a virtual controller in Access Portal.
- Communication Hubs that have already been installed will display at the bottom of the list.
- Communication hubs that have not yet been installed will appear at the top of the list and have an \* next to the name.
- Once a hub has been selected, the locks paired with the hub will be shown.
- For site maintenance where you need to uninstall communication hubs , replace a faulty locks etc. you would need to make use of the installation view as well.

### **Step 3: Licensing Aperio Locks for use in Access Portal**

Aperio locks need to be licensed before they will work with Access Portal. If you already have a license file for you locks, click the “Import Unlock File” button from AADP (Assa Abloy Device Protocol) Settings on the Miscellaneous Settings tab of the AP server.

If you need a license file, click the “Export Unlock File” button. This file contains serial number that your supplier will need to generate the license file.



#### **Step 4: Configuring doors**

After an Aperio Communication hub has been installed, the locks paired at the time of installation will be available to be assigned as readers for a door. Doors are the basic unit to which access can be granted in Access Portal. *(The door configuration view can be found from the main menu by selecting the site menu -> selecting the door sub menu)*

##### **Site map**

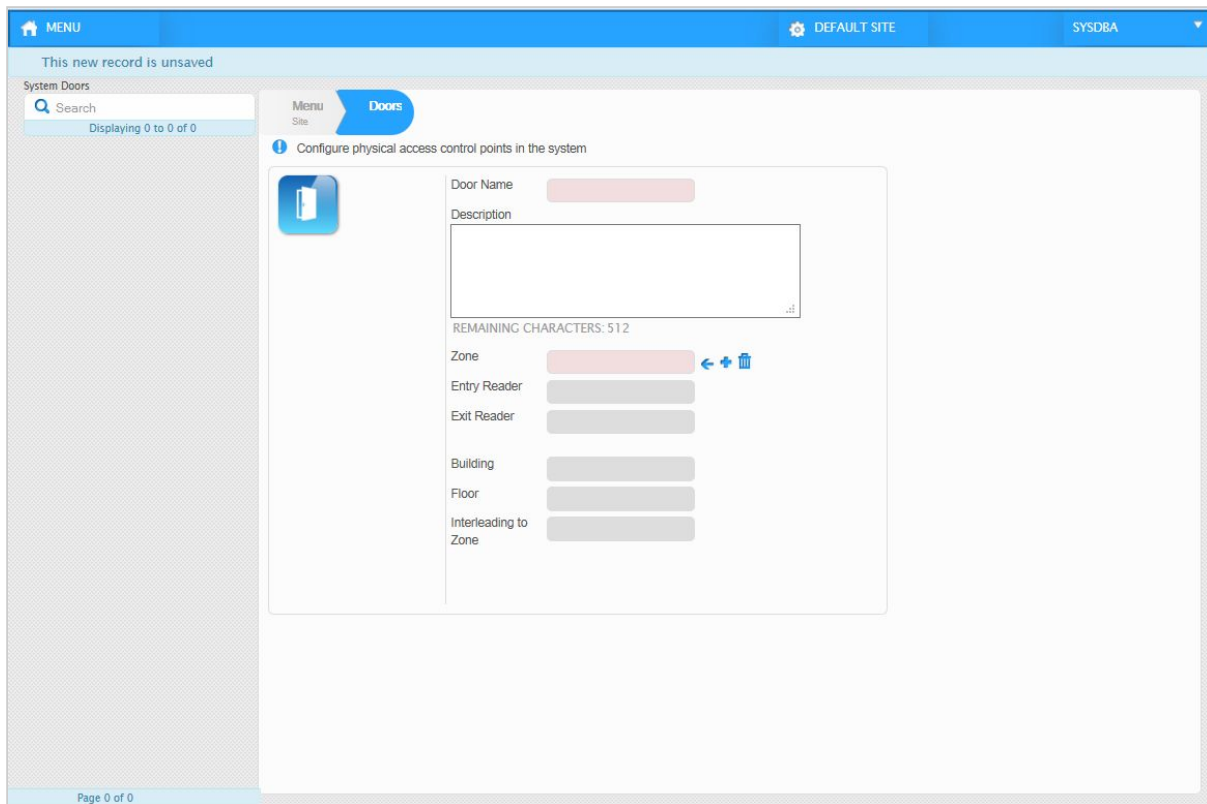
It is a good idea to have a site map handy so that you can check that the required devices have been detected. You can use the site map to check what a door should be named and that the correct entry and exit reader are being configured for a door.

##### **Door Fields**

- Door Name - The name of the door will show when creating areas to give tagholders access to, Live! Transaction viewer and reports.
- The description is used to keep some useful information about the door. When was it last serviced etc.
- Select a zone that the door will belong to. Reader selection will not enable until you have done so.
- Entry reader is the Aperio Lock that is considered the unsecure side of the door or the outside reader.
- Exit reader is the Aperio Lock that is considered the secure side of the door or the inside reader.
- Building - A door can be said to be part of a building. This is useful for reporting.
- Floor - A door can be said to be part of a floor. This is useful for reporting.
- Interleaving Zone indicates that this door leads between two zones. The zone that the door is in and the zone that is selected.

##### **Tips on using the Door View.**

- If no doors have been created, the view defaults to the new door state.
- If a door already exists, you need to click the new button at the top of the view.
- Selections such as zone, Aperio Lock, etc. are made from an indexed searchable selection list. You can search for locks using their Group ID that you should find on your site map.



Access Portal Web Client - Site -> Doors

### To create a door

1. Click the NEW button if the view is not already in the new state.
2. Enter a door name.
3. Enter a description (Optional)
4. Select a zone. (By default, there will be a zone per communications hub that has been installed. The zone that is selected will filter the reader selection options)
5. Select an entry and / or exit reader for the door. (This is where you select the Aperio Locks that you have installed.)
6. Select a building (Optional, no default building exists)
7. Select a floor (Optional, no default floors exist)
8. Select a zone that a door interleads to. (Optional)

# Troubleshooting & FAQ's

## **Does Access Portal support Aperio in offline mode?**

- Not at the moment. Access Portal needs to be online for advanced access control functions such as APB, Door Modes, etc.

## **My Aperio Hub connects to my Access Portal system every minute. Why doesn't it stay connected?**

- It's possible that the access portal software and the aperio hub are using different certificates. Take the aperio hub out of customer mode and wait for it to connect to the access portal system. If the hub stays connected, switch it back the customer mode.

# Appendix A - Access Portal Features

Appendix A defines how Access Portal feature are supported with Aperio Locks

- Access
  - Live! Transactions
  - Linking Management
  - Linking History
  - Tagholders (Including provided variations & custom variation)
  - Batch Operations
  - Access Groups
  - Operator Login
  - Operator Profile
  - Filter Profile
  - Holidays
  - Companies
  - Departments
  - Areas
  - Access Time Pattern
  - Move
  - Bulk Access Group Assignment
- Scheduled Tours
  - Active Tours
  - Tagholders
  - Routes
- Threat Level
  - Live!
  - Behaviour **Partial** - Behaviour is changed, e.g. Tag Mode, Tag with PIN, but there is no support for driving relays.
  - Threat Level History
  - Notifications
- Site
  - Install
  - Zones **Partial** - No Common Zones, Interleading Zones, Zone Counting, etc.
  - Doors
  - Readers **Partial** - Reader terminals are virtual.
  - Controller **Partial** - Controllers are virtual.
  - Building
  - Lift / Elevators
  - Reader Profile **Partial** - there is only support for behaviour.
  - Controller Profile **N/A**
  - Device Time Pattern
  - Time Triggered Action **N/A**
  - Messages **N/A**
  - Common Zone **N/A - TBD**
  - Reason Codes
- System

- Sites
  - Site Codes N/A
- Network Settings N/A
- Network Status N/A - TBD
- Person / Asset Profile
- Services N/A
- User Fields
- Truncation Rules Partial. Behaviour is untested for iClass tags.
- Custom Menus
- Notification Account Settings
- Directory Configuration
- Custom Report Management
- Reports
  - Person / Asset Report
  - Transaction Report
  - Zone Occupancy Report Partial - No Common Zones, Interleading Zones, Zone Counting, etc.
  - Time Base Reports Partial - No Common Zones, Interleading Zones, Zone Counting, etc.
  - Absenteeism
  - Visitor
  - Door Access Report
  - Audit Report
  - Holiday Report
  - Access Group Report
  - Custom Reports
- About
- Downloads
  - Linphone Installer
  - Card Printing
  - MDE Installer Partial - Access Portal uses a UID for authentication, some HID tags such as iClass used with Aperio locks authenticate using an Access ID. The MDE does not read an Access ID so enrollment needs to be done using an Omni Key
  - Omnikey Partial - Can enroll tags.
  - BMTA Installer N/A
  - Morpho Installer N/A
  - Suprema Installer N/A



## Appendix B - Door Mode Support

Appendix B defines how Access Portal Door Mode Patterns are supported with Aperio Locks.

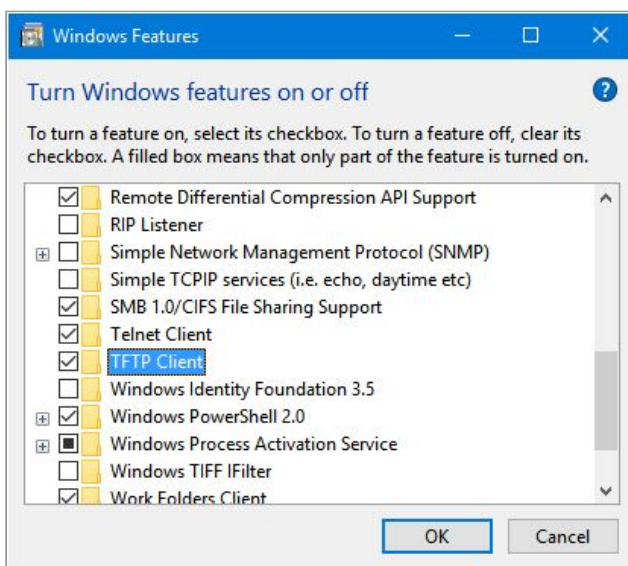
Door Mode Patterns	Supported?	Additional Information
Armed	Supported	Treated as Tag Mode
Emergency	Supported	Treated as Unlocked Mode
Finger	N/A	Denied Biometric Event
Finger with PIN	N/A	Denied Biometric Event
Finger with PIN and Reason Code	N/A	Denied Biometric Event
Finger with Reason Code	N/A	Denied Biometric Event
Lockdown	Supported	
Locked	Supported	
Personal Access Code	Supported	
Personal Access Code and Finger	N/A	Denied Biometric Event
Personal Access Code or Finger	Supported	Treated as Personal Access Code
Tag	Supported	
Tag and Finger	N/A	Denied Biometric Event
Tag and Finger with PIN	N/A	Denied Biometric Event
Tag and Finger with PIN and Reason Code	N/A	Denied Biometric Event
Tag and Finger with Reason Code	N/A	Denied Biometric Event
Tag and Finger, or PAC and Finger	N/A	Denied Biometric Event
Tag or Finger	Supported	Treated as Tag Mode
Tag or Finger with PIN	Supported	Treated as Tag with Pin
Tag or Finger with PIN and Reason Code	Supported	Treated as Tag with PIN and Reason Code
Tag or Finger with Reason Code	Supported	Treated as Tag with Reason Code
Tag with PIN	Supported	
Tag with PIN and Reason Code	Supported	
Tag with Reason Code	Supported	
Unlocked	Supported	

# Appendix C - Firmware Upgrade

## Firmware Upgrade IP Communications Hub

The transfer of the firmware file is not done using the ASSA ABLOY Device Protocol. Instead Trivial File Transfer Protocol (TFTP<sup>1</sup>) is used. This means that the hub has a built-in TFTP server, and that any TFTP client can be used to download the firmware file to the hub. There is no specific command to order a FW upgrade. Instead the downloading of a valid FW file will trigger the FW upgrade procedure in the hub, using that file.

Windows has a built in TFTP client that is disabled by default. It can be enabled from the Windows features list.



*Use a stand alone TFTP client or enable the built in TFTP client from windows.*

## Security

In order to prevent malicious firmware to be installed in the hub, the following protection is provided.

### Authorized file download

The hub will **only allow TFTP communication for a limited time after an authorized restart of the hub has been requested**. An authorized restart can be made either

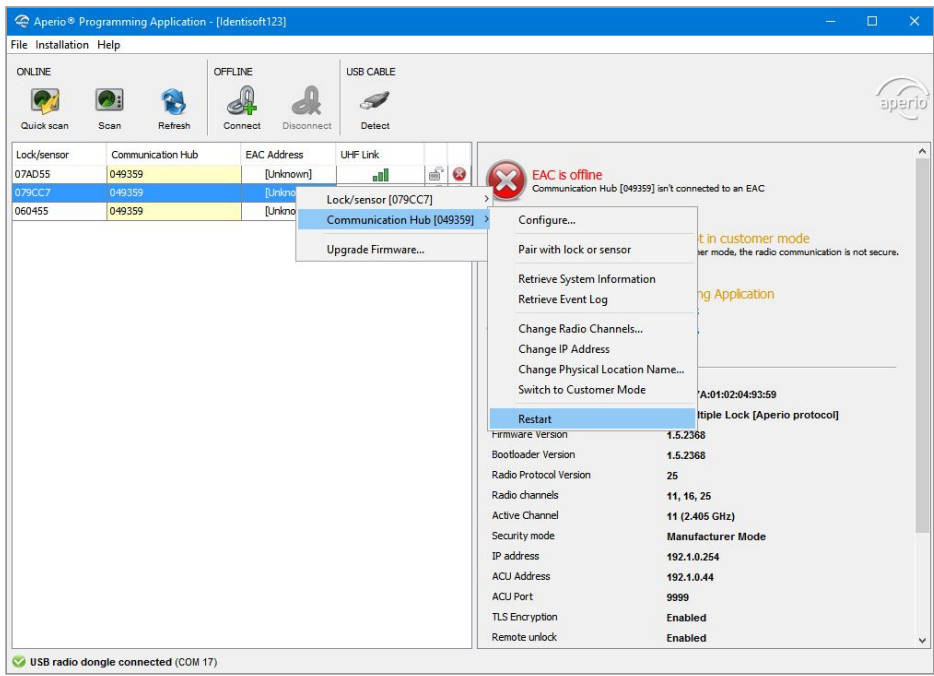
on a secure ASSA ABLOY Device Protocol connection, or

on a secure connection with the Aperio Programming Application.

In both cases the communication for the restart command is protected by a customer specific key.

---

<sup>1</sup> "Trivial File Transfer Protocol - Wikipedia." [https://en.wikipedia.org/wiki/Trivial\\_File\\_Transfer\\_Protocol](https://en.wikipedia.org/wiki/Trivial_File_Transfer_Protocol). Accessed 13 Jan. 2017.



To perform an authorised restart of the hub for firmware upgrade, right click a lock -> select communication hub -> select restart.

**Firmware file encryption**

The firmware files delivered by ASSA ABLOY are encrypted in order to protect the firmware code.

**Firmware file authentication**

The firmware files contain a digital signature that is used to authenticate that the firmware was issued by ASSA ABLOY. If a file is downloaded that cannot be authenticated, it will be discarded by the hub.

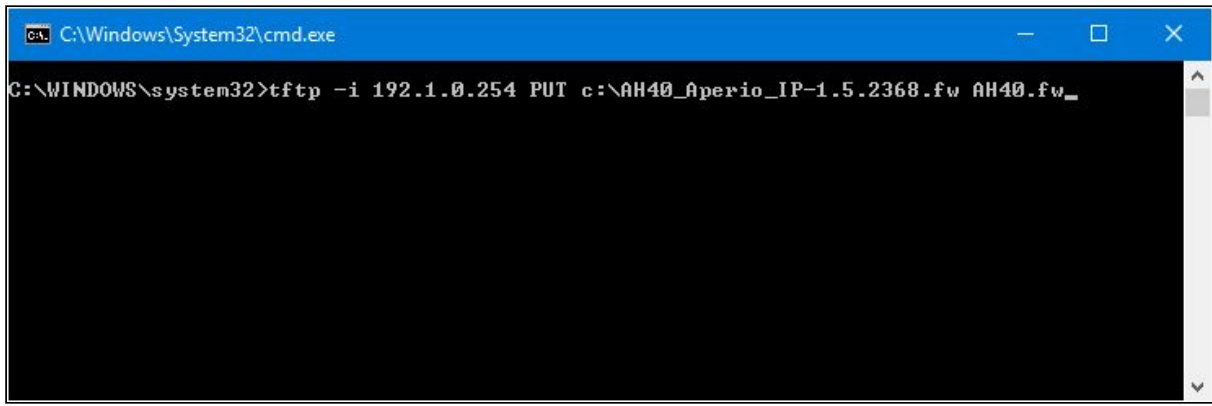
Hub IP address

FW file from ASSA ABLOY

File name to use in the Hub

```
> tftp -i 192.168.0.2 put AH40_Aperio_IP-1.2.3456.fw AH40.fw
```

Syntax for using windows TFTP client to transfer firmware file.



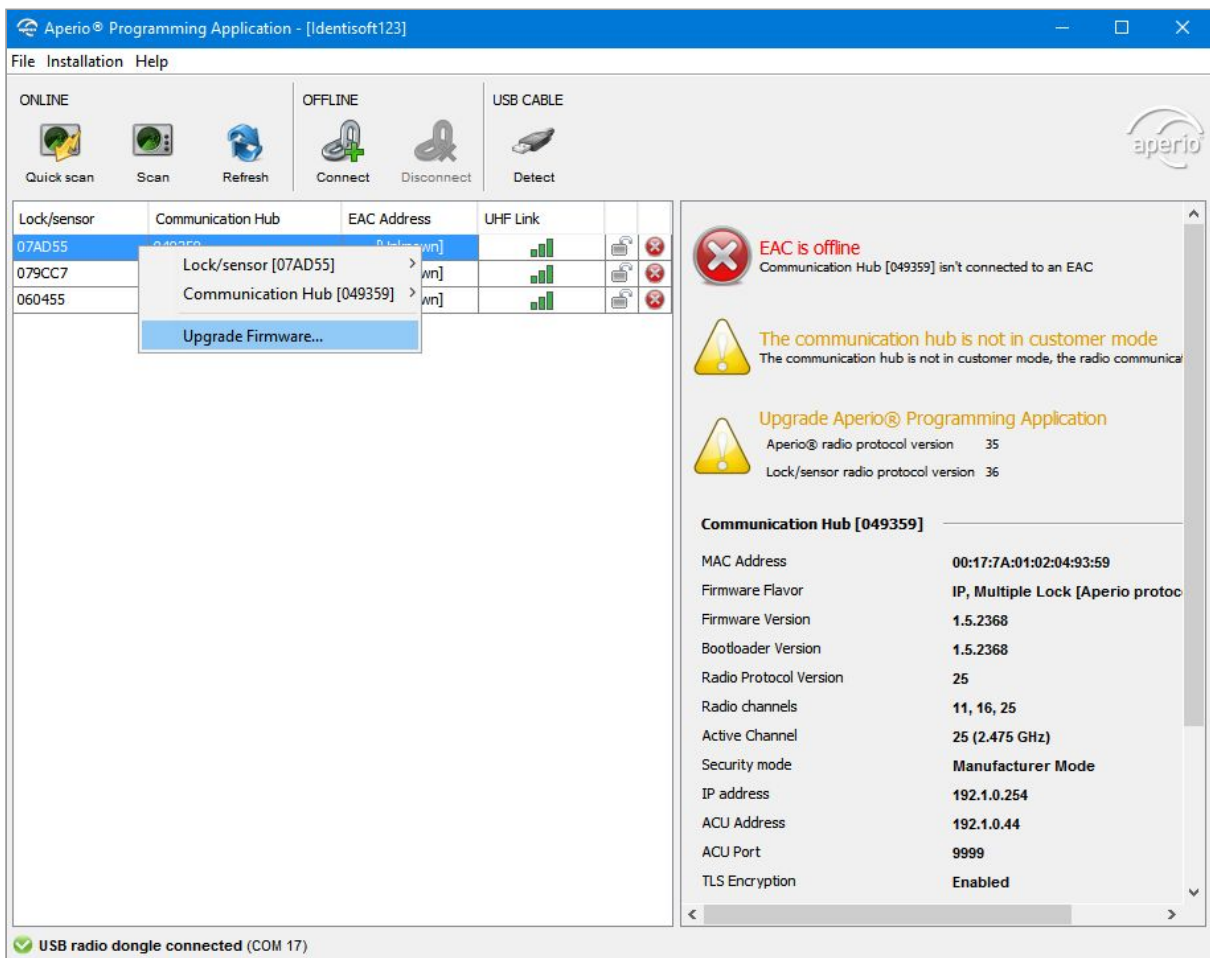
Example of how to use windows TFTP client to transfer firmware file.

Once the file has been transferred, the file will be validated. If the file is valid, the upgrade procedure will start automatically. The firmware upgrade including the file transfer will take approximately 2 minutes, then the hub will restart running the new firmware

## Firmware Upgrade Lock

Upgrading a lock is simpler than upgrading a lock and can be done entirely using the Aperio Programming Application and a person with a tag.

Select the lock to upgrade, select the file to use and enter the file password and follow the prompts. One of the prompts will be to present a tag to the lock being upgraded to confirm that the correct lock was selected.



Firmware Upgrade a Lock. Right click a lock - select Upgrade Firmware. Follow the prompts.