Recommendations for a Secure Installation

Copyright © 2017 IDEMIA

Osny, France

Warning

Copyright © 2017 IDEMIA. All rights reserved.

Information in this document is subject to change without notice and do not represent a commitment on the part of IDEMIA.

This document contains information of a proprietary nature to IDEMIA and is submitted in confidence for a specific purpose. The recipient assumes custody and control and agrees that this document will not be copied or reproduced in whole or in part, nor its contents revealed in any manner or to any person except to meet the purpose for which it was delivered.

This caveat is applicable to all the pages of this document.

This manual makes reference to names and products that are trademarks of their respective owners. MorphoAccess® is registered trademark of IDEMIA.

Made in France

Revision History

The table below contains the history of changes made to the present document.

Version	Date	Description
01	December 2013	Creation of document. [SSE-0000100948-01] US English version of SSE-0000083767-02 document
	October 2015	New reference (2015_2000012312_v1) Add MorphoAccess® SIGMA Lite Series Remove MorphoAccess® 100 Series
02	May 2016	Note about DROWN attack (2015_2000012312_v2) page 33
03	March 2017	Additional information about SSL / TLS implementation
	April 2017	Add MorphoAccess® SIGMA Extreme Series Remove MorphoAccess® J Series Remove MorphoAccess® 500 Series
04	July 2017	Remove From Chapter 7: - MorphoAccess® J Series - MorphoAccess® 500 Series
05	December 2017	Correction on the openssl commands
06	December 2017	Update company name (IDEMIA)
07	August 2018	Modification on the openssl commands: • replace RSA:1024 by RSA:2048 • replace SHA1 by SHA512
08	April 2019	Add recommendation to close the retrofit port
09	May 2019	Update MorphoAccess® VP Series
10	May 2020	Add MorphoWave Compact Add VisionPass

Table of Content

List of Figures

Section 1 : Introduction

Scope of the document

This guide deals with the use of Access and Time Biometric terminals listed below:

- MorphoAccess® SIGMA Series
- MorphoAccess® SIGMA Lite Series
- MorphoAccess® SIGMA Extreme Series
- MorphoAccess® VP Series
- MorphoWave Compact Series
- VisionPass Series

The MorphoAccess® SIGMA Series is made up of the following list of products:

MorphoAccess® SIGMA Series	Fingerprint biometrics	Contactless smartcard reader			Outdoor use
		iCLASS®	MIFARE® DESFire® NFC®	Prox®	
MA SIGMA	✓				✓
MA SIGMA iCLASS	✓	✓			✓
MA SIGMA Multi	✓		✓		✓
MA SIGMA Prox	✓			✓	✓

The MorphoAccess® SIGMA Lite Series is made up of the following list of products:

MorphoAccess® SIGMA Lite Series	Fingerprint biometrics	Contactless smartcard reader			Touch screen	Water Resistant
		iCLASS®	MIFARE® DESFire® NFC	Prox®		
MA SIGMA Lite WR	✓					✓
MA SIGMA Lite iClass WR	✓	✓				✓
MA SIGMA Lite Multi WR	✓		✓			✓
MA SIGMA Lite Prox WR	✓			✓		✓
MA SIGMA Lite+ WR	✓				✓	✓
MA SIGMA Lite+ iClass WR	✓	✓			✓	✓
MA SIGMA Lite+ Multi WR	✓		✓		✓	✓
MA SIGMA Lite+ Prox WR	✓			✓	✓	✓

The MorphoAccess® SIGMA Extreme Series is made up of following list of products:

MorphoAccess® SIGMA Extreme Series Marketing Name	Biometrics	Fake Finger Detection	Contactless smartcard reader			Water Resistant
			iCLASS®	MIFARE® DESFire® NFC	Prox®	
MA SIGMA Extreme iClass	✓		✓			✓
MA SIGMA Extreme Multi	✓			✓		✓
MA SIGMA Extreme Prox	✓				✓	✓
MA SIGMA Extreme FFD iClass	✓	✓	✓			✓
MA SIGMA Extreme FFD Multi	✓	✓		✓		✓
MA SIGMA Extreme FFD Prox	✓	✓			✓	✓

The MorphoAccess® VP Series is made up of the following list of products:

MorphoAccess® VP Series Marketing Name	Multimodal biometrics	Contactless smartcard reader		Outdoor use
		MIFARE®	DESFire®	
MorphoAccess® VP-MD	√	√	√	√

Multimodal biometrics = fingerprint biometrics and finger vein biometrics

The MorphoWave Compact Series is made up of following list of products:

MorphoWave Compact Marketing Name	Biometrics	Fake Finger Detection	Contactless smartcard reader			Water Resistant
			iCLASS®	MIFARE® DESFire® NFC	Prox®	
MorphoWave Compact MD	✓	✓		✓		✓
MorphoWave Compact MDPI	✓	✓	✓	✓	✓	✓

The VisionPass Series is made up of following list of products:

VisionPass Marketing Name	Biometrics	Fake Face Detection	Contactless smartcard reader			Water Resistant
			iCLASS®	MIFARE® DESFire® NFC	Prox®	
VisionPass MD	✓	✓		✓		✓
VisionPass MDPI	✓	✓	✓	✓	✓	✓

Introduction

The present document gathers all recommendations which help to improve the secure level of an access control system using terminals.

For details about installation, please refer to the installation manual specific to the model of each Access and Time Biometric terminal.

Restricted area

In this document, the « restricted area » is the physical location in which access is limited by a system that checks the access rights of the user.

The « free zone » is a physical location where access is free to everybody, without any access rights check.

Usually, an Access and Time Biometric terminal is installed in a « free zone » to control the access to a “restricted area”.

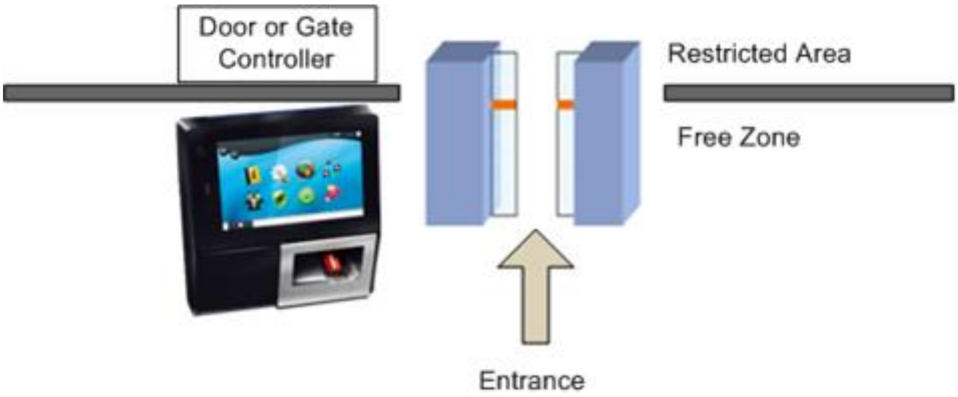


Figure 1 : Restricted area and free zone

General cautions

Cleaning recommendations

The use of a dry cloth is recommended to clean the terminal, especially the biometric sensor. Acid liquids, alcohol or abrasive materials are prohibited.

A noticeable increase of false rejections could occur as a result of inappropriate cleaning method. A false rejection is when access is denied to an authorized user due to biometric check failure.

Warning

The manufacturer cannot be held responsible in case of non-compliance with the following recommendations or incorrect use of the Access and Time Biometric terminal.

Section 2 : Access and Time Biometric Terminal Implementation

Implementation steps

Introduction

The implementation of an Access and Time Biometric terminal is performed by several successive stages:

- Define the functions to be implemented: to prepare the configuration
- Choose the place of the terminal, and verify that it is possible to respect the environment requirements
- Configure the terminal
- Install the terminal

Select the functions of the terminal

This phase consists in determining what the roles of the terminal, in order to identify:

- the functions to be activated and those to be deactivated,
- the connections to be realized, and communication protocols to be implemented,
- the modifications (configuration or development) to make in the systems and the devices which are going to interconnect with the Access and Time Biometric terminal (enrolment station, access central controller, electrical door latch, system of alarm reporting, etc.
- the requested security level for the Restricted area.

Next step consist in choosing the physical emplacement of the terminal.

Terminal location

The place of terminal must be chosen in order to:

- complies with environmental requirements
- restrict the access to the critical functions of the Access and Time Biometric terminal to allowed users only : the cables, connector blocs and configuration workstations must be located in the Restricted area,
- avoid the exposition of the biometric sensor to a of strong intensity light (such as direct sunlight) or fluctuating (such a blinking neon),
- avoid the exposition of the terminal, and especially biometric sensor to an extensive UV radiation.

These requirements are detailed in the « Access and Time Biometric Terminal Installation Conditions» section.

Terminal configuration

It is strongly recommended to configure the Access and Time Biometric terminal before, or at least immediately after the physical installation.

If it is not possible, do not power up the terminal to avoid:

- to let an unauthorized person configure the terminal at his convenience
- to grant the access to the restricted zone, using default access rights check

The configuration must be performed so as to leave active only the required functions, and to reach the required security level

This is detailed in Access and Time Biometric Terminal Configuration section

Terminal Installation

The physical installation has to respect at best the recommendations summarized in the section " Access and Time Biometric Terminal Installation Conditions", and detailed in the installation guide specific to the model of Access and Time Biometric terminal (please refer to “Access and Time Biometric documents ” section).

Warning: it is recommended that the configuration of the terminal must be made before its physical installation, or at the latest immediately after.

Section 3 : Access and Time Biometric Terminal Installation Conditions

Climatic conditions

To avoid any malfunction of the terminal, it is imperative to respect conditions of use.

The manufacturer cannot be held responsible in case of non-compliance with the following recommendations or incorrect use of the terminal.

Temperature and humidity

Do not expose your biometrics terminal to extreme climatic environment. Please respect the limits of the specification given for each terminal.

Ingress Protection Rating (IP)

Do not use the Access and Time Biometric terminal in a very wet area (swimming pool, sauna, seaside, etc.).

If necessary, apply the recommended waterproofing methods.

Access and Time Biometric Terminal	Ingress Protection rating (IP code)	
VP Series	IP65	Outdoor use (when installed on a wall with a watertightness joint) If walls have a rough or uneven surface, a silicon bead may be required between the wall plate and the wall to ensure sealing.
SIGMA Series		
SIGMA Lite Series		Outdoor use (once back door fixed with the 4 screws)
SIGMA Extreme Series		Ruggedized design for harsh environment (IK09)
MorphoWave Compact	IP65	
VisionPass	IP65	

The Access and Time Biometric terminals are designed for environments exposed to the rain and the dust, but it is imperative to insure a good tightness of the part of the terminal in direct contact with its support.

Light environment

The Access and Time Biometric terminal should be installed in controlled lighting conditions.

- Avoid exposure of biometric sensor to a blinking light (such as faulty neon, or the sun through a swinging tree branch)
- Avoid direct exposure of biometric sensor to direct sunlight or to a high power light source
- Avoid exposure of biometric sensor to a powerful UV light

Biometric performances of the terminal can decrease, as a result from bad conditions of lighting.

VisionPass is designed to operate in most environmental conditions. Anyway, to optimize VisionPass performance, it is better to follow the rules below:

- Avoid sunlight coming directly on the device (for instance, avoid installing the device facing a window).
- Avoid direct sunlight on the user's face.
- Avoid strong left/right or top/bottom contrast, and shadows on the user's face due to lighting configuration.
- Prefer a neutral color background in the field-of-view of the product
- Avoid any bright spot light very close to the device (closer than 1 meter)
- Protect the front glass from raindrops as it might affect the sensors

Areas containing combustibles

It is highly recommended not to install the Access and Time Biometric terminal in the vicinity of gas stations or any other installation containing flammable or combustible gases or materials.

Electrostatic Discharge (ESD)

Due to electrostatic discharge, and depending on the environment, synthetic carpeting should be avoided in areas where the Access and Time Biometric terminal has been installed.

Terminal (physical) Installation

Type of fixing and type of support

The access to connectors of the terminal by an unauthorized person is facilitated by a poor quality fixation.

The good behavior of the fixation is directly linked to the solidity of the support (usually a wall, but it could be a totem) to which the terminal is fixed. If the wall is in plaster, it is strongly recommended to reinforce it, but don’t use a metal plate which could reduce the read distance of the contactless card reader of the terminal.

It must be impossible to separate the terminal from its support (for example to access to the cables) in another way than the normal way.

In any case, it is strongly recommended to manage the anti-pulling detection by enabling a relevant action (such as send an alarm to security/maintenance team).

Electrostatic Discharges

Before proceeding, make sure that the person in charge of installation and connections is properly connected to earth, in order to prevent Electrostatic Discharges (ESD) an electromagnetic induction.

For the same reason, the first step of the electric connection of the terminal must be to connect the terminal to the earth.

Protection of cables and connectors

Access to cables and connectors

It must be impossible, for an unauthorized person, to access to the cables used for power supply and communication with configuration station and central access controller

- All the cables (power supply and communication) should come from the restricted area, should be accessible since the restricted area only. For example: the cables cross the wall between the restricted area and the free zone to reach the rear of the terminal.
- When the terminal is fixed to its support, it should be impossible to access to the cables from free zone. The access to the cables can be made only after the dismantling of the terminal (from its support).
- The removing of the terminal from its support must be monitored, and registered by a monitoring system.

Terminal fixed to a wall

When the terminal is fixed to a wall, the access to the command and power cables must not be easy:

- The power and command cables should not be fixed in the same side as the terminal
- otherwise the cables should be protected by an electric duct sealed inside the wall

Terminal fixed on a post

When the terminal is fixed to a post, the access to the command and power cables must not be easy:

- the cables should be inside the post
- if an access trapdoor is required, add a lock on it

Access and Time Biometric terminal power supply

Standalone power supply (with battery)

When the Access and Time Biometric terminal gives access to a restricted area which must be able to be accessed in case of general power down, it must be powered by a secured power source (for example with a battery).

A secure power supply avoids the loss of current date and time in the terminal. This event can occur when the terminal is not powered during a period which exceeds the period of backup of internal calendar and clock normal function.

Please check the documentation provided with the model of Access and Time Biometric terminal to known the period during which the normal function of the calendar and the internal clock is preserved, when external power supply is down. Whatever is the model this period is at least 24 hours.

Power Supply connection

When it is possible, it is recommended to provide the electric power to the Access and Time Biometric terminal through its Ethernet plug (Power Over Ethernet function). Then the system of supervision can detect the disconnection of the terminal by a cyclical sending of "ping" command (ICMP) through the network.

Whatever is the power supply mode, the wiring which brings the electrical energy to the terminal must be accessible to authorized personnel only.

Power Supply should be in the restricted area

The source of power supply itself should be accessible to authorized personnel only. Then it is recommended to place it in the restricted area.

Section 4 : Access and Time Biometric Terminal Configuration

Access and Time Biometric Terminal configuration

When to perform terminal configuration

It is strongly recommended to configure the Access and Time Biometric terminal before its installation, or at least immediately after its installation.

Access to terminal configuration

Access and Time Biometric terminals equipped with a keyboard and a screen provides local administration features (on the terminal itself). Then it is important to restrict the access to these administrations feature to allowed personnel only. The access to administration features is basically protected by a unique numeric password (the same for all administrators).

When the Access and Time Biometric terminal leaves the factory plant, it is ready to use, but in an open configuration, like a numeric padlock initialized with "12345" default code It is thus essential to configure it for its installation: like for a numeric padlock it is necessary to replace the default code, by a personal code.

If a protection by a numeric password is not enough, it is possible to use a biometric check. This is a recommendation when the terminal is in an area where the confidentiality of the password cannot be insured.

Disable all unwanted functions

All the unused functions must be deactivated, to avoid leaving a security in the global access control system.

It is particularly true for the functions used for the recognition of the identity of the user: only the endorsed method should be active.

It's the same for the functions which drive the internal relay, when it is used to give the access to a restricted zone. The use of the relay internal to allow the physical access is misadvised.

Authentication with contactless smartcard

It is strongly recommended to use DESFire® contactless smartcards instead of MIFARE® type, and to deactivate the support of MIFARE® contactless cards.

Indeed, DESFire® contactless cards provide a higher level of protection of user's information than MIFARE® contactless cards.

As soon as the terminal is configured for DESFire® contactless cards, it is necessary to avoid leaving a security break, by letting the terminal accept MIFARE® contactless cards (except during the phase of migration from MIFARE® cards towards DESFire® cards).

It is particularly important when the authentication keys for MIFARE ® contactless are not personalized (which means that MIFARE® cards encoded with default keys are accepted by the terminal).

It is imperative to customize the contactless authentication keys to avoid granting the access to contactless cards encoded with the default authentication keys. The default key values are widely broadcasted, then easy to find.

Anti-tamper and anti-pulling switches management

To prevent the unauthorized accesses to the terminal components, it is strongly recommended to use the Access and Time Biometric terminal function that detects tamper and pulling events.

In case of tamper or pulling out, the terminal opens a contact (available on the terminal connector) and optionally reports the event by a message to a distant system or by a local alarm.

This function is detailed in « Anti-tamper and anti-pulling switches » section.

Biometric check Security level

When the Access and Time Biometric terminal supports a biometric check security level tuning, it is strongly recommended to adjust this level to the required value before or as soon as the physical installation of the terminal.

Threat level

The Access and Time Biometric terminals support a function allowing to adjust the level of control required according to a of threat level.

The typical use case is to harden the control of access rights according to the increase of the threat level. For example, it is possible to select access rights check as indicated in the table below:

Threat level	Checks to do before granting access
Low	Contactless smart card authentication only
Medium	Same as « low » level + biometric check
High	Same as « medium » level + PIN code check
Very High	Same as « high » + white list check (access is denied if the user is not found in the white list)

When this function is not used it must be deactivated, to avoid a fraudulent modification of the of control level for more tolerant one.

Anti-tamper and anti-pulling switches

Installation on the support

The nature of the support of the terminal should not allow access to the internal components of the terminal (power supply, relay, connectors), without activating of the pulling detector.

For example, a wall in crisp material as the plaster is strongly misadvised because it is possible to dig an access to cables without removing the terminal of the wall.

Switches available for each series of Access and Time Biometric terminal

All terminals have both anti-tamper and anti-pulling function switches.

Tamper detection

All the Access and Time Biometric terminal are equipped with a detector which monitors any attempt to access physically to the terminal connectors, or any means to configure the terminal. Actions to perform in case of tamper (reporting, alarm…) must be defined during the configuration of the terminal: by default, the Access and Time Biometric terminal ignores tamper event.

Access and Time Biometric terminal	Intrusion type
VP Series	Opening of the trapdoor: access to the reset button, and to the USB port (terminal configuration)
SIGMA Series	Opening of the case: access to the terminal block, and to the rear USB port (Wi-Fi™ or 3G adapter). The opening of the lateral trapdoor (access to USB port) is not detected, but this port is deactivated by default.
SIGMA Lite Series	Opening of the case: access to the terminal block, and to the rear USB port (Wi-Fi™ or 3G adapter).
SIGMA Extreme Series	Opening of the case: access to the terminal block, and to the rear USB port (Wi-Fi™ or 3G adapter).
MorphoWave Compact Series	Opening of the case: access to the terminal block, and to the rear USB port (Wi-Fi™ or 4G adapter).
VisionPass Series	Opening of the case: access to the terminal block, and to the rear USB port (Wi-Fi™ or 4G adapter).

Pulling detection

All the Access and Time Biometric terminals are equipped with a detector which monitor permanently that the terminal is still in narrow contact with its support. So, any attempt of access to the rear terminal connectors, or the pulling of the terminal from the wall is immediately detected.

Actions to perform in case of pulling (reporting, audible alarm...) must be defined during the configuration of the terminal: by default, the Access and Time Biometric terminal ignores pulling event.

Tamper Switch contact

This relay contact, available on all the models of Access and Time Biometric terminal is open in case of tamper or of pulling out. This management of this contact is not conditioned by a configuration parameter of the terminal: it cannot be disabled.

It is strongly recommended to link this contact to a monitoring system which will store the information and which will warn the concerned staff.

The use of the internal relay of the terminal to command the opening of the door is misadvised. But if this solution is used, it is strongly recommended to introduce the "tamper switch» contact in the wiring of the command of the electric latch of the door.

To disturb a possible intruder, it's better to make the connection between the terminal relay and the contact "tamper switch" by a simple shunt on the terminal connectors. It is recommended to make this connection outside of the terminal (at the end of cables), in the restricted area, as shown in Figure 2 below.

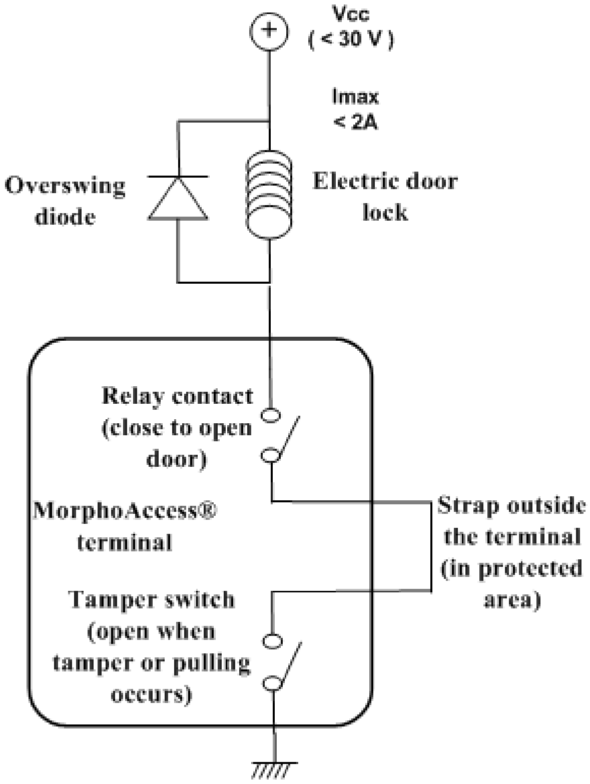


Figure 2 : Tamper switch contact inserted in electric latch command circuit

With an electric diagram such as the one in Figure 2 (sample), a simple short circuit of the internal relay contact, will not open the door in case of tamper or pulling of the terminal.

Tamper/pulling event management

When the terminal detects a tamper or a pulling out, it acts as required by the configuration parameters associated with this function:

- ignore the event (default configuration): useful during the normal maintenance operations, but misadvised in normal operation
- send an alarm message (recommended option), to a distant system, using one of the supported protocol (Wiegand, DataClock, RS485, RS422, Ethernet, 3G, or Wi-Fi™, UDP, TCP, TLS/SSL).
- Issue an audio and visual local alarm (using the buzzer, the status LED and the screen of the terminal).
- Disable access control (access requests are ignored)
- Delete user database content
- Delete contactless authentication keys
- Disable internal relay

When the default disappears, the terminal interrupts the local visual and audio alarm and sends an « end of tamper/pulling default » to the distant system.

It is strongly recommended that the application which receives the « default/end of default » message acts according to the required security level. For example:

- Store the information, with a time stamp and the identity of the terminal (recommended action)
- Send a message to security staff
- Disable access to the area protected by the terminal.
- etc.

Section 5 : Access and Time Biometric Terminal Connections

Access and Time Biometric Terminal connections

Result of local access rights check

This message is issued by the Access and Time Biometric terminal when the local access right check is completed.

In global access control system which include a central access controller, this message is used to require the final decision « access granted/denied » to the central access controller. With this message, the terminal transfers the responsibility of the access allowance to the central access controller. The central access controller performs additional checks, and if access is granted to the user, sends the order of opening of the door to a separate device (a single door controller).

It is strongly recommended that the opening of the door should be directly ordered by the central access control through a single door controller without any direct relation with the terminal. However, it is possible to configure the terminal so that the central access controller activates the internal relay of the Access and Time Biometric terminal, but this configuration is not recommended.

Network connection

The configuration of a Access and Time Biometric terminal can be done through a network, also it is recommended to use a specific network dedicated to the access control system, different from the corporate network.

When possible, it is recommended to install a "access control system" network physically separated from the corporate network, but by default, the separation can be done virtually (for example by using Virtual Private Network).

The "access control" network includes Access and Time Biometric terminals, one or several enrolment stations, door controllers, and one or several central access controllers.

The separation of the network "access control" of the corporate network avoids different cases such as the one listed below:

- access to an Access and Time Biometric terminal configuration by an unauthorized workstation
- fake message send by an Access and Time Biometric terminal simulator to the Central Access Controller (to open a door)
- Access and Time Biometric terminal simulator expecting database content downloading from an enrolment station

These risks are highly reduced by using TLS/SSL secured protocol between an Access and Time Biometric terminal and the others devices.

With an Access and Time Biometric terminal, when the secured protocol TLS/SSL is used, it is recommended to deactivate the configuration of the terminal:

- By USB scripts (especially if default protection key for USB scripts hasn’t been changed)
- By the embedded Web Server application (especially if default HTTPS certificate hasn’t been changed)

With an Access and Time Biometric terminal, it is recommended to close the retrofit port when it is not used, by settting the configuration key comm_channels_state.upgrade_firmware to 0.

Ethernet connection

It is strongly recommended to use shielded cable of category 5 (or better), and to insert an Ethernet repeater (a switch or a hub) every 90 m.

When it is possible it's better to connect the Ethernet cable with the RJ45 connector, rather than using the connector block dedicated to Ethernet (Access and Time Biometric terminal side). When this solution is used, the connection to the connector block must be done with extreme care. Indeed, a low-quality connection can strongly perturb the quality of the Ethernet signals.

It is strongly recommended to connect Rx + and Rx- wires with the same twisted pair, and to do the same thing with Tx + / Tx-but with another twisted pair. This method reduces electromagnetic interference; improve the quality of the signal while reducing the possibility of listening by an intruder.

Whatever is the connection (RJ45 plug or wired connector block), only the authorized staff should have access to it.

Inadvisable protocols

Wiegand, DataClock, and RS422 protocol don’t provide:

- Any guaranty about the identity of the message sender (the Central Access Controller is not able to make the difference between a regular Access and Time Biometric terminal and a fake terminal)
- Any confirmation of the reception of the message (the Central Access Controller may have not received the message, or may have receive an modified message)
- Any anti-replay protection (the message can be intercepted by a device, which send the message).

Recommended communication protocols

It is highly recommended to use an Ethernet connection with TLS/SSL protocol.

A communication through a wireless connection (such as Wi-Fi™ or 3G) can be received in the free zone, this is impossible when the communication is through an Ethernet cable installed in the restricted area.

In addition the TLS/SSL protocol certifies:

- message confidentiality by ciphering
- the identity of the sender of the message, and the identity of the receiver of the message (using mutual authentication).
- Anti-replay of a message: if an unauthorized person succeed to copy a (ciphered message), he can try to send it later, but it will be rejected by the receiver.

When a wired connection cannot be used, then it is highly recommended to activate the TLS/SSL protocol on the wireless connection (either Wi-Fi™ or 3G).

If it is not possible, it is highly inadvisable to use a plain (not ciphered) wireless connection (Wi-Fi™ or 3G).

For a Wi-Fi™ connection, it is also inadvisable to use WEP encryption: the confidentiality of the messages can be broken with little effort. Then is mandatory o use WPA encryption with the most sophisticated key (in terms of number and kind of characters).

Access and Time Biometric terminal internal relay

For a better security it is highly inadvisable to use the internal relay to command directly the opening of the door or of the gate that provides the access to the restricted area.

If it not possible to use a Central Access Controller or a Single Door Controller, then it is recommended to follow the instructions listed below:

- The connections of the electric latch of the door must not be accessible from the free zone.
- The terminal must be strongly fixed on its physical support (a wall or a pole).
- The anti-tamper and the anti-pulling detection must be activated.
- The « tamper switch » contact must be included in the connection of the electric latch, to avoid the opening of the door when the terminal is not closed and in its normal position (please refer to Figure 2 : Tamper switch contact inserted »).

With Access and Time Biometric terminal, it is recommended to reinforce the security of the installation by activating the function that monitors the opening of the door (or of the access).

Section 6 : Sensible Data Management

Authentication keys, passwords

Customize password

It is highly recommended to change the value of the password of terminal equipped with keyboard and screen. This password is used to get access to terminal management functions.

Please, don’t forget to note the new value, and save it in a safe area.

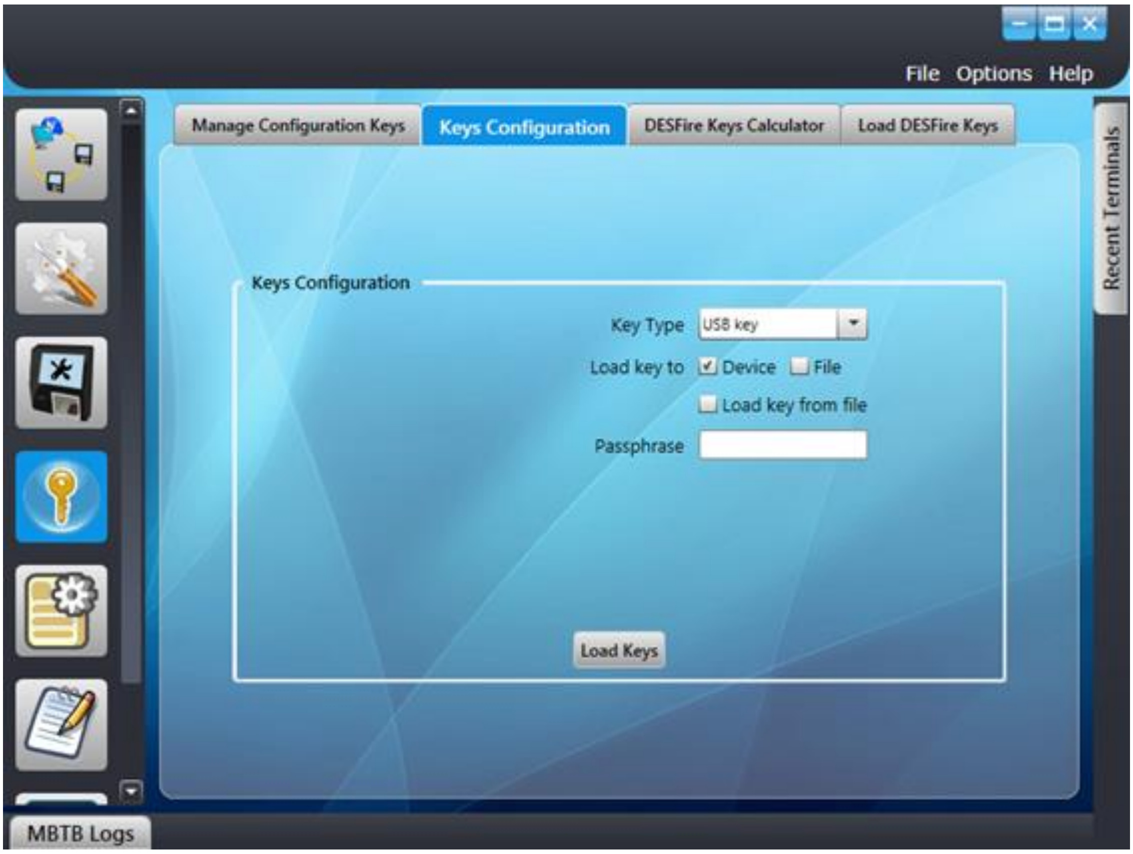
Customize contactless authentication keys

It is highly recommended to change the value of the contactless authentication keys, of terminals equipped with contactless card reader (to see section “Scope of the document").

This password is used to get access to terminal management functions.

Customize USB scripts protection key

It is highly recommended to change the value of the key used to protect USB scripts execution when USB script feature is enabled on the terminal. This key can be changed using MorphoBioToolBox application:



Keys Configuration

Key Type: USB key

Load key to ☑ Device □ File

□ Load key from file

Passphrase:

Password value Confidentiality

The default value of the all password and contactless authentication keys are specified in the documentation of the product, then it is recommended to:

- Restrict the access to the terminal documentation to « need to know » personnel only.
- Customize the value of each password, and each authentication keys as soon as possible (at least immediately after terminal installation).
- Restrict the access to the new values, to « need to know » personnel only.
- Do not hesitate to change again these values in case of suspicion of unwanted or voluntary disclosure.

Backup of customized parameters

It is strongly recommended to backup the new values on a physical support such as paper (stored in a safe place) or a digital file (saved in a software safe).

Do not note it on visible or easily accessible supports (keyboard, datebook, pad...). If necessary, store them in a ciphered file.

According to the wished security level, the backup location can be a simple drawer, or a shielded and fireproofed cupboard.

Date and Time

Date and Time synchronization

If the Access and Time Biometric terminal is used for application requiring high precision time (such as Time and Attendance application), it is recommend synchronizing regularly the Access and Time Biometric terminal time with an external reliable clock.

The synchronization period must be at least one time per day.

It is strongly recommended to use NTP (Network Time Protocol), and to specify the server on whom the terminal has to synchronize automatically.

The Access and Time Biometric terminal internal clock has a +/- $40x10^{-6}$ (ppm) typical time deviation at +25°C (roughly +/- 4 seconds per day).

At +45°C, the time deviation may be up to +/-8 seconds per day.

Date/Time backup

In the case of a default of its power supply, the Access and Time Biometric terminal protects the functioning of its internal clock during more than 24 hours. Then when its power supply is restored, the terminal date and time are still valid. Beyond backup period the risk of synchronization failure increases.

The loss of date and time has an immediate impact on all the records and messages containing the date and the time:

- recording of the access requests (log file)
- sending of the local result of access con

The loss of synchronization of the internal date and time, with external world, can have a more fatal effect on the use of cryptographic key with a validity date. The action listed below could systematically fail:

- mutual authentication, part of the TLS/SSL protocol, used to establish a connection between the terminal and the other devices
- authentication and reading of contactless smartcards such as DESFire® type

In the worst case, the terminal can consider that the current keys are obsolete and thus to refuse any connection with configuration station, enrollment station, and with the central access controller. In addition, the terminal can refuse the DESFire® contactless smartcards of authorized users and administrators.

When the Access and Time Biometric terminal is used in a case which requires synchronicity with the external world, it is mandatory to make sure that its power supply will be interrupted no more than 24 hours

Section 7 : TLS Protocol (SSL)

Overview

Access and Time Biometric terminals support TLS / SSL protocol to:

- Authenticate the server (host) connected to the terminal
- Secure the data exchanged between the server (host) and terminal, through cyphering
- Ensure data integrity

For more information, please visit the website:

https://en.wikipedia.org/wiki/Transport_Layer_Security

Protection of the TLS / SSL data

The configuration of terminals using TLS/ SSL protocol requires to manipulate sensitive data (such as private keys), it is thus highly recommended to protect these data.

When a Public Key Infrastructure (PKI) already exists, it is recommended to insert the management of Access and Time Biometric terminals and the associated system inside this PKI.

For the management of sensitive data, it is recommended to use a dedicated Laptop Computer, in a secure room (Faraday cage, access restricted to authorized personnel only). When it is not used, the dedicated Laptop Computer should be stored in a shielded and fireproofed cupboard.

Versions

Several TLS versions are supported: From SSL v3 to TLS 1.2 for all Access and Time Biometric terminals.

Several cypher suite algorithms are supported (including key exchange, bulk encryption and message authentication code) to secure exchange.

The TLS version and cypher suite algorithm used is negotiated between the terminal and the server (host), by using a handshaking procedure. For all Access and Time Biometric terminals:

- The TLS version can be set using the configuration key: SSL_profile_0.protocol_version
- The cypher suite algorithm can be set using the configuration key: SSL_profile_0.cipher_list

Recommendations about version and cipher suites

Due to known attacks, it is recommended to use following guidelines when configuring TLS:

- TLS version:
    - SSL v2 and SSL v3 MUST NOT be used as they are considered insecure.
    - TLS 1.0 SHALL NOT be used except when higher version of TLS is not available.

- TLS 1.1 SHALL NOT be used except when higher version of TLS is not available.
- TLS 1.2 SHALL be the unique version enabled when it is known that other devices of the network support this version.

- Cipher suite algorithms:
  - NULL cipher suites MUST NOT be used.
  - RC4 cipher suites MUST NOT be used.
  - SHA cipher suites SHOULD NOT be used.
  - Cipher suites offering less than 112 bits of security MUST NOT be used.
  - Cipher suites offering less than 128 bits of security SHOULD NOT be used.
  - Cipher suites based on RSA key transport SHOULD NOT be used as they do not support forward secrecy. These cipher suites have assigned values starting with the string "TLS_RSA_WITH_*".
- Given the foregoing considerations, the following cipher suites are RECOMMENDED for configuration key SSL_profile_0.cipher_list:
  - bit 6 - ECDHE-ECDSA-AES128-GCM-SHA256:ECDH-ECDSA-AES128-GCM-SHA256
  - bit 7 - ECDHE-ECDSA-AES128-SHA256:ECDH-ECDSA-AES128-SHA256
- Other cipher suites available on Access and Time Biometric terminal are ACCEPTABLE.

Note about the DROWN attack

This vulnerability allows retrieving the session key of a TLS connection and then to decrypt the information (username, password…) passed between the client and the server.

A system is vulnerable to a DROWN attack if:

- It allows SSLv2 connections.
- Or if it uses a private key identical to another system allowing SSLv2 connections.

To get around this problem:

- Disable SSLv2 connections.
- Ensure than the private key used is not also used on other systems that allow SSLv2 connections.

For more information, please visit the website https://drownattack.com/

Certificates

The TLS / SSL protocol requires certificates to be generated an inserted in the system.

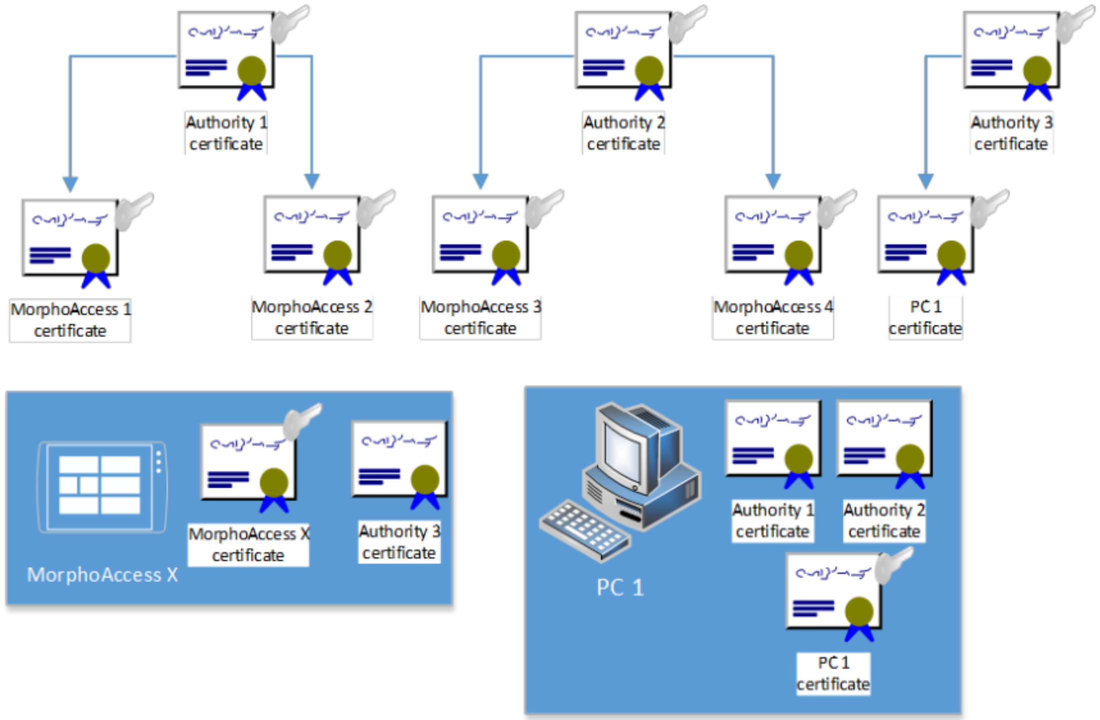
To secure the terminal, one has to load:

- Terminal private key
- Terminal certificate
- Trusted certificate authority or chain of trust of all certificates that will be authorized to connect to the terminal.

These ones should be provided in a pkcs12 archive file with its corresponding password.

If no other solution is available, OpenSSL can be used for the certificate generation: https://slproweb.com/products/Win32OpenSSL.html

Example of certificate for Access and Time Biometric terminal using OpenSSL



Generating the certificate authority

This is not required if a certificate authority already exists

REM Generate certificate request (ca.csr) and private key (ca.key) for CA

```
openssl req -new -newkey rsa:2048 -nodes -out ma5g\ca.csr
-keyout ma5g\ca.key -sha512 -subj
/C=FR/ST=ILEDEFRANCE/O=IDEMIA/OU=URD32/CN=CA/emailAddress=
yourname@yourdomain.com
```

REM generate autosigned CA certificate (ca.pem)

```
openssl x509 -trustout -signkey ma5g\ca.key -days 7500 -req
-in ma5g\ca.csr -out ma5g\ca.pem -sha512
```

REM generate CA.P12 file for autosigned CA certificate, encrypted by 'Admin' passphrase

```
openssl pkcs12 -export -nokeys -in ma5g\CA.bin -aes256 -out
ma5g\CA.p12 -passout pass:Admin
```

Generating the terminal authorization certificate

REM generate MA key (MA.key), certificate request (MA.csr) and certificate (MA.crt)

```
openssl req -new -newkey rsa:2048 -nodes -keyout ma5g\MA.key -out ma5g\MA.csr -sha512 -subj /C=FR/ST=ILEDEFRANCE/O=IDEMIA/OU=URD32/CN=MA/emailAddress=yourname@yourdomain.com
```

```
openssl x509 -req -days 7500 -in ma5g\MA.csr -CA ma5g\ca.pem -CAkey ma5g\ca.key -set_serial 01 -out ma5g\MA.crt -sha512
```

Generating the terminal pkcs12 archive file

REM generate MA.P12 file for MA, encrypted by 'morpho' passphrase

```
type ma5g\MA.crt ma5g\MA.key ma5g\ca.pem > ma5g\MA_full.bin
```

```
openssl pkcs12 -export -in ma5g\MA_full.bin -aes256 -out ma5g\MA_full.p12 -passout pass:idemia
```

Generating the host certificate

REM generate PC key (PC.key), certificate request (PC.csr) and certificate (PC.crt)

```
openssl req -new -newkey rsa:2048 -nodes -keyout ma5g\PC.key -out ma5g\PC.csr -sha512 -subj /C=FR/ST=ILEDEFRANCE/O=MORPHO/OU=URD32/CN=PC/emailAddress=yourname@yourdomain.com
```

```
openssl x509 -req -days 7500 -in ma5g\PC.csr -CA ma5g\ca.pem -CAkey ma5g\ca.key -set_serial 01 -out ma5g\PC.crt -sha512
```

REM generate PC.p12 encrypted by 'maci' passphrase

```
openssl pkcs12 -export -in ma5g\PC.crt -inkey ma5g\PC.key -out ma5g\PC.p12 -passout pass:maci
```

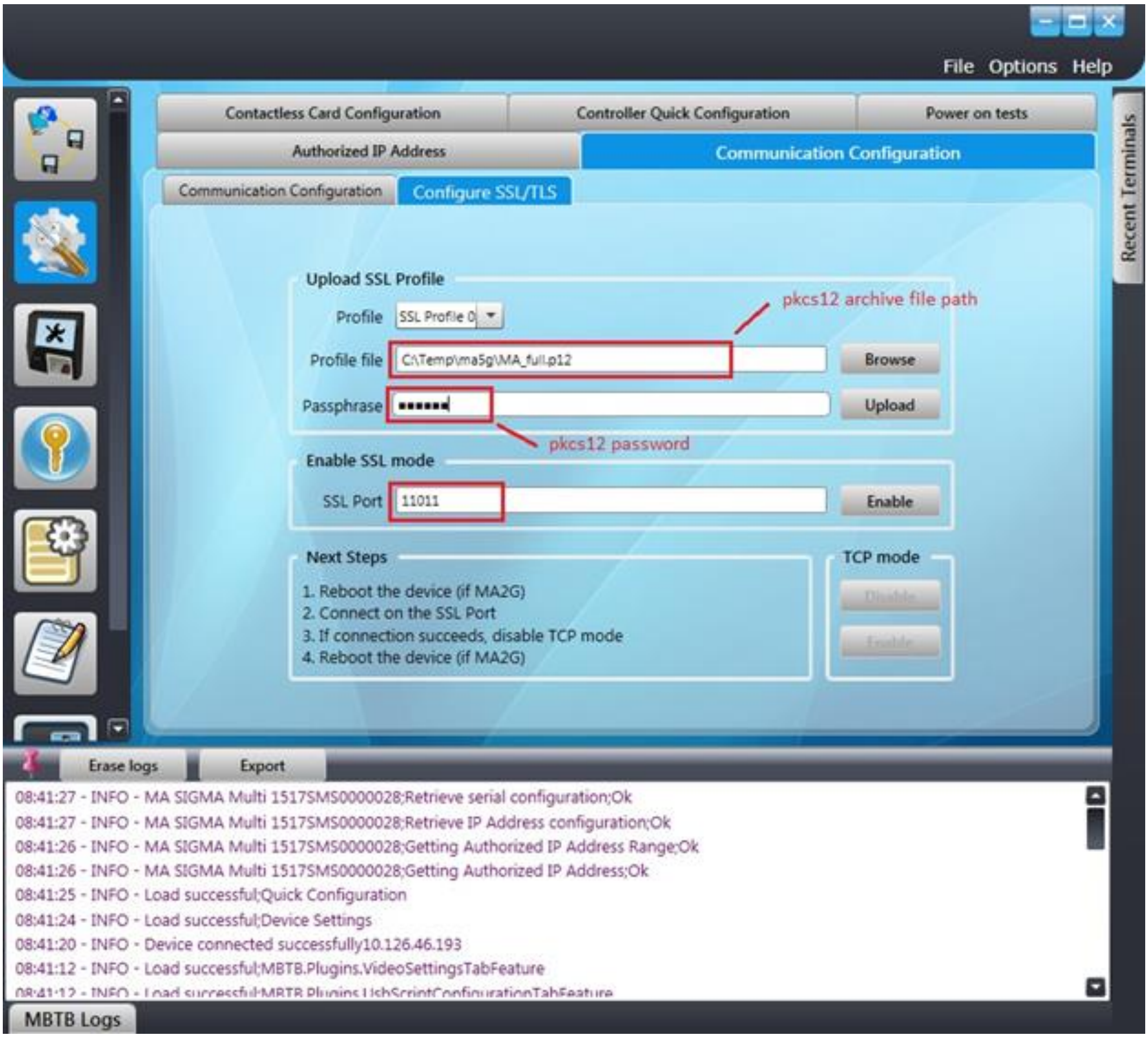
REM generate PC.pem encrypted by 'maci' passphrase

```
openssl pkcs12 -in ma5g\PC.p12 -out ma5g\PC.pem -passin pass:maci -passout pass:maci
```

Configuration of a secured connection between an Access and Time Biometric terminal and MorphoBioToolBox application

Terminal configuration

To configure TLS on terminal, we should load the certificate, its password, and activate the dedicated port.



Upload SSL Profile

Profile: SSL Profile 0

Profile file: C:\Temp\ma5g\MA_full.p12

pkcs12 archive file path

Passphrase: ••••••

pkcs12 password

Enable SSL mode

SSL Port: 11011

Next Steps

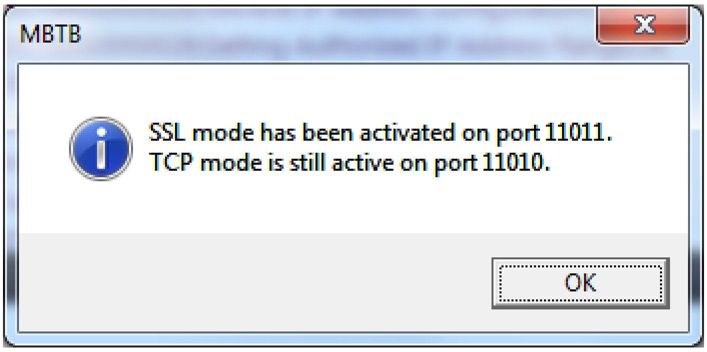
1. Reboot the device (if MA2G)
2. Connect on the SSL Port
3. If connection succeeds, disable TCP mode
4. Reboot the device (if MA2G)

TCP mode

```
08:41:27 - INFO - MA SIGMA Multi 1517SMS0000028;Retrieve serial configuration;Ok
08:41:27 - INFO - MA SIGMA Multi 1517SMS0000028;Retrieve IP Address configuration;Ok
08:41:26 - INFO - MA SIGMA Multi 1517SMS0000028;Getting Authorized IP Address Range;Ok
08:41:26 - INFO - MA SIGMA Multi 1517SMS0000028;Getting Authorized IP Address;Ok
08:41:25 - INFO - Load successful;Quick Configuration
08:41:24 - INFO - Load successful;Device Settings
08:41:20 - INFO - Device connected successfully10.126.46.193
08:41:12 - INFO - Load successful;MBTB.Plugins.VideoSettingsTabFeature
08:41:12 - INFO - Load successful;MBTB.Plugins.UsbScriptConfigurationTabFeature
```

- By default, TCP port is 11010 (in_channel.primary_port) and SSL port is 11011 (in_channel.secondary_port)
- If terminal is configured with the same port for SSL and TCP, only SSL connection will be available
- Enabling SSL is done by setting the configuration in_channel.SSL_conn_mode. With MorphoBioToolBox, it is done clicking on the enable button in the “Configuration SSL/TLS” screen.

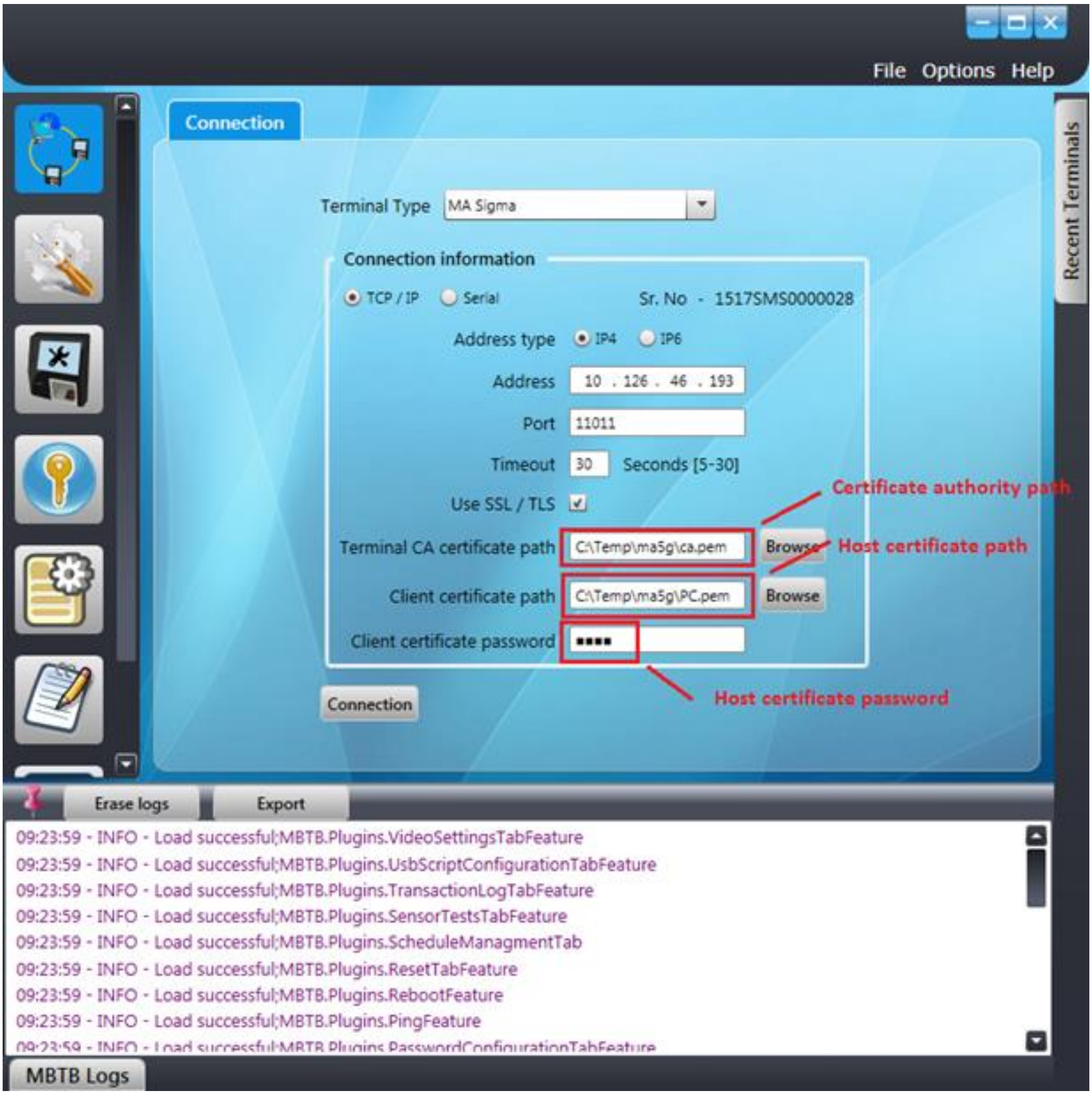
- With MorphoBioToolBox, when activating SSL on port 11010 or 11011, automatically, TCP port is switched on the other port, as indicated in the box message.
- With MorphoBioToolBox, when enabling SSL, TCP is still active, as indicated in the box message. We recommend to not disable it, before having validated a proper SSL communication with the host.



SSL mode has been activated on port 11011.
TCP mode is still active on port 11010.

Host configuration

Once TLS is configured, IDEMIA recommends a connection test with MorphoBioToolBox.



Terminal Type: MA Sigma

Connection information

● TCP / IP ○ Serial

Sr. No - 1517SMS0000028

Address type: ● IP4 ○ IP6

Address: 10 . 126 . 46 . 193

Port: 11011

Timeout: 30 Seconds [5-30]

Use SSL / TLS: ☑

Terminal CA certificate path: C:\Temp\ma5g\ca.pem

Client certificate path: C:\Temp\ma5g\PC.pem

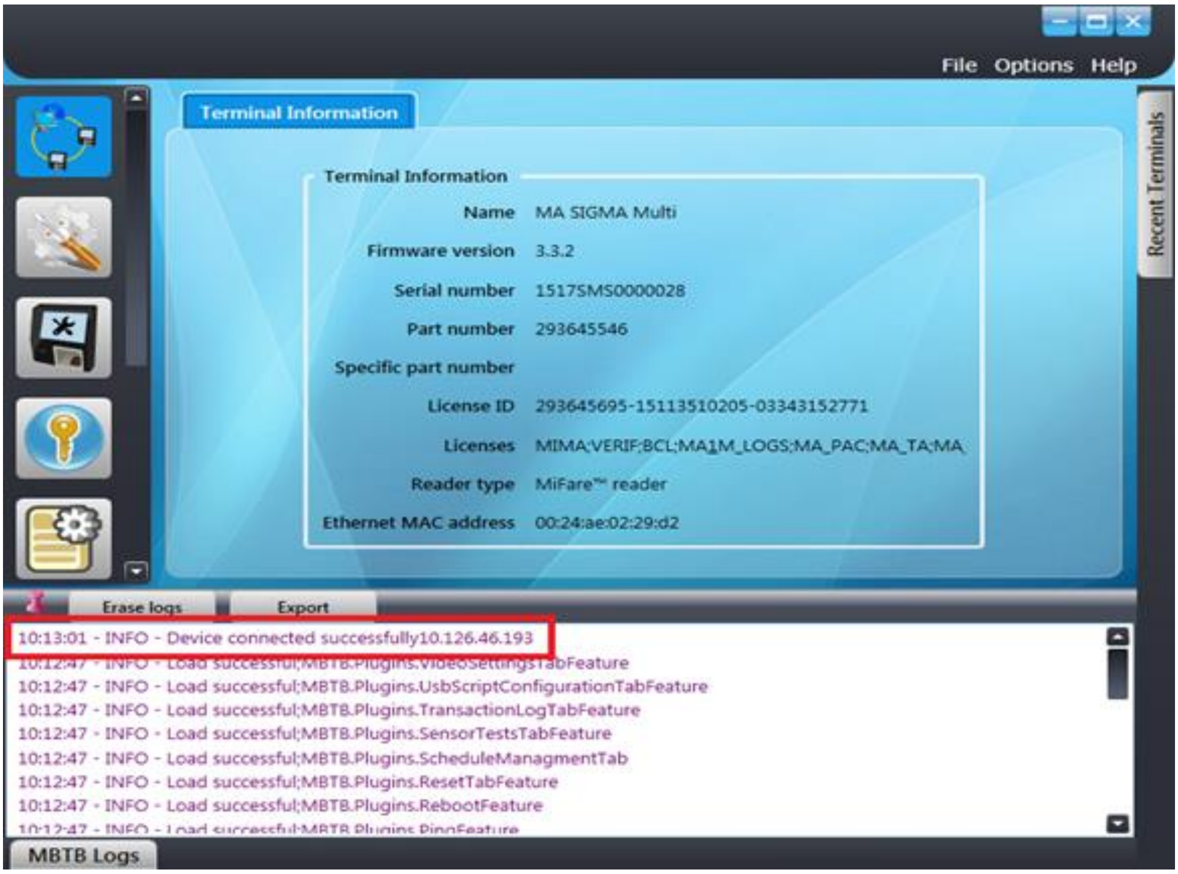
Client certificate password: ****

Certificate authority path

Host certificate path

Host certificate password

```
09:23:59 - INFO - Load successful;MBTB.Plugins.VideoSettingsTabFeature
09:23:59 - INFO - Load successful;MBTB.Plugins.UsbScriptConfigurationTabFeature
09:23:59 - INFO - Load successful;MBTB.Plugins.TransactionLogTabFeature
09:23:59 - INFO - Load successful;MBTB.Plugins.SensorTestsTabFeature
09:23:59 - INFO - Load successful;MBTB.Plugins.ScheduleManagmentTab
09:23:59 - INFO - Load successful;MBTB.Plugins.ResetTabFeature
09:23:59 - INFO - Load successful;MBTB.Plugins.RebootFeature
09:23:59 - INFO - Load successful;MBTB.Plugins.PingFeature
09:23:59 - INFO - Load successful;MBTB.Plugins.PasswordConfigurationTabFeature
```



Terminal Information

Name MA SIGMA Multi

Firmware version 3.3.2

Serial number 1517SMS0000028

Part number 293645546

Specific part number

License ID 293645695-15113510205-03343152771

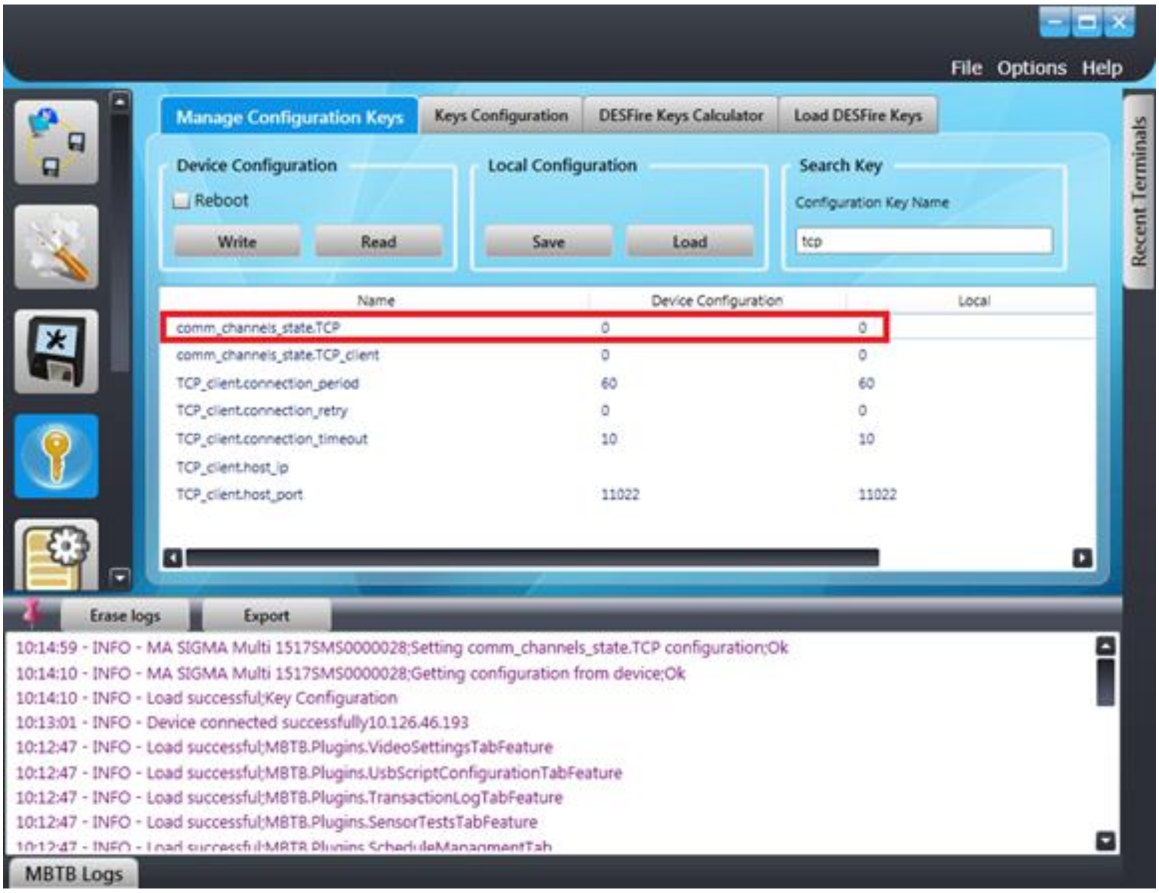
Licenses MIMA;VERIF;BCL;MA1M_LOGS;MA_PAC;MA_TA;MA

Reader type MiFare™ reader

Ethernet MAC address 00:24:ae:02:29:d2

```
10:13:01 - INFO - Device connected successfully10.126.46.193
10:12:47 - INFO - Load successful;MBTB.Plugins.VideoSettingsTabFeature
10:12:47 - INFO - Load successful;MBTB.Plugins.UsbScriptConfigurationTabFeature
10:12:47 - INFO - Load successful;MBTB.Plugins.TransactionLogTabFeature
10:12:47 - INFO - Load successful;MBTB.Plugins.SensorTestsTabFeature
10:12:47 - INFO - Load successful;MBTB.Plugins.ScheduleManagmentTab
10:12:47 - INFO - Load successful;MBTB.Plugins.ResetTabFeature
10:12:47 - INFO - Load successful;MBTB.Plugins.RebootFeature
10:12:47 - INFO - Load successful;MBTB.Plugins.PingFeature
```

After the TLS connection is successfully tested unencrypted TCP communication should be disabled.



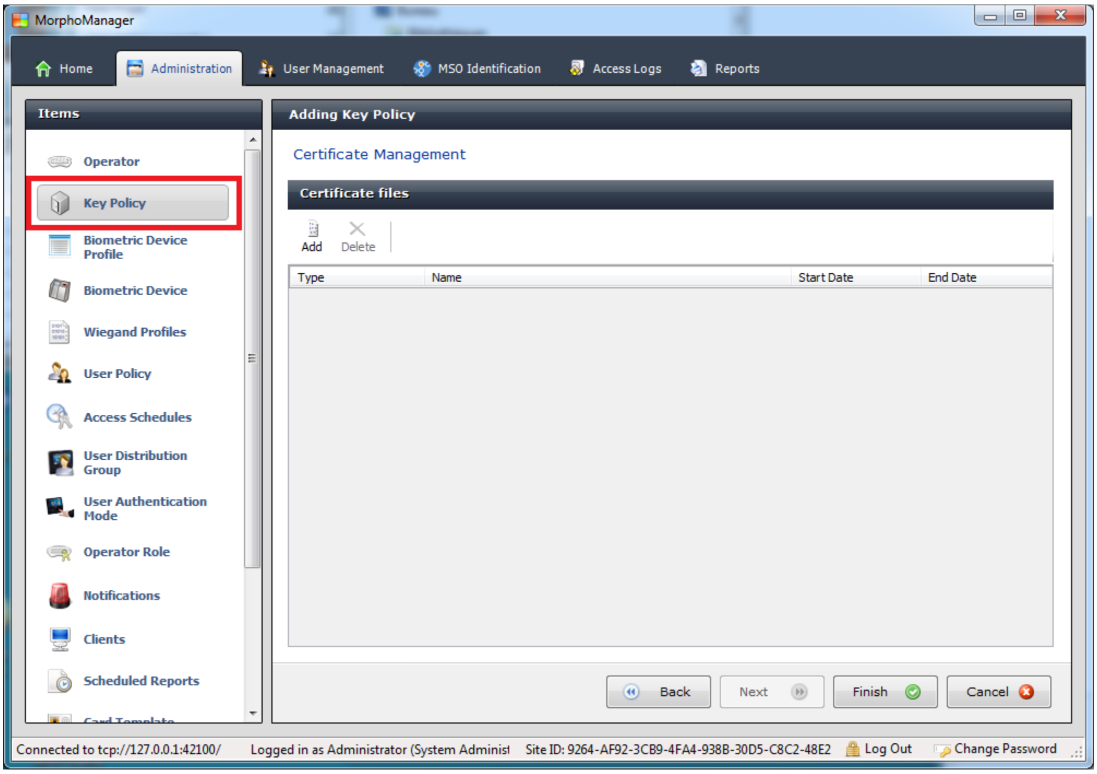
Configuration Key Name: tcp

Name	Device Configuration	Local
comm_channels_state.TCP	0	0
comm_channels_state.TCP_client	0	0
TCP_client.connection_period	60	60
TCP_client.connection_retry	0	0
TCP_client.connection_timeout	10	10
TCP_client.host_ip		
TCP_client.host_port	11022	11022

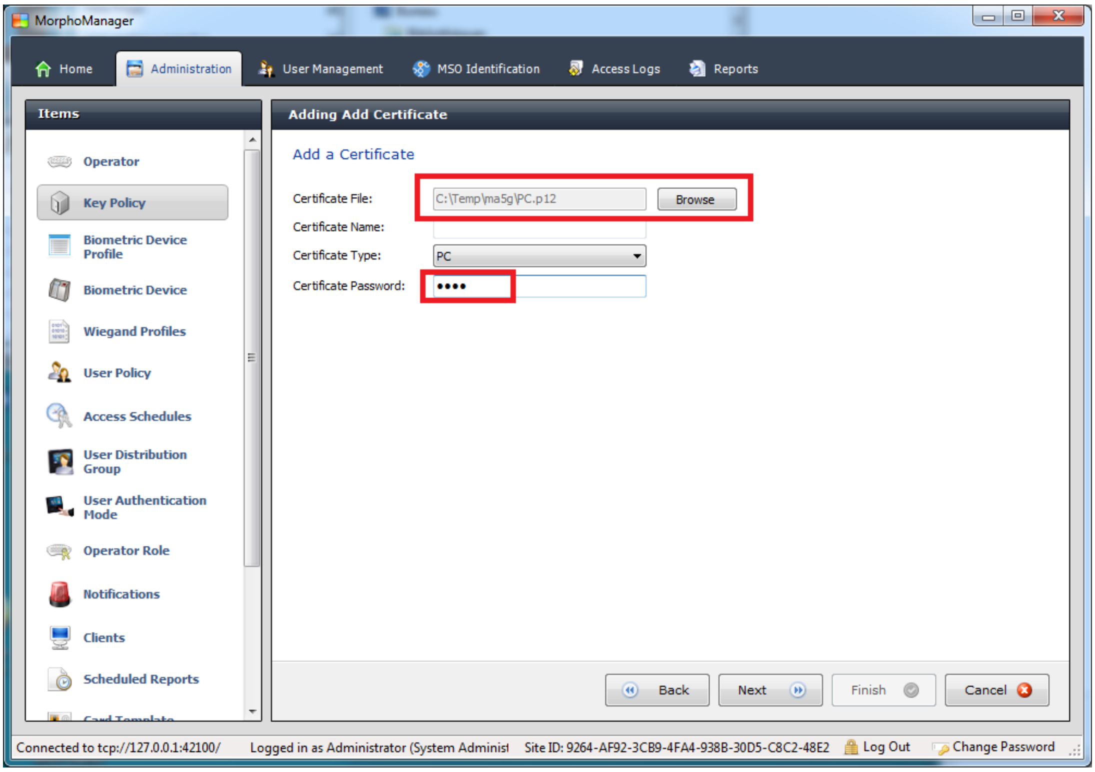
```
10:14:59 - INFO - MA SIGMA Multi 1517SMS0000028;Setting comm_channels_state.TCP configuration;Ok
10:14:10 - INFO - MA SIGMA Multi 1517SMS0000028;Getting configuration from device;Ok
10:14:10 - INFO - Load successful;Key Configuration
10:13:01 - INFO - Device connected successfully10.126.46.193
10:12:47 - INFO - Load successful;MBTB.Plugins.VideoSettingsTabFeature
10:12:47 - INFO - Load successful;MBTB.Plugins.UsbScriptConfigurationTabFeature
10:12:47 - INFO - Load successful;MBTB.Plugins.TransactionLogTabFeature
10:12:47 - INFO - Load successful;MBTB.Plugins.SensorTestsTabFeature
10:12:47 - INFO - Load successful;MBTB.Plugins.ScheduleManagmentTab
```

Configuration of a secured connection between a terminal Access and Time Biometric terminal and MorphoManager application

Add a Key Policy, name it (e.g. SSL_KP), and go to the ‘Certificate Management’ screen.



Select ‘Add’ button, browse to the host certificate pkcs12 (example PC.p12), enter the associated password and press the ‘Next’ button.



Adding Add Certificate

Add a Certificate

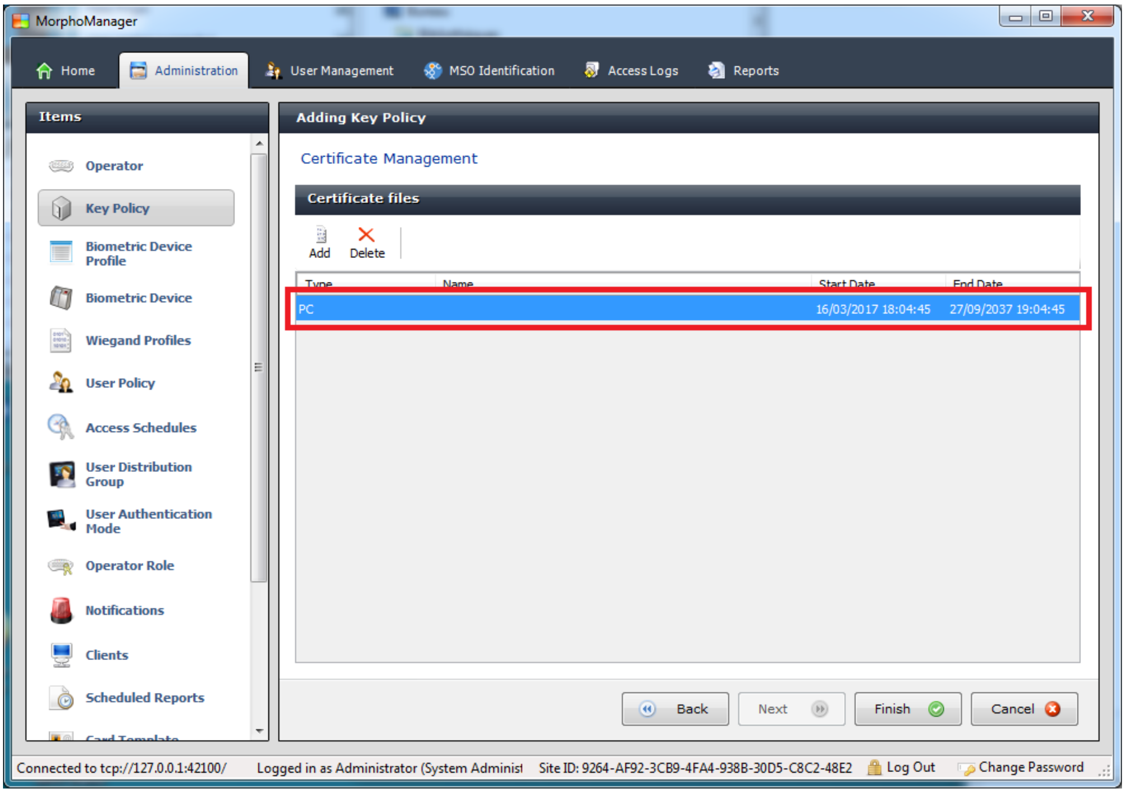
Certificate File: C:\Temp\ma5g\PC.p12

Certificate Name:

Certificate Type: PC

Certificate Password: ••••

Connected to tcp://127.0.0.1:42100/ Logged in as Administrator (System Administ Site ID: 9264-AF92-3CB9-4FA4-938B-30D5-C8C2-48E2



Adding Key Policy

Certificate Management

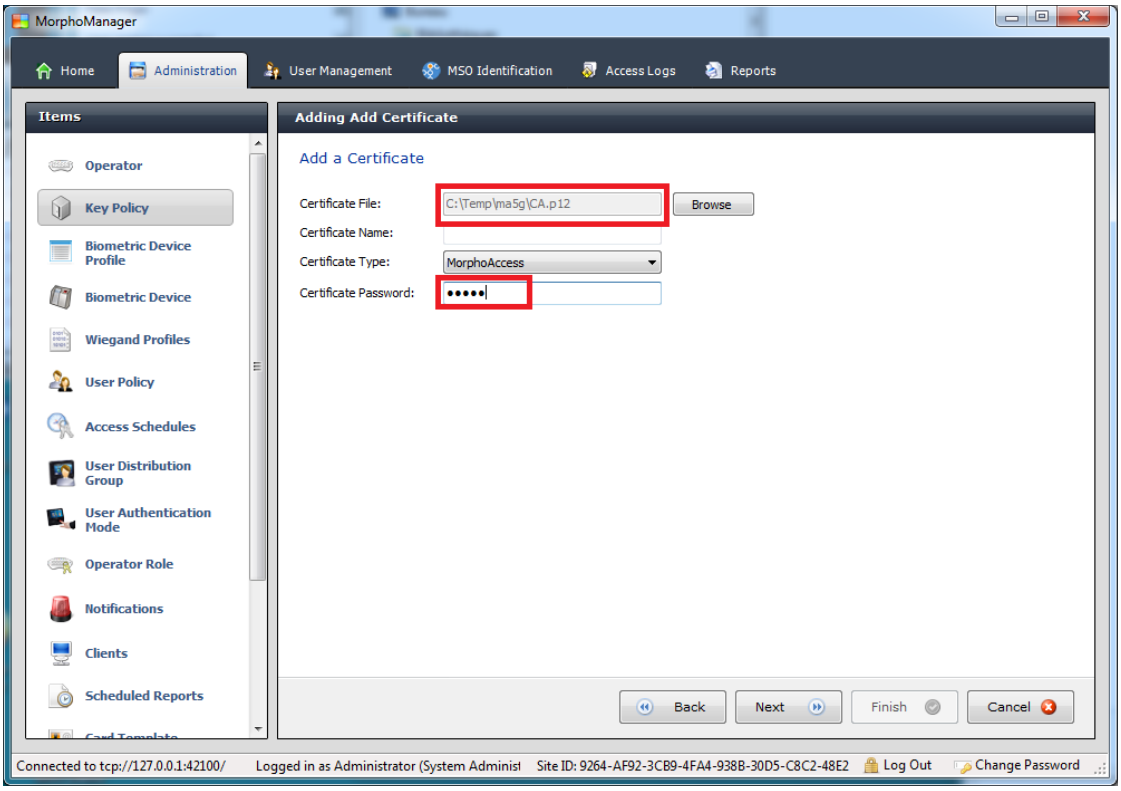
Certificate files

Type	Name	Start Date	End Date
PC		16/03/2017 18:04:45	27/09/2037 19:04:45

Connected to tcp://127.0.0.1:42100/ Logged in as Administrator (System Administ Site ID: 9264-AF92-3CB9-4FA4-938B-30D5-C8C2-48E2

Select ‘Add’ button, browse to the certificate authority pkcs12 (example CA.p12), change the ‘Certificate Type’ to ‘MorphoAccess’, enter the associated password and press the ‘Next’ button.

Warning: even if it will be accepted by MorphoManager, we recommend to not use the terminal certificate because it is containing the private key, not only the public information.



Adding Add Certificate

Add a Certificate

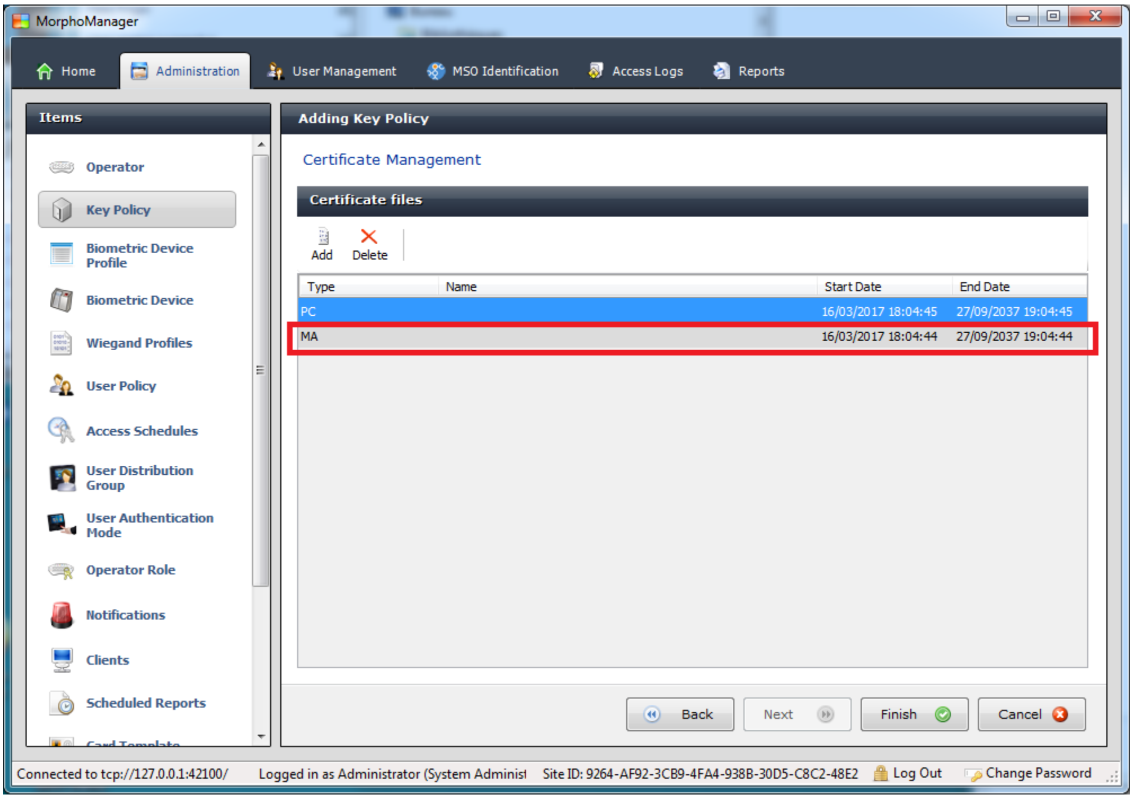
Certificate File: C:\Temp\ma5g\CA.p12

Certificate Name:

Certificate Type: MorphoAccess

Certificate Password: •••••

Connected to tcp://127.0.0.1:42100/ Logged in as Administrator (System Administ Site ID: 9264-AF92-3CB9-4FA4-938B-30D5-C8C2-48E2



Adding Key Policy

Certificate Management

Certificate files

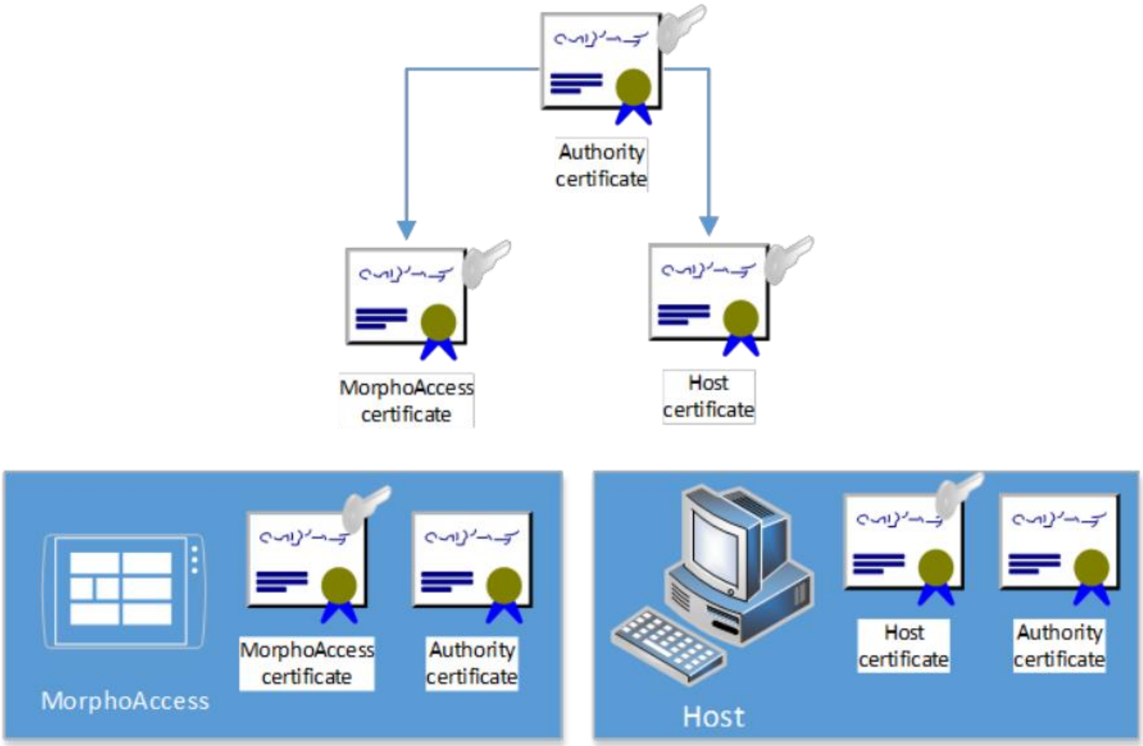
Type	Name	Start Date	End Date
PC		16/03/2017 18:04:45	27/09/2037 19:04:45
MA		16/03/2017 18:04:44	27/09/2037 19:04:44

Connected to tcp://127.0.0.1:42100/ Logged in as Administrator (System Administ Site ID: 9264-AF92-3CB9-4FA4-938B-30D5-C8C2-48E2

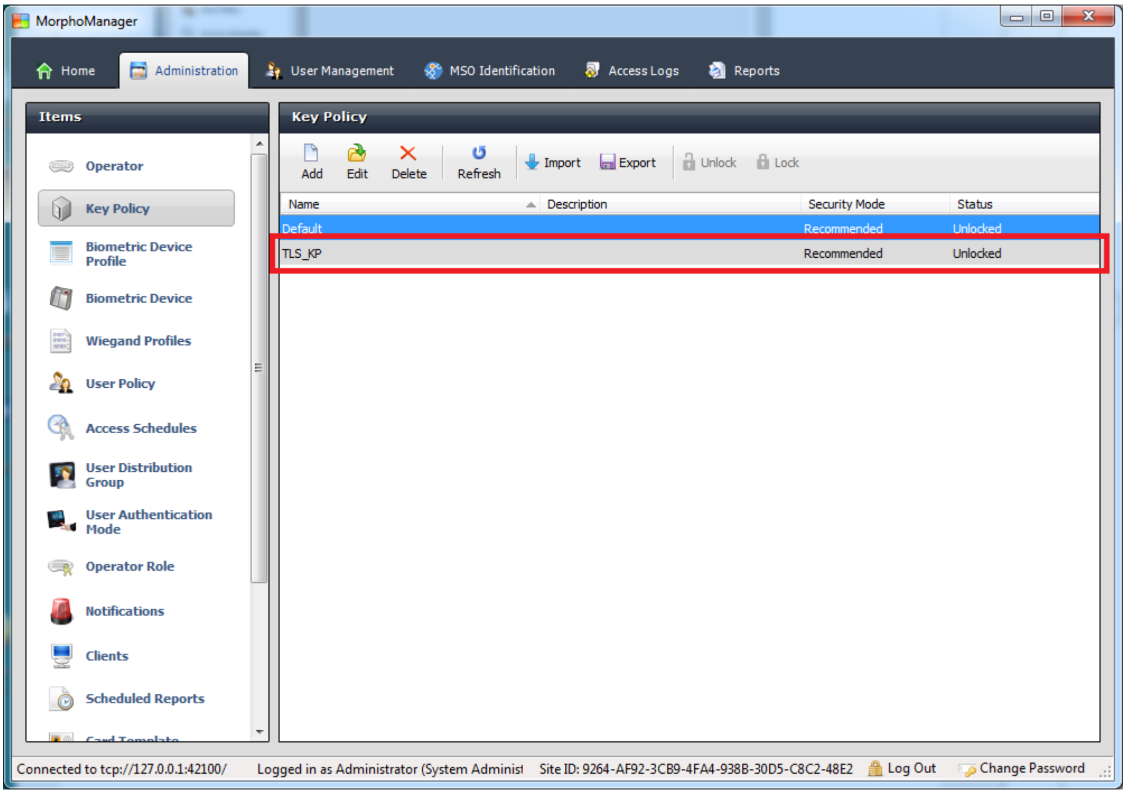
For higher security, you can use a different certificate and/or a different trusted authority for each MorphoAccess Biometric Device. In this case you shall add all the certificates and password into the Key Policy:

- All authorities certificates that signed MorphoAccess certificates, with ‘MorphoAccess’ Certificate Type

All PC certificates signed by authorities trusted by MorphoAccess, with ‘PC’ Certificate Type

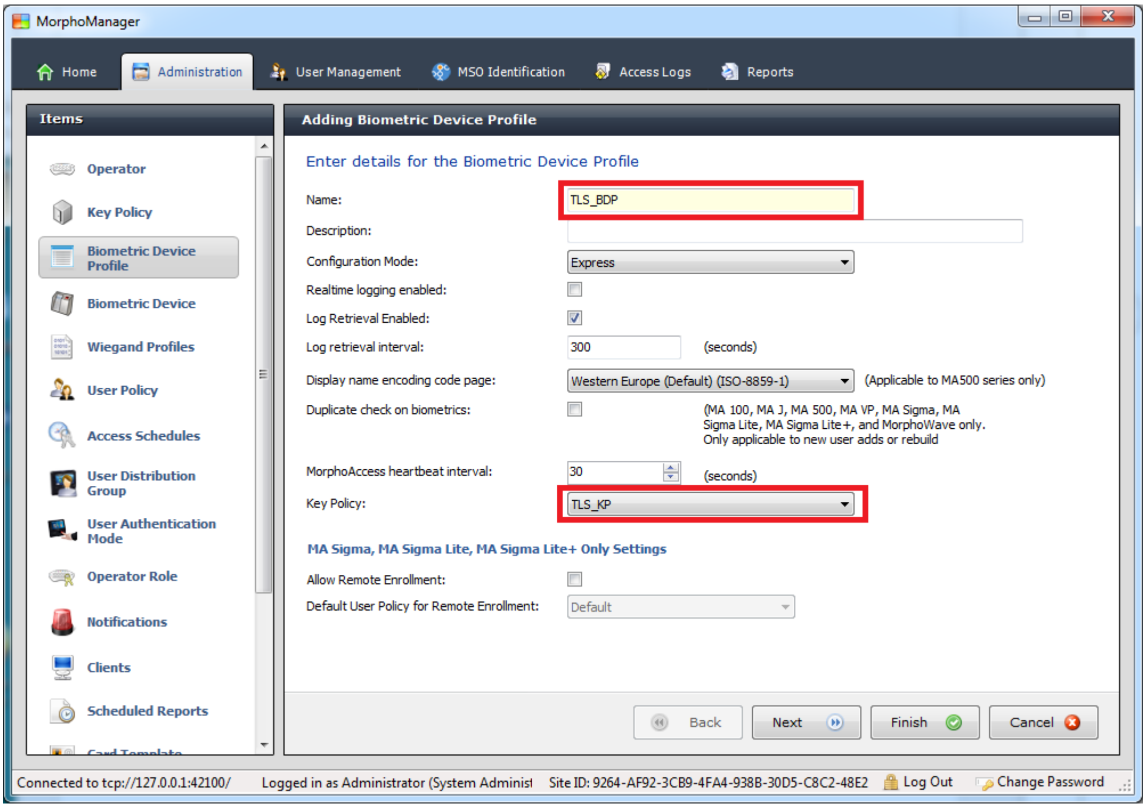


Once complete, press the ‘Finish’ button. The key policy is now created.



Name	Description	Security Mode	Status
Default		Recommended	Unlocked
TLS_KP		Recommended	Unlocked

Add a Biometric Device Profile, name it (e.g. TLS_BDP), and select the correct Key Policy (e.g. TLS_KP).



Adding Biometric Device Profile

Enter details for the Biometric Device Profile

Name: TLS_BDP

Description:

Configuration Mode: Express

Realtime logging enabled: □

Log Retrieval Enabled: ☑

Log retrieval interval: 300 (seconds)

Display name encoding code page: Western Europe (Default) (ISO-8859-1) (Applicable to MA500 series only)

Duplicate check on biometrics: □ (MA 100, MA J, MA 500, MA VP, MA Sigma, MA Sigma Lite, MA Sigma Lite+, and MorphoWave only. Only applicable to new user adds or rebuild

MorphoAccess heartbeat interval: 30 (seconds)

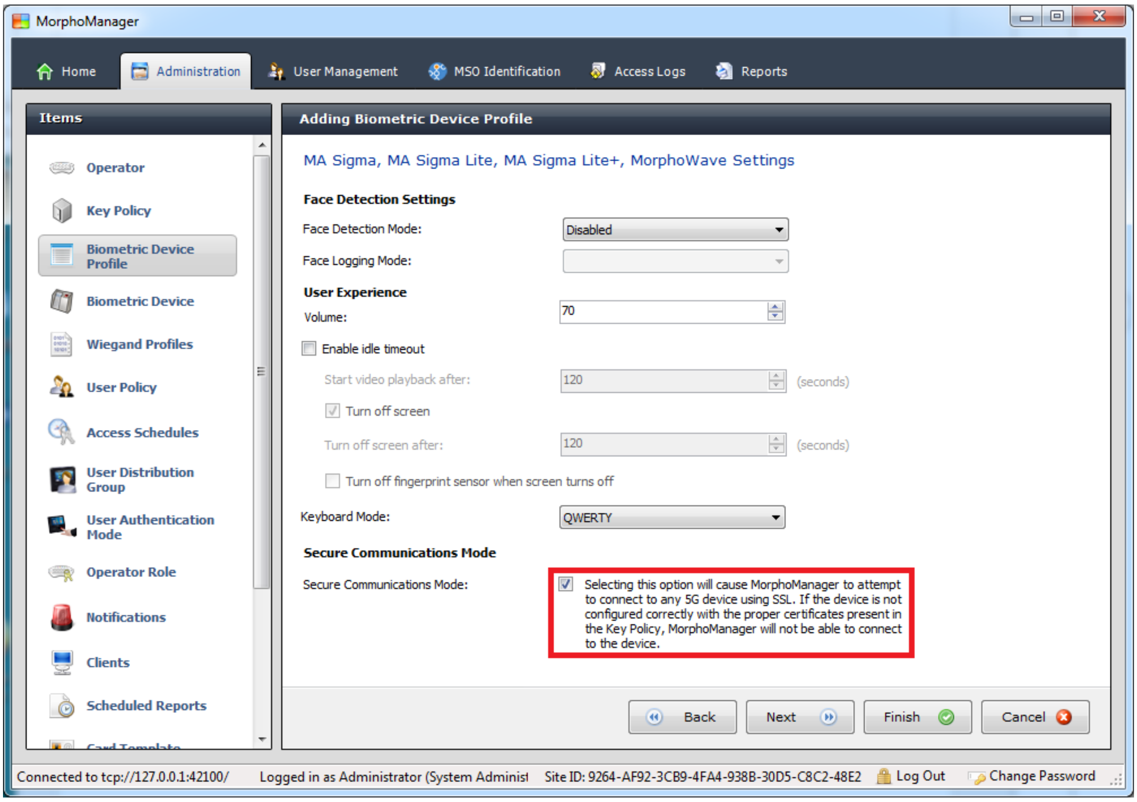
Key Policy: TLS_KP

MA Sigma, MA Sigma Lite, MA Sigma Lite+ Only Settings

Allow Remote Enrollment: □

Default User Policy for Remote Enrollment: Default

Configure all other parameters of the Biometric Device Profile and click on the ‘Finish’ button. The Biometric Device Profile is now available.



Adding Biometric Device Profile

MA Sigma, MA Sigma Lite, MA Sigma Lite+, MorphoWave Settings

Face Detection Settings

Face Detection Mode: Disabled

Face Logging Mode:

User Experience

Volume: 70

□ Enable idle timeout

Start video playback after: 120 (seconds)

☑ Turn off screen

Turn off screen after: 120 (seconds)

□ Turn off fingerprint sensor when screen turns off

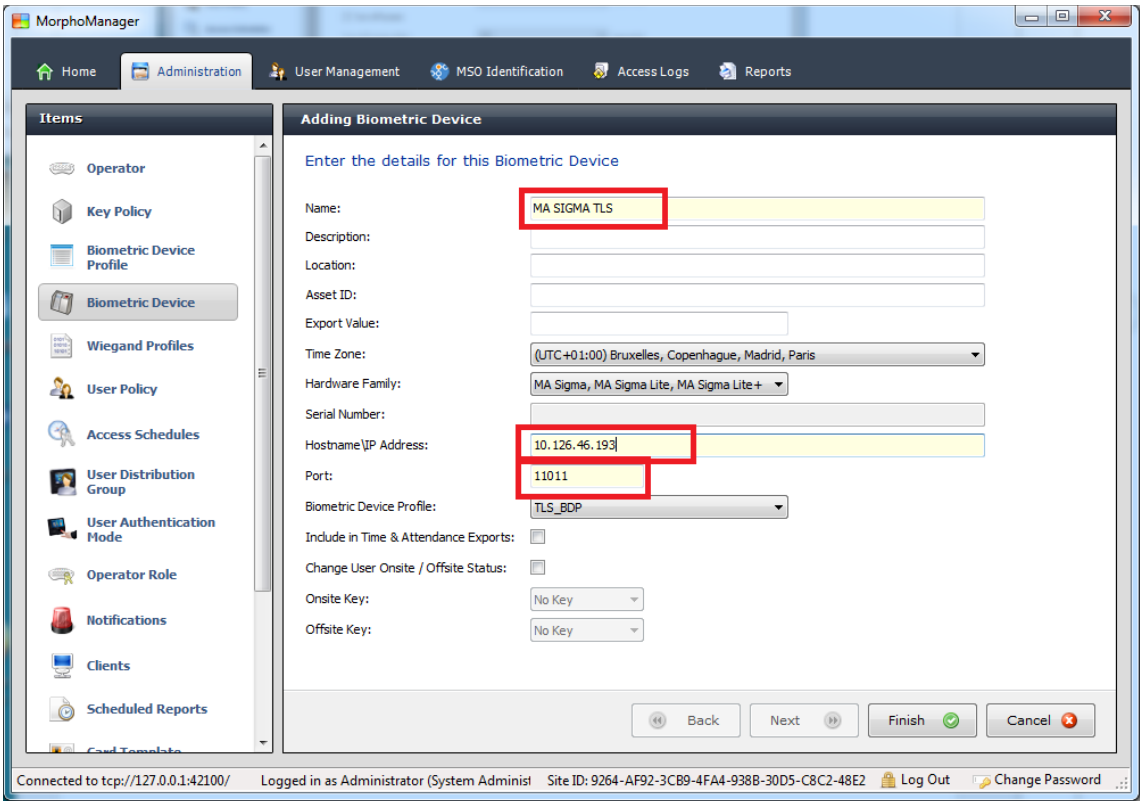
Keyboard Mode: QWERTY

Secure Communications Mode

Secure Communications Mode: ☑ Selecting this option will cause MorphoManager to attempt to connect to any 5G device using SSL. If the device is not configured correctly with the proper certificates present in the Key Policy, MorphoManager will not be able to connect to the device.

Connected to tcp://127.0.0.1:42100/ Logged in as Administrator (System Administ Site ID: 9264-AF92-3CB9-4FA4-938B-30D5-C8C2-48E2

Add a Biometric Device, name it (e.g. MA SIGMA TLS), select the correct Hardware Family, enter the Hostname/IP Address, change the port to the secured one (e.g. 11011), and select the correct Biometric Device Profile (e.g. TLS_BDP), and press the 'Finish' button.



Adding Biometric Device

Enter the details for this Biometric Device

Name: MA SIGMA TLS

Description:

Location:

Asset ID:

Export Value:

Time Zone: (UTC+01:00) Bruxelles, Copenhague, Madrid, Paris

Hardware Family: MA Sigma, MA Sigma Lite, MA Sigma Lite+

Serial Number:

Hostname\IP Address: 10.126.46.193

Port: 11011

Biometric Device Profile: TLS_BDP

Include in Time & Attendance Exports: □

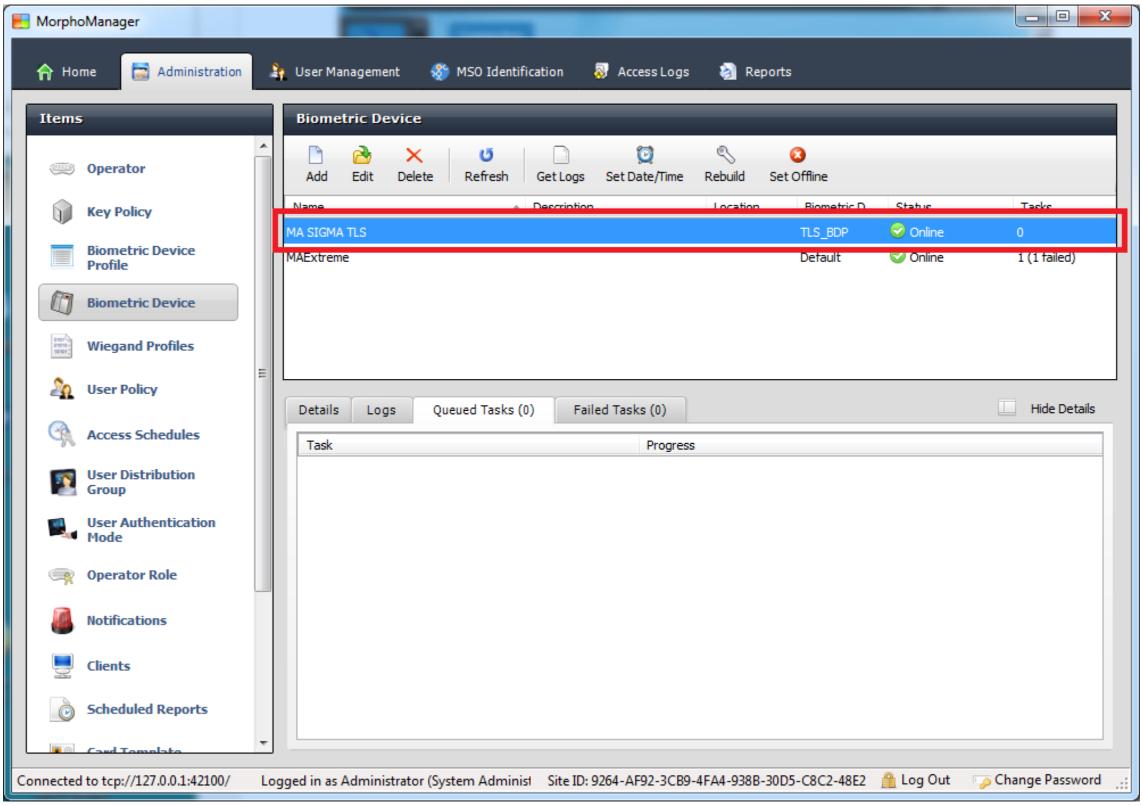
Change User Onsite / Offsite Status: □

Onsite Key: No Key

Offsite Key: No Key

Connected to tcp://127.0.0.1:42100/ Logged in as Administrator (System Administ Site ID: 9264-AF92-3CB9-4FA4-938B-30D5-C8C2-48E2

Then MorphoManager connects to the Biometric Terminal that will turn Online.



Name	Description	Location	Biometric D	Status	Tasks
MA SIGMA TLS			TLS_BDP	✓ Online	0
MAExtreme			Default	✓ Online	1 (1 failed)

Connected to tcp://127.0.0.1:42100/ Logged in as Administrator (System Adminis Site ID: 9264-AF92-3CB9-4FA4-938B-30D5-C8C2-48E2

Configuring SSL using MACI

To configure the terminal, the command:

`Morpho.MorphoAccess.Maci.Terminal.LoadSSLCertificates`

is to be used.

Please refer to MACI documentation for further details.

Annexe 1 : Bibliography

Documents concerning the Access and Time Biometric terminal

How to get the latest versions of documents

The latest version of the documents can be downloaded from our Website at the address below:

www.biometric-terminals.com

(Login and password required).

Access and Time Biometric documents available

Installation guides

These documents describe terminal electrical interfaces, connection procedures and installation procedures.

User's guides

These documents describe the different functions available on the terminal and how to configure the terminal.

Specific User's guides

These documents describe the functions available only with specific products.

Documents for software developers

These documents contain:

- description of all configuration parameters,
- description of all remote commands supported,
- description of all supported contactless cards (and the format of the data stored).

Annexe 2 : Support

Technical Support and Hotline

North America

Mail: support.bioterminals.us@idemia.com
Tel: +1 888 940 7477

South America

Mail: support.bioterminals.us@idemia.com
Tel: +1 714 575 2973

Asia, Pacific:

Mail: support.bioterminals.in@idemia.com
Tel: +91 1800 120 203 020

Europe, Middle-East, Africa

Mail: support.bioterminals@idemia.com
Tel: +33 1 30 20 30 40

Web site

For the latest firmware, software, document releases, and news, please check our websites :

www.biometric-terminals.com
(To get your log in and password please contact your sales representative).

Copyright © 2017 IDEMIA

Head office :

IDEMIA

2, place Samuel de Champlain

92400 Courbevoie France

www.idemia.com