ACCESS AND TIME BIOMETRIC TERMINALS
Customer Security Notice

July 2021

1. VULNERABILITY FIX

IDEMIA is releasing a new version of firmware integrating a fix for security vulnerabilities identified for the following terminals:

- Morpho*Wave* Compact
- VisionPass
- SIGMA Lite and Lite+
- SIGMA Wide
- SIGMA Extreme
- MA VP MD

Please refer to the Security Bulletin SB-IDEMIA-2021-01 for additional technical details.

2. COMPATIBILITY

For security reasons, once a terminal was upgraded to the released version, only subsequent firmware versions can be applied.

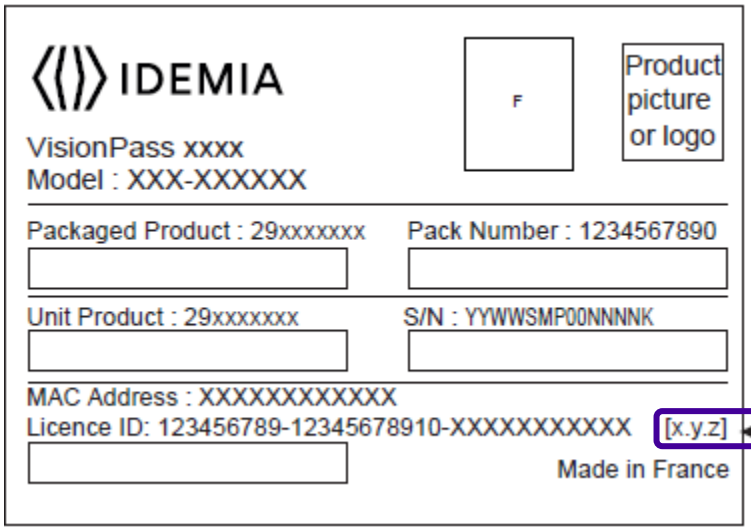
Should you use a terminal not operating with a generic firmware version or in case of any doubt, please contact your IDEMIA product reseller or our support teams before upgrading.

3. STRONG RECOMMENDATION TO USERS

IDEMIA strongly recommends that users of the aforementioned biometric terminals update their devices with versions listed in section 4, as promptly as possible. They now represent the baseline for future enhancements and maintenance.

If you have recently received or will soon receive one of the terminals listed in section 1, IDEMIA recommends to:

- Check the firmware version of the terminal (as documented on the box):



- Upgrade the firmware if the latest version is not already installed.

4. RESOLUTION & INSTALLATION

Vulnerabilities will be patched by upgrading your terminal to the latest available firmware, as noted in the table below. Versions can be downloaded via the IDEMIA customer portal:

Product	Firmware versions to install
MorphoWave Compact	2.6.2
VisionPass	2.6.2
SIGMA Lite	4.9.4
SIGMA Lite+	4.9.4
SIGMA Wide	4.9.4
SIGMA Extreme	4.9.4
MA VP MD	4.9.7

These versions do not deprecate any previous features, ensuring functional compatibility with existing systems. From now on, they are the only versions supported by IDEMIA.

Firmware upgrades can then be processed in different ways, as described in the dedicated documentation available here

5. NEED SUPPORT?

If you require support or assistance, please contact the following support teams by email or phone.

Region	Email	Phone
North America	support.bioterminals.us@idemia.com	+1 888 940 7477
South America	support.bioterminals.us@idemia.com	+1 714 575 2973
Europe, Middle-East, Africa	support.bioterminals@idemia.com	+33 1 30 20 30 40
Asia, Pacific	support.bioterminals.in@idemia.com	+91 8929159665
India	support.bioterminals.in@idemia.com	+91 1800 120 203 020

6. SECURITY AND PERSONAL DATA PROTECTION: GOOD PRACTICES

IDEMIA reminds you to follow these installation guidelines and best practices to enhance the security of your installation:

- Install the biometric terminals in an IP network behind a firewall. When possible, isolate it from the business network and from the Internet.
- Secure the IP communication with TLS.
- Regularly install the latest software updates made available by IDEMIA, to follow our current best practices.
- Periodically review your implementation strategy to ensure alignment with your corporate security policies.

IDEMIA also would like to take the opportunity of this Customer Security Notice to highlight available documentation explaining best practices and recommendations in terms of security and personal data protection. If you are a registered customer, you can find these documents on the IDEMIA customer portal. Otherwise, please ask your IDEMIA products reseller:

- GDPR compliance package - here
- Recommendations for a Secure Installation - here