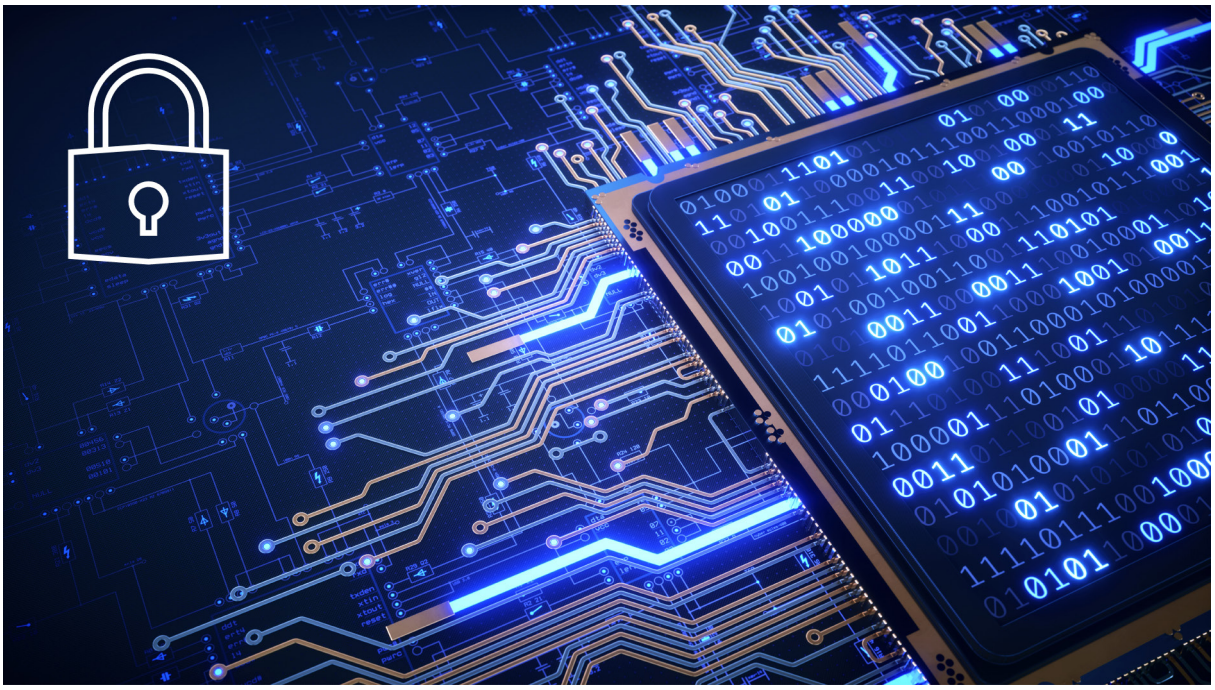
Honeywell
MORLEY IAS
FIRE SYSTEMS

Fire Safety



Cyber Security

Manual

M-167.7-MA-CS-EN / 03.2022

Intended purpose

This product may be used only for the applications outlined in the catalogue and in the technical description, and only in conjunction with the recommended and approved external devices and components.
This documentation contains registered and unregistered trademarks. All trademarks are the property of the respective owners. The use of this documentation does not grant you a licence or any other right to use any name, logo or label referred to or depicted herein.

The information contained in this documentation is provided without warranty.

Safety-related user information

This manual includes information required for the proper use of the products described.

In order to ensure correct and safe operation of the product, all guidelines concerning its transport, storage, installation, and mounting must be observed. This includes taking the necessary care when operating the product.

The term 'qualified personnel' in the context of the safety information included in this manual or on the product itself designates:

- project engineers who are familiar with the safety guidelines concerning fire alarm and extinguishing systems.
- trained service engineers who are familiar with the components of fire alarm and extinguishing systems and the information on their operation as included in this manual.
- trained installation or service personnel with the necessary qualifications for carrying out repairs on fire alarm and extinguishing systems, or who are authorised to operate, earth and label electrical circuits and/or safety equipment/systems.

Symbols

The following information is provided in the interests of personal safety and to prevent damage to the product described in this manual and all equipment connected to it.
Safety information and warnings to prevent hazards endangering the life and health of users and maintenance personnel, as well as causing damage to the equipment itself, are indicated by the following pictograms. Within the context of this manual, these pictograms have the following meanings:

Warning - designates risks for man and/or machine. Non-compliance will result in risks to man and/or machine. The level of risk is indicated by the word of warning.

Note - important information on a topic or a procedure and other important information.

Standards and guidelines - observe configuration and commissioning information in accordance with the national and local requirements.

Dismantling

In accordance with Directive 2012/19/EU (WEEE), after being dismantled, electrical and electronic equipment is taken back by the manufacturer for proper disposal.

Software Downloads
In order to supply the latest features and functionality in fire alarm and life safety technology to our customers, we make frequent upgrades to the embedded software in our products. To ensure that you are installing and programming the latest features, we strongly recommend that you download the most current version of software for each product prior to commissioning any system. Contact Technical Support with any questions about software and the appropriate version for a specific application.

Documentation Feedback
Your feedback helps us keep our documentation up-to-date and accurate. If you have any comments or suggestions about our online help or printed manuals, you can email us.
Please include the following information:

- Product name and version number (if applicable)
- Printed manual or online Help
- Topic Title (for online Help)
- Page number (for printed manual)
- Brief description of content you think should be improved or corrected
- Your suggestion for how to correct/improve documentation

Send email messages to:

FireSystems.TechPubs@honeywell.com

Please note this email address is for documentation feedback only. If you have any technical issues, please contact Technical Services.

This symbol (shown left) on the product(s) and / or accompanying documents means that used electrical and electronic products should not be mixed with general household waste. For proper treatment, recovery and recycling, contact your local authorities or dealer and ask for the correct method of disposal.
Electrical and electronic equipment contains materials, parts and substances, which can be dangerous to the environment and harmful to human health if the waste of electrical and electronic equipment (WEEE) is not disposed of correctly.

LEGAL NOTICES

Disclaimer
In no event shall Honeywell be liable for any damages or injury of any nature or kind, no matter how caused, that arise from the use of the equipment referred to in this manual.
Strict compliance with the safety procedures set out and referred to in this manual, and extreme care in the use of the equipment, are essential to avoid or minimize the chance of personal injury or damage to the equipment.
The information, figures, illustrations, tables, and specifications contained in this manual are believed to be correct and accurate as of the date of publication or revision. However, no representation or warranty with respect to such correctness or accuracy is given or implied and Honeywell will not, under any circumstances, be liable to any person or corporation for any loss or damages incurred in connection with the use of this manual.
The information, figures, illustrations, tables, and specifications contained in this manual are subject to change without notice.
In no event shall Honeywell be liable for any equipment malfunction or damages whatsoever, including (without limitation) incidental, direct, indirect, special, and consequential damages, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss, resulting from any violation of the above prohibitions.

Copyright Notice

Table of Contents

1 Section 1: Introduction 5
1.1 Assumptions and Prerequisites 5
1.2 Applicable Morley-IAS Products 5
1.3 Applicable Physical Connections 5
2 Section 2: General 6
2.1 Threats 6
2.2 Unauthorized Access 6
2.3 Viruses and Other Malicious Software Agents 6
2.4 User Access and Passwords 6
2.5 Memory Media 7
2.6 Software and Firmware Updates 7
2.7 Computers and Access 7
2.8 Decommission 8
2.8.1 Digital Signing 8
3 Section 3: Product Information 10
3.1 AGILE Wireless Fire Alarm System 10

1 Section 1: Introduction

This guide is intended to provide information on security risks and solutions associated with day-to-day use of Morley-IAS products.

1.1 Assumptions and Prerequisites

This guide assumes a high degree of technical knowledge and familiarity with:

- PC administration and operations systems
- Networking systems and concepts
- Security issues and concepts

1.2 Applicable Morley-IAS Products

- MA-1000
- MA-2000
- MA-8000

1.3 Applicable Physical Connections

Physical connections referred to in this manual include:

- Touch Screen/Front Panel
- USB Ports
- RS232 Port
- RS485 Port

2 Section 2: General

2.1 Threats

Security threats applicable to networked systems include unauthorized access, communication snooping, viruses and other malicious software agents.

2.2 Unauthorized Access

This threat includes physical access to the controller and intrusion into the network to which Morley-IAS equipment is connected.
Unauthorized external access can result in the following:

- Loss of system availability
- Incorrect execution of controls causing damage to the equipment
- Incorrect operation and/or spurious alarms
- Theft or damage to the contents of the system
- The capture and modification, or deletion of data causing possible liability to the install site and Honeywell Unauthorized access can result from lack of security of username and password information. Uncontrolled access to the equipment, and uncontrolled, unsecured access to the network.

2.3 Viruses and Other Malicious Software Agents

Malicious Software includes the following:

- Viruses
- Spyware
- Worms
- Trojans

These may be present on a computer which is used for PC configuration software, such as Morley-IAS Programming Tool, that is used to create system configuration to be downloaded into the FACP or modify system configuration uploaded from FACP.
The intrusion of malicious software agents can result in performance degradation, loss of system availability, and the capture, modification, or deletion of data, including configuration, and device logs. Viruses can be transferred by USB devices from other infected systems on the network or malicious internet sites.

2.4 User Access and Passwords

Good password security practices should be followed. This includes ensuring the physical security of passwords and keeping passwords secure. For password protected products, observe the following good practice:

- Ensure physical security of passwords. Avoid writing passwords where they can be seen by unauthorized personnel
- Do not use personally identifiable information as a password, such as social security numbers, addresses, birth dates etc.
- Set the minimum level of access for each user. Do not provide users with privileges they do not need

2.5 Memory Media

Use only authorized removable media that has been scanned and checked for viruses and malware using up to date anti-virus software.
Ensure that memory media is not used for other purposes to avoid risk of infection. Control access to media containing backups to avoid risk of tampering.

2.6 Software and Firmware Updates

System software and firmware updates may be offered from time to time. Ensure that your local representative has up to date contact details and periodically visit the Morley-IAS web site for up-to-date product information.

2.7 Computers and Access

Good security practice should be observed on any PC connecting to Morley-IAS equipment. Operating systems and software should be kept up to date by installing the manufacturers updates, as well as maintaining up to date anti-virus software on all computers which may be directly connected or via a network. Ensure that the computers are regularly scanned for viruses. Only allow files and software from trusted sources to be installed and used on associated computers to avoid malicious software installs. Use only authorized removable media, e.g. CD, DVD, external hard drives, USB memory sticks that have been scanned using up to date anti-virus software.

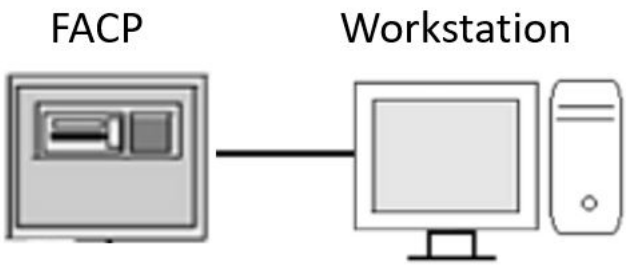


Fig. 1: CLSS Example of connection via VPN

2.8 Decommission

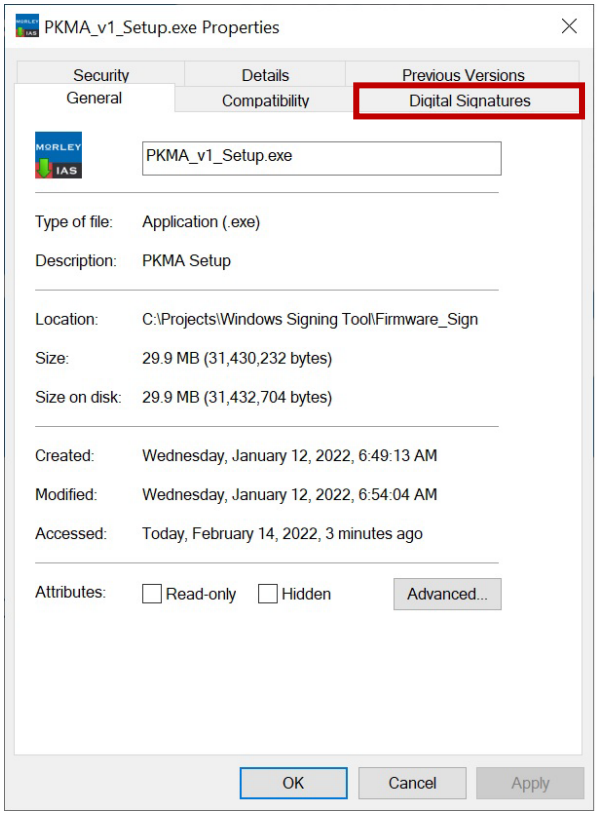
When decommission the system, set the configuration for the panel to default, delete all access accounts and set the master password to a random password on the panel. Delete all configuration files and uninstall associated software from the PC.

2.8.1 Digital Signing

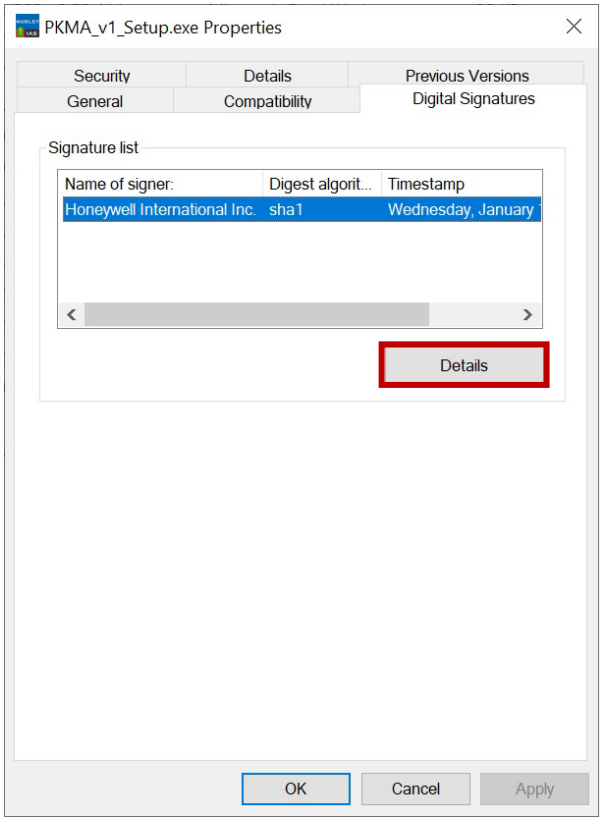
The application setup package is digitally signed using a certificate. A digital signature certificate is used to authenticate the identity of the sender/signer of a document/file and ensure that the original content of the document/file that has been sent is unchanged in transit.
The certification authority used for signing the product installer package is DigiCert® (DigiCert, Inc.).
Website URL: **www.digicert.com**

If an installer package is digitally signed, perform the following steps:

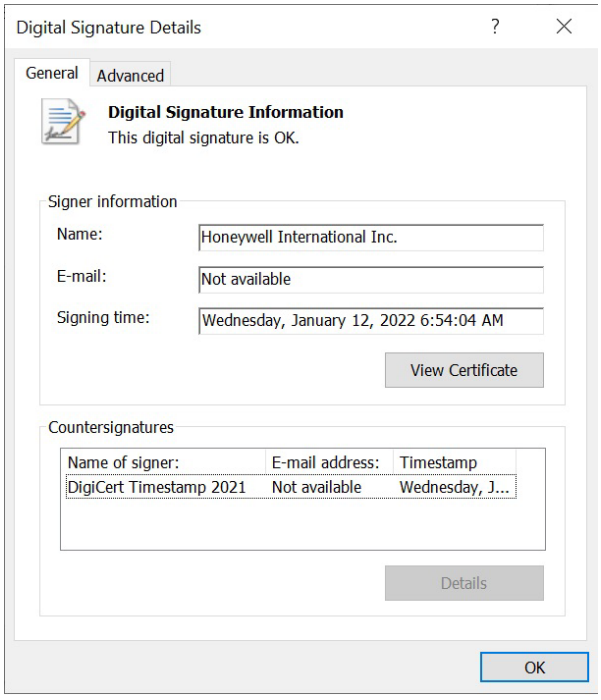
1. Right click the setup file and select **Properties**. Go to the **Digital Signatures** tab in the properties window. If you see signatures listed on the tab, you know that the file has been signed digitally.



2. Under Signature list, select the signature, and click **Details**.



3. You will see information regarding the Code Signing certificate that was used to sign the executable. On the next tab under **Countersignatures**, it will list an entry for a timestamping. If this field is blank, no timestamp exists on this code.



4. You may click on **View Certificate** to display the signature or click on the **Advanced** tab to display signature details as well.

Windows installer verifies the Digital Signatures of the installer packages before installing. To verify the signature manually, use the SignTool that comes with Windows SDK or the utility provided by DigiCert available for download at **https://www.digicert.com/util/DigiCertUtil.exe.**

3 Section 3: Product Information

CAUTION:
CYBERSECURITY RISK
FAILURE TO COMPLY WITH THE RECOMMENDED SECURITY PRACTICES MAY PLACE YOUR SYSTEM AT RISK.

3.1 AGILE Wireless Fire Alarm System

The following Cybersecurity practices are highly recommended when using AGILE Tools:

- When using AGILE Tools to update the firmware of the gateway or gateway devices, ensure updates are performed on a secure/encrypted Wi-Fi Network.
- Ensure the PC running AGILE Tools has full disk encryption. Full encryption of any backed-up data is also recommended.
- The wireless gateway should be secured in a location which is only accessible to authorized personnel.
- When any AGILE gateway or device is decommissioned from service, return the equipment to the factory default state.

Notes

Honeywell
MORLEY IAS Fire Systems
(Pittway Tecnologica, S.r.l.)
Via Caboto, 19/3
34147 Trieste, Italy

M-167.7-MA-CS-EN / 03.2022

Technical changes reserved!