Cybersecurity

Product Security

Document LS10217-000FX-E Rev: A
2/27/2024 ECN: 00045003

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

Find out more at www.fiplex.com.

Table of Contents

Section 1: Introduction

This guide is intended to provide information on security risks and solutions associated with day-to-day use of Fiplex 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 Fiplex Products

- Flex DAS
- Flex BDA
- Flex All-in-One
- Flex BBU (Battery Backup Units)
- pFOMS (Portable Fiplex Operation and Maintenance Software)
- FCS (Fiplex Control Software)

1.3 Applicable Physical Connections

Physical connections referred to in this manual include:

- USB Ports
- Ethernet Port

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 device and intrusion into the connectors to which and from which the devices connect. 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 computer from which the user connects to the device.

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 .

The intrusion of malicious software agents can result in performance degradation, loss of system availability, and the capture, modification, and/or deletion of data, including configuration and device logs. Viruses can be transferred in many ways, such as via USB devices, other infected systems on the network, malicious Internet sites, and e-mail attachments.

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.
- Make sure passwords contain characters, numbers, and a mix of lower and uppercase letters.
- Passwords should be complex enough as to not be easily guessed and should not contain phrases used in common speech.
- Do not use personally identifiable information as a username or password, such as social security numbers, addresses, birth dates etc.

2.5 Memory Media

Use only authorized removable media that has been scanned and checked for viruses and malware using current antivirus 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 periodically. Check to see if the software programming tools warns about the existence of a new software release. Also, periodically visit the Fiplex website for current product information.

2.7 Computers and Access

Good security practice should be observed on any PC connecting to Fiplex equipment. Operating systems and software should be kept current by installing the manufacturer's updates, as well as maintaining the latest antivirus 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 antivirus software.

2.8 Networks, Firewalls, and VPN Connections

Today, computers are periodically or always connected to a network, either public or private. Using a firewall is an industry-proven way to avoid most incoming malicious traffic. Ensure you have your firewall enabled. Where access from untrusted networks is required, such as Internet access, Fiplex strongly recommends the use of a VPN to ensure the security of the connection.

Note that Microsoft Windows does have a built-in firewall enabled by default. Furthermore, almost any modern antivirus software does provide its own firewall which overrides the one provided by the PC's operating system. Ensure that the firewall provided by the antivirus software is also enabled.

Section 3: Product Information

CAUTION: CYBERSECURITY RISK

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

3.1 Flex BDA, Flex DAS, Flex BBUs, and Flex All-in-One

Take the following into consideration to prevent cybersecurity risks with your devices.

- Upon receiving any products, visually inspect the products for tampering and authenticity.
- Install products in a secure location in a secure way, considering both software and hardware vulnerabilities including any physical security pre-requisites, wiring, or conduit considerations.
- Physically protect non-authorized access to the device hardware.
- Physically protect transmission channels as required.
- Change the default password to a unique one and store it on a safe location.
- When configuring a product, only enable required features for the task at hand and adjust the setting to minimum to reduce threat scope.
- Securely use the product, including any special security provisions such as monitoring, logging, privacy compliance, etc.
- Develop a Disaster and Recovery Plan.
- Develop a Backup and Recovery Strategy.
- Install, configure, and maintain antivirus software on all computers which access a Flex device.
- Train end-users on security maintenance tasks upon system delivery.

3.2 pFOMS and Fiplex Control Software

- Install, configure, and maintain antivirus software on all computers which access a Flex device.
- Keep the computer's Operating System updated.
- Check that the software is current by visiting Fiplex's website periodically.
- Check the signature of the installed software.
- Train end-users on software use, because improper use of this software, when a connected to a device, can result in improper configurations, which can affect device operation.

Section 4: Decommission or Uninstallation of the Product

If you need to remove or uninstall the product, follow these steps:

- Reset the device to default values.
- Turn off the device and remove its RF connectors.
- Ensure that trained personnel execute this job, as the device can be damaged if not handled properly.
- For PC tools, delete all configuration files and uninstall pFOMS and/or Fiplex Control Software. Use disk-wiping tool to prevent someone from recovering deleted files.

Fiplex Communications Inc.
2101 NW 79th Avenue Miami, FL 33122
+1 (305) 884-899
info@fiplex.com

fiplex
by Honeywell