Honeywell | Farenhyt™ Series

SWIFT®

Smart Wireless Integrated Fire Technology

Instruction Manual

Document LS10036-000FH-E Rev: G
4/13/2020 ECN: 150692

Fire Alarm & Emergency Communication System Limitations

While a life safety system may lower insurance rates, it is not a substitute for life and property insurance!

An automatic fire alarm system—typically made up of smoke detectors, heat detectors, manual pull stations, audible warning devices, and a fire alarm control panel (FACP) with remote notification capability—can provide early warning of a developing fire. Such a system, however, does not assure protection against property damage or loss of life resulting from a fire.

An emergency communication system—typically made up of an automatic fire alarm system (as described above) and a life safety communication system that may include an autonomous control unit (ACU), local operating console (LOC), voice communication, and other various interoperable communication methods—can broadcast a mass notification message. Such a system, however, does not assure protection against property damage or loss of life resulting from a fire or life safety event.

The Manufacturer recommends that smoke and/or heat detectors be located throughout a protected premises following the recommendations of the current edition of the National Fire Protection Association Standard 72 (NFPA 72), manufacturer's recommendations, State and local codes, and the recommendations contained in the Guide for Proper Use of System Smoke Detectors, which is made available at no charge to all installing dealers. This document can be found at http://www.systemsensor.com/appguides/. A study by the Federal Emergency Management Agency (an agency of the United States government) indicated that smoke detectors may not go off in as many as 35% of all fires. While fire alarm systems are designed to provide early warning against fire, they do not guarantee warning or protection against fire. A fire alarm system may not provide timely or adequate warning, or simply may not function, for a variety of reasons:

Smoke detectors may not sense fire where smoke cannot reach the detectors such as in chimneys, in or behind walls, on roofs, or on the other side of closed doors. Smoke detectors also may not sense a fire on another level or floor of a building. A second-floor detector, for example, may not sense a first-floor or basement fire.

Particles of combustion or "smoke" from a developing fire may not reach the sensing chambers of smoke detectors because:

- Barriers such as closed or partially closed doors, walls, chimneys, even wet or humid areas may inhibit particle or smoke flow.
- Smoke particles may become "cold," stratify, and not reach the ceiling or upper walls where detectors are located.
- Smoke particles may be blown away from detectors by air outlets, such as air conditioning vents.
- Smoke particles may be drawn into air returns before reaching the detector.

The amount of "smoke" present may be insufficient to alarm smoke detectors. Smoke detectors are designed to alarm at various levels of smoke density. If such density levels are not created by a developing fire at the location of detectors, the detectors will not go into alarm.

Smoke detectors, even when working properly, have sensing limitations. Detectors that have photoelectronic sensing chambers tend to detect smoldering fires better than flaming fires, which have little visible smoke. Detectors that have ionizing-type sensing chambers tend to detect fast-flaming fires better than smoldering fires. Because fires develop in different ways and are often unpredictable in their growth, neither type of detector is necessarily best and a given type of detector may not provide adequate warning of a fire.

Smoke detectors cannot be expected to provide adequate warning of fires caused by arson, children playing with matches (especially in bedrooms), smoking in bed, and violent explosions (caused by escaping gas, improper storage of flammable materials, etc.).

Heat detectors do not sense particles of combustion and alarm only when heat on their sensors increases at a predetermined rate or reaches a predetermined level. Rate-of-rise heat detectors may be subject to reduced sensitivity over time. For this reason, the rate-of-rise feature of each detector should be tested at least once per year by a qualified fire protection specialist. Heat detectors are designed to protect property, not life.

IMPORTANT! Smoke detectors must be installed in the same room as the control panel and in rooms used by the system for the connection of alarm transmission wiring, communications, signaling, and/or power. If detectors are not so located, a developing fire may damage the alarm system, compromising its ability to report a fire.

Audible warning devices such as bells, horns, strobes, speakers and displays may not alert people if these devices are located on the other side of closed or partly open doors or are located on another floor of a building. Any warning device may fail to alert people with a disability or those who have recently consumed drugs, alcohol, or medication. Please note that:

- An emergency communication system may take priority over a fire alarm system in the event of a life safety emergency.
- Voice messaging systems must be designed to meet intelligibility requirements as defined by NFPA, local codes, and Authorities Having Jurisdiction (AHJ).
- Language and instructional requirements must be clearly disseminated on any local displays.
- Strobes can, under certain circumstances, cause seizures in people with conditions such as epilepsy.
- Studies have shown that certain people, even when they hear a fire alarm signal, do not respond to or comprehend the meaning of the signal. Audible devices, such as horns and bells, can have different tonal patterns and frequencies. It is the property owner's responsibility to conduct fire drills and other training exercises to make people aware of fire alarm signals and instruct them on the proper reaction to alarm signals.
- In rare instances, the sounding of a warning device can cause temporary or permanent hearing loss.

A life safety system will not operate without any electrical power. If AC power fails, the system will operate from standby batteries only for a specified time and only if the batteries have been properly maintained and replaced regularly.

Equipment used in the system may not be technically compatible with the control panel. It is essential to use only equipment listed for service with your control panel.

Telephone lines needed to transmit alarm signals from a premises to a central monitoring station may be out of service or temporarily disabled. For added protection against telephone line failure, backup radio transmission systems are recommended.

The most common cause of life safety system malfunction is inadequate maintenance. To keep the entire life safety system in excellent working order, ongoing maintenance is required per the manufacturer's recommendations, and UL and NFPA standards. At a minimum, the requirements of NFPA 72 shall be followed. Environments with large amounts of dust, dirt, or high air velocity require more frequent maintenance. A maintenance agreement should be arranged through the local manufacturer's representative. Maintenance should be scheduled as required by National and/or local fire codes and should be performed by authorized professional life safety system installers only. Adequate written records of all inspections should be kept.

Limit-D2-2016

Installation Precautions

Adherence to the following will aid in problem-free installation with long-term reliability:

WARNING - Several different sources of power can be connected to the fire alarm control panel. Disconnect all sources of power before servicing. Control unit and associated equipment may be damaged by removing and/or inserting cards, modules, or interconnecting cables while the unit is energized. Do not attempt to install, service, or operate this unit until manuals are read and understood.

CAUTION - System Re-acceptance Test after Software Changes: To ensure proper system operation, this product must be tested in accordance with NFPA 72 after any programming operation or change in site-specific software. Re-acceptance testing is required after any change, addition or deletion of system components, or after any modification, repair or adjustment to system hardware or wiring. All components, circuits, system operations, or software functions known to be affected by a change must be 100% tested. In addition, to ensure that other operations are not inadvertently affected, at least 10% of initiating devices that are not directly affected by the change, up to a maximum of 50 devices, must also be tested and proper system operation verified.

This system meets NFPA requirements for operation at 0-49º C/ 32-120º F and at a relative humidity 93% ± 2% RH (non-condensing) at 32°C ± 2°C (90°F ± 3°F). However, the useful life of the system's standby batteries and the electronic components may be adversely affected by extreme temperature ranges and humidity. Therefore, it is recommended that this system and its peripherals be installed in an environment with a normal room temperature of 15-27º C/60-80º F.

Verify that wire sizes are adequate for all initiating and indicating device loops. Most devices cannot tolerate more than a 10% I.R. drop from the specified device voltage.

Like all solid state electronic devices, this system may operate erratically or can be damaged when subjected to lightning induced transients. Although no system is completely immune from lightning transients and interference, proper grounding will reduce susceptibility. Overhead or outside aerial wiring is not recommended, due to an increased susceptibility to nearby lightning strikes. Consult with the Technical Services Department if any problems are anticipated or encountered.

Disconnect AC power and batteries prior to removing or inserting circuit boards. Failure to do so can damage circuits.

Remove all electronic assemblies prior to any drilling, filing, reaming, or punching of the enclosure. When possible, make all cable entries from the sides or rear. Before making modifications, verify that they will not interfere with battery, transformer, or printed circuit board location.

Do not tighten screw terminals more than 9 in-lbs. Over-tightening may damage threads, resulting in reduced terminal contact pressure and difficulty with screw terminal removal.

This system contains static-sensitive components. Always ground yourself with a proper wrist strap before handling any circuits so that static charges are removed from the body. Use static suppressive packaging to protect electronic assemblies removed from the unit.

Units with a touchscreen display should be cleaned with a dry, clean, lint free/microfiber cloth. If additional cleaning is required, apply a small amount of Isopropyl alcohol to the cloth and wipe clean. Do not use detergents, solvents, or water for cleaning. Do not spray liquid directly onto the display.

Follow the instructions in the installation, operating, and programming manuals. These instructions must be followed to avoid damage to the control panel and associated equipment. FACP operation and reliability depend upon proper installation.

Precau-D2-11-2017

FCC Warning

WARNING: This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual may cause interference to radio communications. It has been tested and found to comply with the limits for class A computing devices pursuant to Subpart C of Part 15 of FCC Rules, which is designed to provide reasonable protection against such interference when devices are operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user will be required to correct the interference at his or her own expense.

Canadian Requirements

This digital apparatus does not exceed the Class A limits for radiation noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le present appareil numerique n'emet pas de bruits radioelectriques depassant les limites applicables aux appareils numeriques de la classe A prescrites dans le Reglement sur le brouillage radioelectrique edicte par le ministere des Communications du Canada.

Farenhyt™ is a trademark; and **eVance®, Honeywell®**, **Silent Knight®** and **SWIFT®** are registered trademarks of Honeywell International Inc. **Microsoft®** and **Windows®** are registered trademarks of the Microsoft Corporation. **Chrome™** and **Google™** are trademarks of Google Inc. **Firefox®** is a registered trademark of The Mozilla Foundation.

©2020 by Honeywell International Inc. All rights reserved. Unauthorized use of this document is strictly prohibited.

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.

Table of Contents

Section 1: Overview 8
1.1: Purpose 8
1.2: Assumed Knowledge 8
1.3: Additional References 8
1.4: About this Manual 8
1.5: About the Mesh Network 9
1.6: Abbreviations 9
1.7: Cybersecurity Recommendations 9

Section 2: WIDP-WGI Wireless System Gateway 10
2.1: Description 10
2.2: Agency Approvals 10
2.2.1: FCC 10
2.2.2: Federal Institute of Telecommunications 10
2.3: Specifications 10
2.3.1: Environmental Specifications 11
2.4: Magnetic Sensors 11
2.4.1: Mesh Formation Magnetic Sensor 11
2.4.2: Magnetic Sensor 11
2.5: LED Indicators 11
2.6: Installing the Gateway 11
2.6.1: Before Installing 11
2.7: Mounting and Wiring 12
2.7.1: Mounting 12
2.7.2: Wiring 13
2.7.3: Gateway Powered by the SLC 14
2.7.4: Gateway Powered by an External, Regulated +24VDC Source 14
2.8: Configuration and Programming 15
2.8.1: Assign a Profile 15
2.8.2: Remove a Profile 16
Remove a Profile from a Gateway using SWIFT Tools 16
Remove a Profile from a Gateway without using SWIFT Tools 17
2.8.3: Create a Mesh Network 17
2.8.4: SLC Configuration 18
2.9: Operations 19
2.9.1: Modes of Operation 19
Start-up Mode 19
Factory Default Mode 19
Profile Configured 19
Mesh Formation 19
Initial Mesh Restructuring Mode 20
Normal Mode 20
Rescue Mode 20
Mesh Restructuring Mode 20
Bootloader Mode 20
Mesh Upgrade 20
Neighboring Network Scan 20
2.9.2: LED Patterns 20
2.9.3: Lock/Unlock the Gateway 20
Lock/Unlock the Gateway Using SWIFT Tools 20
Password Reset 22
2.9.4: Enable/Disable Max Gateway Trouble Reporting 22
Completed Wireless Network 22
Possible Wireless Mesh Overlap 22
Disabling Max Gateway Reporting 25
2.9.5: Weak Link Trouble Reporting 26
Disable Trouble Reporting at the Gateway Using SWIFT Tools 26
2.9.6: Collapse Network Command 26
Collapse Mesh Network Using SWIFT Tools 26
2.9.7: Silence Network Command 27
Silence Mesh Network Using SWIFT Tools 27

2.9.8: Overlapping Wireless Sensor Networks and Limitations....28
2.9.9: Activation of Wireless Output Devices....28
2.9.10: Avoiding RF Interference....28
2.9.11: Trouble Messages....29

Section 3: Wireless Devices....30
3.1: Description....30
3.2: Agency Approvals....31
3.2.1: FCC....31
3.2.2: Federal Institute of Telecommunications....31
3.3: Specifications....32
3.4: Installing, Mounting, and Wiring Devices....32
3.4.1: Batteries....32
3.5: Configuration and Programming....32
3.5.1: Assigning Profiles....32
3.5.2: Mesh Formation....33
Repeater....33
3.5.3: Restoring a Device to Factory Default....33
3.6: Device Operations....35
3.6.1: Modes of Operation....35
Factory Default Mode....35
Site Survey Mode....35
Profile Assigned Mode....35
Bootloader Mode....35
Mesh Participant Modes....35
3.6.2: LED Indicators....36
3.6.3: Trouble Conditions....36
Trouble Conditions with Fire Protection....36
Trouble States without Fire Protection....36

Section 4: W-SYNC Wireless Synchronization Module....38
4.1: Description....38
4.2: Wiring....38
4.2.1: FACP....38
4.2.2: HPFF8/HPFF12 NAC Expander....39

Section 5: W-USB Adapter....40
5.1: Introduction....40
5.2: Agency Approvals....40
5.2.1: FCC....40
5.2.2: Federal Institute of Telecommunications....40
5.3: Specifications....41
5.3.1: Electrical Specifications....41
5.3.2: Serial Communication Specification....41
5.3.3: Mechanical Specifications....41
5.3.4: Environmental Specifications....41
5.4: Driver Installation....41

Appendix A: SWIFT Tools....44
A.1: Description....44
A.2: Launching SWIFT Tools....44
A.2.1: Creating a New Jobsite....44
A.2.2: Opening an Existing Jobsite....45
A.3: Connecting to the Gateway....45
A.3.1: Accessing a Locked Gateway....45
A.3.2: Creating a New Password for a Gateway....45

Appendix B: Site Survey....46
B.1: Conduct a Site Survey....46
B.1.1: Link Quality Test....46
Basic Requirements of a Link Quality Test....46
Conduct a Link Quality Test....46
Results of a Link Quality Test....47
After a Link Quality Test....47

B.1.2: RF Scan Test 47
Conduct an RF Scan Test 47
Status of an RF Scan Test 47
B.1.3: Retrieving Site Survey Results 48
Appendix C: Troubleshooting and Testing 49
C.1: Troubleshooting 49
C.2: Testing the Gateway and Devices 50
C.2.1: Testing LED Indicators 50
C.3: Testing the Wireless Network 50
C.3.1: Network Topology 51
Parent-Child Devices 51
Orphan Devices 51
Class A Compliance 51
C.3.2: History Events 51
C.3.3: Network Snapshots 51
C.3.4: Network Statistics 51
C.3.5: Device Attributes 51
Appendix D: LED Indicators 53
Appendix E: Firmware Upgrade/Downgrade Instructions 58
E.1: W-USB Adapter Upgrade Procedure 58
E.2: Mesh Network Firmware Upgrade/Downgrade Procedure 59
E.3: Device and Gateway Firmware Upgrade/Downgrade Procedure 59
E.4: Distributed Firmware Updates 60
Index 61

Section 1: Overview

1.1 Purpose

The SWIFT® Network Manual provides an overview of the following:

- Wireless fire alarm system
- Instructions for installing and configuring the wireless devices
- Information on monitoring the status of the wireless devices
- Removal and replacement procedures of the Wireless Gateway
- Testing, maintenance, and firmware upgrade information of the Wireless Gateway

1.2 Assumed Knowledge

This document is created with the assumption that all users are familiar with working on a PC and laptop for configuration purposes. Installers should be familiar with the fire alarm and related service standards. The terminology and level of details of this document reflect this assumption.

1.3 Additional References

The table below provides a list of documents referenced in this manual, as well as documents for selected other compatible devices.

IFP-2100/ECS Fire Alarm Control Panel	LS10143-001SK-E
IFP-300/ECS Fire Alarm Control Panel	LS10145-001SK-E
IFP-75 Fire Alarm Control Panel	LS10147-001SK-E
WIDP-PHOTO Wireless Photo Detector	I56-4273
WIDP-ACCLIMATE Wireless Acclimate Detector	I56-4273
WIDP-HEAT-ROR Wireless Rate Of Rise Heat Detector	I56-4274
WIDP-HEAT Wireless Fixed Heat Detector	I56-4274
WIDP-MONITOR Wireless Monitor Module	I56-4275
WIDP-RELAY Wireless Relay Module	I56-4276
WIDP-PULL-DA Wireless Pullstation	I56-6562
B210W Wireless Detector Base	I56-4064
WAV-RL Red Wall AV Base	I56-6517
WAV-WL White Wall AV Base	I56-6517
WAV-CRL Red Ceiling AV Base	I56-6517
WAV-CWL White Ceiling AV Base	I56-6517
SWIFT Wireless AV Bases	I56-6517
W-SYNC Wireless Sync Module	I56-6518
MDL3 Sync Module	I56-3157
HPFF8 NAC Expander	53499
HPFF12 NAC Expander	53576

1.4 About this Manual

This manual correlates with SWIFT Tools version 4.0 (and higher) and the programming features included in that release. Devices not running the current version of the software will not have the same capabilities. Ensure the latest version of SWIFT Tools is installed for proper functionality.

Systems running version 4.0 (and higher) will:

- require device tamper to remove a profile (return to factory default) with a 60 minute timeout.
- have option to enable/disable max gateway trouble reporting.
- require device tamper to upgrade the firmware on individual devices.

Systems running 4.0 (and higher) will not be able to:

- create profiles in the gateway without using SWIFT Tools.
- distribute profiles from the gateway to devices.
- use devices as profile distributors.

1.5 About the Mesh Network

All devices within the mesh network must be running the same firmware version. Refer to Appendix E, “Firmware Upgrade/Downgrade Instructions” for more information.

Use of these products in combination with non-Honeywell products in a wireless mesh network, or to access, monitor, or control devices in a wireless mesh network via the internet or another external wide area network, may require a separate license from Sipco, LLC. For more information, contact Sipco, LLC or IntusIQ (Ipco), LLC at 8215 Roswell Rd, Building 900, Suite 950. Atlanta, GA 30350, or at www.sipcollc.com or www.intusiq.com.

1.6 Abbreviations

The following table lists the abbreviations and their definitions used in this manual.C

Abbreviation	Definition
AHJ	Authority Having Jurisdiction
ANSI	American National Standards Institute
dBm	Units of RF power (0dBm = 1mW)
FACP	Fire Alarm Control Panel
FCC	Federal Communications Commission
ISM Band	Industrial, Scientific and Medical Radio Bands
LCD	Liquid Crystal Display
LED	Light Emitting Diode
mA	Milliampere
MHz	Megahertz
NFPA	National Fire Protection Association
PC	Personal Computer
RF	Radio Frequency
SLC	Signaling Line Circuit
UI	User Interface
UL	Underwriters Laboratories
WIDP-WGI	Wireless Gateway

1.7 Cybersecurity Recommendations

- When using SWIFT Tools to update the firmware of the gateway or devices, ensure updates are performed in a secure location where no eavesdropping on the wireless signals is possible.
- Ensure the PC running SWIFT 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 SWIFT gateway or device is decommissioned from service, return the equipment to the factory default state by removing profiles.

Section 2: WIDP-WGI Wireless System Gateway

2.1 Description

The WIDP-WGI is a device in a wireless fire system that acts as a bridge between fire alarm control panels (FACPs) and wireless fire devices. All wireless fire devices communicate with the gateway over the wireless network formed by the devices and the gateway.

The gateway is powered by either the SLC loop or by any external +24VDC UL listed power supply. The gateway uses the IDP protocol on the SLC to communicate with the panel and a proprietary wireless protocol to communicate with wireless fire devices. The following graphic is an illustration of the components of the SWIFT Network.

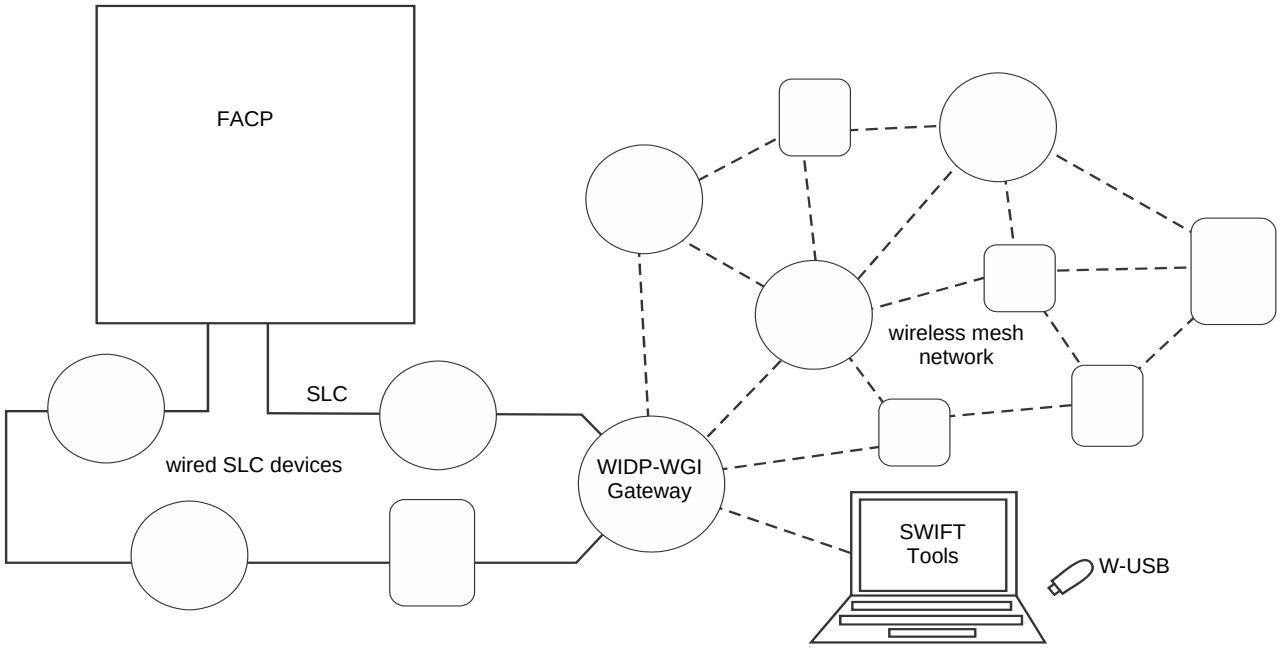


Figure 2.1 SWIFT Network

2.2 Agency Approvals

2.2.1 FCC

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.
3. **FCC ID: PV3WFSGW**

WARNING: DO NOT MAKE CHANGES TO THE EQUIPMENT

CHANGES OR MODIFICATIONS NOT EXPRESSLY APPROVED BY THE MANUFACTURER COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

2.2.2 Federal Institute of Telecommunications

This device utilizes the Honeywell915 rev A radio module and complies with IFETEL standard(s).

IFT: RCPHOSW14-1983

2.3 Specifications

Following are the specifications of the wireless gateway.

Specifications	Data
External Supply Electrical Ratings	18V-30V
SLC Electrical Ratings	15V-30V
Maximum current when using the external supply	40mA
Maximum current when using the SLC power supply	24mA
Maximum SLC Resistance	50Ω
Minimum signal strength level needed at the receiver for a primary path with weak link trouble reporting enabled.	-55dBm

Minimum signal strength level needed at the receiver for a secondary path or primary path with weak link trouble reporting disabled.	Must be 18 dBm higher than the noise floor down to a minimum of -80dBm[1]
Maximum ambient noise level	-85dBm[1]
Maximum RF Power Output	+17dBm (Tx power level without antenna)
Radio Frequency	Lower ISM Band (902 - 928MHz).

1 Ensure that the primary path signal strength level is within recommended guidelines to assure proper communication in the mesh network.

2.3.1 Environmental Specifications

System	Operating Temperature	Storage Temperature	Humidity
Gateway	0°C-49°C / 32°F-120°F	-10°C- 60°C / 14°F-140°F	10 to 93% RH, Non-condensing

2.4 Magnetic Sensors

Magnets must have a holding strength of 10 lbs or greater. Use either the north or south pole of the magnet to activate sensors.

2.4.1 Mesh Formation Magnetic Sensor

The mesh formation magnetic sensor (refer to Figure 2.2) transitions the gateway in and out of mesh formation mode. The initial activation of the sensor puts the gateway in mesh formation mode (as long as it contains a profile). A subsequent activation of the magnetic sensor transitions the gateway out of mesh formation and into the initial mesh restructuring and normal mode. The gateway can be placed back into mesh formation mode by activating the magnet sensor once again. The LED next to the profile magnet sensor turns on green for ½ a second when the sensor is activated..

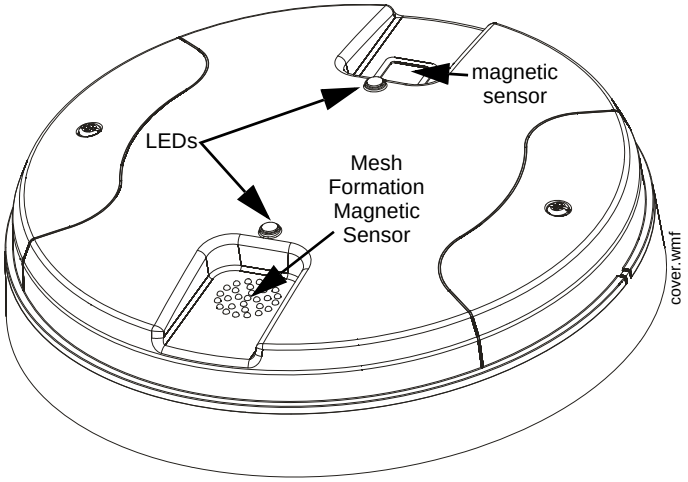


Figure 2.2 LEDs and Mesh Formation Sensor on the WIDP-WGI

2.4.2 Magnetic Sensor

The square magnetic sensor can be used to start a communication session with SWIFT Tools. See Section A.3 on page 45 for more information.

2.5 LED Indicators

The two LEDs on the gateway blink in the same pattern to allow the LED to be viewed from any angle. LED patterns are explained in Appendix D.

2.6 Installing the Gateway

2.6.1 Before Installing

Choose a location for the gateway that is clean, dry, and vibration-free. The area should be readily accessible with sufficient room to easily install and maintain the gateway. Metal obstructions impede the radio frequency communication and should be avoided. Carefully unpack the system and inspect for shipping damage if any. All wiring must comply with the national and local codes for fire alarm systems.

2.7 Mounting and Wiring

WARNING: POLYPROPYLENE ELECTRICAL INSULATION MATERIAL

ENSURE THAT THE POLYPROPYLENE ELECTRICAL INSULATION MATERIAL COVERING THE PRINTED CIRCUIT BOARD INSIDE THE GATEWAY IS NOT REMOVED OR TAMPERED WHILE INSTALLING OR CLEANING.

2.7.1 Mounting

The gateway has two major pieces, the cover and the mounting plate. The mounting plate is mounted to the wall or ceiling, and field wiring is connected to it. The cover contains the printed circuit board and is fastened to the mounting plate once the wiring is completed.

Mount the mounting plate directly to an electrical box on the ceiling or wall. The plate mounts directly to a 4″ square (with and without plaster ring), 4″ octagon, 3 1/2″octagon, single gang or double gang junction boxes. If an electrical box is not available, the mounting plate can be mounted to any flat surface and the wiring can be connected via the knockout points in the mounting plate.

To mount the gateway:

1. Pull the wiring through the opening in the mounting plate.
2. Mount the mounting plate to the junction box or ceiling. See Figure 2.3 below.
3. Connect field wiring to the terminals, as described in Section 2.7.2.
4. Connect necessary jumpers where applicable, as described in Section 2.7.3.
5. To mount the cover, align the locating pins on the cover to the corresponding slots in the mounting plate. See Figure 2.4.
6. Secure the cover by tightening the mounting screws.

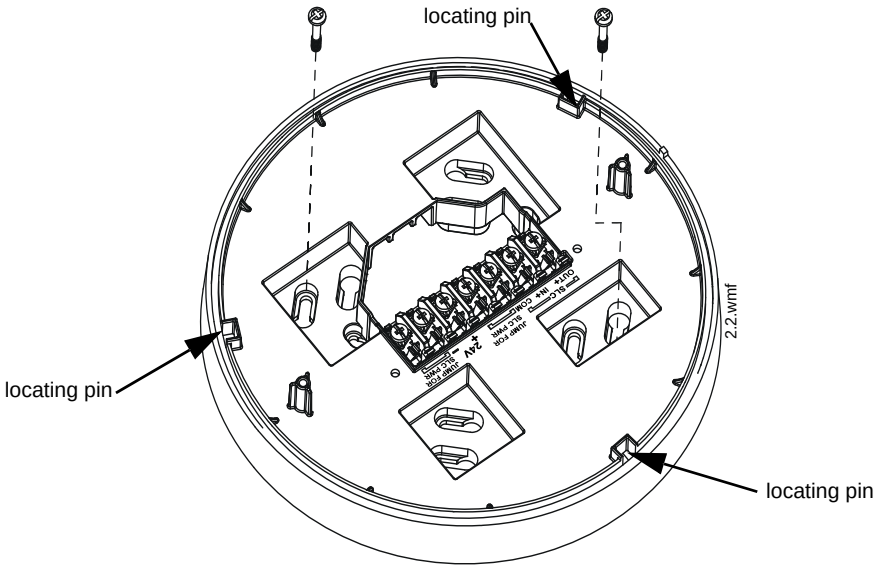


Figure 2.3 Mounting Plate for Wireless Gateway

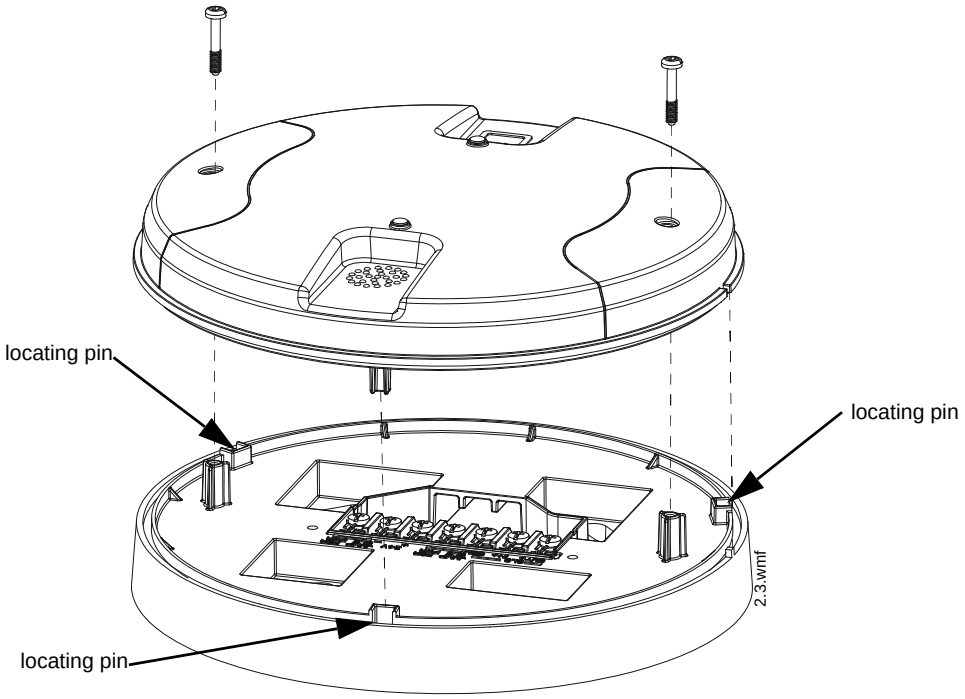


Figure 2.4 Attaching Cover to Mounting Plate

2.7.2 Wiring

- All wiring must be installed in compliance with the National Electrical Code and the local codes having jurisdiction.
- 12-18 AWG is recommended.

For wiring connections:

1. Strip about 3/8” of insulation from the end of the wire.
2. Slide the stripped end of the wire under the appropriate terminal and tighten the screw.

NOTE: Do not loop the wire under the screw terminals.

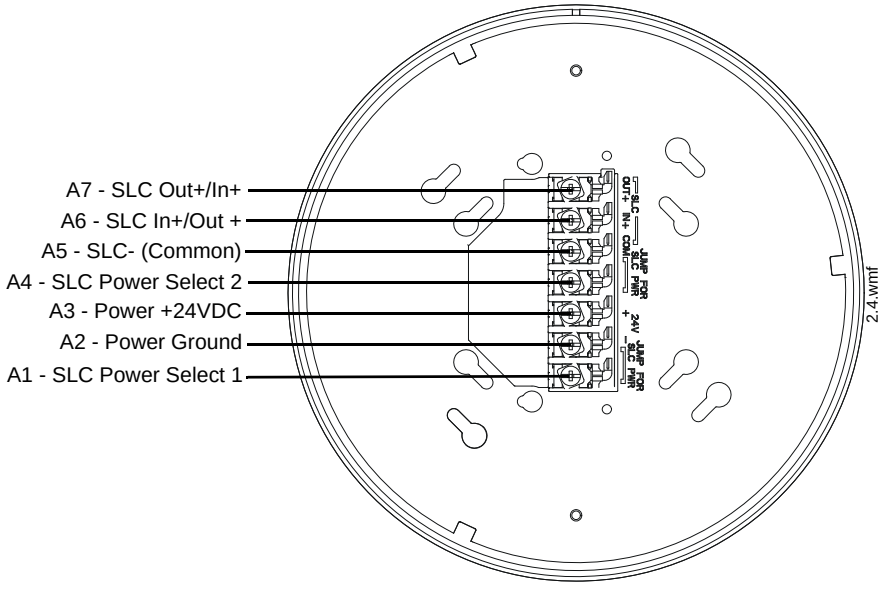


Figure 2.5 WIDP-WGI Mounting Plate - Terminal Layout

2.7.3 Gateway Powered by the SLC

To power the gateway using the signaling line circuit, connect the gateway as described in the table and graphic below:

Terminal Pins	Description
A5 and A7	SLC - (Common) & SLC Output +
A5 and A6	SLC - (Common) & SLC Input +
A4 and A5	Jumper selection to enable power from the SLC supply. (Insert Jumper when using SLC power.)
A3	Unused
A1 and A2	Jumper selection to enable power from the SLC supply. (Insert Jumper when using SLC power.)

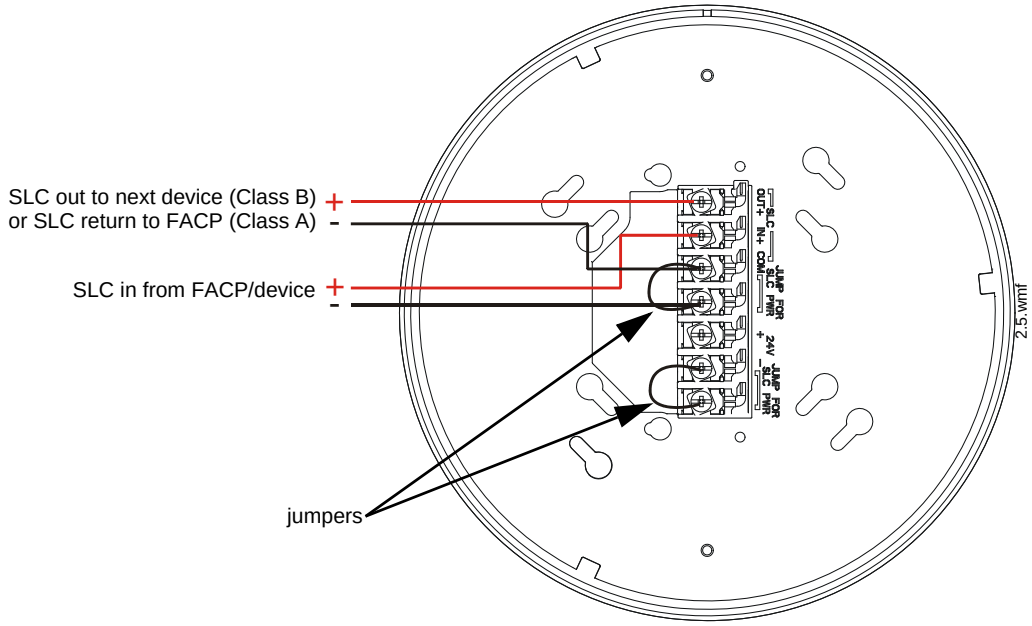


Figure 2.6 Wiring Connections: WIDP-WGI Powered by the SLC

NOTE: Use of the same wire gauge is recommended if there are multiple connections to the same terminal.

The gateway provides isolation of short circuits on the SLC in Class A (Style 6) installations. SLC connections are power-limited by the panel. An interruption in the SLC that causes a loss of power at the gateway for more than 100ms may result in a trouble condition and loss of fire protection provided by the wireless devices for approximately 15 minutes. Use of an external +24V power source (not SLC power) is recommended for installations that require fire protection in the presence of short circuits, including Class A applications and applications that use isolator modules.

2.7.4 Gateway Powered by an External, Regulated +24VDC Source

To power the gateway using an external, regulated +24VDC source, connect the gateway as described in the table and drawing below.

Terminal Pins	Devices Powered
A5 & A7	SLC Output
A5 & A6	SLC Input
A4	Unused
A2 & A3	+24VDC input. Voltage range from +18VDC to +30VDC. Use only power-limited device circuits.
A1	Unused

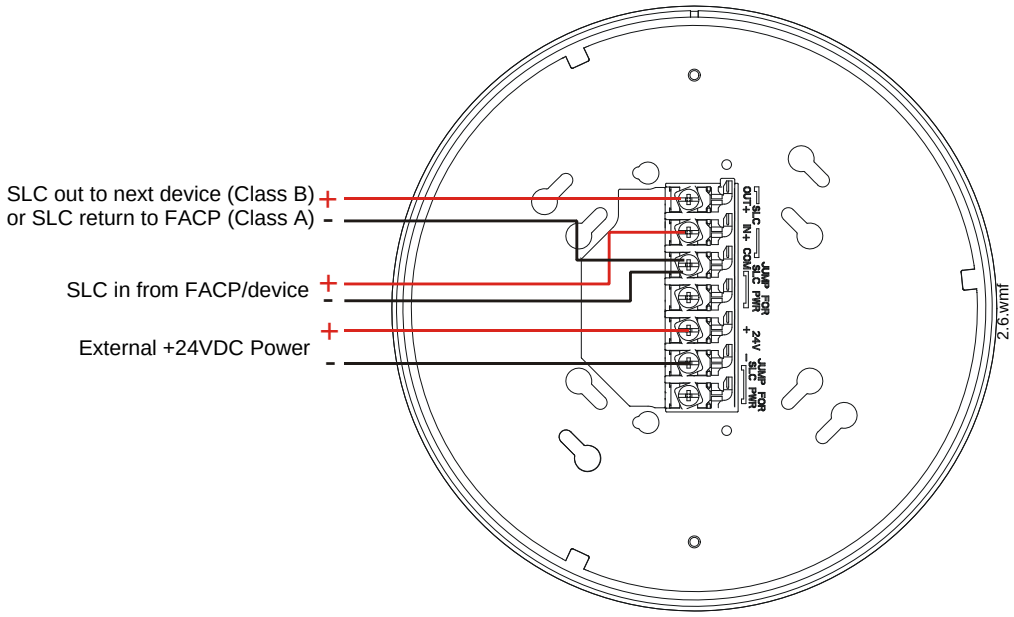


Figure 2.7 Wiring Connections: WIDP-WGI Powered by an External, Regulated +24VDC Source

NOTE: It is recommended to use the same wire gauge if there are multiple connections to the same terminal.

The gateway provides isolation of short circuits of the SLC in Class A (Style 6) installations. SLC connections are power-limited by the panel. +24VDC must be power-limited by the source.

2.8 Configuration and Programming

To successfully configure and/or program the gateway:

1. Create a profile. A profile binds a gateway and the devices in a mesh network together. The profile will contain a mesh ID that is used when forming the associations. All devices, including the gateway, require a common profile.
2. Assign a profile using SWIFT Tools. Assign the profile to every device that will be a part of the mesh. This will enable all the devices that have that profile to form associative links when the mesh is formed.
3. Form the mesh. The mesh cannot be formed until the profile is assigned to the gateway and to its devices.

Perform the follow steps using SWIFT Tools.

2.8.1 Assign a Profile

To assign a profile to the gateway using SWIFT Tools:

1. Connect the W-USB device to your laptop. For more information on the W-USB adapter, refer to Section 5, “W-USB Adapter”, on page 40.
2. Launch SWIFT Tools. Refer to Appendix A for more information.
3. From the Home Screen, select the **Create Mesh Network** function.
4. **Create** a new profile or **Import** an existing profile as required.
5. Select and open the profile to be assigned to the gateway from the Name drop-down box in the Profile section.

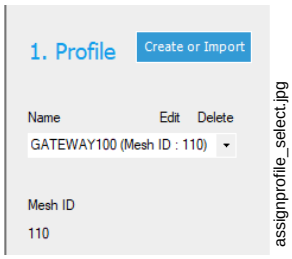


Figure 2.8 Selecting a Profile

6. Power on the gateway within approximately 20 feet of the laptop running SWIFT Tools.
7. Place the devices with batteries installed within 20 feet of the laptop, with a minimum of 3 feet between each device. If the devices were inadvertently installed in the building prior to assigning them profiles, either remove them to bring them near the laptop or bring the laptop near each of the installed devices in order to assign them the profile.

8. Ensure that the **Scan On** selection box in the **Communicator Window** is checked.
9. Select the gateway from the **Communicator Window** on the right side of the Tools screen.

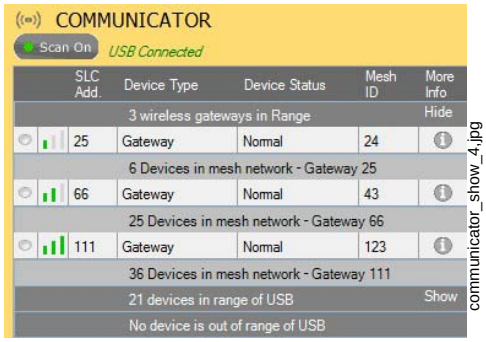


Figure 2.9 Gateway Selection

10. Click **Assign**.

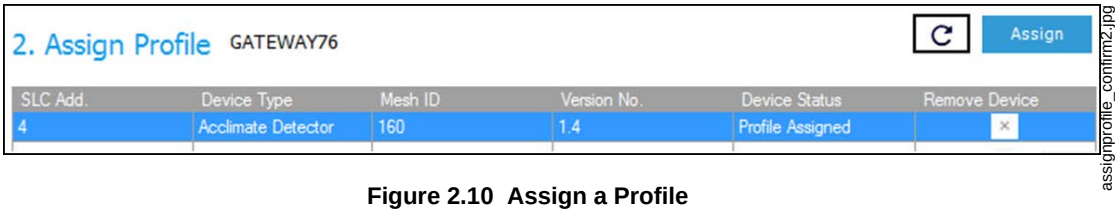


Figure 2.10 Assign a Profile

The gateway is now included in the list of devices with a profile assigned. The LEDs on the gateway will turn on green for 10 seconds after the profile has been received.

2.8.2 Remove a Profile

Remove a Profile from a Gateway using SWIFT Tools

1. Connect the W-USB adapter to your laptop. For more information on the W-USB device, refer to Section 5, “W-USB Adapter”, on page 40.
2. Launch SWIFT Tools. Refer to Appendix A, “SWIFT Tools” for more information on launching the SWIFT Tools application.
3. From the Home Screen, select the **Site Survey**, **Create Mesh Network**, or **Diagnostics** function.
4. Click **Operations** and select **Set device to factory default**.



Figure 2.11 Operations Menu

5. The **Reset Devices** screen appears, displaying the gateway and other devices that have a profile assigned. Click to select the gateway and click **Reset** to remove the profile.

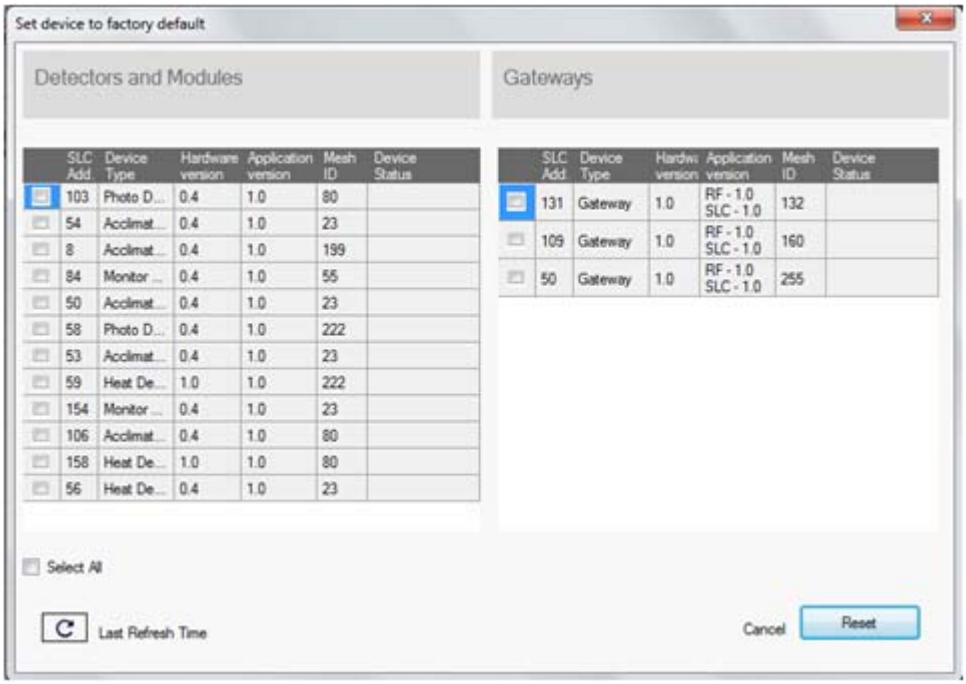


Figure 2.12 Reset Devices Screen

The profile is removed and the gateway is reset to factory default state. Refer to Section 3.5.3 on page 33 for information on returning devices to the factory default state.

Remove a Profile from a Gateway without using SWIFT Tools

1. Start with the gateway powered off. The process is performed during start-up.
2. Power on the gateway using SLC power or external +24V. Refer to Sections 2.7.3 and 2.7.4 for more information.
3. Verify the gateway is in the profile modification state. The gateway is in the profile modification state when both the LEDs on the gateway double blink yellow every second for ten seconds.
4. Activate both magnetic sensors on the gateway within ten seconds of start-up while the double yellow blink is active. If the ten second window is missed, power down the gateway and repeat the process starting at step 1.

The LEDs on the gateway will blink green every second for five seconds indicating that the profile is removed.

NOTE: If a gateway has been locked using SWIFT Tools, the ability to remove a profile using magnets is no longer available.

2.8.3 Create a Mesh Network

To create a mesh network using the SWIFT Tools, perform the following steps.

1. Connect the W-USB device to your laptop. For more information on the W-USB adapter, refer to Section 5, “W-USB Adapter”, on page 40.
2. Launch SWIFT Tools. Refer to Appendix A for more information.
3. From the Home Screen, select the **Create Mesh Network** function.
4. Proceed to the second step of the **Create Mesh Network** function by clicking the arrow marked **Next** at the bottom of the screen.
5. Click to select the desired gateway displayed in the **Gateways in Range** table.

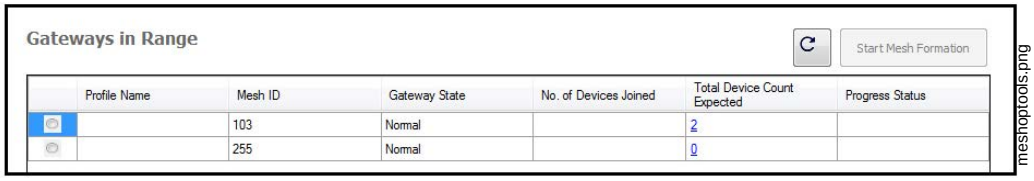


Figure 2.13 Gateways in Range Table

6. The **Enter password for Gateway** screen is displayed. Enter the password and follow the on-screen instructions. Note that, once accessed, the login will be valid for only 30 minutes. For additional information, refer to “Lock/Unlock the Gateway” on page 20.
7. Click **Start Mesh Formation**.
8. A message is displayed. Click **Yes** to proceed or click **No** to cancel.
9. The **Mesh Formation** screen is displayed indicating that the mesh formation is in progress.

- The **Progress Status** column indicates progress status of the selected gateway.
- The **No. of Devices Joined** column indicates the number of devices that are in the mesh network including the gateway.
- The **Total Device Count Expected** column indicates the number of devices expected to join including the gateway. This field is editable. Click in to the field to edit the number of device count expected.

10. Once the expected count of devices have joined the mesh, a message is displayed to show that the Mesh formation is complete and an option is given to choose to start mesh restructuring immediately or wait for any other devices to join.

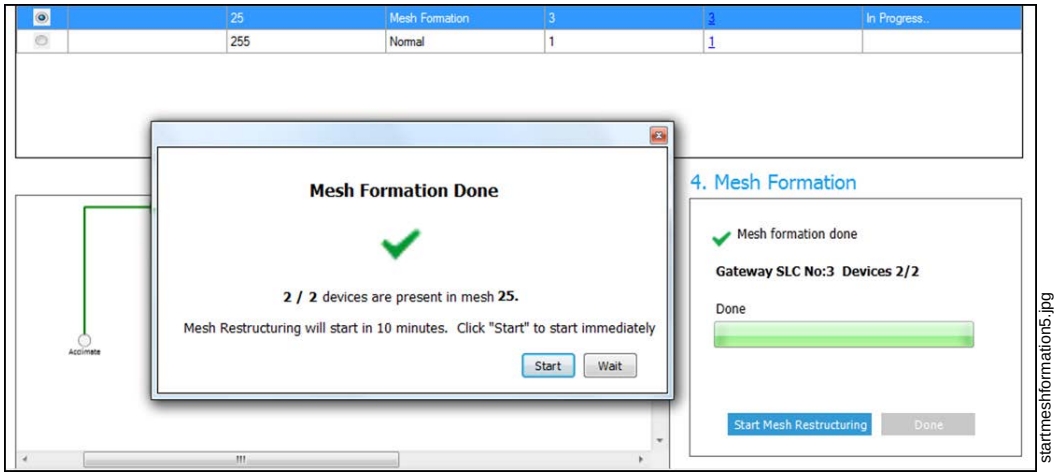


Figure 2.14 Completed Mesh Formation Screen

11. Start Mesh Restructuring (by either waiting or clicking **Start**). Once Restructuring is initiated, the progress displays. When Mesh Restructuring is complete, the following success message is shown. For further operating instructions, refer to Section 2.9, “Operations”.

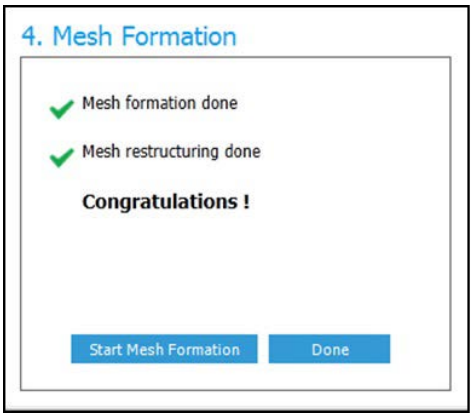


Figure 2.15 Completed Restructuring Screen

2.8.4 SLC Configuration

The gateway:

- ✓ communicates with the control panel via the SLC.
- ✓ is only compatible with Gateway firmware version 2.1 or higher.
- ✓ occupies one module SLC address. Set the address using the rotary dials on the gateway prior to installation.

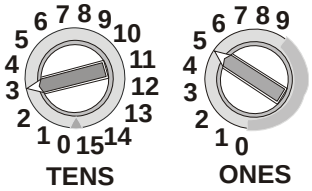


Figure 2.16 Address Rotary Switches

The SLC point uses the following configuration parameters:

- Type Code Label: Wireless Gateway

A gateway does not initiate alarms but the point is used for event reporting.

NOTE: When a wireless relay, wireless AV base, or wireless sync module is in use, module device count must be limited to 109 modules per loop. This includes wired and wireless modules that are on the same loop. The module address range must be within 1-109.

2.9 Operations

2.9.1 Modes of Operation

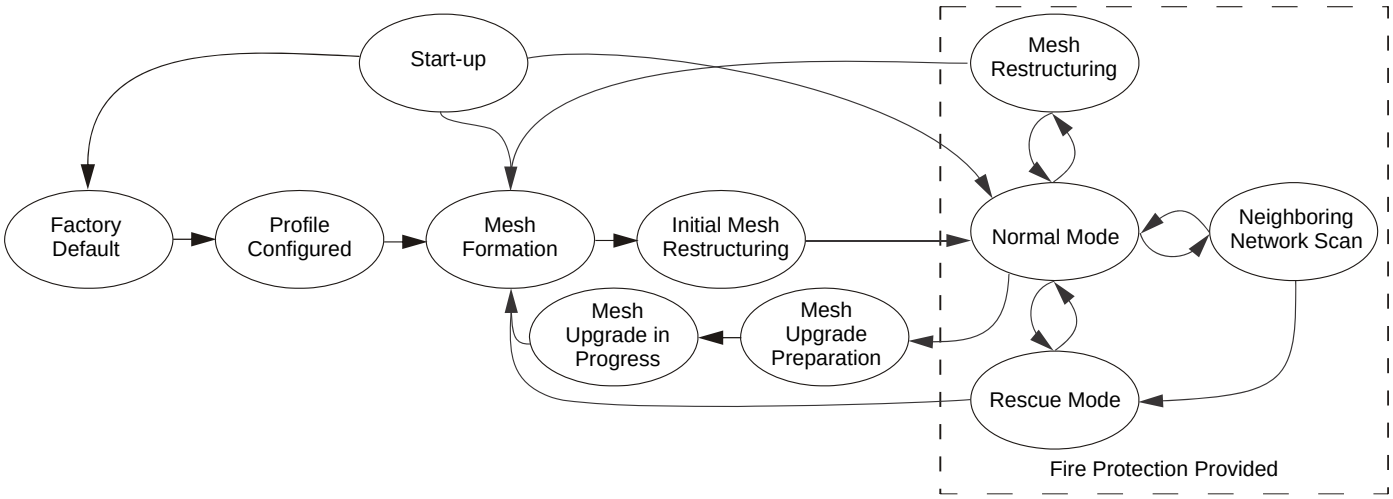


Figure 2.17 Gateway Modes Of Operation

Start-up Mode

Start-up mode is a temporary mode of operation. During start-up mode a profile can be created or removed. The start-up period lasts for 10 seconds. If a particular unit contains a profile, the LEDs double blink yellow every second. If the unit does not contain a profile, the LEDs double blink red every second.

During start-up, the gateway does not provide fire protection nor does it respond to the FACP.

After start-up, the gateway proceeds to the **factory default** mode if no profile exists. In the presence of a profile, the gateway will proceed to **mesh formation** mode if it was previously part of a mesh network or **normal mode** if it was *not* previously part of a mesh network.

Factory Default Mode

Factory default mode is the initial mode of the gateway. In this mode, the gateway and peripheral devices do not provide any fire protection. The gateway does not communicate with wireless detectors or modules in factory default mode. The only wireless communication in factory default mode is between the gateway and SWIFT Tools. SWIFT Tools must be within 20 feet of the gateway for proper communication. The gateway must be assigned a profile before continuing configuration.

The gateway reports a “NO PROFILE” trouble to the FACP. The gateway reports “Factory Default” to the communicator display of SWIFT Tools.

Transitions back to Factory Default mode are not shown in the above diagram. However, any time the profile is removed from the gateway, it will return to Factory Default mode.

Profile Configured

The gateway enters the profile configured mode once a profile is assigned by SWIFT Tools. Profile configured mode is a temporary mode before the gateway transitions to mesh formation or normal mode.

The gateway does not provide fire protection in the profile configured mode. While in the profile configured mode, the gateway reports a “RF MESH NOT FORMED” or “RF MESH” trouble to the FACP. The gateway reports “Profile Assigned” to the communicator display of the SWIFT Tools application.

Mesh Formation

The gateway must have a profile before entering mesh formation mode. The gateway and the peripheral devices do not provide any fire protection in this mode. The gateway enters mesh formation mode:

- ✓ after creating a profile using the mesh formation sensor.
- ✓ after activating the mesh formation sensor with a magnet when the gateway contains a profile.
- ✓ automatically after start-up when the gateway was previously part of a mesh.
- ✓ by a command from the SWIFT Tools application.

A gateway in mesh formation mode instructs all devices in the mesh to also transition to mesh formation mode. The gateway and all communicating devices search for new or lost devices with the same profile to join the network.

If the gateway automatically entered mesh formation after start-up, mesh formation will terminate 10 minutes after the last device has joined or after all existing devices are recovered. If new devices are found or if mesh formation was initiated by the user, then mesh formation terminates after a period of 10 minutes without any new devices joining the mesh. At any point Mesh formation can be terminated by user interaction by activating the magnet sensor again or by using the SWIFT Tools application.

The gateway reports a “RF MESH FORMING” or “RF MESH” trouble when it is mesh formation mode with additional devices in the mesh. The gateway reports “Mesh Formation” to the communicator display of the SWIFT Tools application.

Initial Mesh Restructuring Mode

Initial mesh restructuring mode automatically runs after each **mesh formation**. The gateway and peripheral devices do not provide fire protection during the initial mesh restructuring mode. Mesh restructuring analyzes signal strengths between devices. The gateway designates the primary and secondary communication paths between devices that provide a redundant path for all transmissions. Mesh restructuring automatically terminates once all devices have a redundant communication path and signal strengths that meet the requirements of primary and secondary transmission paths. Any device that does not have a redundant path or meet the requirements for signal strength will report a fault.

The gateway reports a “RF MESH FORMING” or “RF MESH” trouble to the FACP. The gateway reports “Restructuring” to the communicator display of the SWIFT Tools application.

Normal Mode

Normal mode is the network’s standard operating state. The mesh network has been formed and is providing fire protection. The mesh network will continuously search for additional devices with a matching profile to join the mesh. To avoid interference, the mesh network periodically checks for adjacent mesh networks created by Honeywell. The gateway reports “Normal” to the communicator display of the SWIFT Tools application.

Rescue Mode

During normal mode, if an out-of-network device with a matching profile is discovered by the network, the gateway will trigger rescue mode in all communicating devices. All devices in communication continue to provide fire protection during rescue mode but also search for a lost or added device. Rescue mode automatically terminates 3 minutes after the last device is rescued and returns to normal mode. The gateway does not report troubles during rescue mode but reports “Rescue” to the communicator display of the SWIFT Tools application.

Mesh Restructuring Mode

In addition to the initial mesh restructuring mode, mesh restructuring is automatically performed after any restoration of communication to a device or to recover from a link failure (Class A fault). Mesh restructuring that occurs during normal mode does not generate a trouble message. During mesh restructuring, fire protection is provided by all devices that are participating in the mesh communication. The gateway reports “Restructuring” to the communicator display of the SWIFT Tools application.

Bootloader Mode

The gateway enters the bootloader mode when its firmware is being updated using SWIFT Tools. The gateway does not communicate with the FACP during bootloader mode. The gateway reports “Bootloader” to the communicator display of the SWIFT Tools application.

Mesh Upgrade

Starting with version 3.0, firmware updates for the wireless mesh devices (detectors, monitor module, relay, etc.) can be broadcast over the mesh network. Fire protection will not be provided during the upgrade process.

SWIFT tools will be used to initiate and monitor the upgrade process. During the upgrade process each device in the mesh will appear as a no answer or invalid reply. Refer to Section E.4 on page 60 for more information on the mesh upgrade process.

Neighboring Network Scan

A Mesh network will identify adjacent mesh networks for the purpose of avoiding communication collisions and for time synchronization to ensure end-to-end latency compliance. Fire protection will be provided during a neighboring network scan by all devices that are participating in the mesh communication. The gateway reports “Neighboring Scan” to the communicator display of the SWIFT Tools application.

2.9.2 LED Patterns

The LED indicator patterns are provided in Appendix D on page 53.

2.9.3 Lock/Unlock the Gateway

The gateway can be locked to prevent access to the magnetic sensors and to password-protect all wireless interactions. The lock function can be performed by SWIFT Tools. When SWIFT Tools is used to lock the gateway, a password must be provided for all future interactions, including unlocking the gateway. If the gateway was previously locked with a password from SWIFT Tools, the previous password will be applied. Use this password for all future interactions with the SWIFT Tools application.

Lock/Unlock the Gateway Using SWIFT Tools

To lock/unlock the gateway:

1. Connect the W-USB device to your computer. For more information on the W-USB adapter, refer to Section 5.
2. Launch the SWIFT Tools application. Refer to Appendix A, “SWIFT Tools” for more information.

3. From the Home Screen, select the **Site Survey**, **Create Mesh Network**, or **Diagnostics** function.
4. Click **Operations**. The following screen is displayed.



Figure 2.18 Operations Menu

5. Select **Gateway Operations** to lock/unlock the gateway. The Lock/Unlock Gateway screen displays the list of gateway/gateways that are in the range of the W-USB adapter connected to your /Laptop.

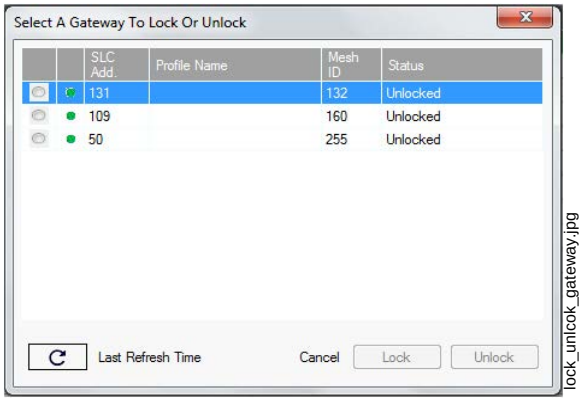
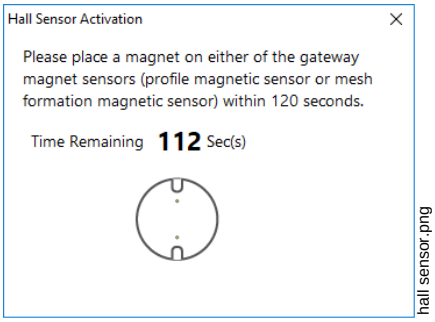


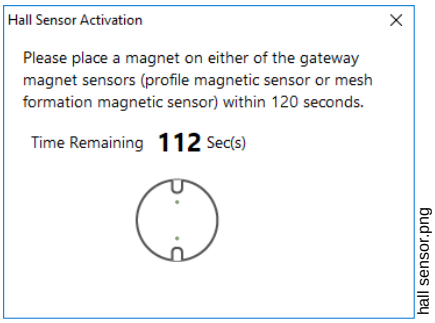
Figure 2.19 Lock/Unlock Screen

6. Select desired gateway and click **Lock** or **Unlock** as required.
   - **To lock the gateway**
     1. Click Lock. The **Gateway Password** screen is displayed.
     2. Enter the verification password in the Verification Password field and click **OK**.
     3. A Hall Sensor Activation window displays. The LED on the gateway blinks yellow indicating the gateway is waiting for hall sensor activation.



     4. Place a magnet on either of the gateway sensors within 120 seconds.
     5. The LED blinks normal upon hall sensor activation. The gateway is locked and a confirmatory message is displayed.
   - **To unlock the gateway**
     1. Click Unlock. The **Gateway Password** screen is displayed.
     2. Enter the verification password in the Verification Password field and click **OK**.

3. A Hall Sensor Activation window displays. On hall sensor activation, the LED on the gateway blinks yellow.



4. Place a magnet on either of the gateway sensors within 120 seconds.
5. The LED blinks normal upon hall sensor activation. The gateway is unlocked and a confirmatory message is displayed.

Password Reset

To reset the password, contact technical support.

2.9.4 Enable/Disable Max Gateway Trouble Reporting

This feature is used to determine if the permitted number of Honeywell SWIFT systems that can co-exist in range of each other without reducing overall performance has been exceeded. The default setting is On (enabled).

Completed Wireless Network

Turning off the MAX GATEWAY trouble reporting in this case prevents subsequent installation attempts from causing a trouble on a properly installed and commissioned system. When the wireless installation is completed and there are no possibilities of overlapping systems, turn off MAX GATEWAY trouble reporting when all three of the following conditions are true:

1. The entire fire system installation has been completed.
2. There is no MAX GATEWAY trouble indication present in the completed system.
3. The system has been inspected, tested, and approved by the authority having jurisdiction.

Possible Wireless Mesh Overlap

Generally, only four SWIFT wireless mesh gateways, along with their associated devices, are permitted to be installed within an overlapping wireless region. The MAX GATEWAY trouble is generated when a fifth gateway mesh is detected and the maximum limit is exceeded. When there is a MAX GATEWAY trouble present in the system, it is permitted to turn off MAX GATEWAY trouble reporting after completing the following evaluation method with successful results. For the result to be successful, the signal strength between devices in any one mesh must be at least 20 dB stronger than the signals seen from another mesh. If the 20 dB requirement is not met, or if the evaluation cannot be performed due to access restrictions, the number of overlapping mesh systems must be reduced to four to ensure the wireless system performs according to UL requirements. This could mean that additional mesh systems cannot be installed in the area.

NOTE: Signal strength is represented using negative numbers. So, 30 is 20 dB stronger than 50. Refer for Figure 2.23 for an example.

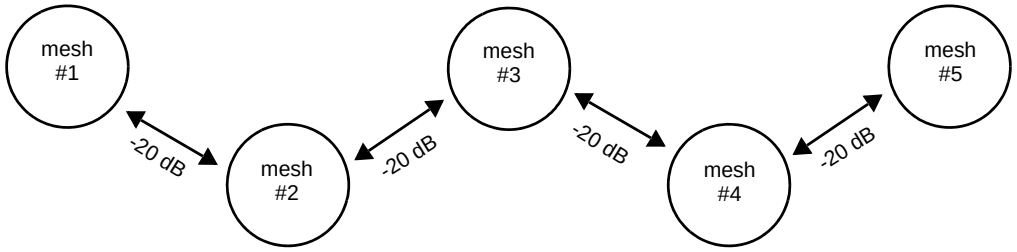


Figure 2.20 Basic Overlapping Mesh Example

■ Evaluation Process

1. Locate all the SWIFT wireless mesh systems in the area. Access to all mesh gateways in the area and to the closest edge devices between overlapping meshes is required and the SLC addresses of the edge devices must be known. The edge devices that must be accessible are located at the ends of the dotted lines represented in Figures 2.21 and Figure 2.24. If location of devices or access to them is not possible, the addition of a fifth wireless mesh is not permitted in this area.
2. Identify the devices on the edge of each mesh.
3. Find the closest edge device from each mesh to the closest edge of the new mesh. Except as noted in Figure 2.25, four pairs of devices should be identified given there are five overlapping meshes in the area.

4. Perform a link test between each of the four device locations (Mesh 1 to Mesh 5, Mesh 2 to Mesh 5, Mesh 3 to Mesh 5, and Mesh 4 to Mesh 5) using a separate pair of test devices. Refer to Appendix B, “Site Survey” for instructions on how to perform a site survey. Use SWIFT Tools to identify the signal strength/link quality for each of the four link tests and record these values.

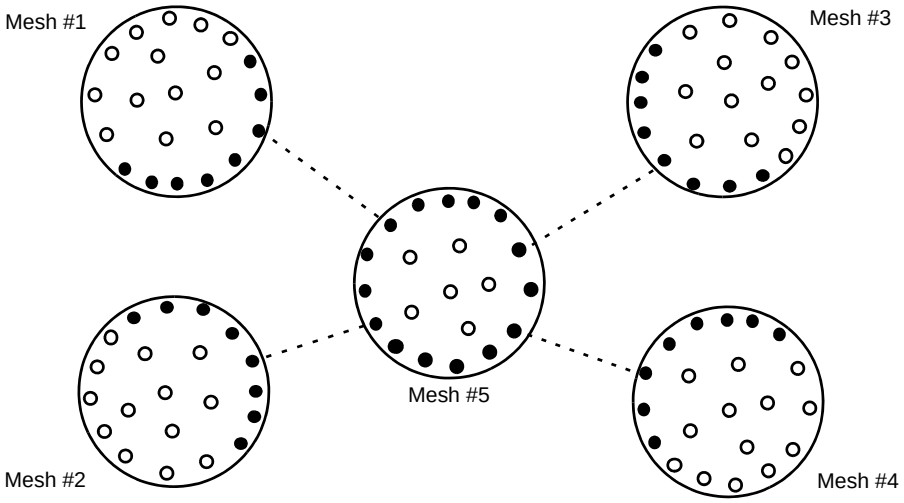


Figure 2.21 Perform a Link Test with the Fifth Mesh

5. Use network statistics from the gateway to determine link strength between edge devices in each mesh.

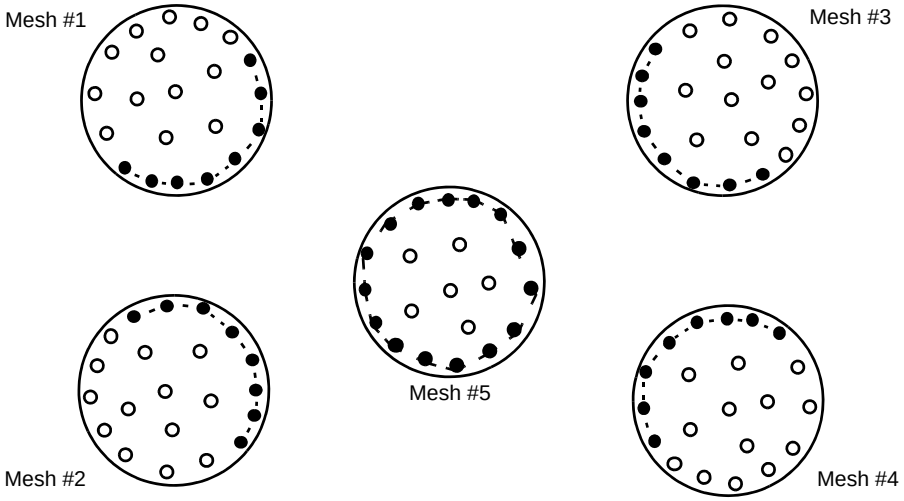


Figure 2.22 Perform Link Test within Each Mesh

6. Export network statistics to Excel for each gateway, and by using the SLC address tab for each edge device, review the primary and secondary parent link strengths for each edge device in each mesh system.

Network Statistics Report
Site Name : Northford
Location/Description :
Date : 1/16/2019

Device Attribute	Device Attribute Value
Device Serial Number	3306284176
Device Slot Number	48
Device SLC Address	17
Device Type	Photo Detector
Parent 1 Slot Number	50
Parent 2 Slot Number	49
Min RSSI Received From Parent 1	37
Min RSSI Received From Parent 2	60
Current RSSI Received From Parent 1	25
Current RSSI Received From Parent 2	54
Time Sync Correction From Parent 1	2
Time Sync Correction From Parent 2	0
Worst Case Time Sync Correction From Parent 1	2
Worst Case Time Sync Correction From Parent 2	1
Watch Dog Reset	0
Device Rejoin Count	0
Partial Link Recovery Count	0
Last Failed State	59
Present Noise Floor	218
Minimum Noise Floor	233
Maximum Noise Floor	208
PHY Threshold	190
Interference Detection Count	14

... | Slot 47 (D34) | Slot 48 (D17) | Slot 49 (D26) | ⊕

In this case, 25 would be the stronger link.

Figure 2.23 Review Network Statistics

7. Make a list of the strongest links for all edge devices in each mesh.
8. From the collection of values recorded in step 7, identify the lowest value on the list of these links in each mesh.
9. Compare that lowest value from each mesh to the corresponding link values in step 4.
10. If the values in step 8 are at least 20dB higher that the values in step 4, continue to step 11. If they are not, installation of Mesh #5 is not allowed.
11. Repeat this process from step 4, identifying device pair locations for each mesh (Mesh 1 to Mesh 2, Mesh 1 to Mesh 3, Mesh 1 to Mesh 4, Mesh 2 to Mesh 3, Mesh 2 to Mesh 4, and Mesh 3 to Mesh 4).

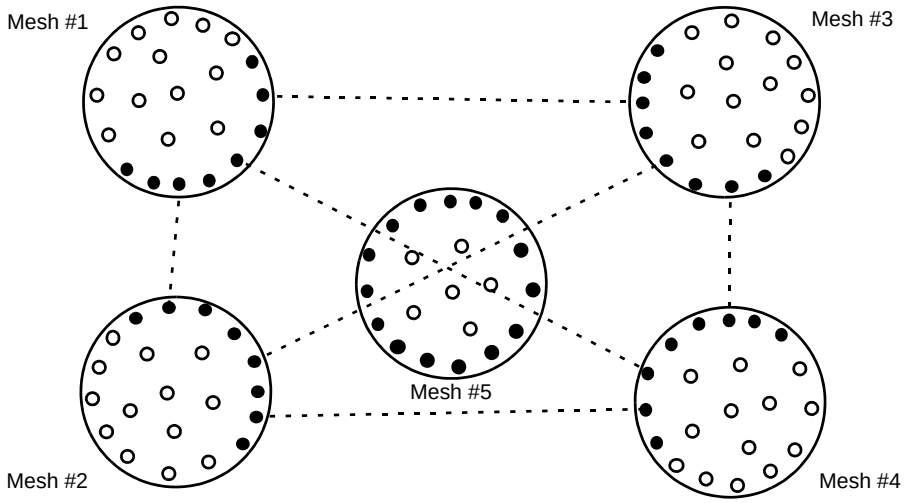


Figure 2.24 Perform a Link Test Across Existing Mesh Networks

12. If all the values are at least 20 dB higher in step 10, MAX GATEWAY trouble reporting can be disabled.

NOTE: If the mesh networks are installed vertically in a high-rise building or horizontally in adjacent buildings, the evaluation in steps 4-11 only needs to be performed on the mesh edge devices between different meshes on adjacent floors.

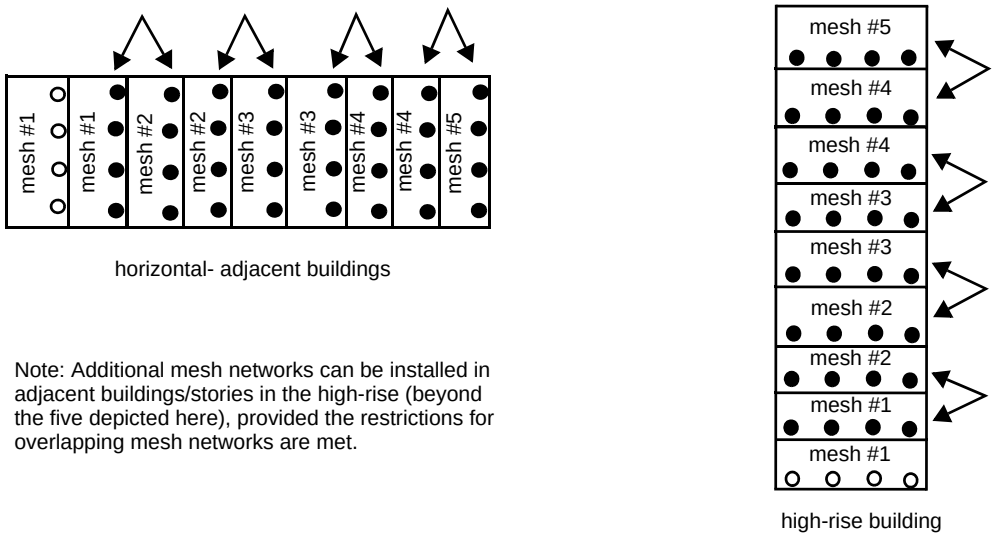


Figure 2.25 Perform a Link Test in High-rise/Adjacent Buildings

Disabling Max Gateway Reporting

Once the criteria for disabling MAX GATEWAY troubles are met, follow the steps below to turn off reporting. Reporting must be disabled for every gateway in the area.

1. Connect the W-USB device to your computer. For more information on the W-USB adapter, refer to Section 5.
2. Launch the SWIFT Tools application. Refer to Appendix A, “SWIFT Tools” for more information.
3. From the Home Screen, select the **Diagnostics** function.
4. Select a Gateway from the communicator panel.
5. Click **View Mesh**. SWIFT Tools will display Lock/Unlock option. Refer to Section 2.9.3 on page 20 for additional information.
6. Click **Advanced Functions**. A drop-down list is displayed.

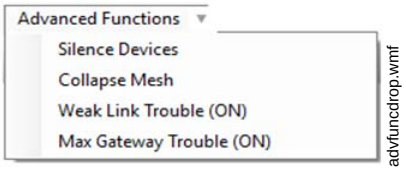


Figure 2.26 Advanced Functions Options

7. Click **Max Gateway troubles (On)**. The **Max Gateway troubles** screen is displayed.

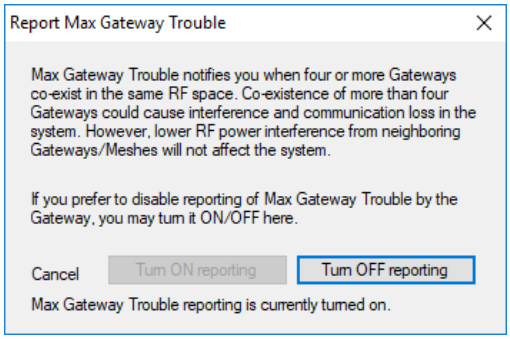


Figure 2.27 Report Max Gateways Troubles Option

8. Click **Turn off reporting**. The trouble reporting is now disabled.

2.9.5 Weak Link Trouble Reporting

The SWIFT Network uses two paths of communication for each device. To establish the link between devices as a viable communication path, the signal strengths must meet the limits provided in Section 2.3. The SWIFT Network implements a higher threshold for primary connections to provide an extra layer of robustness and immunity from interference. A weak link trouble condition is initiated for any device that does not have at least one connection at the primary threshold. This is an optional setting that can be disabled to ignore the weak link trouble condition. The trouble can be disabled at the gateway.

Disable Trouble Reporting at the Gateway Using SWIFT Tools

To disable trouble reporting at the gateway through SWIFT Tools:

1. Connect the W-USB device to your computer. For more information on the W-USB adapter, refer to Section 5.
2. Launch the SWIFT Tools application. Refer to Appendix A, “SWIFT Tools” for more information.
3. From the Home Screen, select the **Diagnostics** function.
4. Select the desired gateway from the communicator panel.

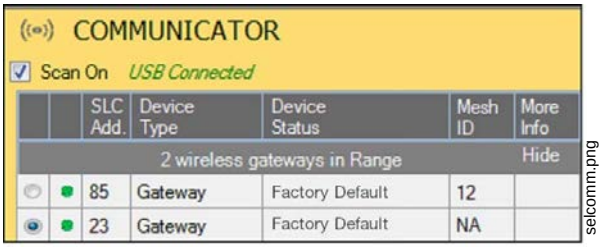


Figure 2.28 Communicator Panel

5. Click **View Mesh**. SWIFT Tools will display Lock/Unlock option. Refer to Section 2.9.3 on page 20 for additional information.
6. Click **Advanced Functions**. A drop-down list is displayed.

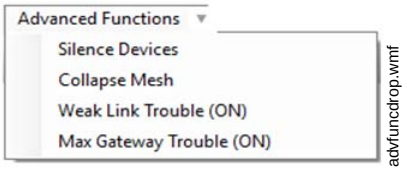


Figure 2.29 Advanced Functions Options

7. Click **Weak links troubles (On)**. The **Report weak links troubles** screen is displayed.

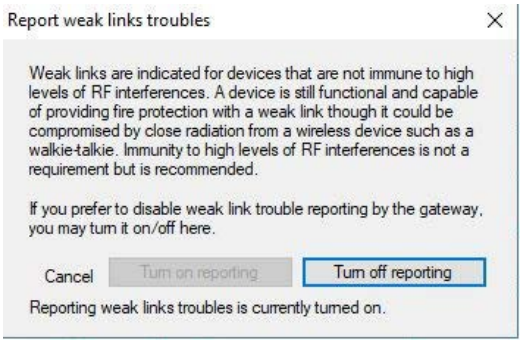


Figure 2.30 Report Weak Links Troubles Option

8. Click **Turn off reporting**. The trouble reporting is now disabled.

2.9.6 Collapse Network Command

The collapse command is a diagnostic function to break the mesh network. All devices will retain the profile information but will be removed from the mesh. The mesh can be reformed by activating mesh formation.

CAUTION: FIRE PROTECTION DISABLED

FIRE PROTECTION FROM WIRELESS DEVICES IS DISABLED WHEN A COLLAPSE NETWORK COMMAND IS ISSUED.

Collapse Mesh Network Using SWIFT Tools

To collapse the mesh network using the SWIFT Tools:

1. Connect the W-USB device to your computer. For more information on the W-USB adapter, refer to Section 5.

2. Launch the SWIFT Tools application. Refer to Appendix A, “SWIFT Tools” for more information about the programming utility.
3. From the Home Screen, select the **Diagnostics** function.
4. Select a Gateway from the communicator panel.
5. Click **View Mesh**. SWIFT Tools will display Lock/Unlock option. Refer to Section 2.9.3 on page 20 for additional information.
6. Click **Advanced Functions** on top of the mesh display. A drop-down list is displayed.

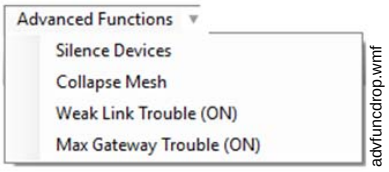


Figure 2.31 Advanced Functions Options

7. Click **Collapse Mesh**. The **Collapse mesh network** screen is displayed.



Figure 2.32 Collapse Mesh Network Option

8. The network is now collapsed and a confirmation message is displayed as shown below.

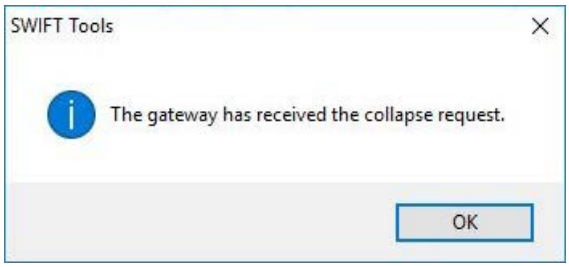


Figure 2.33 Collapse Mesh Network Confirmation

2.9.7 Silence Network Command

The silence network command is a diagnostic function to turn off all radio communication from the wireless devices for a set amount of time. All devices will retain the profile information but will be removed from the mesh. The devices will not send or receive any wireless communication until the set time expires or the device is rebooted. The mesh network can be reformed at the end of the silence period or after the device is restarted.

CAUTION: FIRE PROTECTION DISABLED

FIRE PROTECTION FROM WIRELESS DEVICES WILL BE DISABLED WHEN A SILENCE COMMAND IS ISSUED.

Silence Mesh Network Using SWIFT Tools

To silence the mesh network:

1. Connect the W-USB device to your computer. For more information on the W-USB adapter, refer to Section 5.
2. Launch the SWIFT Tools application. Refer to Appendix A, “SWIFT Tools” for more information on the programming utility.
3. From the Home Screen, select the **Diagnostics** function.
4. Select a Gateway from the communicator panel.
5. Click **View Mesh**. SWIFT Tools will display Lock/Unlock option. Refer to Section 2.9.3 on page 20 for additional information.

6. Click **Advanced Functions** on top of the mesh display. A drop-down list is displayed.

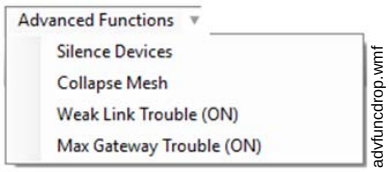


Figure 2.34 Advanced Functions Options

7. Click **Silence Devices**. The **Silence mesh network** screen is displayed.
8. Select the time interval to silence the wireless devices from the dropdown list and click **Yes**.

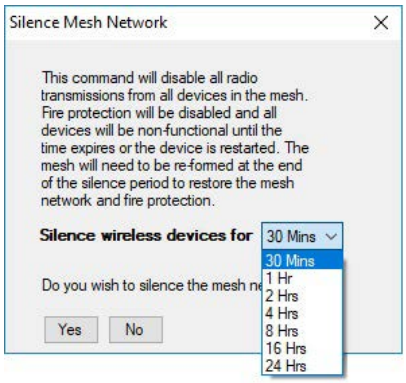


Figure 2.35 Silence Mesh Network Screen

9. The network is silenced and confirmation is displayed as shown below.

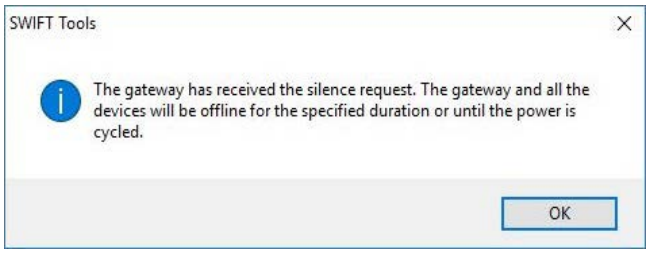


Figure 2.36 Silence Mesh Network Confirmation Message

2.9.8 Overlapping Wireless Sensor Networks and Limitations

The SWIFT Network technology shares the RF spectrum with other Honeywell Fire Wireless Sensor Network systems. Honeywell Fire has generally established a limit of 4 overlapping networks (4 gateways maximum and their associated devices) to avoid congestion in the RF spectrum. If more than 4 networks are detected, a MAX GATEWAY system trouble will be generated. To resolve this trouble, any instances of disruptive overlap need to be removed. Refer to Appendix C, “Troubleshooting and Testing” for suggestions on removing overlap between wireless networks. The trouble will be self-restoring up to 36 hours after the condition is resolved. To expedite the trouble resolution, transition the network that is reporting the trouble in and out of mesh formation mode.

2.9.9 Activation of Wireless Output Devices

Wireless input modules (pull stations and monitor modules) may be programmed to activate wired notification appliances anywhere in the system and wireless input modules may be programmed to activate wireless output devices including relay modules, sync modules, and AV devices within the same wireless mesh network. Wireless input modules are not permitted to be programmed to activate wireless outputs in another wireless mesh. Wireless detector programming is not restricted since the alarm condition is determined by the fire panel.

2.9.10 Avoiding RF Interference

The SWIFT wireless mesh network uses radio frequency hopping spread spectrum technology to communicate in the 900 MHz ISM band (902MHz to 928MHz). Other commercial and industrial products also operate in this band. If two-way radios or other wireless communication devices are used during the installation process, it is recommended that they be kept at least 4 feet away from the Farenhyt wireless devices or that they operate on a different frequency band to ensure rapid mesh formation.

A properly installed SWIFT wireless mesh network with primary link reporting enabled will be highly immune to RF interference from other wireless products even when they are nearby. The use of the weak link reporting feature is highly recommended. If the system is installed in a controlled environment where other 900 MHz ISM band devices will not be present, the primary link reporting feature may be disabled to permit greater distances between installed devices if required.

The SWIFT wireless mesh network will be able to automatically detect and avoid certain types of in-band channel interference (often caused by two-way radios) by using an alternate channel set. The system will log detection and avoidance of this kind of interference in the gateway history as “Walkie Talkie Mode” Entry or Exit.

2.9.11 Trouble Messages

Trouble Message	Type	Description	Course of Action
RF JAMMING or JAMMING	Non-latching	The gateway is being overloaded with RF energy and is unable to receive messages from other devices.	Identify any RF emitters in close proximity of the gateway and remove them or relocate the gateway.
SOFTWARE MISMATCH or SOFTWARE	Non-latching	Software mismatch between the application code for the RF processor and the SLC processor.	Use SWIFT Tools to identify the mismatch, and update the processors as necessary for compatibility.
RF MESH FORMING or RF MESH	Non-latching	The gateway and attached devices are searching for additional devices to join the mesh. The wireless system is not able to provide fire protection during this time.	Wait until all desired wireless devices are communicating and are members of the mesh network. Once all desired devices are in the mesh network, the mesh forming mode can be terminated by the user by activating the Mesh formation magnetic sensor or by using the SWIFT Tools. If no action is taken, this mode will automatically exit 10 minutes after the last device joins.
RF MESH NOT FORMED or RF MESH	Non-latching	The gateway contains a profile but has not formed a mesh.	To form a mesh, refer to“Create a Mesh Network” on page 17.
RF MESH REFORMING or RF MESH	Non-latching	The gateway is performing the initial identification and assignment of optimal communication paths for the mesh network. The wireless system is not able to provide fire protection during this time.	No action needed. The duration of this event correlates to the number of devices in the mesh. A fully loaded mesh may take up to 5 minutes to restructure.
NO PROFILE	Non-latching	The gateway is in the factory default state and is not providing fire protection.	A profile needs to be assigned to the gateway before a mesh can be formed.
ADDRESS FAULT or ADDR FAULT	Non-latching	There is either a device in the mesh set to address 0 or there is a duplicate address used for another wireless module at the address of the gateway.	The offending device (detector or module set at address 0 or module at the same address as the gateway) will be indicating the LED pattern for address fault. Find and resolve that device.
RF OVERLAP	Non-latching	Wireless communication reliability is compromised due to the installation limits of Farenhyt wireless systems being exceeded. This trouble may also be interpreted as Max Gateways. Refer to Appendix C.1.	Investigate for overlapping or adjacent wireless systems produced by Farenhyt. Reduce the instances of overlap by removing systems, or devices in the overlapping region. Refer to Section 2.9.8 on the installation limits for the Farenhyt wireless system.
RF DEVICE NO ANSWER or DEV NO ANS	Latching trouble; remains active for the first 90 seconds before it can be cleared with a system reset.	A wireless device that was part of the mesh has dropped from the mesh. The trouble is reported at the FACP 90 seconds after the device drops from the mesh.	Initiate a system reset at the FACP at least 3 minutes after the trouble was initiated to clear. If the device was intentionally removed, no further action is needed. If the device was not intentionally removed, refer to panel history or active panel troubles to investigate the cause of the disturbance.

Table 2.1 Trouble Messages

Section 3: Wireless Devices

3.1 Description

The SWIFT Network consists of the following devices:

WIDP-PHOTO - Wireless Photoelectric Smoke Detector FCC ID: AUBWFSSD

The wireless photoelectric smoke detector is powered by four CR123A batteries. It has a sensor head to detect smoke and LEDs to indicate the activation and trouble status.

Base address set by the code wheels on the sync module will use:

- Type Code: Wireless Det:Photo

WIDP-ACCLIMATE - Wireless Acclimate Detector FCC ID: AUBWFSSD

The wireless Acclimate detector is powered by four CR123A batteries. It has a sensor head to detect smoke and LEDs to indicate activation and trouble status.

Base address set by the code wheels on the sync module will use:

- Type Code: Wireless Det: Acclimate

WIDP-HEAT-ROR - Wireless Rate of Rise Heat Detector FCC ID: AUBWFSSD

The rate of rise heat detectors are powered by four CR123A batteries. The detectors have LEDs to indicate the activation and trouble status.

Base address set by the code wheels on the sync module will use:

- Type Code: Wireless Det: Heat

WIDP-HEAT - Wireless 135° Fixed Heat Detector FCC ID: AUBWFSSD

The fixed heat detectors are powered by four CR123A batteries. The detectors have LEDs to indicate the activation and trouble status.

Base address set by the code wheels on the sync module will use:

- Type Code: Wireless Det: Heat

WIDP-MONITOR - Wireless Addressable Monitor Module FCC ID: AUBWFSMM

The wireless monitor module is powered by four CR123A batteries. It can be connected to a switch within three feet of its location or wired directly to the pull station. The module has LEDs to indicate the activation and trouble status.

Base address set by the code wheels on the sync module will use:

- Type Code: Wireless Switch - Manual Pull

WIDP-RELAY - Wireless Addressable Relay Module FCC ID: AUBWFSRM

The wireless relay module is powered by four CR123A batteries. It provides the system with a dry-contact output for activating a variety of auxiliary devices, such as fans, dampers, control equipment, etc. Addressability allows the dry contact to be activated, either manually or through panel programming, on a select basis. The module has an LED to indicate the activation and trouble status.

Base address set by the code wheels on the sync module will use:

- Type Code: Wireless Relay - Output

WIDP-PULL-DA - Wireless Addressable Pull Station FCC ID: AUBWFSPS

The wireless pull station is powered by four CR123A batteries. The module has an LED to indicate the activation and trouble status.

The pull station will occupy one module address.

- Type Code: Wireless Switch - Manual Pull

SWIFT Wireless Addressable AV bases FCC ID: AUBWFSAV

The wireless AV base is powered by eight CR123A batteries. Four of the CR123A batteries are used to power the notification element and four of the CR123A batteries are used to power the radio communication element. The module has an LED to indicate the activation and trouble status. The module requires a non-compact wall or ceiling System Sensor L-series notification device (ordered separately). A notification device with an audible component must be set to a non-coded setting (i.e. continuous or Temp3). Each AV Device requires two (2) consecutive SLC addresses on the fire panel. Use the rotary code wheels on the AV device to set the base address. The AV Device will also occupy the address following the base address. (Base +1)

The base address on the AV base will require the following configuration:

- Type Code: Wireless Relay - Output

Base+1 address will use the following configuration:

- Type Code: NAC Module - Output Point

Wireless related trouble events described in Section 3.6.3 will be indicated at the base address. Open circuit at the base+1 address will indicate a missing notification device. Short circuit at the base+1 address will indicate a incorrectly configured or faulted notification device.

Both module points will be used to drive the output of the AV unit to the desired pattern below:

Base Address	Base+1 Address	Notification Pattern
OFF	OFF	Off
ON	OFF	Strobe Only (Audible Silenced)
ON	ON	Strobe & Audible active
OFF	ON	Magnet Test mode (Strobe & audible activate when magnet is placed on the unit)

NOTE: To configure an audible/visual unit to silence only the audible component with a signal silence command, configure both addresses to activate for the alarm condition, the base address shall be non-silenceable and the base+1 shall be silenceable with the appropriate resound settings.

W-SYNC - Wireless Addressable Sync Module FCC ID: AUBWFSSM

The wireless sync module is 24VDC externally powered and requires 4 supplemental CR123A batteries. The module has an LED to indicate the activation and trouble status. The wireless sync module will occupy two consecutive SLC module addresses.

Base address set by the code wheels on the sync module will use:

- Type Code: Wireless Relay - Output

Base+1 address will use the following configuration:

- Type Code: NAC Module - Output

Wireless related trouble events described in Section 3.6.3 will be indicated at the base address.

The end of line supervision of the monitor input and the power monitoring of the external 24VDC supply will be indicated at the base+1 address.

The following table indicates the output state.

Base Address	Base+1 Address	Control Output Signal	Synchronization Output Signal
OFF	OFF	Low (inactive)	Low (inactive)
ON	OFF	High (active)	Strobe Only (Audible Silenced)
ON	ON	High (active)	Strobe & Audible active
OFF	ON	High (active)	Magnet Test mode

NOTE:
1. To configure a NAC circuit, with audible and visual units, to silence only the audible component with a signal silence command, configure both addresses to activate for the alarm condition. The base address shall be non-silenceable and the base+1 shall be silenceable with the appropriate resound settings.
2. When the sync module is being used for delivering only the synchronization signal (i.e. applications with the MDL3), it is recommended to leave the base address point constantly active to eliminate any delay in initial synchronization.

NOTE: When a wireless relay, wireless AV base, or wireless sync module is in use in the system, module device count must be limited to 109 modules per loop. This includes wired and wireless modules that are on the same loop. The module address range must be within 1-109.

3.2 Agency Approvals

3.2.1 FCC

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

WARNING: DO NOT MAKE CHANGES TO THE EQUIPMENT

CHANGES OR MODIFICATIONS NOT EXPRESSLY APPROVED BY THE MANUFACTURER COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

3.2.2 Federal Institute of Telecommunications

This device utilizes the Honeywell915 rev A radio module and complies with IFETEL standard(s).

IFT: RCPHOSW14-1983

3.3 Specifications

The following are the specifications for the wireless devices.

Specification	Data
Radio Frequency	Lower ISM Band (902-928 MHz)
Maximum power output	+17dBm
Minimum signal strength level needed at the receiver for a primary path with weak link trouble reporting enabled.	-55dBm
Minimum signal strength level needed at the receiver for a secondary path or primary path with weak link trouble reporting disabled.	Must be 18 dBm higher than the noise floor down to -80dBm
Maximum ambient noise level	-85dBm
Minimum battery life	2 years (where the activation of a wireless device is used for fire purposes only)

Table 3.1 Wireless Device Specifications

3.4 Installing, Mounting, and Wiring Devices

For information on installing the wireless devices, refer to the documents referenced in Section 1.3 on page 8.

3.4.1 Batteries

Install either Panasonic CR123A or Duracell DL123A batteries.

WARNING: RISK OF FIRE AND BURNS

DO NOT RECHARGE, OPEN, CRUSH, HEAT ABOVE 212°F (100°C), OR INCINERATE. KEEP BATTERY OUT OF REACH OF CHILDREN AND IN ORIGINAL PACKAGE UNTIL READY TO USE. DISPOSE OF USED BATTERIES PROMPTLY. REPLACE BATTERY WITH PANASONIC CR123A OR DURACELL DL123A. USE OF ANOTHER BATTERY MAY PRESENT A RISK OF FIRE OR EXPLOSION.

WARNING: RISQUE D'INCENDIE ET DE BRÛLURES

NE PAS RECHARGER, OUVRIR, ÉCRASER, CHAUFFER AU-DESSUS DE 212°F (100°C) OU INCINÉRER. GARDEZ LA BATTERIE HORS DE PORTÉE DES ENFANTS ET DANS L'EMBALLAGE D'ORIGINE JUSQU'À CE QU'ELLE SOIT PRÊTE À L'EMPLOI. JETEZ RAPIDEMENT LES PILES USAGÉES. REMPLACEZ LA BATTERIE PAR PANASONIC CR123A OU DURACELL DL123A. L'UTILISATION D'UNE AUTRE BATTERIE PEUT PRÉSENTER UN RISQUE D'INCENDIE OU D'EXPLOSION.

3.5 Configuration and Programming

Device configuration starts with assigning a profile.

3.5.1 Assigning Profiles

To assign a profile, the device must be in a factory default state. A single red light flashes on the LED confirming that the device is in the default state. To restore the device to factory default state, refer to Section 3.5.3, "Restoring a Device to Factory Default".

SWIFT Tools must be used to assign a profile.

1. Connect the W-USB device to your computer. For more information on the W-USB adapter, refer to Section 5.
2. Launch the SWIFT Tools application. Refer to Appendix A, "SWIFT Tools" for more information on the programming utility.
3. From the Home Screen, select the **Create Mesh Network** function.
4. Create a new profile or import an existing profile as required.
5. Select and open the profile to be assigned to the gateway from the Name drop-down box in the Profile section.

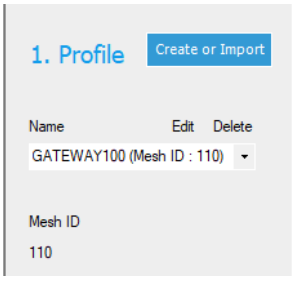


Figure 3.1 Creating or Importing a Profile

6. Power on the device within approximately 20 feet of the laptop running SWIFT Tools.
7. Ensure that the **Scan On** selection box in the communicator panel is checked.

8. Select the device from the **Communicator** panel.

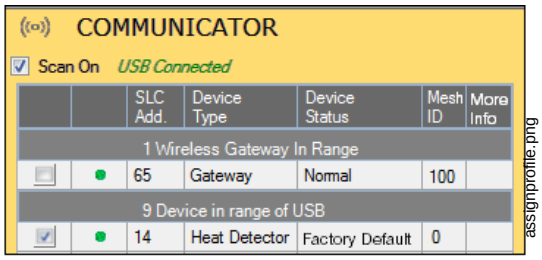


Figure 3.2 Selecting a Device

9. Click **Assign**. The device is now included in the list of devices with a profile assigned. When the profile is assigned, the green LEDs turn on steady for 10 seconds.

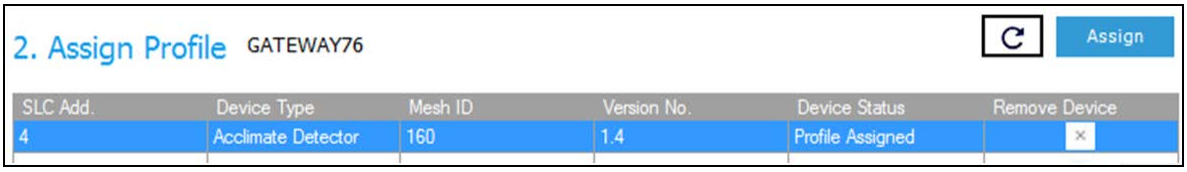


Figure 3.3 Assigning a Profile

10. If more devices need to be assigned profiles, all devices that have been assigned profiles in the Assign Profile table must be removed by clicking the “x” prior to adding the new devices.

NOTE: Only 49 devices can be assigned to one Gateway.

3.5.2 Mesh Formation

To add a device to a mesh, refer to the topic2.8.3, "Create a Mesh Network". To form a mesh network, ensure that the gateway is powered on and contains a profile. Activate the mesh formation (refer to Figure 2.2) magnetic sensor on the gateway.

Repeater

The SWIFT Network does not require the use of a dedicated repeater as all wireless devices act as repeaters. When the repeater function is needed in a location where no specific fire function is required, a wireless monitor module or another device can be installed to act as a repeater.

3.5.3 Restoring a Device to Factory Default

SWIFT Tools must be used to restore a device to its factory default state.

1. Connect the W-USB device to your computer. For more information on the W-USB adapter, refer to Section 5.
2. Launch the SWIFT Tools application. Refer to Appendix A, “SWIFT Tools” for more information on the programming utility.
3. From the Home Screen, select the **Site Survey**, **Create Mesh Network**, or **Diagnostics** function.
4. Click **Operations** and select **Set device to factory default**.

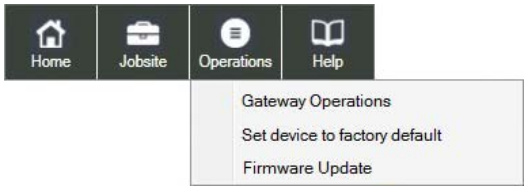


Figure 3.4 Operations Menu

5. Tamper the device (or activate the hall sensor on the detector) and place powered-on devices that are to be reset in range of the W-USB adapter. Once the device has been tampered (or hall sensor activated), a 60 minute countdown will start for profile removal.

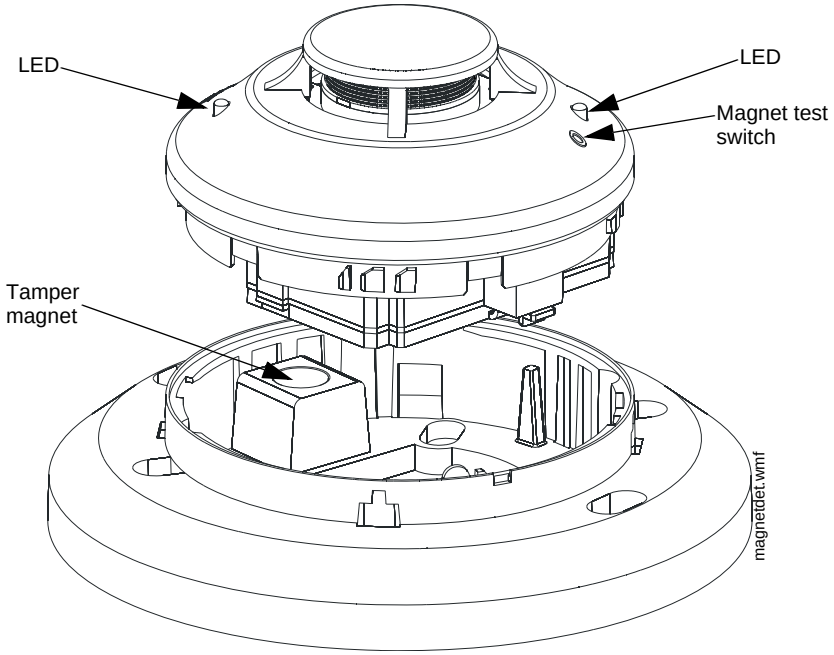


Figure 3.5 Magnetic Sensor on a Detector

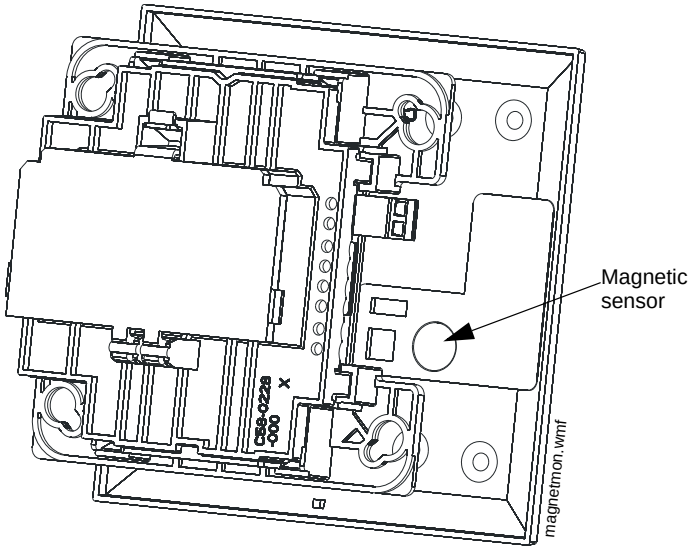
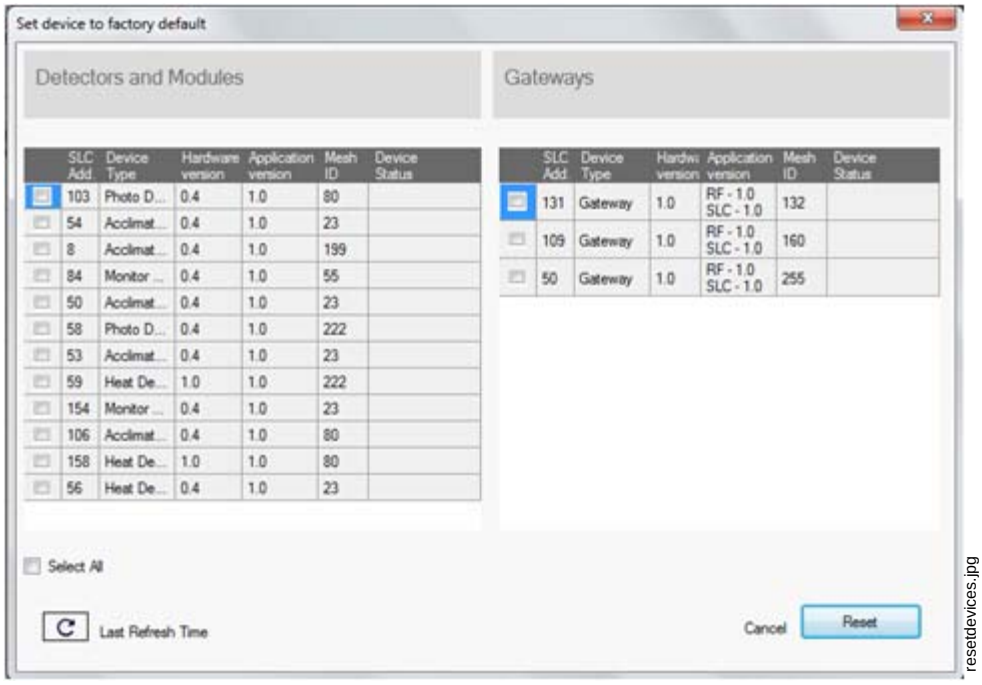


Figure 3.6 Magnetic Sensor on a Module

6. The **Reset Devices** screen appears, displaying the gateway and other devices that have a profile assigned. Click to select the desired device and click **Reset Device** to remove the profile.



resetdevices.jpg

The profile is removed and the device is reset to the factory default state.

3.6 Device Operations

3.6.1 Modes of Operation

Factory Default Mode

In this mode, the devices are not associated with the gateway. A profile must be assigned to associate the device with the gateway. For further information on assigning a profile, refer to Section 2.8.1, “Assign a Profile”, on page 15. A device cannot perform any fire protection in the factory default state. In default mode, the devices will be viewable in the communicator window of SWIFT Tools with the state displayed as “Factory Default”. A device in factory default can be used for site survey.

Site Survey Mode

A site survey assesses and qualifies a site for installing a SWIFT network. The site survey view in SWIFT Tools gives the Radio Frequency (RF) assessment of the site. The tool reports the suggested device spacing based on the data collected during the site survey. This helps to improve the reliability and performance of a SWIFT network in the wireless fire alarm system. A device cannot perform any fire protection in the site survey mode. A device that is ready to enter site survey will indicate “pending site survey” in the communicator section of SWIFT Tools. A device in site survey will not communicate with SWIFT Tools and will be listed as “offline” in the communicator section. For more information on performing a site survey, refer to Appendix B.

Profile Assigned Mode

In this mode, devices are associated with the gateway but are not active participants in the mesh network. A device that is not in the tampered state can join a mesh network in formation or during rescue mode. For further information on mesh formation, refer to “Mesh Formation Mode” on page 36. For more information on rescue mode, refer to “Rescue Mode” on page 36.

Devices are not enabled for fire protection until they become part of a mesh network. A device will show a or no answer/missing at the FACP.

In this mode, devices are viewable in the communicator window of SWIFT Tools. If the device has a profile and is in the tampered state, it will indicate a status as “Profile Assigned-Tamper”. A non-tampered device will indicate “active scan” as it searches for a mesh network.

Bootloader Mode

In this mode, a device is ready for an update. It cannot participate in a mesh network and cannot provide fire protection. The device is viewable in the communicator window of SWIFT Tools with the status “Bootloader”. To remove a device from bootloader mode, refer to Appendix C.

Mesh Participant Modes

Devices that are in the mesh network no longer communicate directly with SWIFT Tools. SWIFT Tools must communicate with the gateway for status information on a device that has joined a mesh. The gateway will respond to the FACP for the device at the address set with the SLC rotary address wheels.

■ Mesh Formation Mode

In this mode, a device is an active participant in a mesh that is forming. The LED will blink green then yellow every 6 seconds. The device cannot perform any fire protection in this state. The device responds to its SLC address with an “INITIALIZING” trouble. For further information on mesh formation mode, refer to “Section 3.5.2”.

■ Initial Mesh Restructuring Mode

In this mode, the mesh network is formed and is in the process of establishing stronger communication paths. The LED will blink yellow every 6 seconds. The device cannot perform any fire protection in this state. The device responds to its SLC address with a “INITIALIZING” trouble.

■ Normal Mode

In normal mode, the mesh network is formed and provides fire protection. The LED will blink every 18 seconds. The LED flash can be disabled by panel configuration. If a device is in trouble, it is indicated by the trouble messages.

■ Rescue Mode

In rescue mode, a devices is an active participant of a mesh network. It will search and retrieve any device that has lost communication with the network. Rescue mode is indicated by a green LED blink every 12 seconds for up to 3 minutes.

3.6.2 LED Indicators

The two LEDs on the devices blink in the same pattern to allow the LEDs to be viewed from any angle. The LED indicators are provided in Appendix D on page 53.

3.6.3 Trouble Conditions

The following trouble conditions are unique to the battery powered RF devices.

Trouble Conditions with Fire Protection

The devices indicate the following trouble conditions with a single yellow LED blink every 14 seconds. The wireless device will still perform fire protection during the following trouble states.

■ Low Battery

The low battery event denotes:

- The device has a minimum of one week power left to perform the required operations.
  Or
- One (or more) of the batteries is missing or dead.

The low battery event is a latching condition. To clear the low battery event, tamper the device and replace all four batteries. When a device is tampered, it drops out of the mesh network and attempts to rejoin as soon as the batteries are replaced and the tamper event is cleared. If the device has dropped from the mesh prior to the tamper event, a system reset has to be issued to clear the low battery trouble. The panel displays “LOW BATTERY” or “LOW BATT” during a low battery condition.

■ Weak Link

The weak link trouble denotes a connection of insufficient primary parent link signal strength. To resolve a weak link, reduce the distance between devices, place them away from obstructions, or add a repeater. Tamper the device when moving it to a new location. Restart mesh formation after a repeater is installed or after a device has been relocated and the tamper condition is cleared. Terminate mesh formation once the devices have joined the mesh or allow mesh formation to timeout. Restructuring will automatically start and the gateway will reevaluate the link connectivity between all devices and select suitable signal paths.

Weak link trouble reporting can be disabled at the FACP or at the gateway for installations not requiring primary link connectivity. Refer to Section 2.9.5 for more information on disabling weak link trouble reporting. Refer to the troubleshooting section for more information on resolving a weak link condition.

The panel displays “WEAK LINK” for a device that is in the weak link condition.

■ Class A Fault

The Class A fault denotes a single connection path from the device. The wireless system is a Class A system requiring two communication paths for normal operations. To remedy the Class A fault, ensure adequate device spacing. The use of a repeater may be required. The wireless mesh is a self-healing network. If the trouble is not cleared within 5 minutes, additional actions may be required. Refer to the troubleshooting section for tips on resolving Class A fault conditions.

The panel will display “RF CLASS A” during a Class A fault condition.

Trouble States without Fire Protection

■ Jamming

Jamming occurs when a device is overloaded with an interfering RF signal but is able to send outgoing messages. A jamming event is detected after 20 seconds of exposure to the jamming signal. In the event of jamming, the device will drop from the mesh network. The panel displays “RF JAMMING” during a jamming condition.

■ Duplicate Address

Two wireless devices on the same mesh network that are set to the same SLC address will report a duplicate address trouble at the FACP. The gateway will respond to the panel with the device type of the first device to join.

The panel displays “DBL ADDR” during a duplicate address condition.

■ Tamper

A tamper trouble indicates that a detector is not firmly attached to its base or the cover plate is not properly attached to a module. The tamper condition is annunciated in the following ways:

Device Indication The yellow LED on the device turns on steady for 4 seconds followed by a blink pattern of yellow, yellow, red every 15 seconds immediately after the tamper condition.

Panel Indication Devices that are in the tampered condition report a latching trouble event. The event is active for 90 seconds before it can be removed with a system reset. Once the event is removed, the device reports a “TAMPER” until the device is restored or the point is removed from the database.

Clearing the Tamper To clear the tamper,

- For a detector, ensure that the magnet has not been removed from the base and the detector is locked together with its base.
- For a module, ensure that there is a magnet in the cover plate and it is securely fastened to the device in the correct orientation.

Once the tamper event is cleared, the LEDs in the device turn on steady for 2.5 seconds, in the following color patterns that denote the battery status.

- **Green -** All the four batteries are installed and fresh. The device has a minimum one year of normal operation.
- **Yellow -** All the four batteries are installed, and one or more is no longer fresh. This device has between a minimum of 1 month and 1 year of operation.
- **Red -** One or more of the batteries are low in power and/or the device has a minimum of one week of operation.

After the device displays the current battery condition, it attempts to join the mesh network in the rescue mode or normal mode. This is indicated by a double yellow blink every 3.4 seconds. If a device does not find its mesh in the rescue mode, it searches for its mesh under formation. This is indicated by a double yellow blink every 20 seconds.

■ No Answer

A device that is not in the mesh, displays a “MISSING” message at the FACP. Follow the steps in “Mesh Formation Mode” on page 36 to have a device join the mesh.

■ Device Initialization

A device reports a device initialization trouble when it is part of a mesh network but is not capable of performing fire protection. This is the case for mesh networks that are still forming or going through initial restructuring. The panel displays “INITIALIZING” during a device initialization condition.

Section 4: W-SYNC Wireless Synchronization Module

4.1 Description

The wireless synchronization module works with wireless AV bases to provide audio and visual synchronization of a wireless notification appliance to a wired notification appliance. Synchronization is only available with notification appliances that use the System Sensor synchronization protocol. The W-SYNC also provides wireless control and monitoring of a Notification Appliance Circuit (NAC) expander or power supply. It does not support the "whoop" pattern.

The wireless synchronization module operates from 24VDC power with supplemental battery support. A trouble will be generated at the panel if batteries are not installed or at a low battery level. Synchronization is not available during supplemental battery operation. For more information on the W-SYNC, refer to *Document I56-6518* that ships with the product.

4.2 Wiring

The W-SYNC may be wired to compatible FACPs using an MDL3 Sync Module or the HPFF8/HPFF12 NAC Expanders. The synchronized output wiring must be contained in the common enclosure of modules or wired in conduit in enclosures mounted within 20 feet of each other in the same room with wiring in conduit.

When Class A zones are used, power supply wiring must be contained in the common enclosure with the W-SYNC, or the power supply and W-SYNC must be in enclosures within 20 feet of each other in the same room with wiring in conduit.

4.2.1 FACP

Wire the W-SYNC to the FACP as shown below.

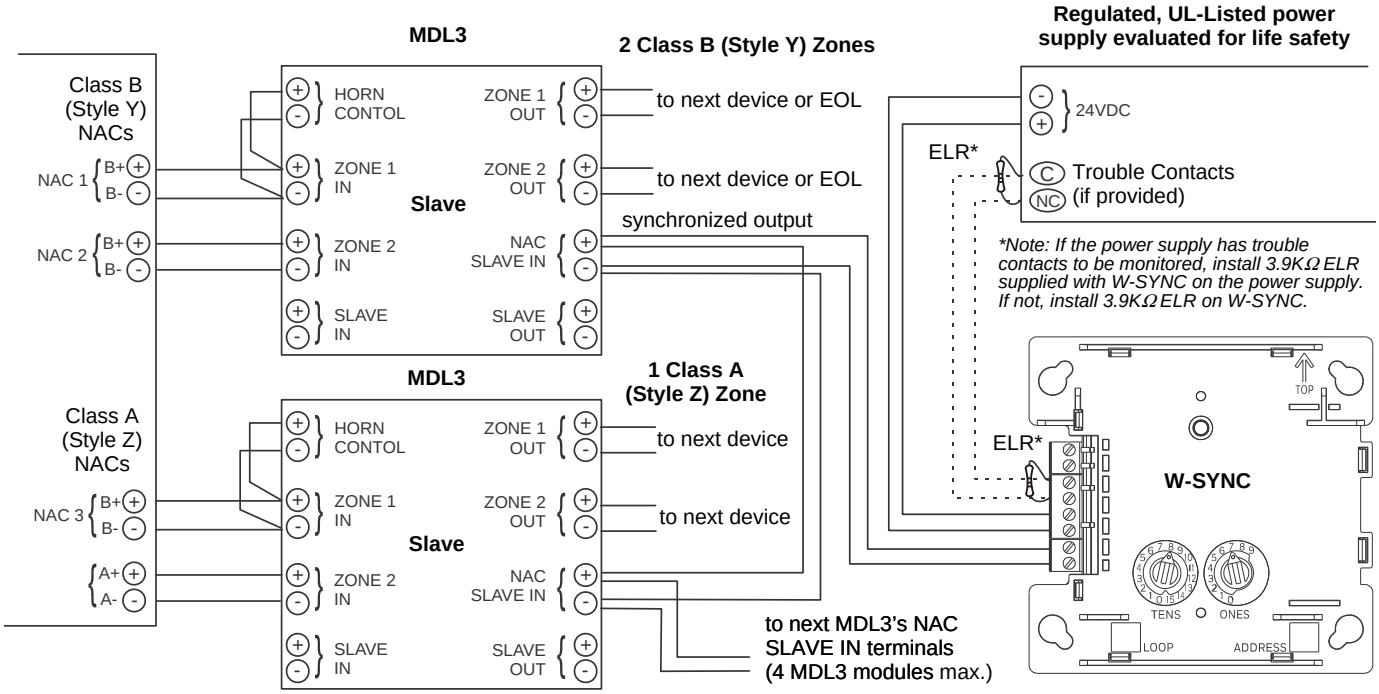


Figure 4.1 W-SYNC Wiring to FACP

4.2.2 HPFF8/HPFF12 NAC Expander

When using the HPFF8 or HPFF12 to power the W-SNYC module, set the DIP switches on the HPFF8/HPFF12 as follows:

- SW1- OFF
- SW2- OFF
- SW3- OFF
- SW4- OFF
- SW5- ON
- SW6- OFF

Wire the W-SYNC to the HPFF8/12 as follows):

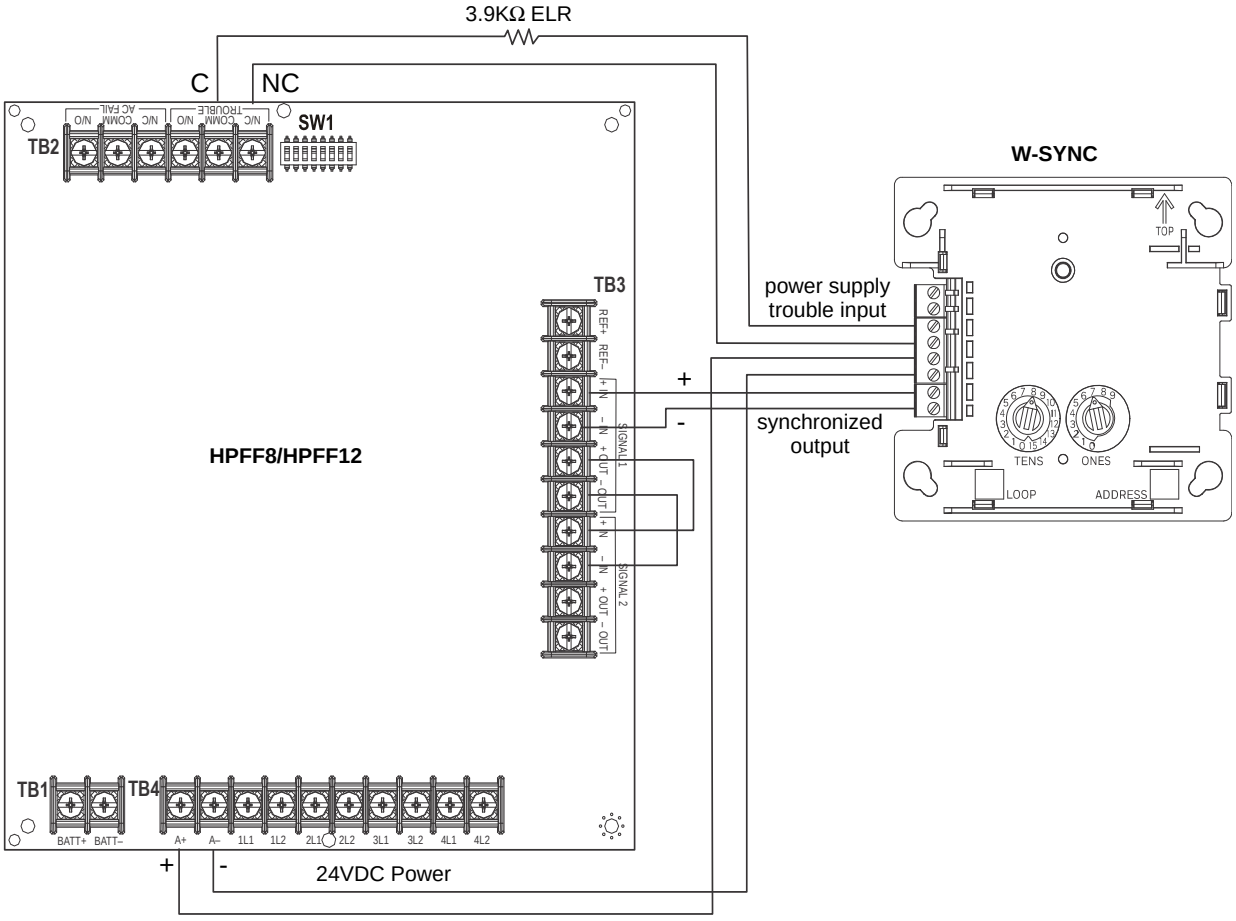


Figure 4.2 W-SYNC Wiring to HPFF8/HPFF12

Section 5: W-USB Adapter

5.1 Introduction

The W-USB adapter is a software interface that can be connected to a PC (running SWIFT Tools) through a USB port. It communicates with the RF devices using the same frequencies as the mesh protocol. This device is powered directly by the USB port.

The LED gives an indication of power and initialization status.

Color	Description
Red	Device has power but is not initialized or the driver is missing.
Yellow	Device is initialized and ready.
Blue	Device is updating or failed to load properly. Complete the update or re-power the device. If problems persist, contact technical support.

The W-USB adapter has an adjustable USB connector to facilitate connection by reducing the size when connected to a laptop/tablet.

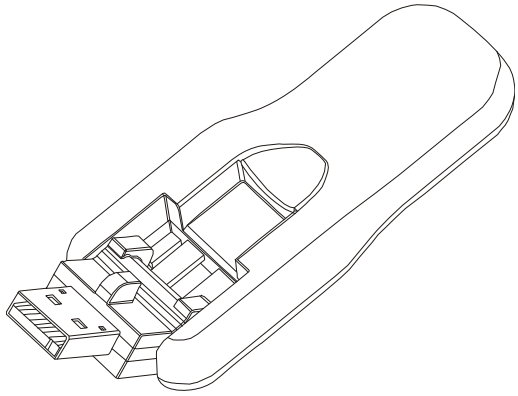


Figure 5.1 W-USB Adapter

5.2 Agency Approvals

5.2.1 FCC

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

FCC ID: PV3WFSADPT

WARNING: DO NOT MAKE CHANGES TO THE EQUIPMENT.

CHANGES OR MODIFICATIONS NOT EXPRESSLY APPROVED BY THE MANUFACTURER COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

5.2.2 Federal Institute of Telecommunications

This device utilizes the Honeywell915 rev A radio module and complies with IFETEL standard(s).

IFT: RCPSYWU14-1829

5.3 Specifications

5.3.1 Electrical Specifications

- Operating voltage: 4.3 VDC - 5.5 VDC (5VDC typical)
- Supply current: 25 mA - 85 mA (33 mA typical)

5.3.2 Serial Communication Specification

- USB standard 2.0

5.3.3 Mechanical Specifications

- USB Connector type A
- Length with connector closed: 3 in. (76.2 mm)
- Length with connector open: 3.8 in. (96.2 mm)
- Thickness on connector side: 0.5 in (13 mm)
- Thickness on antenna side: 0.3 in. (8.4 mm)
- Width: 1.2 in. (31.2 mm)
- Weight: 0.7 oz. (19.5 g)

5.3.4 Environmental Specifications

- Humidity: 10%RH - 93%RH, non-condensing
- Maximum operating temperature: 32°F - 122°F (0°C - 50°C)
- Storage temperature: 14°F - 140°F (-10°C - 60°C)

5.4 Driver Installation

NOTE: Install SWIFT Tools before attempting to install the driver.

To install a driver:

1. Insert the W-USB adapter into the PC. The W-USB adapter is detected and is displayed in the Computer Management screen as a **SWIFT USB Communication Device**.

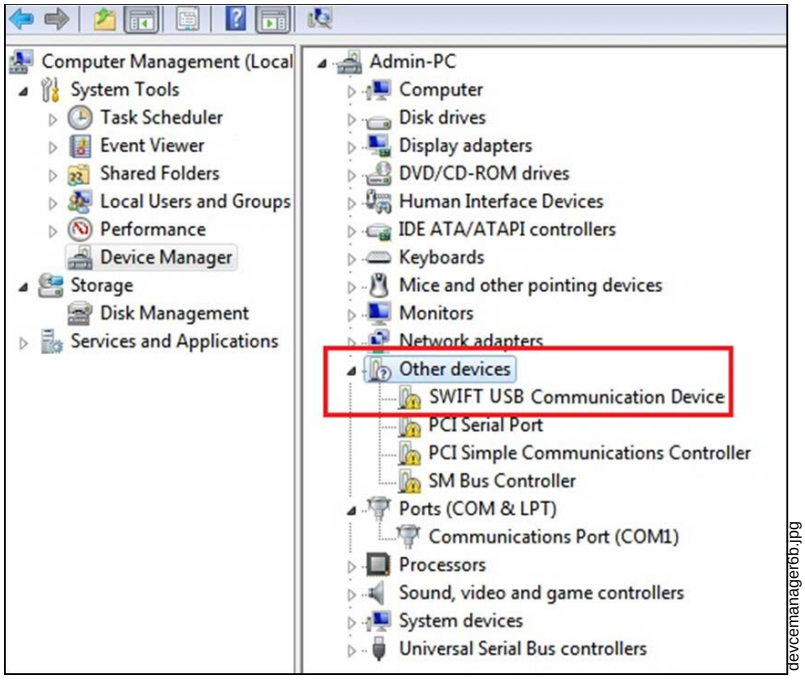


Figure 5.2 Computer Management Screen

2. Right click on **SWIFT USB Communication Device** and select **Update Driver Software**.

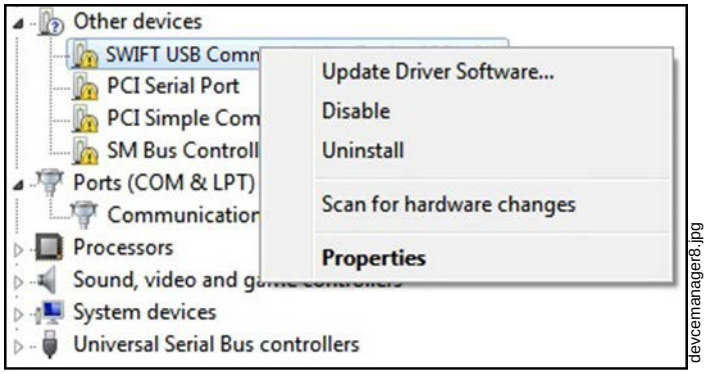


Figure 5.3 Update Driver Software

3. Select the **Browse my computer for driver software** option.

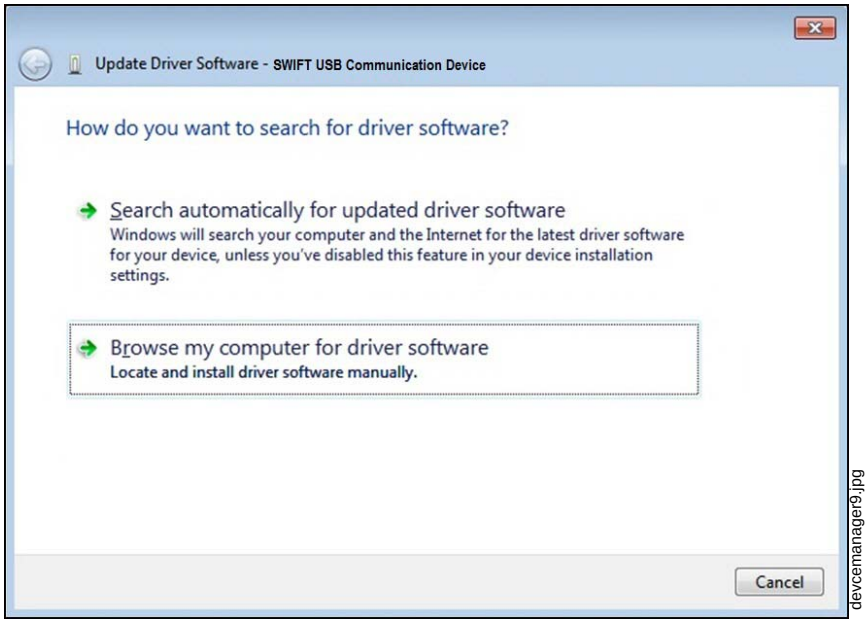


Figure 5.4 Browse Computer for Driver Software

4. The Browse dialog box appears. Click **Browse**. Navigate to the folder: C:\Program Files\Honeywell\Device Driver. Click **Next**.



Figure 5.5 Browse Folder for Driver Software

5. The confirmation message displays when the driver software is updated successfully.

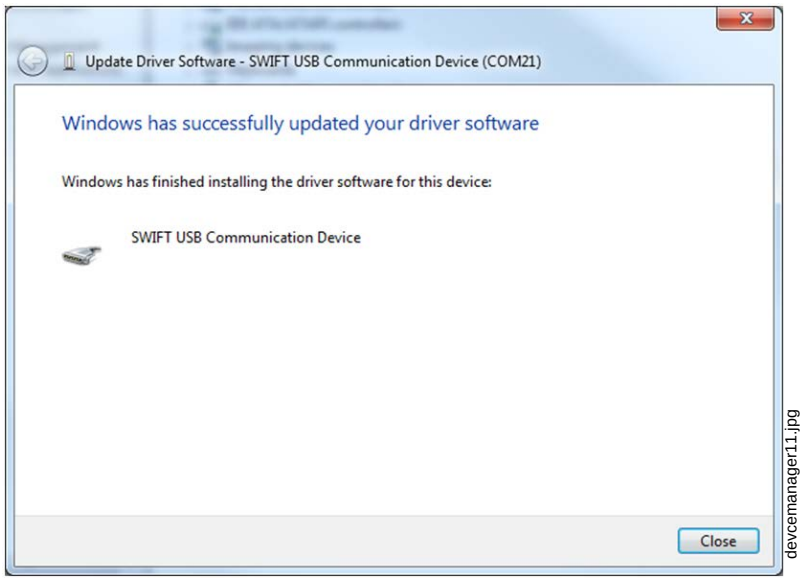


Figure 5.6 Driver Software Update Confirmation

The newly installed device will now display on the computer management screen under Ports.

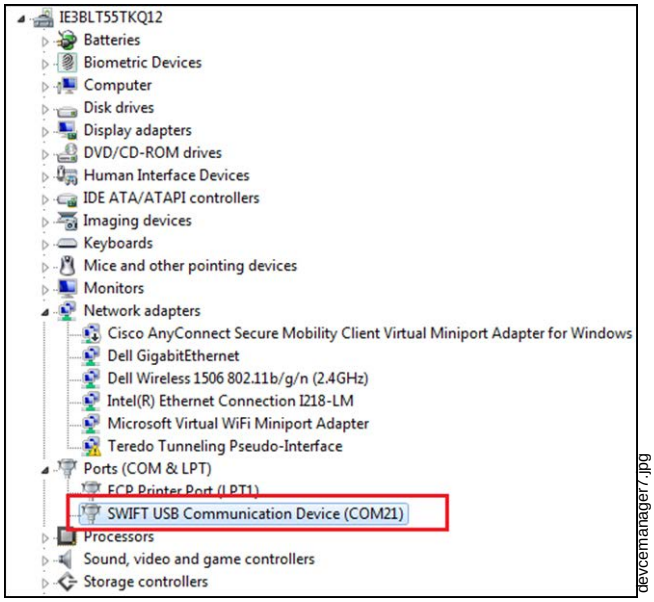


Figure 5.7 New Communications Port

If SWIFT Tools detects an incompatible W-USB adapter connected, it will prompt a message to update the W-USB adapter firmware.



Figure 5.8 Incompatible W-USB Adapter Message

If you get this error message, update the W-USB adapter through the Firmware Update feature in the Operations section of SWIFT Tools.

Appendix A: SWIFT Tools

A.1 Description

SWIFT Tools is a standalone desktop Windows® application. It is a configuration and maintenance tool for the gateway and devices of the SWIFT Network. Site surveys, device configurations, and diagnostic functions are all part of SWIFT Tools. SWIFT Tools can be installed on a PC or a laptop and communicates with the gateway and wireless devices through USB-based user interface. Connect the W-USB to the computer to invoke the SWIFT Tools application. At any point, only one instance of SWIFT Tools can run on a laptop or PC.

SWIFT Tools has the following utilities:

- ✓ Site Survey view
- ✓ Creating Mesh Network
- ✓ Diagnostic view

SWIFT Tools works in a wireless environment with the gateway and devices within a range of approximately 20 feet.

SWIFT Tools is designed for systems running Microsoft Windows. Minimum system requirements are listed below.

Component	Minimum Requirement
Operating System	Windows 7 and Windows 8 (32 bit and 64 bit)
Hard Drive	20 GB hard drive space with minimum 1GB free space on hard disk.
RAM	Minimum 512MB RAM
Processor speed	1GHz minimum (2.4 GHz recommended) Processor, 512K Cache
Regional Settings	English (United States)

Table A.1 System Requirements

A.2 Launching SWIFT Tools



To launch SWIFT Tools,

1. Click **Start**, point to **All Programs**, click **SWIFT Tool**, and then **SWIFT Tool**. The following screen is displayed. Alternatively, SWIFT Tools can be opened through a shortcut located on the desktop.
2. The **SWIFT Tools** screen is displayed. Create a new jobsite or open an existing one.

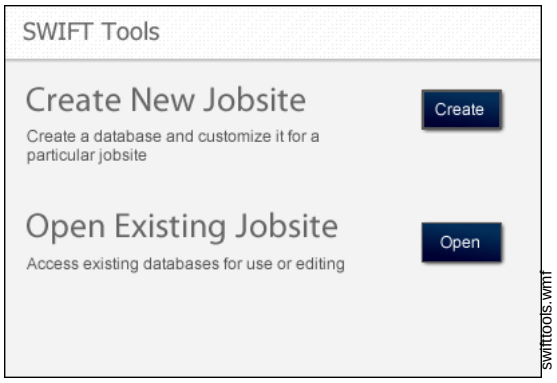


Figure A.1 SWIFT Tools Screen

A.2.1 Creating a New Jobsite

To create a new jobsite:

1. Click **Create** from the SWIFT Tools screen.
2. Enter the name of the new jobsite in the **Jobsite Name** field.
3. Enter the **Location/Description** if any, and click **Create**.
4. The **Create Project** dialog box opens. Navigate to the desired folder location where the project will be saved.
5. Click **Save**.

The jobsite is created and the following screen is displayed. From this screen a site survey may be conducted, a mesh network may be created, and troubleshooting may be performed. Click the **Start** button for the desired function.

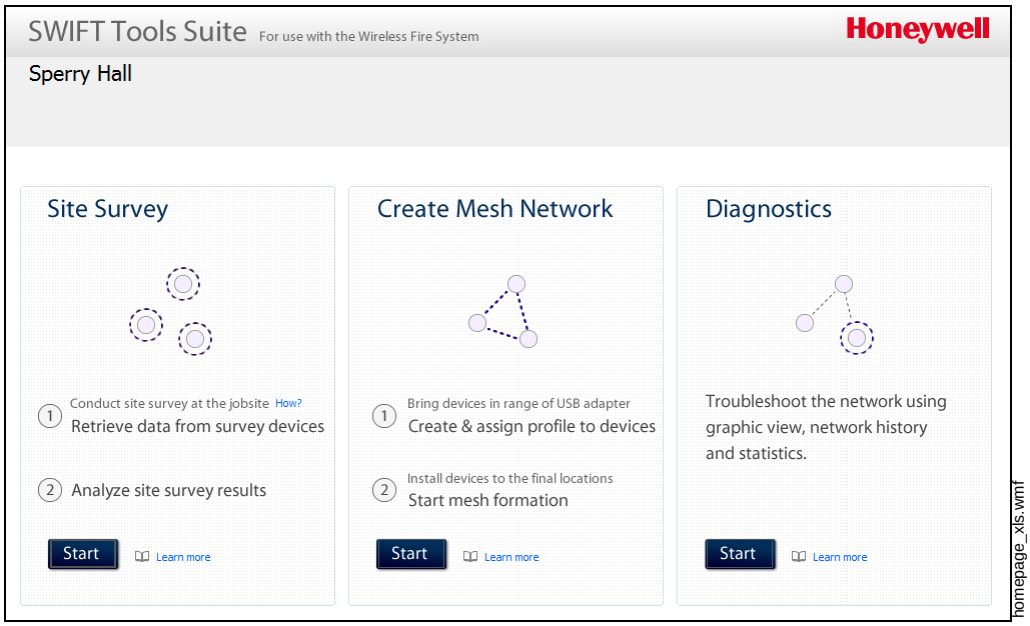


Figure A.2 Home Screen

For more information on performing a site survey, refer to Appendix B. To create a mesh network, see page 17. For help with diagnostics, refer to Appendix C.

A.2.2 Opening an Existing Jobsite

To open an existing jobsite:

1. Click **Open** from the SWIFT Tools screen.
2. Navigate to the folder containing the jobsite file. Select to highlight the file and click **Open.**

The existing jobsite is opened and Home screen is displayed. From this screen a site survey may be conducted, a mesh network may be created, and diagnostics may be performed. Click the **Start** button for the desired function.

For more information on performing a site survey, refer to Appendix B. To create a mesh network, see page 17. For help with diagnostics, refer to Appendix C.

A.3 Connecting to the Gateway

For security purposes, access to the gateway via SWIFT Tools requires the user be present inside the building and have physical access to the gateway before they can establish a limited duration communication session that times out after a period of inactivity. To connect to the gateway via SWIFT Tools, perform the following steps.

A.3.1 Accessing a Locked Gateway

1. Select the desired gateway.
2. Enter a valid password into SWIFT Tools.
3. SWIFT Tools will show a 120 second timer.
4. Use a magnet to activate either of the two sensors on the gateway within the 120 second time-frame. The LEDs will turn on steady yellow. The gateway LEDs will blink green and then resume normal operation.
5. Communication between the Tools and the gateway is now available. The system has a 30 minute inactivity timer. If no activity is detected within 30 minutes, the connection between the Tools and gateway will close. The user will need to repeat steps 1-3 to reconnect.

A.3.2 Creating a New Password for a Gateway

1. Select the desired gateway.
2. Assign a valid password to SWIFT Tools.
3. SWIFT Tools will show a 120 second timer.
4. Use a magnet to activate either of the two sensors on the gateway within the 120 second timeframe.The gateway LEDs will turn on steady yellow.
5. The LED resumes to normal operation once magnet is activated or the wait for Magnet Activation times out. Communication between the Tools and the gateway is now available till the user accesses. The system has a 30 minutes inactivity timer. If no activity is detected within 30 minutes, the connection between the Tools and gateway will close. The user will need to repeat steps 1-3 to reconnect.

Appendix B: Site Survey

A site survey is recommended to assess and qualify the site prior to installing a SWIFT network. The site survey consists of a link quality test and RF scan test. After both tests are completed, the results of the site survey can be obtained using SWIFT Tools. The information provided by SWIFT Tools is used for site qualification, maximum device spacing identification, and configuring the network. This helps to improve the reliability and performance of the wireless network in the wireless fire alarm system.

B.1 Conduct a Site Survey

B.1.1 Link Quality Test

A link quality test is a quick and repeatable test that provides immediate feedback on device connectivity. The link quality test sends data from one device to another to test for data loss and measure the signal strength. In a link test, the device addresses are set in the range of 001 to 150. A minimum of two devices are needed to conduct a link quality test.

A link test is conducted between two or more devices. The link test starts when a device that is in the “pending site survey” state has its tamper condition cleared. The device will send a burst of data to the next address lower than its own address. The lower addressed device will automatically return the link quality test results for display using the device LEDs. For example, clearing the tamper condition on a detector set to address 2 (D002) will make the detector enter the link quality test. D002 will send a burst of data to a device at address 001 (either detector or module). The device at address 001 will measure the signal strength and count the data received in the burst and return the information to D002. The results of the test will be displayed at D002. The test can be repeated by tampering D002 to return it to the “pending site survey” mode and then clearing the tamper.

Basic Requirements of a Link Quality Test

To conduct a link test:

- ✓ two or more devices (detectors) are required.
- ✓ devices must be in factory default state. The LEDs on the device will blink single or double red to confirm it is in the factory default state. Refer to Section 3.5.3 on page 33 for more information on setting the device to factory default state.
- ✓ device addresses can bet set in the range of 1 to 150.

Conduct a Link Quality Test

To conduct a link quality test:

1. Remove the batteries from the devices that will be used for the site survey and set the SLC address. To set an SLC address, use a flathead screwdriver to adjust the rotary switches on the device.
    1. For the first device used in a site survey, set the SLC address to 001.
    2. For each subsequent device, use the next highest SLC address (up to address 150). For example, the first device was set to 001, set the second device to 002, and the third device to 003, etc.
2. Bring the first device (001) to the first location to conduct the test.
3. Insert *one* battery into the device. Inserting more than one battery deters the device from entering the site survey mode. The device is ready for site survey mode if the LED blinks yellow every 5 seconds.
4. Clear the tamper condition to proceed with the test. To clear the tamper condition on a detector, insert the detector into the base and twist to lock the detector completely into the base. To clear the tamper condition on a module, attach the faceplate to the module. When the tamper is cleared, the LEDs on the device starts blinking yellow every ½ second for approximately 20 seconds. The results appear in approximately 20 seconds and the LEDs on the first device change to solid red. This is due to the absence of a lower-addressed device with which to form a pair. This result is expected from the 1st device when a link quality test is performed.
5. Bring the second device (002) to the second location and insert *one* battery into the device. The device is ready for site survey mode if the LED blinks yellow every 5 seconds.
6. Clear the tamper condition to proceed with the test. To clear the tamper condition on a detector, insert the detector into the base and twist to lock the detector completely into the base. To clear the tamper condition on a module, attach the faceplate to the module. When the tamper is cleared, the LEDs on the device starts blinking yellow every 1/2 second for approximately 20 seconds. The results appear in approximately 20 seconds.
7. Repeat for subsequence devices.
8. The device will conduct a link test to the next lowest address; in this case device 001. The result of the link test from 002 to 001 is displayed by the LEDs on device 002. Refer to Table B.1 below.
9. Once the link test is complete between 002 and 001, continue for address 003, 004, etc. for all devices that will be used in the site survey. This test may be repeated any number of times. For devices addressed to 101 or higher, the test must be repeated, if desired, within five minutes of the last concluded test or the devices will start an RF scan test.

Results of a Link Quality Test

The following table explains the LED patterns before and during a link quality test.

State	Pattern	LED	Results & Description
Site survey pending	Double blink every 5 seconds	Red	Device is tampered, ready and waiting to start a site survey link quality test
Link quality test in progress	Single blink every ½ seconds	Yellow	Transmission of data to another device.
Link quality test complete	On steady	Red	Failure - no data received
Link quality test complete	Single blink every 5 seconds	Red	Poor - partial data received or signal strength measured lower than the acceptable limit for a primary or secondary link (-81dBm or lower)
Link quality test complete	2 blinks every 5 seconds	Green	Good - all data received at a signal strength acceptable for a secondary link but not for a primary link (-66dBm to -80dBm)
Link quality test complete	3 blinks every 5 seconds	Green	Great - all data received at a signal strength acceptable for a secondary link and marginally acceptable for a primary link (-51dBm to -65dBm)
Link quality test complete	4 blinks every 5 seconds	Green	Excellent - all data received at a signal strength acceptable for a primary link (-50dBm or better)

Table B.1 LED Patterns of Link Quality Test Results

The LED pattern for a link quality test will continue to be displayed until the device is tampered or the batteries die for a device that is addressed 100 or lower. For devices addressed 101 to 150, the result will be displayed until the device starts the RF Scan.

To repeat the link quality test, toggle the tamper state. To toggle the tamper state on a detector, twist the detector in the base counter-clockwise as if removing the detector from the base, then twist it back in clockwise to lock it in. To toggle the tamper state on a module, remove the faceplate and then reconnect it. Once the device is tampered, it will return to the pending site survey state. Once the tamper is cleared, the link quality test will be restarted. Only the results for the last link quality test are retained.

After a Link Quality Test

Retrieve the link quality test results for devices 001-100. To retrieve the site survey results, refer to the topicB.1.3, "Retrieving Site Survey Results"at the end of this section. For devices 101-150, wait to retrieve the link quality results until the device starts an RF Scan test.

B.1.2 RF Scan Test

A Radio Frequency scan test is conducted to assess and measure the background noise and interference from other wireless systems if any, in the site. The RF Scan test can be conducted individually or following the link quality test. An RF Scan test will be conducted for any device with an SLC address set between 101 and 150 at the end of a Link Quality Test.

Conduct an RF Scan Test

To conduct an RF scan test, follow the same procedure for a link quality test. However, the device addresses for an RF scan test must start at 101 and have the subsequent devices address set as 102, 103, etc. Each device will conduct the link quality test as described above, then transition to the RF scan test 5 minutes after the last link quality test is performed to or from that device.

If several devices are being tested, it is possible that some devices will start and complete the link test and progress to the RF scan test while other devices are finishing the link quality test. The RF Scan test may take up to 70 minutes. The time remaining and the test status are displayed at the device using the LEDs. The LED patterns are shown below.

Status of an RF Scan Test

State	Pattern	LED	Status
In Progress- 70 minutes remaining	7 short blinks every 30 seconds	Red	Bad
		Green	Good
In Progress- 60 minutes remaining	6 short blinks every 30 seconds	Red	Bad
		Green	Good
In Progress- 50 minutes remaining	5 short blinks every 30 seconds	Red	Bad
		Green	Good
↓	↓		
In Progress- 10 minutes remaining	1 short blink every 30 seconds	Red	Bad
		Green	Good
RF Scan Test Complete	On Steady	Red	Bad
		Green	Good

Table B.2 RF Scan Test Status - LED Pattern

B.1.3 Retrieving Site Survey Results

To retrieve the site survey results:

1. Return the device to “Pending Site Survey” or “Factory Default” mode. This is done by tampering devices that have completed a link quality test or by rebooting devices that have completed an RF scan test.

CAUTION: SITE SURVEY RESULTS WILL BE REPLACED

DO NOT CLEAR THE TAMPER ON A DEVICE THAT IS IN THE “PENDING SITE SURVEY” STATE OR THE EXISTING RESULTS WILL BE REPLACED.

2. Plug the W-USB adapter into the laptop/PC where SWIFT Tools has been installed.
3. Bring the devices within a range of approximately 20 feet from the W-USB adapter connected to the laptop/PC.
4. Log into SWIFT Tools and retrieve the data.

Appendix C: Troubleshooting and Testing

C.1 Troubleshooting

Problem	Description	Action
Class A fault condition	Device has a single parent connection, and is missing the redundant class A connection.	If a suitable parent is available, the background mesh restructuring routine should self-heal the network. If the network does not self-heal after ten minutes, reduce spacing between devices or utilize SWIFT Tools for suggested repeater placement to add stronger parents. Activate mesh formation to trigger a mesh restructuring routine to re-evaluate the trouble condition after taking action.
Jamming	Jamming occurs when a device is overloaded with an interfering RF signal and is unable to process incoming messages, but is able to report the condition to its parents.	A jammed device will automatically remove itself from the mesh network after reporting the jamming. The device will attempt to self-heal and recover into the network. Identify any possible sources of the jamming signal and see if the spacing from the device to the jamming source can be increased to an acceptable range. A site survey RF scan test can be used to categorize the jamming signal.
Low battery	One or more of the four batteries are missing/dead and/or the device has a minimum of one week of operation remaining.	To clear the low battery event, tamper the device and replace all four batteries. When a device is tampered, it drops out of the mesh network and attempts to rejoin as soon as the batteries are replaced and the tamper event is cleared. Once a low battery trouble is indicated there is a minimum of one week of operation before the device is non-functional.
Duplicate address/ Illegal address	Two or more wireless devices on the same mesh network that are set to the same address report a duplicate address trouble. An address set to zero will report an illegal address.	Change the address of the device(s) to avoid duplication and error.
Mesh formation does not find all devices	A device does not connect to the gateway/mesh network	Verify the device has a profile. Verify that the profile matches the profile in the gateway. Two different profiles may use the same mesh ID. Remove and re-profile the device to guarantee the correct profile. Verify the device is powered and the tamper condition is cleared. Check to ensure the tamper magnet has not become dislodged. Check the device spacing and the range from the device to the mesh. A site survey link test can be used to verify connectivity from one location to another.
Mesh restructuring does not end	The gateway/mesh network appears to be stuck in mesh restructuring	Use SWIFT Tools to investigate for the presence of interference such as Walkie talkie/ RFID reader or unstable devices (dropping and joining). Interference such as Walkie talkie/ RFID reader will prohibit restructuring from fully executing. Devices joining a mesh will delay the restructuring event.
Devices drop during operation	A device drop event is indicated in history.	Device drop is the predecessor to a Missing trouble. Inspect the area for any changes to the environment that could block radio communication. Use a site survey RF Scan to check for any interference and use a site survey link test to check the connectivity from the device to its closest neighbor.
RF Overlap (Max gateways) trouble reported	The number of Honeywell SWIFT systems that can co-exist in range of each other has been exceeded.	Use the network statistics provided by SWIFT Tools to identify the interfering networks and the nature of the fault. The networks will be listed by a unique number; this is not the serial number of the gateway. One or more of the systems will need to be powered down to clear the fault. Where possible, maximize the number of devices on a mesh network to reduce the number of total mesh networks; i.e. use one mesh network with 50 devices instead of two mesh networks with 25 each. Restructure the layout of the mesh networks to group devices and the gateway to avoid overlap. It may take 36 hours for the fault to clear. This can be expedited by toggling the state of mesh formation.
Device does not rejoin the mesh after battery replacement	Device is an invalid reply/no answer after replacing the batteries.	Verify the tamper condition is cleared. Use mesh formation to have the device rejoin the mesh network. Low battery and tamper are both latching conditions. Ensure a reset has been initiated to clear those events.
Low battery trouble reported after battery replacement	Low battery trouble is still indicated after replacement.	Use the network statistics provided in SWIFT Tools to see the battery voltage measured for each individual battery. Verify that each battery is present and at a suitable voltage level. The low battery trouble is a latching trouble, ensure a reset has been initiated since the replacement.

Problem	Description	Action
Site survey does not find a link	Solid red results for the link test	Verify the addresses of the devices used during the test. The lower addressed device must complete its link test before the device at the next higher address starts the link test. Verify the devices are in range of each other.
SWIFT Tools does not import site survey data	Selecting the device in the communicator in SWIFT Tools does not have an effect	The device does not have any site survey results to be imported. It has not found a link during the link test and/or it has not collected any data for an RF Scan.
SWIFT Tools says device/gateway is out of range	Device or gateway is not communicating to SWIFT Tools	Verify the device or gateway is powered on and in a state that supports SWIFT Tools communication. For instance, a device in the mesh network does not communicate to SWIFT Tools. It communicates to the gateway. A device that has completed a site survey does not communicate to SWIFT Tools until it returns to the pending site survey state or factory default state. Move the W-USB adapter in range of gateway/devices.
Scan does not find any devices	All devices are out of range	Verify at least one device is in range of SWIFT Tools, the W-USB adapter is connected, and the scan is on. SWIFT Tools processes the messages faster with multiple devices in range. If only one device is in range it can take up to 1 minute for the scan to detect the device.
Site survey devices are not displayed in the communicator of SWIFT Tools.		Verify the device is in the pending site survey mode or factory default mode. The device will not communicate with SWIFT Tools while it is in site survey mode.
FACP reports Missing for the gateway	Gateway is not communicating with the panel	Verify the gateway is set to a valid address.
FACP reports Missing for the wireless devices	FACP does not recognize the detectors	Verify using SWIFT Tools that the devices are part of the mesh network.
Device does not receive a profile	A profile request has been initiated but timed out before receiving a profile	Ensure the gateway or distributor is still in distributor mode. Ensure the device is in range of the gateway or distributor. If there are multiple devices in range, the might be interfering with the profile transfer. Move the distributor and device to a different area or shut down the peripheral devices.
Application download fails	SWIFT Tools failed to finish a download	Verify the number of devices in range of the W-USB adapter during the download does not exceed the recommended limit of 10 devices. Verify the device is in range and powered on during the download process.
Device is in bootloader	Device/Gateway is indicating the LED pattern for bootloader and it is indicated as being in bootloader in the communicator of SWIFT Tools.	The device failed to load or initialize the application. Reboot the device. If it is still in bootloader, the application will need to be updated using SWIFT Tools. If problem persists, contact technical support.

C.2 Testing the Gateway and Devices

The gateway must be tested after installation and be part of a periodic maintenance program. The testing methods must satisfy the Authority Having Jurisdiction (AHJ). The gateway provides optimum performance when tested and maintained in compliance with NFPA 72 ordinances.

C.2.1 Testing LED Indicators

For more information on LED indicators, refer to Appendix D, “LED Indicators”, on page 53.

C.3 Testing the Wireless Network

Using the SWIFT Tools application, users can:

- Diagnose and troubleshoot the wireless network and connectivity of the devices.
- Monitor the wireless network topology, quality of the communication links between the devices, live and historical event reports for troubleshooting purposes.
- View the parent-child relationship and the signal strength between the two devices, and identify the device that has lost the communication link with the wireless network.

In addition, SWIFT Tools:

- Communicates with the gateway to retrieve live information about the connectivity and status of the devices.
- Stores the wireless network data such as network map, parent-child information, device information, history events, and network statistics.

The SWIFT Tools application allows retrieval of the following information for diagnosing and troubleshooting purposes.

- Network Topology

- History of Events
- Network Snapshots
- Network Statistics
- Device Attributes

C.3.1 Network Topology

Parent-Child Devices

The parent-child relationship between the devices in the wireless network is displayed using the directional arrows.

Orphan Devices

A device that is not linked with any other device in the wireless topology is an orphan device. The device is represented as an orphan device due to one of the following reasons:

- The device was originally a part of the wireless network and was dropped.
- When the network topology was retrieved, the device detail was not retrieved.
- The network connections are saturated and parent-child connection with the device is not established.

Class A Compliance

Each device must comply with Class A guidelines. Every device must have two parent devices to be compliant with the Class A guidelines.



NOTE: The device image in SWIFT Tools is altered to depict that it does not meet the required guidelines.



NOTE: Class A guidelines are not applicable to the gateway.

Selecting a device from the graphical representation and clicking either left or right allows you to view the following details. The Network Topology window allows you to click either left or right on any connected or orphan device.

C.3.2 History Events

History events of the wireless network can be retrieved and viewed using SWIFT Tools for troubleshooting purposes. This report provides information on when the device gets connected with the wireless network, mode change, and slot change details.

C.3.3 Network Snapshots

Network snapshots can be retrieved and viewed using SWIFT Tools for troubleshooting purposes. The network snapshot helps to analyze how the wireless network is functioning over a period of time.

C.3.4 Network Statistics

Network statistics of the wireless network can be retrieved and viewed using SWIFT Tools for troubleshooting purposes. The network statistics provide information on the attributes and RSSI of a device. The attributes provide information on the retransmission count and device re-join events. The retransmission count is the number of times a device retransmits the wireless signal. The device re-join events is the number of times the devices get disconnected from the wireless network and get connected with the wireless network. The RSSI of a device displays the parent-child relationship between the devices.

C.3.5 Device Attributes

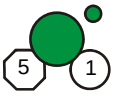
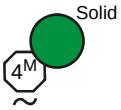
Device attributes can be retrieved and viewed using SWIFT Tools for troubleshooting purposes. The attributes of a device such as low indication, removal indication, level, tamper fault, and others are retrieved.

Notes

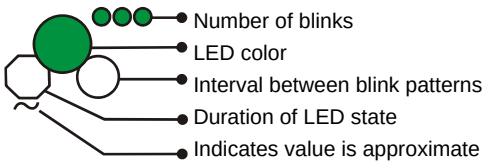
Appendix D: LED Indicators

The LED indicator patterns for the wireless gateway and wireless devices are shown in the tables below.

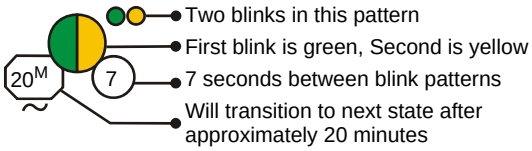
Figure D.1 Gateway LED Patterns

LED Pattern	Condition	Action Required
 Bootloader normal	Device is ready to update	
 Bootloader Firmware update	New application code is being downloaded	
 Mesh formation	Gateway is forming the mesh and looking for devices that are not in the mesh	Wait until all devices join the mesh and then terminate mesh formation
 Profile removed	Gateway has returned to the factory default state	
 Profile accepted	Gateway is now profile assigned	
 Mesh update in progress/Mesh update -parent node	Gateway is updating the mesh/Parent nodes are updating child nodes	
 Normal mode/ background mesh restructuring	Normal operation of the gateway	
 Rescue mode	Gateway and the mesh network are searching for any device that is not in the mesh network with the same profile	
 Profile assigned	Gateway is starting up with a profile	Activate both magnetic sensors simultaneously within 10 seconds to remove a profile

Legend



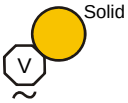
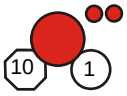
Example:



All units are in seconds. “M” indicates Minute. “V” indicates Variable.

ledgate1_4.0.wmf

Figure D.2 Gateway LED Patterns (Continued)

LED Pattern	Condition	Action Required
 1st mesh restructuring	Mesh is formed and initializing	Ensure all devices in the mesh have a valid address
 Normal mode	The gateway is in the mesh and may be in trouble	Refer to the FACP to identify the trouble and possible solution
 Rescue mode	Gateway and the mesh are searching for any device that is not in the mesh network with the same profile. The gateway may be in trouble	
 Address zero trouble	The gateway address is set to zero	Ensure all devices in the mesh have a valid address
 Mesh update ready	Received command from SWIFT Tools to start a firmware update	
 Factory default	Gateway is starting up without a profile	
 Waiting for a profile	Gateway is in factory default mode	Use SWIFT Tools to assign a profile
 Normal mode/ background mesh restructuring	Gateway is in the mesh	
 Rescue mode	Gateway and the mesh network are searching for any device that is not in the mesh network with the same profile	

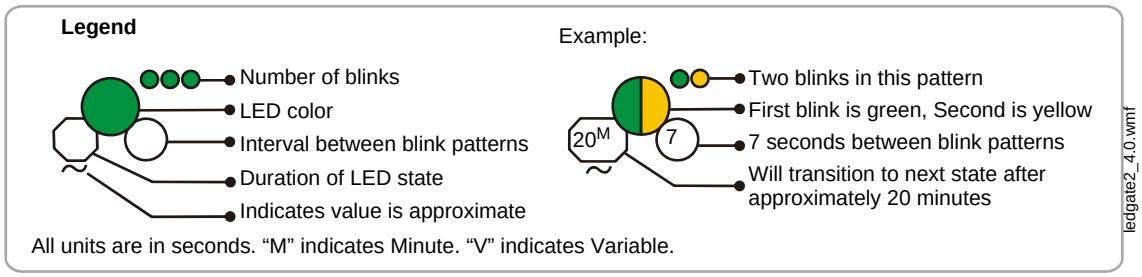


Figure D.3 Device LED Patterns

LED Pattern	Condition	Action Required
Bootloader normal	Device is ready to update	Use SWIFT Tools to initiate download
Slot request rejected	Device is not permitted into the mesh	Confirm device count and software version
Mesh forming	Device is part of the mesh and looking for devices that are not in the mesh	
Sustained tamper	Device is tampered	Ensure detector is seated in the base and the module has the faceplate on
Bootloader firmware update	New application code is being downloaded	
Profile removed	Device has returned to the factory default mode	
Profile received	Device now has a profile assigned	
Battery check: all batteries are fresh	Maximum battery life remaining in device	
Profile removal timeout started	Remove the profile from the tampered/hall sensor activated device within 60 minutes	
Active/Alarm state	Device has been activated	
Rescue mode	Device is in the mesh and looking for lost devices	
Normal mode or tested walktest	Device is in the mesh or it has been tested in a walktest.	
Mesh update -parent node	The gateway is updating parent nodes in the mesh	
Mesh update idle	Devices that are included in mesh update are complete and waiting for the whole mesh to finish updating	
Mesh updating	Green and yellow flicker pattern indicates that data packets are being received by the device.	
Self test fail	Device has failed internal self diagnostics.	Restart the device. If problem persists, contact technical support

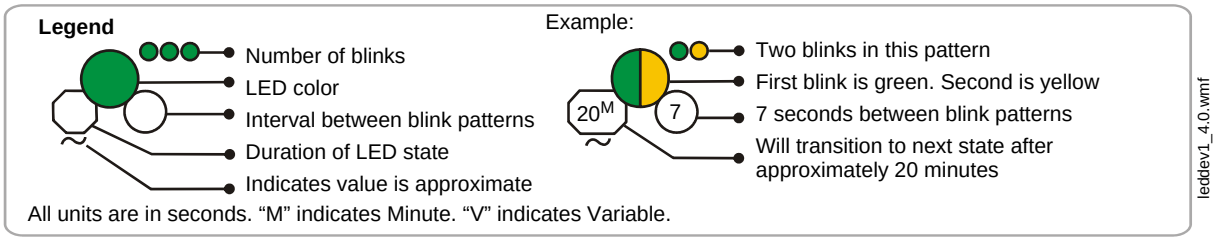
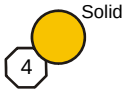
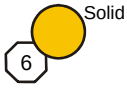
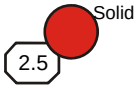
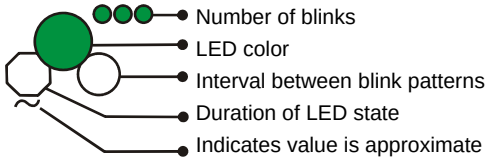


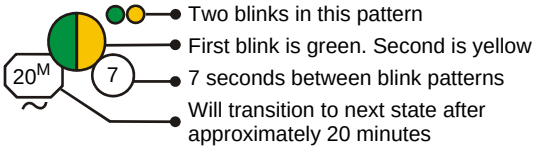
Figure D.4 Device LED Patterns (Continued)

LED Pattern	Condition	Action Required
 Active/Alarm state	Device has been activated	
 Low battery cut-off	Device is functioning	Replace batteries
 Rescue mode	Device is in the mesh, looking for lost devices, and may be in trouble	Refer to the panel to identify the trouble and possible solution
 Battery Check: all batteries present	Minimum of 6 months battery life remaining	
 Searching for mesh (in rescue mode)	Profile is assigned and device is searching for the mesh.	Ensure the mesh is in rescue mode or wait for timeout to search mesh in formation mode.
 Searching for mesh (in formation mode)	Profile is assigned and device is searching for the mesh	Ensure the mesh is in formation mode
 1st mesh restructuring	Mesh is formed and initializing	
 Normal mode	Device is in the mesh and may be in trouble	Refer to the FACP to identify the trouble and possible resolution.
 Tamper entry	Device has just been tampered	Ensure detector is seated in the base and the module has a faceplate
 Discovered mesh	Device discovered the mesh	
 Normal mode	Device is in the mesh	
 Rescue mode	Device is in the mesh and looking for lost devices	
 Battery Check: weak	Less than 6 months battery life left or not all 4 batteries are present	Ensure all 4 batteries are present or replace the batteries
 Active/Alarm state	Device has been activated	
 Waiting for a profile	Device is in factory default mode	Use SWIFT Tools to assign a profile.
 Pending site survey	Device is in factory default mode and is ready to enter site survey mode	Clear the tamper condition within 1 minute to enter site survey mode

Legend



Example:



All units are in seconds. “M” indicates Minute. “V” indicates Variable.

leddev2_4.0.wmf

Notes

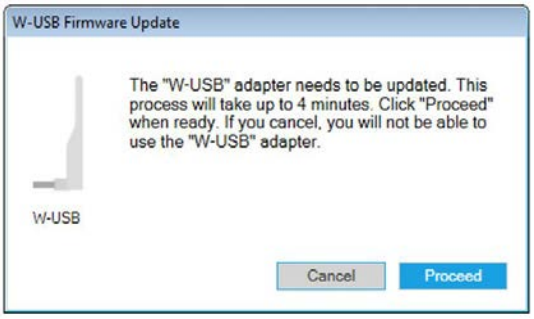
Appendix E: Firmware Upgrade/Downgrade Instructions

To ensure proper system operation, this product must be tested in accordance with NFPA 72 after any programming operation or change in site-specific software.

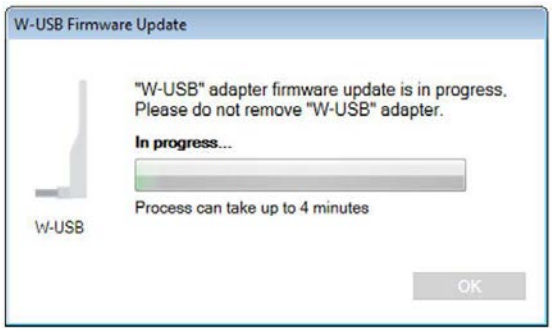
E.1 W-USB Adapter Upgrade Procedure

The following procedure provides firmware upgrade instructions for the W-USB adapter. Ensure the latest version of SWIFT Tools is installed. SWIFT Tools and firmware can be downloaded from www.farenhyt.com. There are multiple .bin files with the zip file. Save the files to a folder. The W-USB adapter will auto-update if the SWIFT Tools and W-USB adapter versions are incompatible.

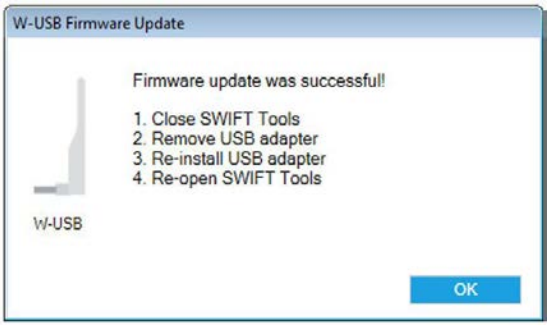
1. Insert the W-USB adapter into the PC and launch SWIFT Tools. A pop-up message confirming the W-USB adapter update will be displayed.



2. Click Proceed. The following screen will display.



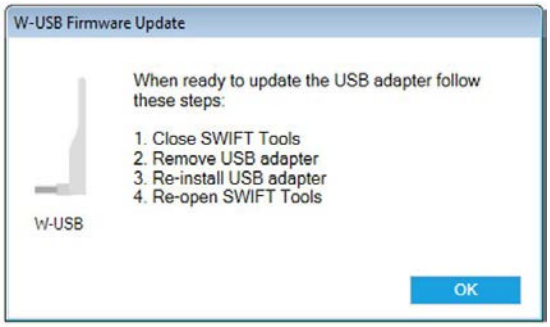
3. If the USB update is successful, the following screen will display.



4. If the USB update fails, the following screen will display.



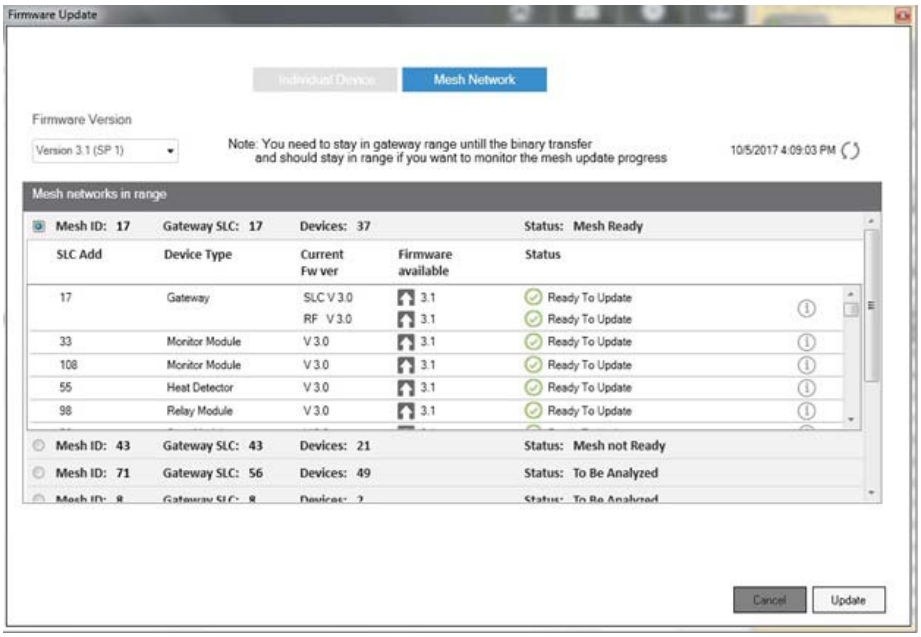
5. If the USB update is declined by clicking Cancel at step 1, a re-update procedure will display.



E.2 Mesh Network Firmware Upgrade/Downgrade Procedure

The following procedure provides firmware upgrade and download instructions for the gateway mesh. Ensure the latest version of SWIFT Tools is installed. SWIFT Tools and firmware can be downloaded from www.farenhyt.com. There are multiple .bin files with the zip file. Save the files to a folder.

1. Launch SWIFT Tools and navigate to the home screen and select either **Site Survey**, **Create Mesh Network**, or **Diagnostics**.
2. Ensure the gateway is in range of the W-USB adapter and the PC running SWIFT Tools.
3. Click on the **Operations** menu and select **Firmware Update.**
4. Select the Mesh Network tab from the displayed screen. The **Firmware Update** screen is displayed.



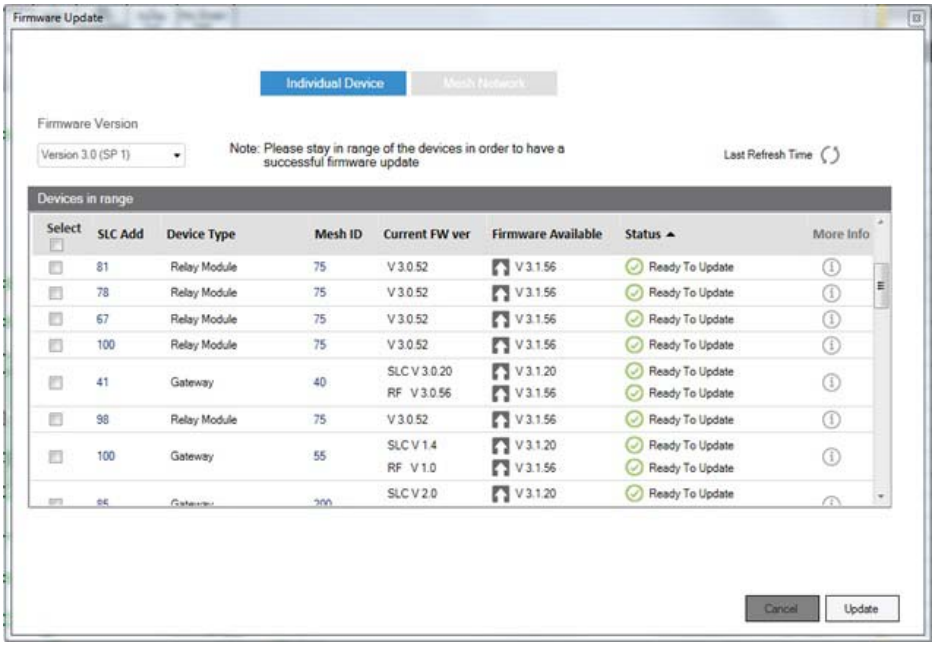
5. Select the Service Pack from the Firmware Version drop-down box or click Choose File and then browse for the service pack zip file from your local drive and click OK.
6. Select the respective gateway and follow the on-screen instructions and wait until the mesh feasibility check finishes.
7. Click Update. As the mesh update progresses, the status bar will update.

E.3 Device and Gateway Firmware Upgrade/Downgrade Procedure

The following procedure provides firmware upgrade and download instructions for the wireless devices and gateway. Ensure the latest version of SWIFT Tools is installed. SWIFT Tools and firmware can be downloaded from www.farenhyt.com. There are multiple .bin files with the zip file. Save the files to a folder.

1. Launch SWIFT Tools and navigate to the home screen and select either **Site Survey**, **Create Mesh Network**, or **Diagnostics**.
2. Ensure devices are powered on and in range of the W-USB adapter and the PC running SWIFT Tools.
3. Tamper the device (or activate the hall sensor on the detector). Once the device has been tampered (or hall sensor activated), a 60 minute countdown will start for firmware upgrade.

4. Click on the **Operations** menu and select **Firmware Update.**



5. Select **Service Pack** from the **Firmware Version** drop-down box or click **Choose File** from the **Firmware Version** drop-down box and browse for the service pack zip file from your local drive and click **OK**. The file will then load.
6. After selecting the respective service pack zip files, click **Update**.

E.4 Distributed Firmware Updates

Firmware updates for devices in the mesh network can be distributed via the mesh network from the gateway. SWIFT Tools is required to initiate the firmware upgrade procedure.

An entire mesh network of devices can be upgraded assuming certain preconditions are met:

✓ all devices are running application code version 4.0 or higher,

NOTE: Although version 3.0 supports updates via the mesh network, the nature of the security release in version 4.0 requires use of the individual device update method described in Section E.3 above.

✓ there are no active “low battery” troubles,
✓ there are no active “class A” connectivity fault conditions,
✓ the mesh is in “normal mode”.

Failure to meet the preconditions will be indicated via SWIFT Tools, and must be remedied before the mesh upgrade can continue.

CAUTION: NO FIRE PROTECTION
DURING THE UPDATE, THE MESH NETWORK WILL NOT PROVIDE FIRE PROTECTION.

All wireless points associated with the mesh network will be indicating a “no answer” trouble or “invalid reply”. There are two phases to the mesh upgrade procedure.

Phase 1 - Mesh upgrade preparation:

SWIFT Tools must stay in communication with the gateway during the mesh upgrade preparation phase.

The user will initiate the upgrade process via SWIFT Tools, and SWIFT Tools will proceed to automatically update the SLC application code of the gateway, the RF application code of the gateway, and transfer the new device application code to the gateway. The user may cancel the process at any point during the mesh upgrade preparation. Mesh upgrade preparation can take 5 to 15 minutes depending on the number of downloads that are needed.

Phase 2 - Mesh upgrade in progress:

The gateway will distribute the new application image to the mesh network of devices during this phase. SWIFT Tools is not required to be in communication during this phase, but will provide indication of the progress of the upgrade when it is in communication. The distribution of the new application image may take up to 90 minutes depending on the number of devices in the mesh network.

The gateway will automatically execute mesh formation at the completion of the mesh upgrade. Any devices that did not successfully complete the upgrade will need to be upgraded individually.

Index

A

abbreviations **9**
additional references **8**
assign profile **32, 35**
assumed knowledge **8**
attributes **51**

B

bootloader **20, 35**

C

Class A compliance **51**
class A fault **36**
clear tamper **37**
collapse network command **26**
communication **45**
configuration **15**
configure profile **19**
CR123A batteries **30**
creating jobsite **44**

D

device
- attributes **51**
- bootloader **35**
- factory default **35**
- initial mesh restructuring mode **36**
- LED indicators **36**
- mesh formation **36**
- mesh participant **35**
- network snapshots **51**
- network statistics **51**
- normal mode **36**
- profile assigned **35**
- rescue mode **36**
- site survey **35**

device indication **37**
device initialization **37**
device operations **35**
device spacing **46**
devices **30**
- Class A compliance **51**
- configuration and programming **32**
- installing **32**
- orphan **51**
- parent-child **51**

disable trouble reporting **26**
dongle **40**
duplicate address **37**

E

event reporting **18**

F

factory default **19, 33, 35**

G

gateway **10**
- bootloader **20**
- collapse network **26**
- configuration **15**
- description **10**
- disable trouble reporting **26**
- factory default **19**
- initial mesh restructuring **20**
- LED indicators **11**
- lock/unlock **20**
- mesh formation **17, 19**
- mesh restructuring **20**
- mesh upgrade **20**
- mounting **12**
- neighboring network scan **20**
- normal mode **20**
- password reset **22**
- power **14**
- profile configure **19**
- profile distribution **18**
- programming **15**
- remove profile **17**
- rescue mode **20**
- restrictions **28**
- RF interference **28**
- silence network **27**
- SLC configuration **18**
- SLC connections **14**
- specifications **10**
- start-up **19**
- weak link trouble **26**
- wiring **13**

H

heat detector **30**

I

initial mesh restructuring **20**
initial mesh restructuring mode **36**
initialization **37**
installing devices **32**
interference **28**
isolator modules **14**

J

jamming **37**
jobsite
- new **44**
- open **45**

jumper **12**

L

LED indicators **11, 17, 36**
link quality test **46**
- procedure **46**
- requirements **46**

lock **20**
low battery **36**

M

magnet **45**
magnetic sensor **11, 17, 33**
max gateway trouble **22**
mesh formation **17, 19, 33, 36**
mesh network **19**
mesh participant **35**
mesh restructuring **20**
mesh upgrade **20**
modes of operation **19, 35**
module
- assigning profiles **32**
- batteries **30**

module configuration **32**
module installation **32**
monitor module **30**
mounting **12**

N

neighboring network **20**
neighboring network scan **20**
network installation restrictions **28**
network limit **28**
network snapshots **51**
network statistics **51**
network topology **51**
no answer **37**
normal mode **20, 36**

O

opening jobsite **45**
operations **19**
orphan devices **51**
overlapping networks **28**

P

panel indication **37**
parent-child devices **51**
password reset **22**
profile
- assigned **35**
- configure **19**
- remove **16**
- removing **17**

profile distribution **18**
programming **15**
pull station **30**

R

related documents **8**
remove profile **16, 17**
repeater **36**
reporting
- max gateway trouble **22**

rescue mode **20, 36**
restrictions **28**
- installation **28**

RF interference **28**
RF scan test **47**

status **47**
RF spectrum **28**

S

security **45**
silence network command **27**
site survey **35, 46**
SLC configuration **18**
SLC connections **14**
smoke detector **30**
specifications **10, 41**
spectrum **28**
RF **28**
spread **28**
spread spectrum **28**
start-up **19**
SWIFT Tools **44, 50**

T

tamper **37**
clear **37**
testing **50**
transmission **20**
trouble condition **20, 26**
trouble messages **29**
trouble reporting
disable **26**
troubleshooting **49**

U

unlock **20**
upgrade
mesh **20**

W

walkie talkie mode **29**
weak link **36**
trouble reporting **26**
WIDP-WGI **10**
specifications **10**
wireless devices **30**
wireless gateway **10**
wiring **13**
W-USB **40**
specifications **41**

Manufacturer Warranties and Limitation of Liability

Manufacturer Warranties. Subject to the limitations set forth herein, Manufacturer warrants that the Products manufactured by it in its Northford, Connecticut facility and sold by it to its authorized Distributors shall be free, under normal use and service, from defects in material and workmanship for a period of thirty six months (36) months from the date of manufacture (effective Jan. 1, 2009). The Products manufactured and sold by Manufacturer are date stamped at the time of production. Manufacturer does not warrant Products that are not manufactured by it in its Northford, Connecticut facility but assigns to its Distributor, to the extent possible, any warranty offered by the manufacturer of such product. This warranty shall be void if a Product is altered, serviced or repaired by anyone other than Manufacturer or its authorized Distributors. This warranty shall also be void if there is a failure to maintain the Products and the systems in which they operate in proper working conditions.

MANUFACTURER MAKES NO FURTHER WARRANTIES, AND DISCLAIMS ANY AND ALL OTHER WARRANTIES, EITHER EXPRESSED OR IMPLIED, WITH RESPECT TO THE PRODUCTS, TRADEMARKS, PROGRAMS AND SERVICES RENDERED BY MANUFACTURER INCLUDING WITHOUT LIMITATION, INFRINGEMENT, TITLE, MERCHANTABILITY, OR FITNESS FOR ANY PARTICULAR PURPOSE. MANUFACTURER SHALL NOT BE LIABLE FOR ANY PERSONAL INJURY OR DEATH WHICH MAY ARISE IN THE COURSE OF, OR AS A RESULT OF, PERSONAL, COMMERCIAL OR INDUSTRIAL USES OF ITS PRODUCTS.

This document constitutes the only warranty made by Manufacturer with respect to its products and replaces all previous warranties and is the only warranty made by Manufacturer. No increase or alteration, written or verbal, of the obligation of this warranty is authorized. Manufacturer does not represent that its products will prevent any loss by fire or otherwise.

Warranty Claims. Manufacturer shall replace or repair, at Manufacturer's discretion, each part returned by its authorized Distributor and acknowledged by Manufacturer to be defective, provided that such part shall have been returned to Manufacturer with all charges prepaid and the authorized Distributor has completed Manufacturer's Return Material Authorization form. The replacement part shall come from Manufacturer's stock and may be new or refurbished. THE FOREGOING IS DISTRIBUTOR'S SOLE AND EXCLUSIVE REMEDY IN THE EVENT OF A WARRANTY CLAIM.

Warn-HL-08-2009.fm

Honeywell Security & Fire
12 Clintonville Road
Northford, CT 06472-1610
203-484-7161
www.honeywell.com

LS10036-000FH-E | G | 01/19
©2020 Honeywell International Inc.

Honeywell