Honeywell

Honeywell Connected Life Safety Services

CLSS Pathway

Cellular and IP Communicator

HW-AV-LTE-M

Installation and Operation Manual

P/N:LS10340-000HW-E | REV. A | SEP/30/2021
ECN: 00004957

Table of Contents

Section 1: General Information

1.1 About This Manual

This *CLSS Pathway Installation and Operation Manual* provides detailed procedures about installation, commissioning, and troubleshooting the *CLSS Pathway* communicator.

The manual describes:

- the CLSS Pathway communicator,
- its installation environment,
- mounting and connecting the device
- initial configurations, and
- troubleshooting

Using This Manual

This manual is written with the understanding that the user is trained in the operations and services required for this product.

Honeywell reserves the right to modify and revise this manual without notice.

Usages

In this manual, product name usages are as below:

- The *CLSS Pathway* may also be referred as the *communicator*
- The *Connected Life Safety Services* mobile App may also be referred as the *CLSS App*

1.2 Information Sources

Honeywell offers suitable information sources based on informational requirements.

1.2.1 Training Modules

Training modules are available when logged onto:
https://fire.honeywell.com/#/help-videos

1.2.2 Related Documents

The table below lists documents related with the *CLSS Pathway*:

Product Type: CLSS Pathway	
For This Purpose ...	**Refer to ...**
Install and wire the CLSS Pathway inside an enclosure	CLSS Pathway - *Product Installation Document* P/N: LS10338-000HW-E
Quickly install and configure for the central station communication	CLSS Pathway - *Quick Start Guide* P/N: LS10339-000HW-E
Use various installation and configuration options	CLSS Pathway - *Installation and Operation Manual* (This document) P/N: LS10340-000HW-E

1.3 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 documents, you can email us.

Please include the following information:

- Product name and version number (if applicable)
- Printed document or Online Help
- Topic title (for Online Help)
- Page number (for printed document)
- A brief description of content you think should be improved or corrected
- Your suggestion for how to correct/improve documentation

Send email messages to:

FireSystem.TechPubs@Honeywell.com

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

1.4 Revision History

Table 1.1: Dates and Changes

Date	Change Details
Rev. A	
September 30, 2021	First release of the document.

1.5 Agency Listings and Approvals

These listings and approvals apply only to the module specified in this document. In some cases, listing may be in process.

UL

ETL No. 5013005, conforms to following UL standards:

- UL864 – Control Units and Accessories for Fire Alarm Systems

FCC Statements (USA)

This equipment complies with FCC rules Part 15, FCC registration No. XMR201707BG96 and operation is subject to the following conditions:

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

1.6 Limited Liability

The user agrees that despite the Device could reduce the risk of fire, or other dangers, it does not guarantee against such events. Honeywell will not take any responsibility regarding personal, property or revenue loss while using the Device. Honeywell responsibility according to local laws does not exceed the value of the purchased system. Honeywell is not affiliated with GSM operators providing cellular services, therefore is not responsible for network services, coverage, or its operation.

1.7 Manufacturer Warranty

The Device carries a non-transferable hardware limited warranty by the manufacturer. This warranty does not cover any postal or labor costs for the removal and re-installation of the Device. This warranty does not cover any subscriber agreements or failure of services provided under the terms of such subscriber agreements, or failure of cellular, GPRS, LAN or other related networks functions and services.

The warranty is not valid if the device has been modified or used in a manner contrary to its intended purpose and does not cover damage to the Device caused by installation or removal of the Device or any of its components. This warranty is voided if the Device has been damaged by improper maintenance, SIM card removal, accident or unreasonable use, negligence, acts of God, neglect, improper service, or other causes not arising out of defect in materials or construction. This warranty does not cover the elimination of externally generated static or noise, or the correction of antenna problems or weak signal reception, damage to software, accessories or alarm system external components, cosmetic damage or damage due to negligence, misuse, abuse, failure to follow operating instructions, accidental spills or customer applied cleaners, damage due to environmental causes such as floods, airborne fallout, chemicals, salt, hail, windstorms, moisture, lightning or extreme temperatures, damage due to fire, theft, loss or vandalism, damage due to improper storage and connection to equipment of another manufacturer, modification of existing equipment, faulty installation or short circuit.

Honeywell will not be liable in any event of incidental, special or consequential damages (including loss of profits), and the Client shall have no claim against Honeywell for termination of contracts, indemnification, compensation for loss of customers, loss of profits, prospective profits, distribution rights, market share, goodwill, investments made or any similar losses that may result from any faults in the operation of the Device and the services provided by Honeywell.

1.8 Safety Instructions

- A qualified technician must check this device, once a year.
- The HW-AV-LTE-M device contains a radio transceiver operating in LTE CAT-M1 band.
- Do not use the Device with medical devices, in places or where it could interfere with other devices and cause any potential danger.
- Do not expose the Device to high humidity, chemical environment, or mechanical impacts.
- Do not use the Device in hazardous environment. Do not store or install the Device in overheated, dusty, wet or overcooled places.
- The Device is mounted in limited access areas. Any system repairs must be done only by qualified, safety aware personnel. Do not disassemble or refit the Device. Do not attempt to personally repair it.
- Main power must be disconnected before any installation or tuning work starts. The device installation or maintenance must not be done during stormy conditions.
- The device must be powered by DC 12-29V power supply.
- Blown fuses or any other components of the Device must not be replaced by the user.
- Keep the Device dry. Any liquid, i.e., rain, moisture, may destroy or damage the inside circuitry.
- Handle carefully. Do not vibrate or shake it violently.
- Do not clean it with chemicals or detergent.
- Please read the user manual carefully before installation and operation of the Device. Otherwise, it may not work properly or be damaged.

1.9 Technical Support

For support in the USA contact Honeywell Technical Support at:

- Email: CLSS.Tech@honeywell.com
- Website: fire.honeywell.com
- Address:

  Honeywell International Inc.

  12 Clintonville Rd.

  Northford, CT 06472

  (203)-484-7161

1.10 Disclaimer

Images in the document are for reference purpose only and are subject to change. All trademarks, service marks, word marks, design marks, and logos are property of their respective owners.

Section 2: Overview

The *CLSS Pathway* (HW-AV-LTE-M) is a dual-path cellular communicator, which runs on a 24-volt power from its panel. It supports both AT&T and Verizon LTE networks, and uses any of them with a stronger signal. It transmits Contact ID data from its fire panel to the panel's central monitoring station.

2.1 Operational Modes

The communicator can operate in one of the following mode:

- Dialer Capture Mode: Gets contact ID data from the panel's dialer interface.
  With the panel: Connects to the telephone ports.
- Dry Contact Relay Monitor Mode: Monitors the dry contact relay outputs.
  With the panel: Connects to the dry contact relay terminals.

2.1.1 Working with a Central Monitoring Station

In a sole-path connection, it uses the default cellular connection only.

The communicator has dual-SIMs to support AT&T and Verizon cellular connections. Between these two, the cellular connection with stronger signal strength takes care of the data transmissions.

In a dual-path connection, it can use both cellular as well as LAN connections. The LAN will be the primary communication path and the cellular connection will be the backup connection.

2.2 Main Features

- Universal Panel Compatibility
  - Dial capture interface supporting the Contact ID
- Exceptional Redundancy
  - Dual-SIM device
- Connection monitoring
  – Adjustable fault reporting time
- High reliability due to multiple transmission channels
  - LTE CAT-M1/LAN and redundant servers
- The CLSS Site Manager
  - Web-based application for device configurations, administration, and remote firmware updates
- The Connected Life Safety Services App
  – Supports alarm, events, and email notifications
- Can use sole path (Cellular only) or dual path (Cellular as well as LAN)
- Optional four inputs for monitoring Fire Alarm Panel dry contact relays
- 24V auxiliary constant power directly from the panel

2.3 Specifications

Table 2.1: CLSS Pathway Specifications

Operational Requirements	
Supply Voltage	+12V to +29V DC
Current	Standby: 60mA Peak: 200mA
Frequency	LTE CAT-M1 700/850/1700/1900/2100 MHz
GSM Providers	AT&T, Verizon, or other networks available in the area
Physical Characteristics	
Dimensions	2.48” x 3.54” x 1.26”
Weight	2.56 oz without antenna
Room Conditions	
Temperature	0°C to 49°C (32°F to 120°F)
Relative humidity	1% to 85% | Non-condensing

2.4 CLSS Pathway Parts

Part Name	Part Number
CLSS Pathway 	HW-AV-LTE-M
Enclosure with mounting plate 	HW-AV-ENC

Section 3: Security Recommendations

3.1 For Users

An administrator should:

- Regularly review the user roles and permissions for a CLSS account
- Immediately remove users who should no longer have access to CLSS

A technician should:

- Use discretion to allow or deny a location access request.
- Disconnect the *CLSS App* from the *CLSS Gateway*, once the required activity is completed.
- Turn OFF the location access in the CLSS App's **Security Settings**, when location access is not required.

3.2 Potential Risks

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

Unauthorized Access

Unauthorized access results from unsecured user name and password, uncontrolled access to the equipment, or uncontrolled and unsecured access to the network.

It results the following:

- Loss of system availability
- Incorrect execution of controls causing damage to the equipment
- Incorrect operation, spurious alarms, or both
- Theft or damage to the contents of the system
- Capture and modification or deletion of data causing possible liability to the installation Site and Honeywell

■ User Access and Passwords

Observe the following good practices:

- Ensure physical security of passwords. Avoid writing user names and passwords where they can be seen by unauthorized personnel.
- Ensure that passwords contain characters, numbers, and a mix of lower and uppercase letters.
- Passwords should be complex and not easily guessed; and, should not contain phrases used in common speech.
- Do not use personally identifiable information as a password, such as social security numbers, addresses, birth dates.
- Set the minimum level of access for each user.
- Do not provide users with privileges that they do not need.
- Periodically audit user accounts and remove any that are no longer required.

Memory Media

- Use only authorized removable media.
- Use an up-to-date anti-virus software to scan the removable media and check for viruses and malware.
- Ensure that the memory media is not used for other purposes to avoid risk of infection.
- Control access to media containing backups to avoid risk of tampering.

Software and Firmware Updates

System software and firmware updates may be offered from time to time.

Ensure that your local representative:

- Has the up-to-date contact details, and
- Periodically visits the Honeywell web site for up-to-date product information

Viruses and Other Malicious Software Agents

Malicious Software include the following:

- Viruses
- Spyware
- Worms
- Trojans

These may be present in a computer using a Monitoring Station Software or in a USB pen drive, which is used to copy data to computer.

The intrusion of malicious software agents can result in performance degradation, loss of system availability, and the capture, modification, or deletion of data — including configuration and device logs.

USB devices from other infected systems on the network or malicious Internet sites can also transfer viruses.

Network and Firewall Setup

Inbound (In) Port: The port another computer uses to access a gateway functionality. An application on the gateway will be actively listening on this port for client connections.

Outbound (Out) Port: The gateway uses outbound ports to connect to Internet or *CLSS Site Manager*. The Cloud services in the *CLSS Site Manager* will be listening on these ports waiting for a connection from the gateway.

By default, block all inbound and outbound connections and allow only the ports listed in the below table:

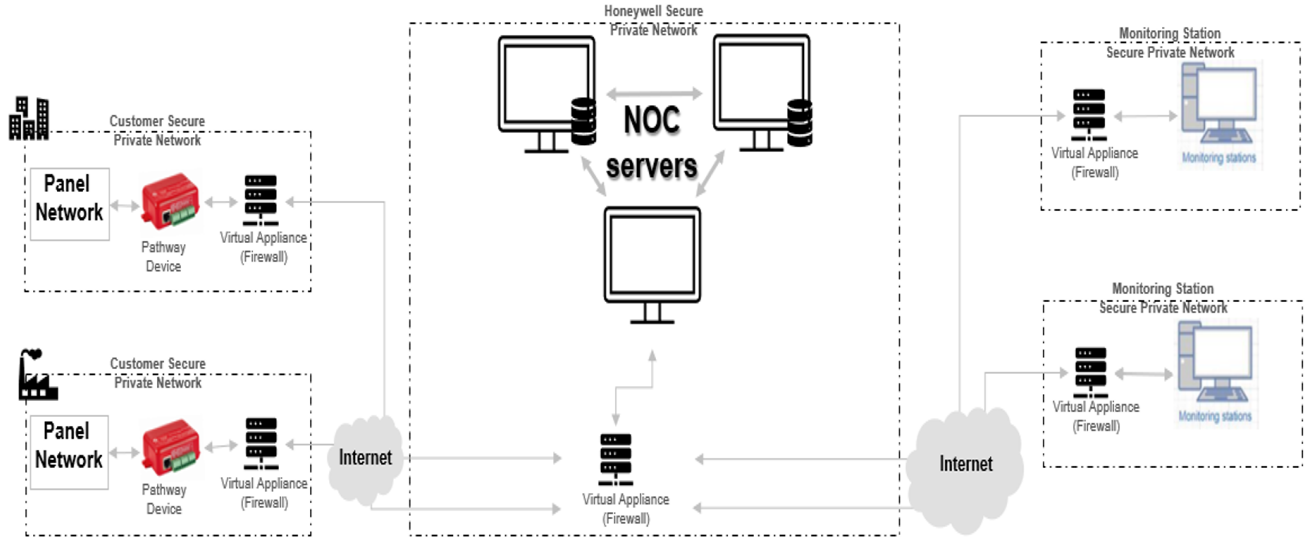
Port Number	Type	IN/OUT	Purpose/Remarks
443	HTTPS - TCP	Bidirectional	NOC APIs communications with a Supplier Cloud and *CLSS Site Manager*
1433	TCP	Bidirectional	NOC Server and SQL DB private network-based communications
9000	TCP	Bidirectional	Pathway devices and NOC communications
9000	UDP	Bidirectional	Pathway devices and NOC heartbeat communications
6000 - 6030	TCP	Bidirectional	Monitoring station and NOC communications

The *CLSS Pathway* device sends alarms to *CLSS Site Manager*, using the below endpoints:

Region	All End-points
West US	• https://fireclssnocwus.honeywell.com/clssnocalarmrcvr/ • https://fireclssnocwus.honeywell.com/clssnocapisrv/
East US	• https://fireclssnoceus.honeywell.com/clssnocalarmrcvr/ • https://fireclssnoceus.honeywell.com/clssnocapisrv/

Securing the Monitoring Stations

- Good security practices should be observed on the Monitoring Station PCs.
- Operating systems and software should be kept up to date by installing the manufacturers updates, as well as maintaining up-to-date anti-virus software on all computers, which may be connected directly or via a network.
- For monitoring stations, it is recommended to use secure VPN channel, which must be placed behind the firewall.
- It is suggested to use hardware receiver as an adapter at the monitoring station.
- For the CLSS Pathway devices, it is recommended to use secure private network, and keep them behind the firewall.
- Only authorized personnel should get access to private network.
- Best industry standards should be followed while configuring the firewall policies.
- Devices should be safely installed in the secure zone and they must be out of reach to unauthorized personnel.
- Ensure that the computers are regularly scanned for viruses.
- Only install files and software from trusted sources and use only them on associated computers to avoid malicious software.
- Use only authorized removable media. For example, use CD, DVD, external hard drives, or USB memory sticks, which have been scanned using up-to-date anti-virus software.



Section 4: Central Station Communications

As per the settings in *CLSS Site Manager* and *CLSS* App, the *CLSS Pathway* sends events from a panel to a specified Central Monitoring Station.

4.1 Prerequisites

1. The organization's administrator configuring *CLSS Site Manager* requires a CLSS account
2. A technician installing the *CLSS Pathway* requires a CLSS account
3. The *CLSS Site Manager* should already have details of the Customer, Site, and Building
4. Central station details such as its account number, DNIS number, and prefix number should be available
5. Serial number and the configuration key of the CLSS Pathway. (Available on the Quick Start Guide.)

4.2 Receiving a CLSS Account for Your Organization

Configuring the CLSS Pathway requires a CLSS account. If you already have the CLSS account, then proceed to section 4.3, "Assigning the Device to a Customer".

If You Do Not Yet Have a CLSS Account. Your organization's Administrator* should visit *fire.honeywell.com* or scan the QR code below for instructions to request a CLSS Account:

* That Administrator is someone who can sign on behalf of the organization.

Using the CLSS account received, the Administrator should add customers and employees in *CLSS Site Manager*. Refer to the help section of *CLSS Site Manager* for more information.

4.3 Assigning the Device to a Customer

Associate your device with a CLSS *Site* and *Building* for your *Customer*.

1. Log into the *CLSS* mobile App.
2. Tap the three dots at the top-right corner of the dashboard
3. Tap **Install Dialer Capture**.
4. Follow the on-screen instructions.

4.4 Configuring the Central Station Alerting

A. Add a Central Station to Your CLSS Account The organization's Administrator should do this one-time task for each central station associated with the panel.

1. Log onto *CLSS Site Manager:* fire.honeywell.com
2. Click your profile icon at the top-right corner and select **External Accounts**.
3. Click **ADD NEW** at the **Central Stations** section in the **External Accounts** page.
4. Follow the on-screen instructions.

B. Assign a Central Station Account to the Device Provide the central station account details associated with the specific site.

1. Log onto *CLSS Site Manager:* fire.honeywell.com
2. Navigate to the *Customer > Site*, where the device is installed.
3. Click the **Feature Activation** icon at the bottom of the left sidebar.
4. Click the **CLSS Pathway** section at the left.
5. Click on your CLSS Pathway communicator in the list.
6. Click **Configure Central Station Alerting** in the details view.
7. Follow the on-screen instructions.

Section 5: Mounting and Wiring

Mounting the communicator should take place within a UL-listed Honeywell enclosure, such as HW-AV-ENC.

NOTE: For UL installations, the communicator must be mechanically secured to a UL-listed enclosure, such as a UL-listed junction box.

5.1 Prerequisites

1. Know whether to install CLSS Pathway for dialer capture or for panel relay monitoring
2. Know whether to install the CLSS Pathway for dialer capture with LAN (dual-path communications) or without LAN (sole path)
3. The panel should be programmed to support the CLSS Pathway

5.2 Programming the Connected Panel

Program according to the panel's programming document.

- Enabling the PSTN dialer of the panel
- Selecting the DTMF mode (for tone dialing)
- Selecting the Contact ID communication format
- Providing any telephone number for dialing. Ex: 999999
- Entering the 4-digit account number
  NOTE: If the panel has two central stations at two locations, program each account identically.

5.3 Before Mounting

- Inform the central monitoring station to put your CLSS Account on test.
- If installing on an existing operational panel, inform the operator and the local authority that the panel will be a temporarily out of service.
- Ensure that the panel is powered down.

5.4 Important

- Check that you have the communicator, 3-ft antenna, and the *Quick Start Guide* from the carton box.
- Only a regulated UL-listed UOJZ, UTOU, or NBSX control panel or power supply should power the communicator.
- The communicator must be connected to a UL-listed control panel with power limited circuits.
- For UL installations, secure the communicator to a UL-listed enclosure, such as a UL-listed junction box.
- Install the communicator only at a dry indoor location.
- The location and wiring methods must be in accordance with the National Electrical code, ANSI/NFPA 70.
- Install in accordance with the National Fire Alarm and Signaling Code, NFPA 72.
- Mount the communicator inside an enclosure, for example HW-AV-ENC, as shown in Figure 5.1 below.
- Enclosure should be close nipple to the fire alarm control panel.

5.5 To Mount the Communicator

1. In the *Quick Start Guide*, locate the installation sticker at the bottom right of the last page.
2. Check that the sticker has the serial number and the configuration key to program the communicator.
3. Place the sticker on the inside lid of the enclosure for programming steps and for future reference.
4. Mount the enclosure box on the wall next to the fire panel using the wall mounting holes.
5. If using the HW-AV-ENC enclosure, mount it onto the two mounting holes as in Figure 5.1 and secure it with the hardware supplied with the enclosure.
6. For other enclosures, use the communicator box' mounting flanges as a template to drill holes for appropriate sized mounting hardware. (Not supplied).
7. Slide the box onto the mounting studs and secure with the hex nuts provided in the enclosure kit.

5.6 Installing the Antenna

The antenna comes with an SMA connector, which provides easy connection with the communicator.

IMPORTANT

- Do not use a damaged antenna with the communicator. Replace the damaged antenna immediately.
- Use only a manufacturer approved antenna. Non-approved antennas or modifications could impair service quality, damage the device, and violate FCC regulations.
- A location below the ground level or a metal structure may impact the network coverage.
- The antenna should be positioned perpendicularly to the ground, either right side up or upside down.
- Keep the antenna away from any sources interfering with or blocking the RF signal. For example, a metal object may shield the cellular radio RF signal.
- The antenna should be at least 7.8" (20 cm) away from people.
- The antenna must not be co-located or operating with any other antenna or transmitter.
- Ensure that the panel supplies 24V DC power from its constant power output.

5.6.1 To Connect the Antenna

1. Route the antenna cable through the small rubber grommet located on the top left side of the enclosure.
2. Attach the magnet at the bottom of the antenna onto the top wall of the enclosure.
3. Locate the antenna connector on top of the communicator.
4. Thread the antenna cable end onto the antenna connector and tighten.
5. Loop the excess cable length inside the enclosure.

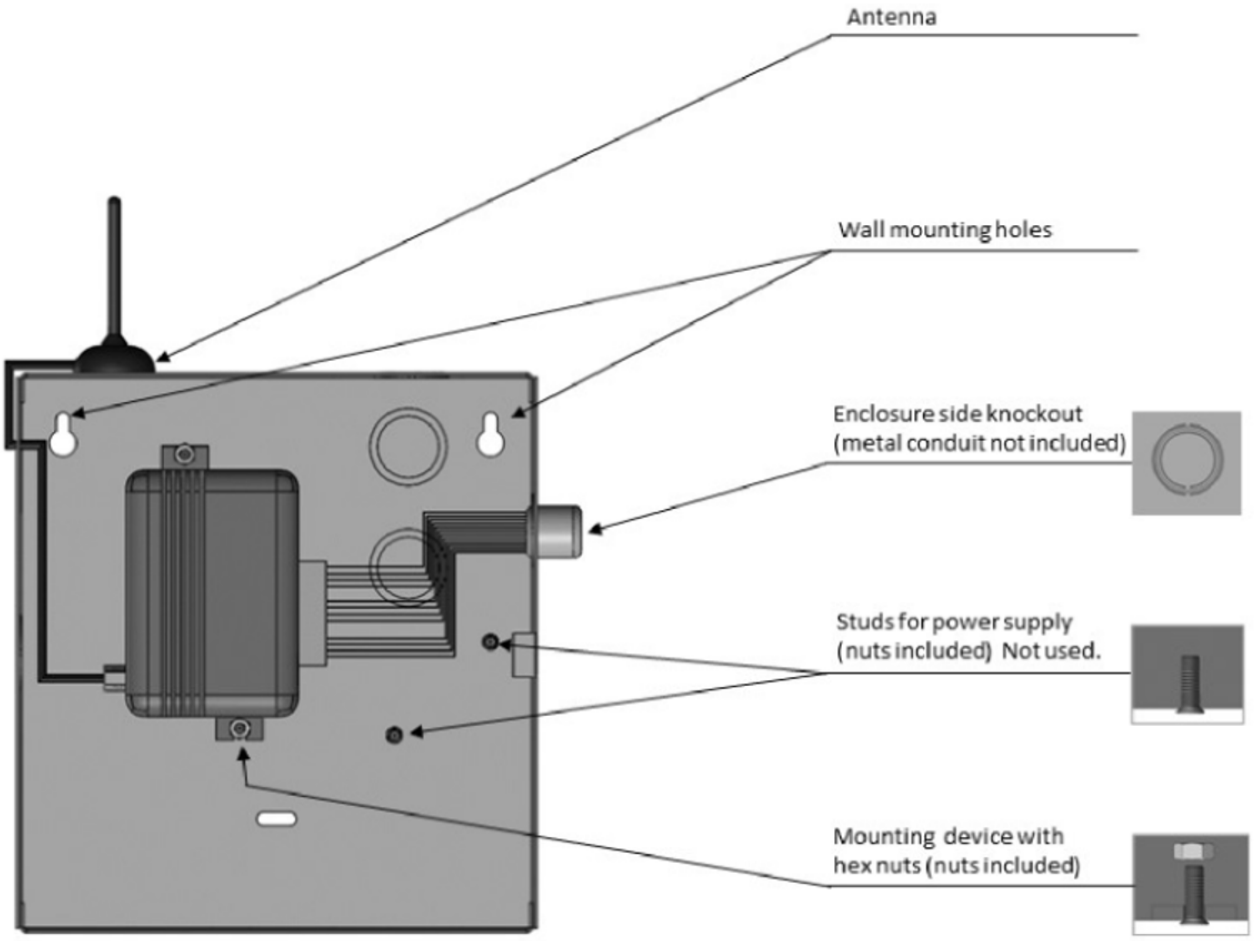


Figure 5.1: CLSS Pathway Inside the Enclosure

5.7 Wiring the Communicator

You can wire the communicator either for capturing dialer data from a panel's dialer interface or for monitoring dry contact relay outputs.

5.7.1 Wiring for Dialer Capture

For dialer capture, you connect both telephone dialer ports of the fire panel with the communicator. If a dual-path connection is needed, connect the LAN port of the CLSS Pathway with the customer's network router.

Preparations

- For panel dialer ports with 8-pin RJ type connectors, use an RJ45 connector with the other end as a pigtail.

- Use only the Pin 4 wire, which is typically Blue with White stripe, for RING connection.
- Use only the Pin 5 wire, which is typically solid Blue, for TIP connection.
- Cut all other wires.
- Enclosure should be close nipple to the fire alarm control panel.
- All wirings must be within a conduit.
- The terminal strips can accommodate solid or stranded wires with sizes from 14 to 22 AWG.

To Wire the Panel with the Communicator

Panel's Terminal	Panel's Connector	Connections at CLSS Pathway
AUX	+	Connect to +
GND	-	Connect to -
PRIMARY DIALER	RING	Connect to RING
	TIP	Connect to TIP
BACKUP DIALER	RING2	Connect to RING2
	TIP2	Connect to TIP2

CAUTION: DO NOT USE RESETTABLE POWER TERMINALS.

5.8 Powering ON

1. Power ON the communicator and the panel.
2. Ensure that the panel and the communicator are receiving power.
3. Ensure that the Green LED on the communicator is continuously ON indicating successful connections.

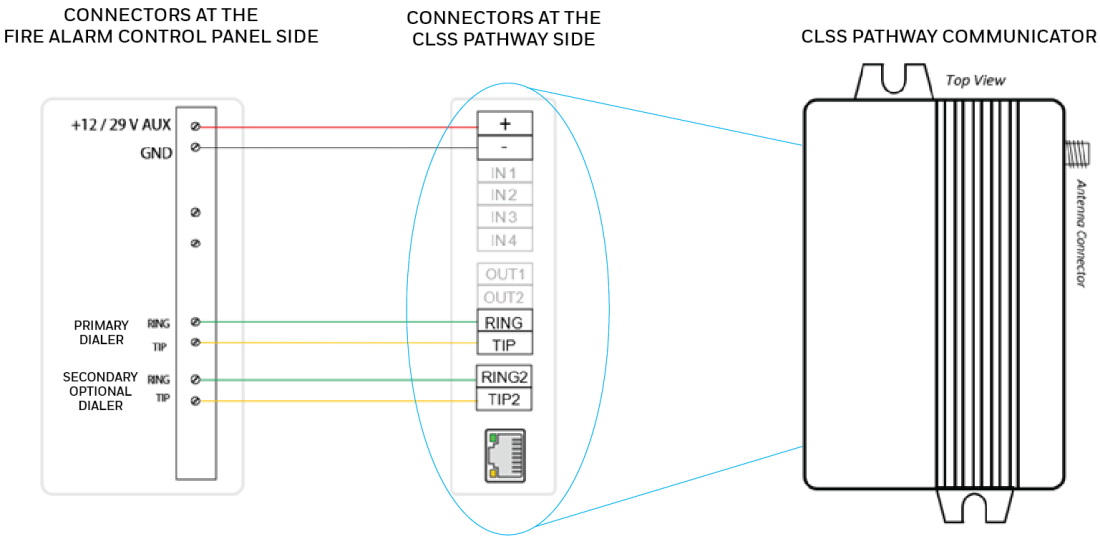


Figure 5.2: Wiring for Dialer Capture

5.8.1 Wiring for Dry Contact Relay Outputs

The communicator can be wired to monitor dry contact relay outputs. This wiring is done without connecting to a dialer interface.

CAUTION: ALL WIRING MUST BE WITHIN A CONDUIT.

CAUTION: DO NOT USE RESETTABLE POWER TERMINALS.

To Wire for the Dry Contact Relay Outputs

1. Install a 10K resistor between the communicator ground and its each input.
2. Connect the panel relay terminals and the communicator as in the Figure 5.3.
3. Ensure that the connections are as in the below table:

Panel's Terminal	Connections at CLSS Pathway
AUX	Connect to AUX +
GND	Connect to GND
Trouble Relay Output	Connect to the IN1 port
Fire Alarm Relay Output	Connect to the IN2 port
Supervision Alarm Relay	Connect to the IN3 port
Water Flow Relay Output	Connect to the IN4 port

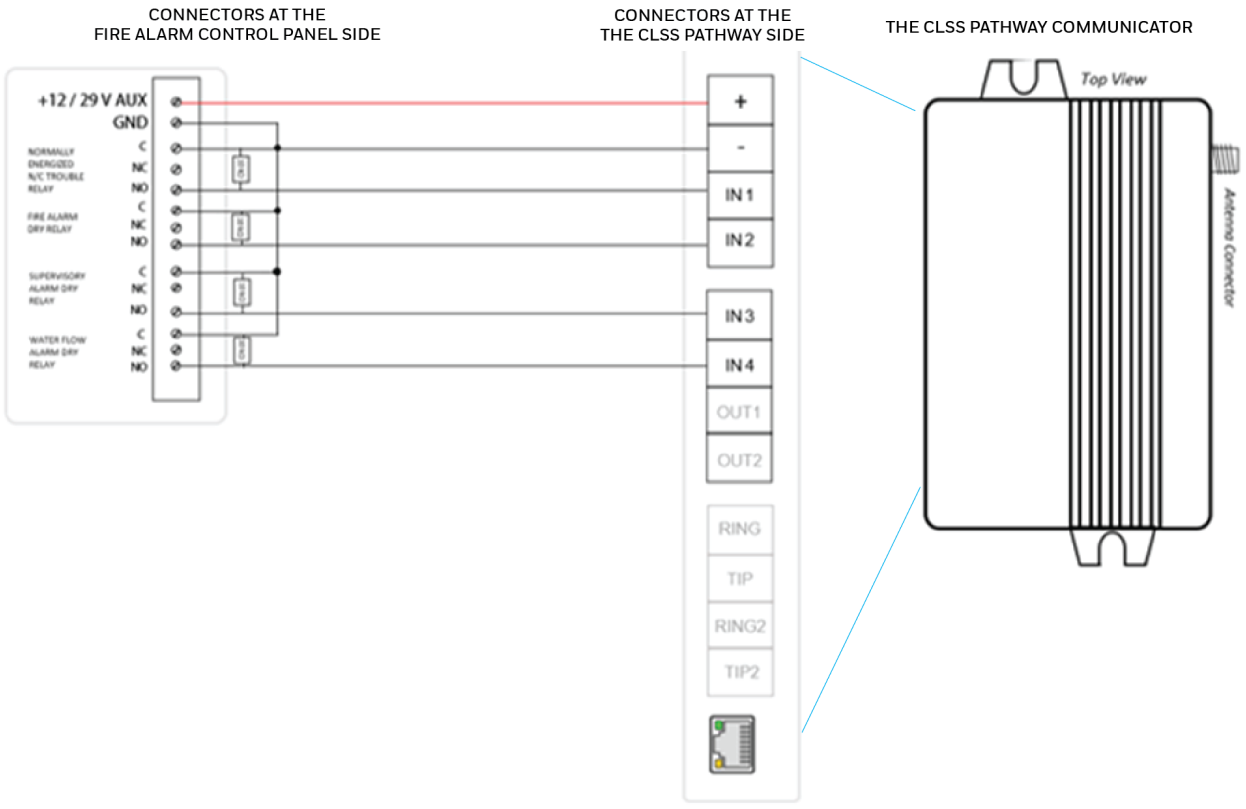


Figure 5.3: Wiring for Dry Contact Relay Monitoring

5.8.2 Powering ON

1. Power ON the communicator and the panel.
2. Ensure that the panel and the communicator are receiving power.
3. Ensure that the Green LED on the communicator is continuously ON indicating successful connections.

NOTE: Refer to the Section 6: "Troubleshooting" if there is an issue and resolve it.

5.9 Activating the Central Station Communication

CAUTION: BEFORE ACTIVATING THE CENTRAL STATION COMMUNICATION, CHECK ALL THE CONNECTIONS.

When the CLSS Pathway receives its first event from its panel, it registers itself with *CLSS Site Manager* and the central monitoring station, and then becomes active.

The panel event appearing on *CLSS Site Manager* confirms that the communicator is activated. You can create a test event on the panel to perform this one-time activation.

Tip! You can now check connection results such as the signal strength in the *CLSS* App.

5.10 For Dual-path Communications

1. Connect the LAN port of the communicator to the customer's network.
2. Observe that the Yellow LED for network connectivity is flashing to indicate a live Ethernet connection.

5.11 Verifying the Communications

The RJ45 connector LEDs should have the following states:

Yellow LED RJ45 Connector	Indication
The LED is Constantly ON	Connected with good signal
Green LED RJ45 Connector	**Indication**
The LED is Blinking	Cable connection and communication with the router are good.

NOTE: Refer to the Section 6: "Troubleshooting" if there is an issue and resolve it.

5.12 Cellular Signal Strength

Once the CLSS Pathway is activated, you can check the signal strength shown on the activation screen in the *CLSS* App.

NOTE: The signal bar shown is in the RSSI (Received Signal Strength Indicator) rating format. The signal bar is *not* in the dBm rating!

Signal Bar	Signal Strength Rating
1	1 to 9
2	10 to 15
3	16 to 23
4	24 to 31

5.12.1 Improving the Signal Quality

Honeywell recommends that the signal strength rating should be 5 or above for a consistent good connection.

If the signal rating is lower than 5, reposition the antenna, and monitor the signal strength bars in the *CLSS* App.

If required, contact Honeywell Technical Support.

Section 6: Troubleshooting

CONNECTION TROUBLES

Resolved Status Indication: The Communicator LED starts flashing. Continuous ON indicates a good connection.

LED Status	Possible Cause(s)	Corrective Action(s)
OFF	The communicator is not connected to the panel.	Ensure that the wirings are as per the wiring diagrams.
	The panel is not supplying power.	Measure the AUX output of the panel.
	The communicator device is damaged.	Replace with an undamaged communicator.
Flashing Slow	Trying to establish connection.	Reposition the antenna.
	No cellular signal available.	
Flashing every 5 seconds	Low signal connectivity	Reposition the antenna.

LAN NETWORK TROUBLES

Resolved Status Indication: The RJ45 connector's flashing LED indicates data transfer. Continuous ON indicates a good connection with the panel and router.

LED Status	Possible Cause(s)	Corrective Action(s)
	Yellow LED	
OFF	The LAN cable is not plugged into the communicator.	Ensure that the wirings are as per the wiring diagrams.
		Measure the AUX output of the panel.
		Replace with an undamaged communicator.
	Green LED	
OFF	The router is not providing an IP via DHCP.	Check your DHCP server settings, if DHCP is in use.
	There is no Internet access.	Use another device in the same network and check your router settings.

EVENT TROUBLES

Resolved Status Indication: The RJ45 connector's flashing LED indicates data transfer. The *Connected Life Safety Services* App as well as *CLSS Site Manager* start receiving events.

Trouble	Corrective Action(s)
If no events are received	1. Verify the RING and TIP connections. ✓ Ensure that the RING and TIP terminals are connected to a TELCO ring and tip and *not* to the R-1/T-1 terminals. ✓ Ensure that there is no connection trouble. 2. Then, check for communication failure error messages at the panel and fix the error, if any. 3. Disable the *Wait for Dial Tone* options in the panel.
Cellular connectivity issues	1. Go to the **Device Registration** screen in the CLSS App. 2. Ensure that the signal strength shown on it is at least one to two bars. 3. Reposition the antenna for higher signal strength.

12 Clintonville Rd
Northford, CT 06472

(203) 484-7161

140 Waterside Rd
Leicester LE5 1TN, UK

+44 (0) 203 4091779

Honeywell