

# Connected Services Gateway Setup Guide for FireClass Fire Panels

Rev. C



05791466






# Contents

Introduction.....	5
SafeLINC Cloud system components and functions.....	6
Connected Services Gateway card.....	6
SafeLINC Web Architect UI.....	7
Language support on the gateway platform.....	8
Overview of the fire panels and CSG interfaces with the panels.....	8
Supported fire panel firmware versions.....	8
CSG setup for FireClass fire panels.....	9
Setting up the CSG for an Ethernet interface connection to the fire panel.....	9
Configuring the CSG.....	9
Creating the FireClass panel configuration.....	10
Registering the CSG card on SafeLINC Web Architect.....	11
Connecting the CSG and fire panel over Ethernet.....	11
Setting up and configuring the gateway to the serial interface of the fire panel.....	13
Updating the fire panel configuration.....	13
Configuring the FC50x Fire Panel for the CSG.....	13
Updating the CSG configuration for serial interface.....	13
Connecting the CSG to a fire panel over serial interface.....	13
Configuring the cellular network.....	14
Configuring the APN for the cellular network.....	14
Limitations.....	15
Access point name.....	15
The building network.....	15
CSG for central station connection.....	17
Supported fire panel firmware versions to central station connection.....	17
Configuring the panel for central station reporting.....	17
FC70X/FC60X series panel settings and faults.....	17
MT1 FC501, FC503, FC506 panel settings and faults.....	18
Configuring the CSG for central station reporting.....	19
CSG soft restart.....	21
Central station connection status indicators on Gateway.....	22
IP path supervision.....	22
CSG operational flow.....	23
Initial setup.....	23
Updating the firmware.....	24
Updating the firmware locally.....	24
Over-the-air updates.....	24
Troubleshooting a blinking panel indicator.....	25
Remote Gateway download.....	26



# Introduction

This document is a guide for internal project teams involved in setting up the Connected Services Gateway (CSG) card and the corresponding SafeLINC Cloud Services. FireClass panels can connect to the SafeLINC Cloud Services by interfacing to the CSG card either through the Ethernet interface or the serial interface of the fire panel. The CSG also supports central station reporting for connected FireClass panels on Ethernet interface and MT1 -FC50xx on Serial interfaces.

 **Note:** You must have knowledge of FireClass fire panels and understand how to use FireClass Express tools to configure the respective fire panels.

# SafeLINC Cloud system components and functions

The CSG card provides SafeLINC Cloud connectivity services to the FireClass fire panels. The CSG can connect to the SafeLINC Web Architect using the building Internet, or through a cellular connection. You can establish connection to the panel using the Ethernet interface, or the serial interface of the CSG card.

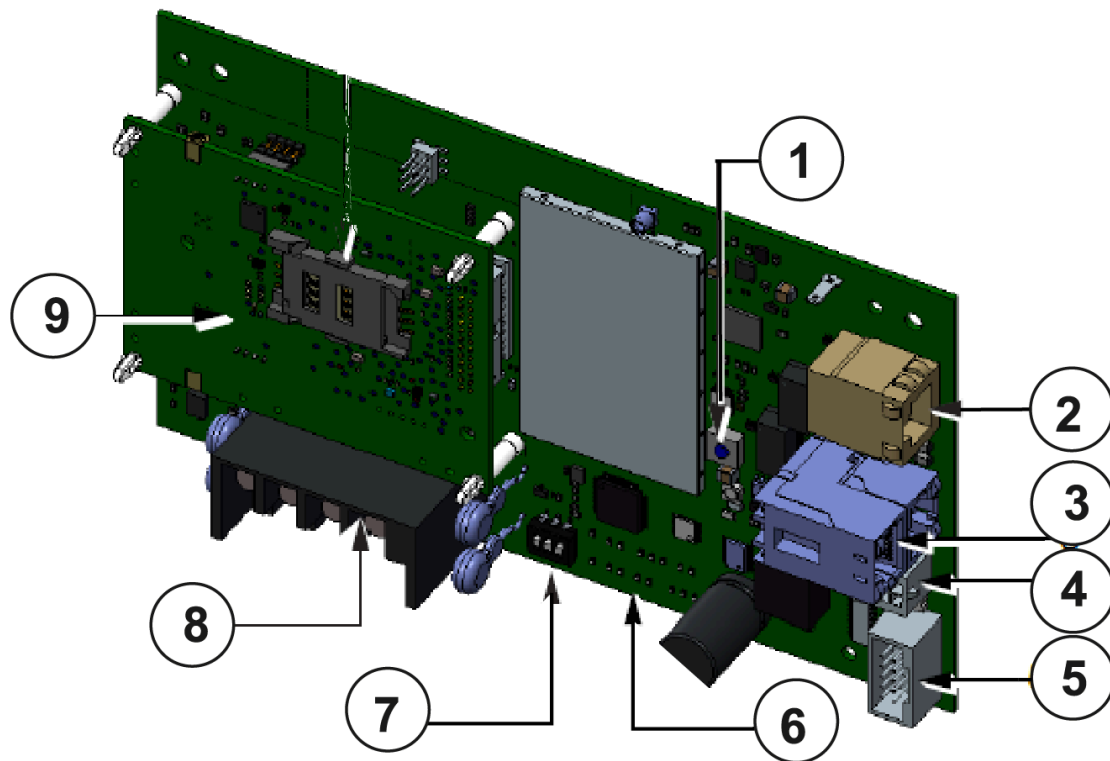
The CSG provides two interfaces for SafeLINC Cloud connection:

- IP
- Cellular

## Connected Services Gateway card

The CSG card is a hardware module interfacing with the fire panel to provide SafeLINC Cloud connectivity and services.

**Figure 1: Connected Services Gateway card**



Callout	Description
1	Reset switch
2	LAN Ethernet: connects to building LAN You must use a shielded Ethernet cable.
3	Panel Side Ethernet 1/2: fire panel side Ethernet ports: connects to fire panel
4	Pin 4 power connector
5	Serial port: connects CSG module to fire panel over serial interface

Callout	Description
6	Status LEDs
7	<b>Unused:</b> Configuration DIP switches
8	<b>Unused:</b> NA telephone connection
9	<b>Optional:</b> Cellular module

The CSG reports the following events to cloud:

- All Alarm events
- All Fault events
- Pre Alarm events (CAT6 - Pre-Alarm Events)
- Gas Alert
- Warning
- Walk Test
- Generic/Information
- Disable/Enable (Panel Event log only)
- Output State

## SafeLINC Web Architect UI

For more information about the features of SafeLINC Web Architect, refer to the Help section of the web user interface (UI): <https://eu.safelinc.johnsoncontrols.com/help/en-US/>. The main features of the SafeLINC Web Architect include:

- Asset management, user access, upgrading gateway firmware, and panel status
- Notification settings configuration: email and push notification with the mobile app
- Reports: you can download event log reports from the web UI
- Web UI supports 15 languages

The supported languages are:

- America
  - English
  - French (Canada)
  - Spanish (Latin America)
  - Portuguese (Brazil)
- Europe
  - German
  - Danish
  - Czech
  - Dutch
  - French
  - Italian
  - Polish
  - Portuguese
  - Spanish
  - Swedish
  - Turkish

## Language support on the gateway platform

The CSG, SafeLINC Web Architect UI, and SafeLINC Cloud Mobile App supports languages, see [SafeLINC Web Architect UI](#).

To ensure that the web UI and mobile app show your chosen language, configure the fire panel to operate in the same language. If you do not configure the fire panel in this way, the web UI and mobile app display events in the same language as the fire panel language.

## Overview of the fire panels and CSG interfaces with the panels

**Table 1: EU-Gateway (EUCSG) and supported fire panel interface matrix**

Panel interface	FireClass FC32, FC64, and FC240	FireClass FC700	FireClass FC503, FC506
Ethernet	—	X	—
COM1 (RS800 format)	X	X	—
COM1 (third-party interface)	X	X	—
PC link (T-link format)	—	—	X

## Supported fire panel firmware versions

**Table 2: Panel firmware versions**

Panel interface	FireClass FC32, FC64, and FC240	FireClass FC700	FireClass FC503, FC506
Ethernet	—	V29.2 and higher	—
COM1 (RS800)	—	—	—
COM1 (TPPI)	V23.0 and higher	V29.2 and higher	—
PC link (T-link format)	—	—	V1.03.04 and higher



# CSG setup for FireClass fire panels

The CSG supports both Ethernet and serial interface with the fire panel. Ensure that you have one of these interfaces available on the panel for interfacing with the CSG card.

## Setting up the CSG for an Ethernet interface connection to the fire panel

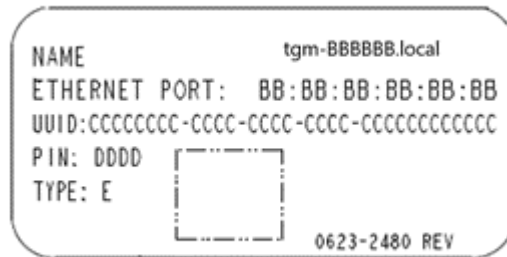
### Configuring the CSG

#### About this task:

You can configure the CSG from the Gateway local webserver. Access the Gateway local webserver using the URL: `tgm-x1x2x3.local/`, where `x1x2x3` are the last three bytes of MAC ID printed on the CSG hardware. For example, the MAC ID label on the CSG board printer Ethernet Port is `00.01.02.03.04.ab.bc`, the URL is `tgm-04abbc.local/`.

You can see the URL labeled NameL tg-BBBBBB.local on the Gateway board, see [Figure 2](#).

**Figure 2: CSG Label for URL and MAC addresses**

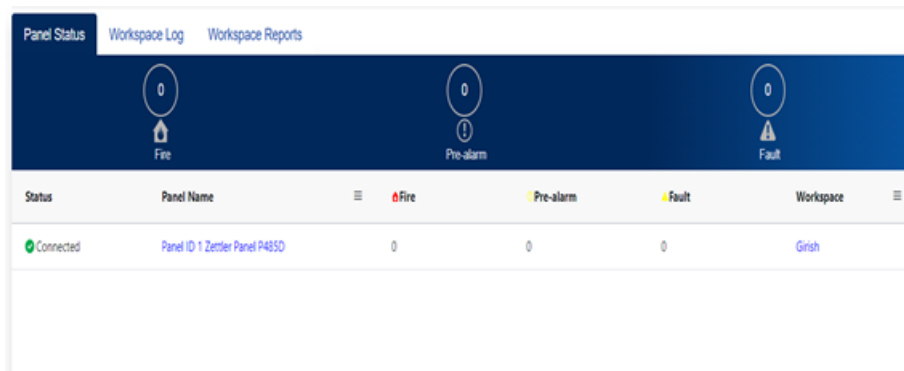


1. Connect the CSG Ethernet port, labeled Panel P1-2 port, to your local PC with an Ethernet cable. See [Figure 1](#), item 3.
2. Turn on the CSG using a suitable 24 V power supply.
3. Set the PC/laptop IP address as shown in [Configuring the CSG](#).
4. Open your browser and enter the URL `tgm-x1x2x3.local/` to load the gateway web page.
5. Click **Configuration**.  
Use the following user name and password to access the Gateway Configuration, Central Station and Panel Configuration tabs:
  - Username: Admin
  - Password: 579146
6. Enter the configuration details in the form and click **Update**.
  - ⚠ **WARNING:** The serial number is unique for each panel. Use the last 12 digit serial number displayed on the panel cabinet. Do not use random digits.
7. Remove the Ethernet cable from the system or PC, and connect the open network or building Internet cable to the Lan-P3 port on the CSG.
  - ℹ **Note:** You can use the panel ID, panel type, and panel details configured in the web page on the cloud. For example, if using the following configurations on the gateway:
    - Panel ID: 01
    - Panel Type: P485D

- Panel Detail: Panel P485D

The panel appears as shown in [Figure 3](#). For the MT1 Panel Series, select FC501/FC503/FFC506, or the panel cannot connect to the CSG/SafeLINC.

**Figure 3: Panel view on SafeLINC**

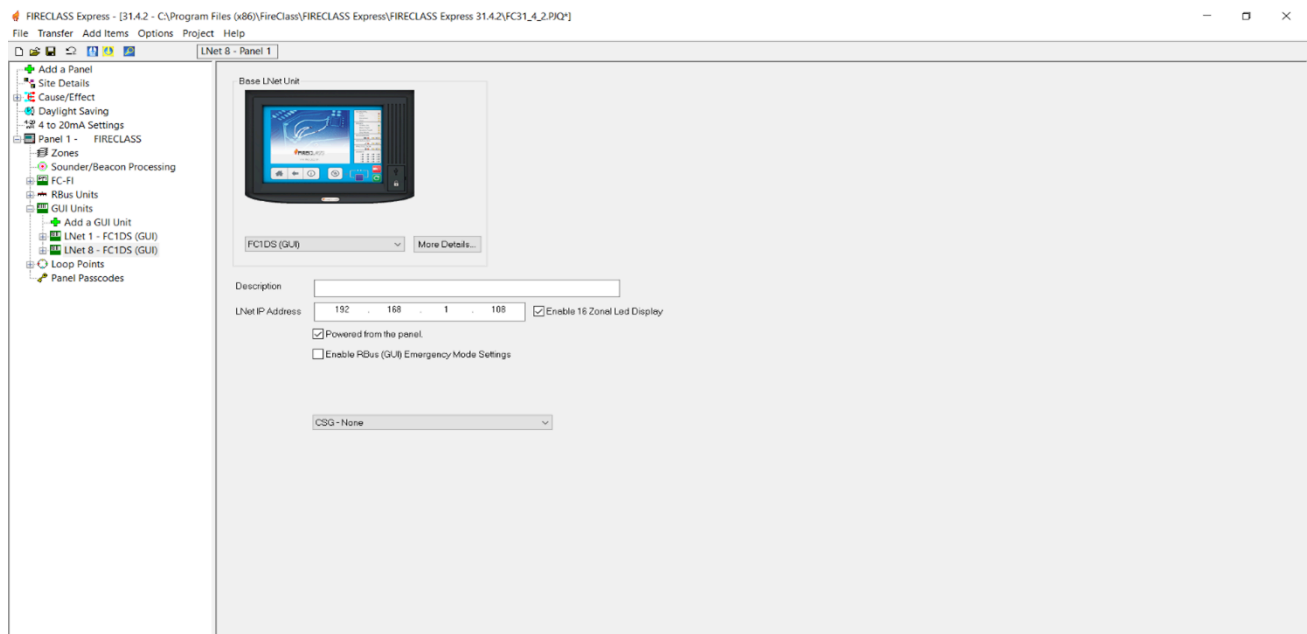


- The CSG Panel-P1-2 Port IP address is preset to 192.168.1.109. Based on the LNET node IP setting, configure it using the CSG local webserver.  
LAN-P3 IP is configured as DHCP by default. You can also configure LAN-P3 IP to a required network setting through CSG local webserver.
  - Go to the local CSG webserver page `tgm-x1x2x3.local/` and click *Gateway Configuration*.
  - Update the required Panel P1-2 port and LAN-P3 port IP address.
- ❗ **Note:** Update Panel P1-2 when you change the Fire Panel IP address.
- Select the required features, and restart when you complete the CSG configuration.
  - Remove the Ethernet cable from the system or computer, and connect the open network or building Internet cable to the Lan-P3 port on the CSG.

### Creating the FireClass panel configuration

- Update the FireClass fire panel configuration using FireClass Express tool.
- Add a GUI node and update the IP address as 192.168.1.109 to connect the CSG to the GUI node, see [Figure 4](#).

**Figure 4: Updating a FireClass panel configuration for CSG Ethernet interface**



## Registering the CSG card on SafeLINC Web Architect

### About this task:

You must be invited as a user with the appropriate permissions for SafeLINC Web Architect to register your CSG card to the SafeLINC Web Architect UI.

Registering the CSG card on the web UI enables the CSG card for cloud services and shows the status of the fire panel in the web UI and in the mobile app.

1. Use the UUID and PIN on the CSG hardware unit to add the CSG card in the Devices view.
  - ① **Note:** The UUID is located on the CSG card and the format will look similar to CCCCCCCC-CCCC-CCCC-CCCCCCCCCCCC.The CSG card contains the PIN in a six-digit format.
2. Go to **Quick Actions** drop-down and click **Add New Gateway**.
3. Using the UUID and PIN on the CSG hardware unit, add the CSG card in the *Devices* tab.
  - ① **Note:** For more detail about SafeLINC refer to the help menu in the SafeLINC web architect. [https://eu.safelinc.johnsoncontrols.com/help/en-US\\_NEW/](https://eu.safelinc.johnsoncontrols.com/help/en-US_NEW/)

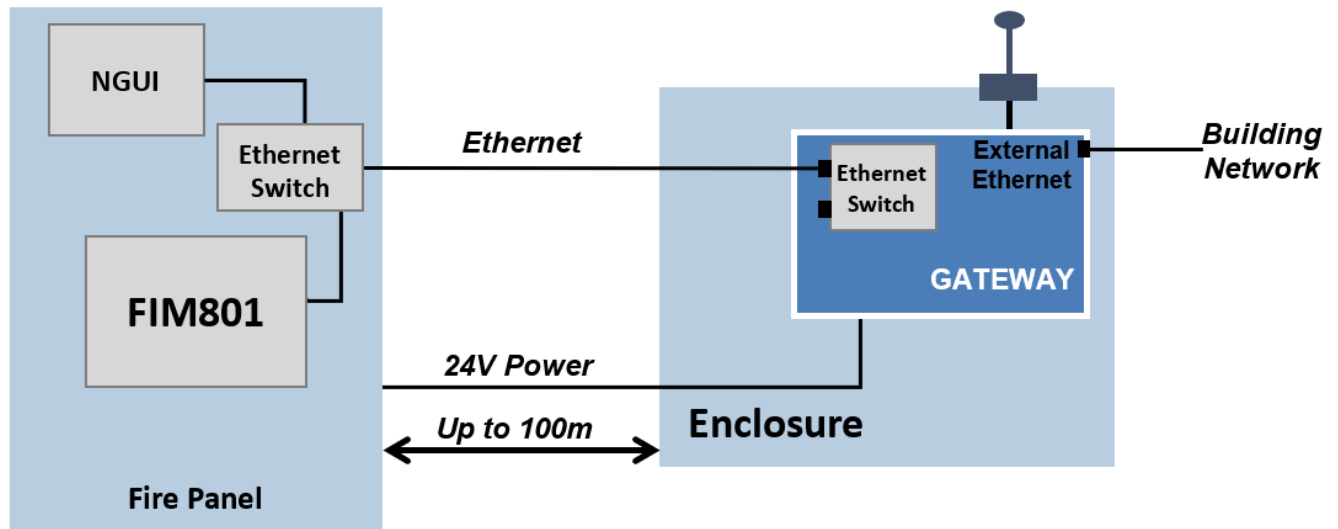
## Connecting the CSG and fire panel over Ethernet

### Before you begin:

You must use a PCS800: PROFILE Ethernet Switch.

1. Connect the PCS800: PROFILE Ethernet Switch between the GUI and panel motherboard. The CSG can also connect on the same switch using Ethernet Internet interface. You can mount switches inside the fire panels. See [Figure 5](#).
2. With an Ethernet cable, connect the CSG port marked as Panel-P1-2 port to the Ethernet switch mounted inside the panel or to the motherboard Ethernet port, depending on the panel type. See [Figure 5](#).

Figure 5: Gateway connected to a FireClass FC700 fire panel



When you complete the steps in sections [Configuring the CSG](#) to [Connecting the CSG and fire panel over Ethernet](#), power up the fire panel and gateway. The fire panel appears in your workspace on the SafeLINC web UI and mobile app.

For the first setup, when you see the fire panel under the registered gateway, you need to restart the gateway. The gateway is ready to use for the remote monitoring service.

- **Important:** Reset the fire panel when you complete all configuration and make a connection on the Ethernet or Serial interface.

# Setting up and configuring the gateway to the serial interface of the fire panel

## Updating the fire panel configuration

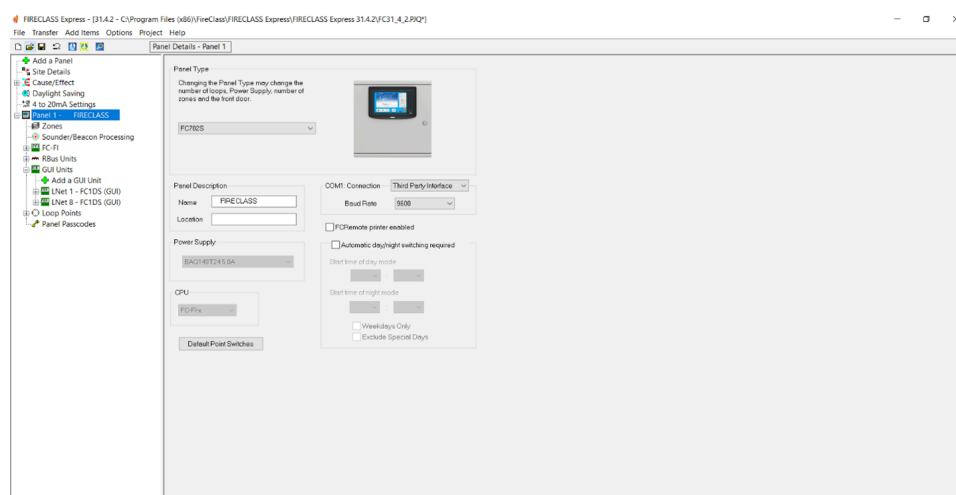
### About this task:

The CSG connects with a FireClass panel using the COM1 port of the panel on the FIM800 or FIM801 board.

The supported protocols on serial interface are RS800 and third-party interface (TPPI) at 9600 baud rate.

1. Configure the panel for TPPI or RS800 using the FireClass Express tool on the COM1 serial interface at 9600 baud rate.

**Figure 6: Configuring a FireClass panel using FireClass Express tool for serial interface**



2. Update the fire panel with the new configuration.

## Configuring the FC50x Fire Panel for the CSG

Refer to the respective FC50x installation and user manual to install and configure the CSG with the FC50x. Enable the CSG from the FC50x panel UI. The FC50x supports the serial interface to connect with the CSG.

Go to **Program Menu > Login > System [8]** and press **Enter** until you get to the Communication Card option. Select either FC500IP/PSTN or CSG. Once the CSG is selected the panel resets itself.

- Installation Manual: 120.515.873\_FC-FC500-P-I-01
- User Guide: 120.515.922\_FC500-QKUSR

## Updating the CSG configuration for serial interface

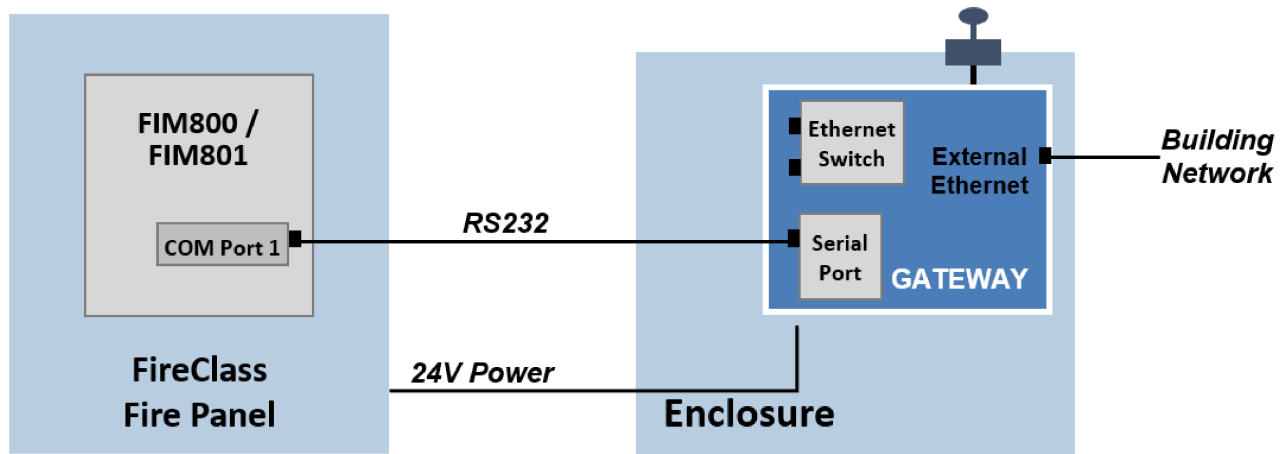
See [Configuring the CSG](#).

## Connecting the CSG to a fire panel over serial interface

1. Ensure that you configure the fire panel and CSG as outlined in the section [Updating the fire panel configuration](#).
2. Restart the CSG and wait for five minutes for the CSG to turn on.

3. Connect an FireClass FC32, FC64, or FC240 panel or a CPU800 to the Gateway Serial Port (P1) connector, as shown in [Figure 7](#).

**Figure 7: CSG connected to a FireClass FC32, FC64, or FC240 fire panel with CPU800 over serial interface**



► **Important:**

- Reset the fire panel when the configuration and serial interface connection is complete.
- Do not use both interfaces of the CSG, serial, and Ethernet connection Panel-P1-3, to connect to the fire panel simultaneously. Only one interface works at any time.

## Configuring the cellular network

The CSG provides cellular connection support in addition to the building's Internet connection for cloud connectivity. Configure APN settings to match the SIM card, and mount the cellular modem onto the CSG hardware.

For setup information, refer to the *Cellular Module and Antenna Installation Guide 579-1459*.

### Configuring the APN for the cellular network


**Before you begin:**

Follow the steps in [Configuring the CSG](#) to connect the CSG to your computer.

1. Open a browser to load the CSG local web server with the process described in [Configuring the CSG](#).
2. Click **Network**, and select **Cellular modem configuration**, see [Figure 8](#).
3. Select or enter the correct APN for your SIM.
4. When you complete the configuration, restart the gateway.

❗ **Note:** For limitations related to configuring the APN and building network IP, see [Limitations](#).

**Figure 8: APN configuration for a cellular connection**



**CONNECTED SERVICES GATEWAY**

[Home](#) [Status](#) [Network](#) [Download Logs](#) [Update](#) [Panel Configuration](#) [Gateway Configuration](#) [Central Station](#) [Level 4 Logout](#)

**CELLULAR MODEM CONFIGURATION**

**APN Configuration**  
Current APN: Unknown

UserName	
Password	
Authentication	<div>CHAP ▾</div>
New APN	<div><div><input checked="" type="radio"/> iot0718.com.attz</div><div><input type="radio"/> m2m.com.attz</div><div><input type="radio"/> Other: <input style="width: 100px;" type="text"/></div></div>
<div style="display: flex; justify-content: space-around;"><div style="background-color: #333; color: white; padding: 5px 15px; border-radius: 3px;">Apply</div><div style="background-color: #333; color: white; padding: 5px 15px; border-radius: 3px;">Read</div></div>	

## Limitations

### Access point name

You can update the new access point name (APN) for any cellular provider using the **Network** tab at URL:192.168.1.109 see [Figure 8](#). However, the APN username and password settings are not available with the current release. The username and password options are preset to be blank and the authentication method is **chap**.

**❗ Note:** SIM cards that require a username and password do not work in the Gateway.

### The building network

For panels that support Ethernet GUI, the IP address range is in the 192.168.1.x series.

The Gateway panel Ethernet port IP address is fixed at 192.168.1.109

If you provide the building network IP address in the same subnet mask as 192.168.1.x, the panel P1 and P2, and LAN P3 ports cannot work together.

The panel's LNET Fault Active/Restoring process is in progress.

### Troubleshooting network connectivity

► **Important:** You must connect a router in the building network to provide the IP address range for a LAN P3 connection.

Setting up the TP-LINK router:

1. Connect to the router with a laptop, open the web browser and enter the default router URL, 192.168.1.1.
2. Enter the router password to redirect to the router home page
3. Click **Advanced**.
4. Click **LAN Settings**.

Figure 9: LAN Settings tab

The screenshot shows the TP-Link web interface with the 'LAN Settings' tab selected. The 'DHCP Server' section is active, displaying various configuration options. The IP Address field is currently set to 192.168.1.1, which is the target for modification in step 5. The 'Save' button is located at the bottom right of the settings area.

Field	Value
MAC Address	98-DA-C4-79-63-9E
IP Address	192 . 168 . 1 . 1
Subnet Mask	255.255.255.0
IGMP Snooping	<input type="checkbox"/> Enable
Second IP	<input type="checkbox"/> Enable
DHCP	<input checked="" type="checkbox"/> Enable
IP Address Pool	192 . 168 . 1 . 100 - 192 . 168 . 1 . 199
Address Lease Time	1440 minutes (1-2880. The default value is 1440 )
Default Gateway	192 . 168 . 1 . 1 (Optional)
Default Domain	(Optional)
Primary DNS	0 . 0 . 0 . 0 (Optional)
Secondary DNS	0 . 0 . 0 . 0 (Optional)

5. Modify the IP address from 192.168.1.1 to 10.10.1.1.
6. Click **Save** to restart the router.



# CSG for central station connection

The CSG supports the following three interfaces for central station connection:

- Dual Line Phone DACT
- 10/100 Base-T Ethernet
- Cellular

You can configure the CSG for primary and secondary stations to connect with DACR. If both paths are working, any event in the fire panel reports to primary DACR. If the primary path is down, all the events report to secondary DACR.

The gateway supports CSG event base reporting to central station, and you can configure CID event codes. These are the supported event types:

- Fire
- Fault
- Pre-Alarm

## Supported fire panel firmware versions to central station connection

**Table 3: Panel firmware versions**

Panel interface	FireClass FC700/FC60XX	FireClass FC501, FC503, FC506
Ethernet	V31.4.11 and higher	Not Applicable
COM1 (RS800)	Not Supported	Not Applicable
COM1 (TPPI)	Not Supported	Not Applicable
PC link (T-link format)		V1.03.04 and higher

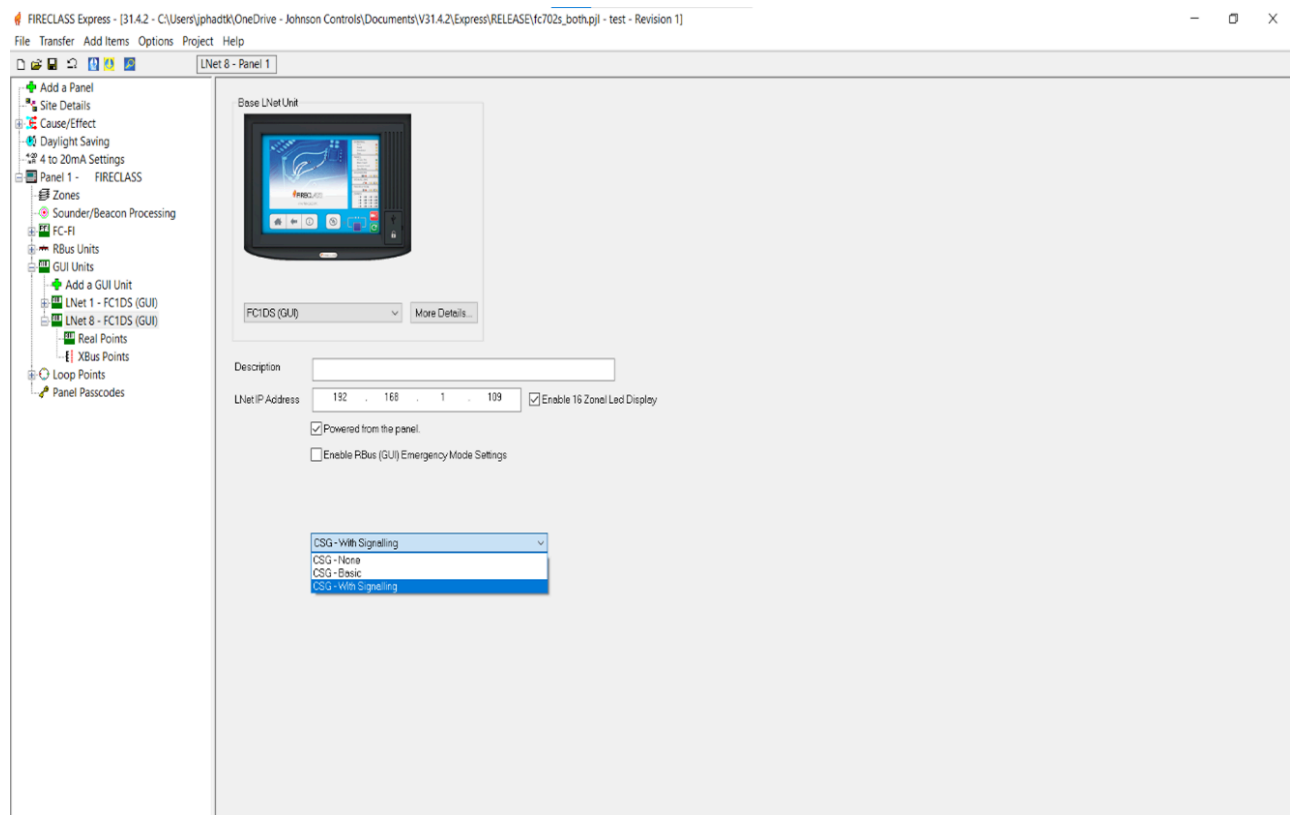
## Configuring the panel for central station reporting

### FC70X/FC60X series panel settings and faults

#### Creating the panel configuration

1. Update FireClass fire panel configuration using FireClass Express tool.
2. Add a GUI node and update the IP address as 192.168.1.109 to connect the CSG to the GUI node, see [Figure 10](#).
3. Select **CSG -with Signaling Option** for central station reporting and fault to display on the panel UI.

**Figure 10: Configuring the panel settings**



### Faults on the panel interface

The IP Communicator Gateway provides the panel with any failures that occur.

The failure conditions that the IP Communicator reports are as follows:

- Primary Path Down - Pseudo 11.
- Secondary Path Down - Pseudo 12.
- Signaling Ackn - Pseudo 15
- Signaling Fault - Pseudo 16: Grp Signaling Fault :048
- The CSG transmits signaling ACK to the panel when it successfully delivers a fire event to the central station. The panel Signaling LED Indicator indicates this.

Map these faults on the panel LNET GUI Pseudo.

If any of the paths are down, the CSG sends the fault input to the fire panel and displays on the panel GUI. If both primary and secondary paths are down, the CSG sends a signal fault to the fire panel, and this is indicated on the signaling fault LED indicator and the UI.

### MT1 FC501, FC503, FC506 panel settings and faults

#### Create the panel configuration

For the FC501/FC503/FC506 panels, enable the CSG for Panel UI or FC Console. There is no configuration. Refer to the relevant panel user manual for configuring and installing CSG with Connected Service Gateway for Central Station or SafeLINC.

To access the panel UI click **Program > System > Selected CSG option**.

### Faults on the panel interface

The IP Communicator Gateway provides the panel with any failures that occur.

Table 4 lists the failure conditions that the IP Communicator reports.

**Table 4: Panel interface faults**

Fault	LED behavior	GUI display
Primary Path down	<b>FAULT</b> LED indicating	Fault list <b>Primary Path</b> displays
Secondary Path down	<b>FAULT</b> LED indicating	Fault list <b>Secondary Path</b> displays
SafeLINC	<b>FAULT</b> LED indicating ① <b>Note:</b> Not currently supported in panel	Fault list <b>SafeLINC</b> displays
Signaling Ackn	<ul style="list-style-type: none"><li>• Fire Signal ON(Red) LED indicates the status of the events transmit to Central Station</li><li>• - LED steady indicates the transmission was successful.</li><li>- LED blinking indicates the transmission is in progress</li></ul>	
Signaling Fault	<ul style="list-style-type: none"><li>• Fire Signal Fault (Amber) LED indicates the status of the Central Station connection status.</li><li>- LED Steady indicates CSG is Disabled.</li><li>- LED Blinking indicates Central Station Connection has broken down. (When both paths are down).</li></ul>	

## Configuring the CSG for central station reporting

### About this task:

Access the gateway local web server

URL: `tgm-x1x2x3.local/`.

The last three bytes of Mac ID printed on CSG hardware is x1x2x3. For example, if the MAC ID label on CSG board printer Ethernet Port is 00.01.02.03.04.ab.bc, then the URL is `tgm-04abbc.local/`.

Set user system/PC IP to **DHCP**.

1. Connect the gateway panel interface Ethernet port, labeled panel P1-2 port to your computer using Ethernet cable. See [Figure 1](#), item 3.
2. Open the web Browser and enter the URL: `tgm-x1x2x3.local/` and press **Enter** to load the gateway web page.

3. Use the following username and password to access the *Gateway Configuration, Central Station, and Panel Configuration*:
  - Username: Admin
  - Password: 579146
4. Enable the Central Station feature and on the *Gateway Configuration* tab configure Gateway Building Ethernet port IP [lan-p3] address for Internet connectivity.
5. Go to **Central Station > Path Configuration** to configure the Central Station primary and secondary paths, use the following in your configuration:
  - Account code: your 4 digit account code
  - Interface Type: IP or PSTN or Cellular
  - Based on selected interface or channel type: Station IP or PSTN, phone number
  - Local or Source Port number, if both the primary and secondary path are IP or cellular, then the local port must not be same, or configure it as 0 for both
  - Remote port or destination port
  - Your five digit DNIS account number
  - Your encryption key, 128 bit

❗ **Note:** Your encryption key is optional, however use encryption for secure central station reporting.

**Figure 11: Central Station Path Configuration settings**

CENTRAL STATION PATH CONFIGURATION

Central Station Features  
☐ Primary Path    ☒ Dual Path

Primary Communication Path Configuration

Account Number:   
 Channel:

IP/CELLULAR Address Book  
 IP Address:   
 Local Port:   
 Remote Port:   
 Heartbeat Frequency:  (min: 30 sec, max:3600 sec)  
 Dnis:  (min: 0, max:99999)  
 Use Encryption:   
 Encryption Key:  (16 bytes hex value)

Secondary Communication Path Configuration

Account Number:   
 Channel:

IP/CELLULAR Address Book  
 IP Address:   
 Local Port:   
 Remote Port:   
 Heartbeat Frequency:  (min: 30 sec, max:3600 sec)  
 Dnis:  (min: 0, max:99999)  
 Use Encryption:

- ❗ **Note:** You can select primary path or dual path.
6. Go to **Central Station > Event Code Configuration**. You can configure or update the following CID codes:
    - Fire Alarm
    - Fault
    - PreAlarm

- GasAlert
- 7. Select the events to be communicated to central station. Click **Delete** to remove the Event Fault or PreAlarm, and the event does not send to the central station.
- ① **Note:** You cannot delete the event **Fire**.
- 8. To add Fault or PreAlarm to central station events, click **Add Event Code**.

#### Event Codes

Name	Active Code	Restoral Code		
FIRE	110	110	Edit	
FAULT	330	330	Edit	Delete
PREALARM	118	118	Edit	Delete
GASALERT	151	151	Edit	Delete

Add Event

Name	Active Code	Restoral Code
FAULT	<input type="text" value="Enter 3 digit valid cid active"/>	<input type="text" value="Enter 3 digit valid cid restor"/>

Submit Cancel

- 9. Click the drop-down under **Name** and select the event name **FAULT** or **PREALARM** event. Update the respective **Active Code** and **Restoral Code** for selected event, and click **Submit**.
- 10. To change the **Active Code** of an event, select **Edit**. A new tab opens where you can edit the **Active Code** or **Restoral Code**. Click **Submit**.  
You can edit the active and restoral CID codes for other system event codes:
  - AC MAIN'S FAULT
  - BATTERY FAULT
  - LOOP FAULT
  - EARTH FAULT
  - PRIMARY PATH
  - SECONDARY PATH
  - OUTPUT FAULT
- 11. To save your configuration and apply changes, restart the gateway. If you connect the panel and internet cable after synchronizing the panel and gateway, the panel will connect the DACR.

## CSG soft restart

When you configure the gateway for SafeLinc or central station reporting, you must restart the CSG

### About this task:

To restart the CSG follow these steps:

- 1. In the CSG, click **Central Station**, and select **Option Configuration**.
- 2. Update **Option Configuration**, and select **Update**.
- 3. A **Reboot** button appears. Click to restart the CSG. You can also restart the CSG by removing the power cable.

## Central station connection status indicators on Gateway

**Table 5: Central station connection status indicators**

Central Station connection status	LED5 (Primary path indicator)	LED6
Primary and secondary paths up	Green ON	Yellow OFF
Any one path down	Green ON	Yellow blinking
Both paths down	Green OFF	Yellow blinking

### IP path supervision

The CSG IP path is supervised, at set intervals, in a heartbeat frequency. The CSG sends a signal to the receiver and sends another signal to the receiver if it misses or does not receive a response due to an IP Path down delay. When the maximum number of retries has been reached, the CSG reports that the path is down and reports the fault to the fire panel.

Consider the following scenario:

**Example:**

IP Path Down Delay = 300 seconds

Heartbeat frequency = 100 seconds

Maximum retries = Path Down Delay/Signal Freq  
=  $300/100 = 3$

In this example, if three signals time out, or are missed, the CSG reports that the IP path is down.

If a LAN interface Ethernet cable disconnects, the gateway immediately reports that the IP path is down.

### IP path down restore

If the IP path is down due to an unreachable central station receiver, the CSG restores the IP Path event after five consecutive heartbeats. For example, if the heartbeat is set at 30 seconds, it restores the path in  $5 \times 30 \text{ seconds} = 150 \text{ seconds}$ .

# CSG operational flow

You can connect the CSG to FireClass fire panels over an Ethernet interface or over serial interface COM1, see [Table 1](#).

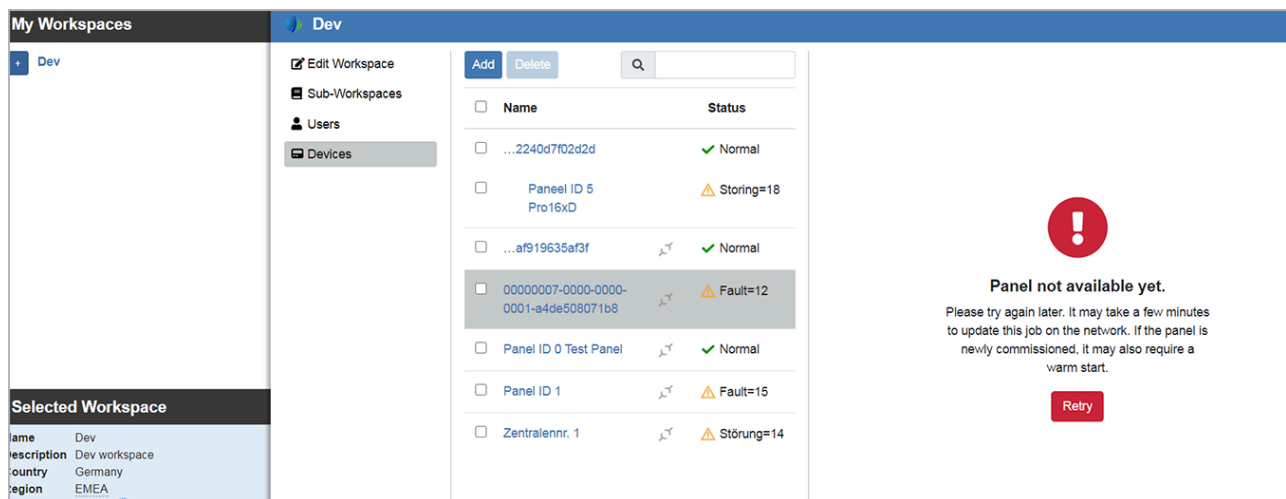
When the gateway is connected to a FireClass fire panel over the Ethernet interface, see [Setting up the CSG for an Ethernet interface connection to the fire panel](#), the panel transmits all configuration data and event history logs to the gateway. When the gateway and the fire panel are synchronized, the gateway transmits the panel status to the SafeLINC Cloud.

If the gateway and fire panel interface connect over serial interface, follow the setup procedure as shown in [Setting up and configuring the gateway to the serial interface of the fire panel](#).

The panel sends the event information to the gateway on the serial interface when you complete the setup and connect the gateway to the fire panel.

If the fire panel initially connects to the gateway, you see the panel status as shown in [Figure 12](#).

**Figure 12: Initial registration of the fire panel on the web UI**



## Initial setup

For an initial setup, you must restart the CSG. After approximately five minutes the panels live status appears on the web UI and mobile app.

The CSG is now set up. The cloud reports any supported event that the fire panel generates, and you can view the event details on the web UI and mobile app.

The CSG supports both the Ethernet and a cellular connection for cloud connectivity. If the CSG has both connections simultaneously, and the Ethernet is down, the CSG uses the secondary path for cloud connectivity.

When the gateway re-establishes a cloud connection, the CSG resynchronizes the panel status to the cloud platform. You receive notifications of new events if there are any differences between the last updated status to the cloud and panel after resynchronization, but the event is not shown on the event log.

**Note:** You can use the event log to record any events that are reported when the panel is live. Resynchronization for IP or serial connection is the same as between the fire panel and the CSG.

# Updating the firmware

You can update the gateway firmware locally or over-the-air remotely. After a firmware update, the gateway restarts.

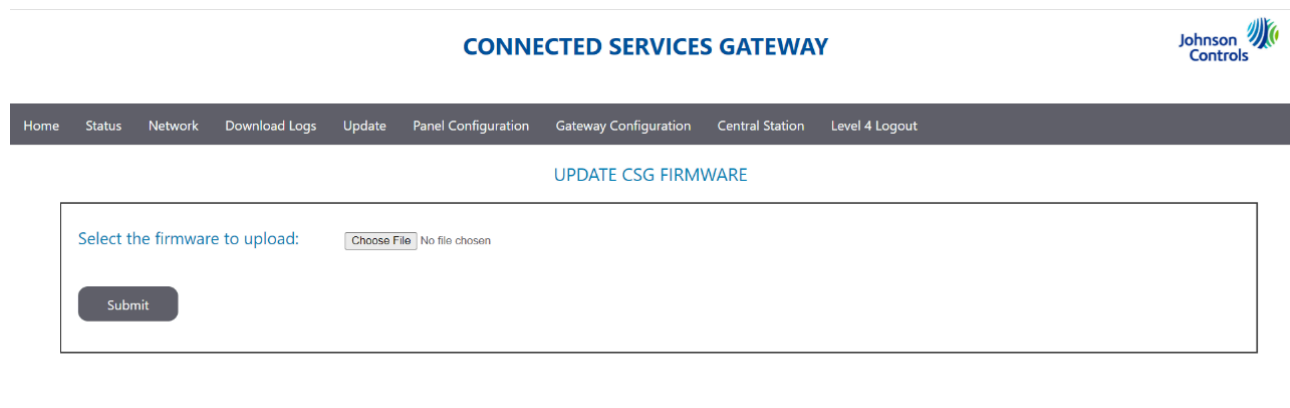
## Updating the firmware locally

### About this task:

You can update gateway firmware locally on the CSG card.

1. Connect the gateway Ethernet port Panel-P1-2 port to your PC using an Ethernet cable following the steps in [Configuring the CSG](#).
2. Open your browser and enter the URL `192.168.1.109` to load the gateway web page.
3. Click **Update**, see [Figure 13](#).
4. Your username and password are required to access the *Update Tab* pages:
  - Username: Admin
  - Password: 567891
5. Upload the gateway firmware build file, for example, file format `tycofpp-image-eucsg-xx-xxxx.tar.gz`.
6. After approximately five minutes the gateway updates and automatically restarts.

**Figure 13: Updating the firmware locally**



## Over-the-air updates

### About this task:

When the gateway firmware is available over the cloud and the gateway is live, you can update it with the latest released firmware over-the-air (OTA).

- ① **Note:** Perform a fire reset in the panel when the firmware is updated and the gateway restarts, so the gateway synchronises with the fire panel and updates the cloud as a serial connection in one-way communication, if the panel interface has a serial connection.

To apply OTA updates to the gateway:

1. Log on to SafeLINC Web Architect.
2. In the Devices view, select the gateway you want to update.
3. In the drop-down menu, select the firmware version to update, and click **Update**.



## Troubleshooting a blinking panel indicator

During installation, if the CSG panel indicator (LED8/LED7) starts blinking after you configure the CSG connection to the panel, there are configuration issues.

To recover the CSG into normal status follow these steps:

1. Open CSG local webserver with the procedure described in [Configuring the CSG](#).
2. Go to **Download Logs**.
3. Go to the **Factory Reset** section.
4. Click on **Clear Files**.
5. Restart the CSG.
6. When the restart is complete, reconfigure the CSG with all the input.

## Remote Gateway download

1. Go to your SafeLINC workspace dashboard.
2. Click on **Gateway Management**.
3. Select the required gateway.
4. Click on **Request Gateway Log**.
5. Wait for five minutes for the request to complete.