Shooter Detection Systems™

Gateway (GW) APPLICATION SOFTWARE R3.4.0

SDS INDOOR GUNSHOT DETECTION SYSTEM

Version R3.4.0 Dated 12/07/2023

300 NEWBURYPORT TURNPIKE | ROWLEY, MA 01969 | 1-844-SHOT911

Change / Rev	Date	Description of Change	Author	Pages Affected
3.4.0	15 Oct 23	Updates to match R3.4.0 GW Release	SHJ	All
3.1	15 Oct 21	Updates to match R3.1 GW Release	RaF / AJF	All
2.1	9 Feb 21	Updates to match R2.1 GW Release	FrB	All
2.0	23 May 19	Updates to match new R2.0 GW Release	RaF	All
1.8	20 Jun 18	Final updates for the R1.6.x GW Release	RaF	

Shooter Detection Systems, LLC
300 Newburyport Turnpike
Rowley, Massachusetts 01969
844-SHOT911
sales@shooterdetectionsystems.com
support@shooterdetectionsystems.com

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 Product Overview

1.1 Architecture

The SDS Indoor Gunshot Detection System features the world's finest acoustic and IR gunshot detection sensors and software. The System includes some number of DS Wired Power over Ethernet ("PoE") Gunshot Detection Sensor and/or SDS Wireless Gunshot Detection Sensor to provide full coverage of the space to be protected. Via a standard Local-Area-Network (LAN), the SDS Gunshot Detection sensors are connected to an SDS Gateway, which supplies the software applications needed to monitor and maintain the system and provide gunshot alert information to the customer. A representative SDS Indoor Gunshot Detection System is shown in Figure 1.

The **SDS Gateway (GW)** is an application to connect to the sensors and aggregate their information, making the data available to the Situational Awareness (SA) and many other applications and notification systems. The GW provides a management tool to configure and test the sensors, upgrade their embedded firmware, monitor their status, and show any detected issues. The GW is easily configured via sharing information with the SDS Situational Awareness (SA) application for system setup and maintenance. The GW supports multiple networks, one of which is intended to be on a "private" network with the SDS sensors while the other can be "public" providing access to the external applications.

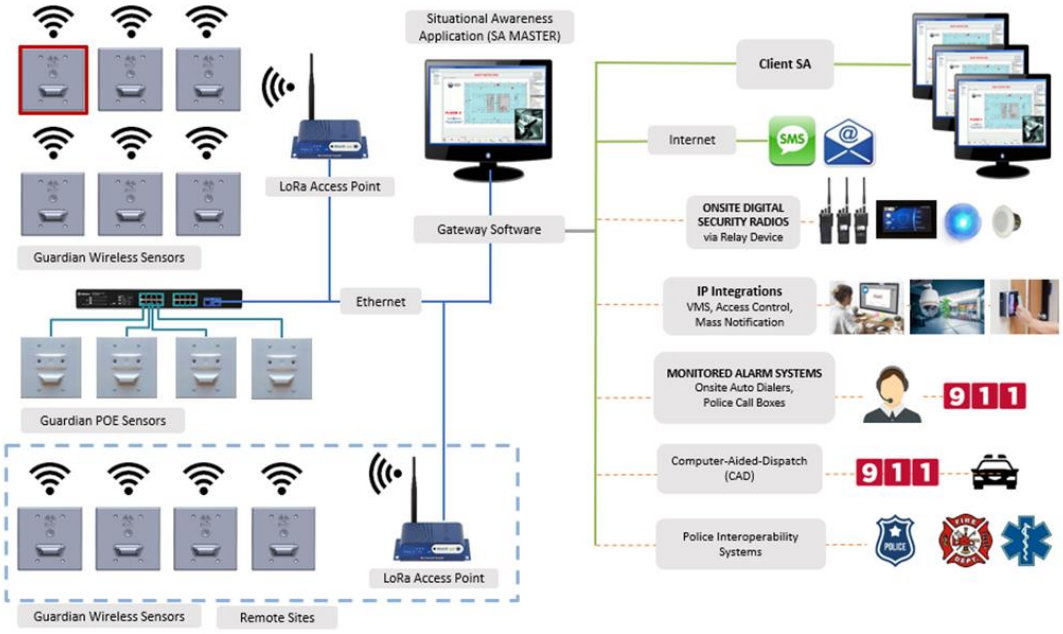


Figure 1 – SDS Indoor Gunshot Detection System Architecture

1.2 Features

The GW-Server typically provides the capability to manage and monitor low-level details of the SDS sensors. The GW Admin tool does not require a separate login and currently is, by design, limited to accessing the GW Server from the same machine. The admin can monitor the health of each sensor as well as external connections being made to the system from 3rd Party integrations. The GW has monitoring and management consoles for the SDS Wired Power over Ethernet ("PoE") Gunshot Detection Sensor (GRDN-200x wired sensors) and the SDS Wireless Gunshot Detection Sensor (GRDN-300x wireless sensors). The GW manages the sensor's mode of operation including normal operation and a test mode for maintenance activities. The GW also manages the FW upgrades and SSL Certificate management for the GRDN-200x sensors.

IMPORTANT: As of GW release R3.x when running with the SA R4.x the Sensor configuration information is **all** managed via the SA. Do not hand edit the "nodes.csv" file.

1.3 Application Note References

There are several application notes (App Note) associated with the SDS GW administration. These App Notes are referenced in this document as appropriate. The referenced App Notes are:

1. SDS Gateway License Request / SDS Gateway License Install
2. Configuring Gateway External Connections
3. Sensor Configuration File
4. SDS Sensor Tester
5. SDS Common Certificate
6. GW Advanced Settings

2 SDS Gateway Architecture

The GW application is typically installed, refer to Section 3, on a customer or dealer/partner provided machine (PC, Blade or VM). SDS does not resell server hardware.

The GW is only accessed by the system administrator. The GW acts as an access point for the sensors, connecting to each one and then providing other applications with a single interface to monitor and control (optional) the sensors. No applications other than the GW connects to the sensors.

Shown in Figure 2 below is the opening GW front page which provides a quick-look summary of the sensors as well as the number of connections to the system.

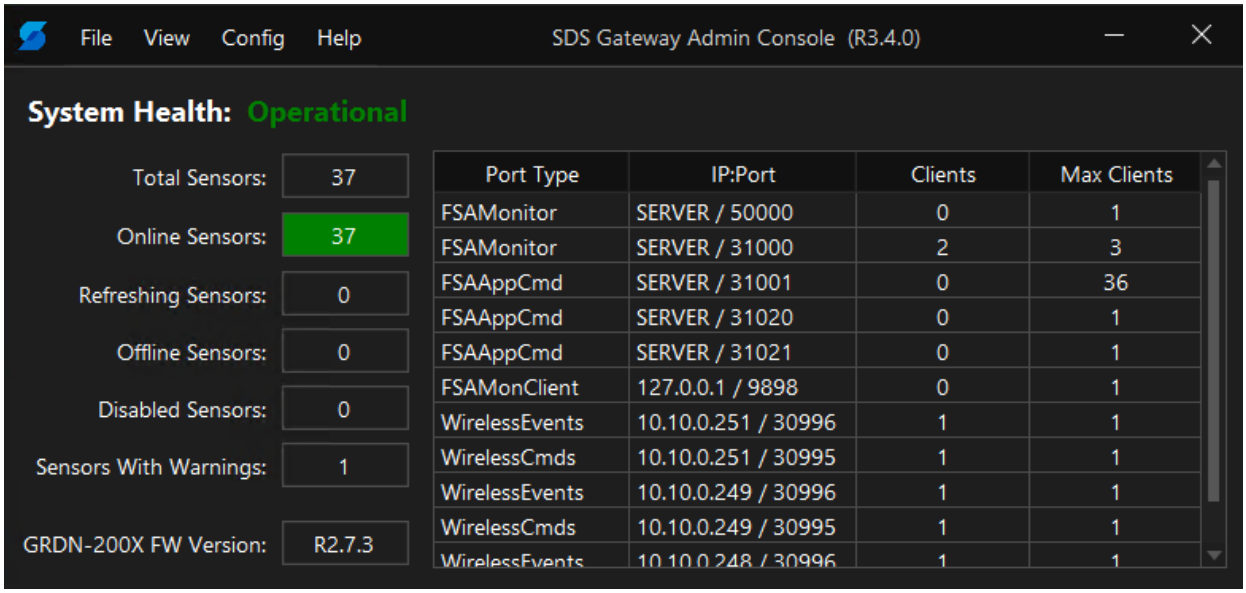


Figure 2 – Gateway System Status (Front Page)

3 Installing the GW Application

The GW Application installation file is named Installer_SDSGWServer_XXX.exe where XXX is the current version. To install GW, place the installation file on the desktop.

3.1 Welcome Screen

Once the installer is launched, the following welcome screen displays application name and options to continue or cancel.

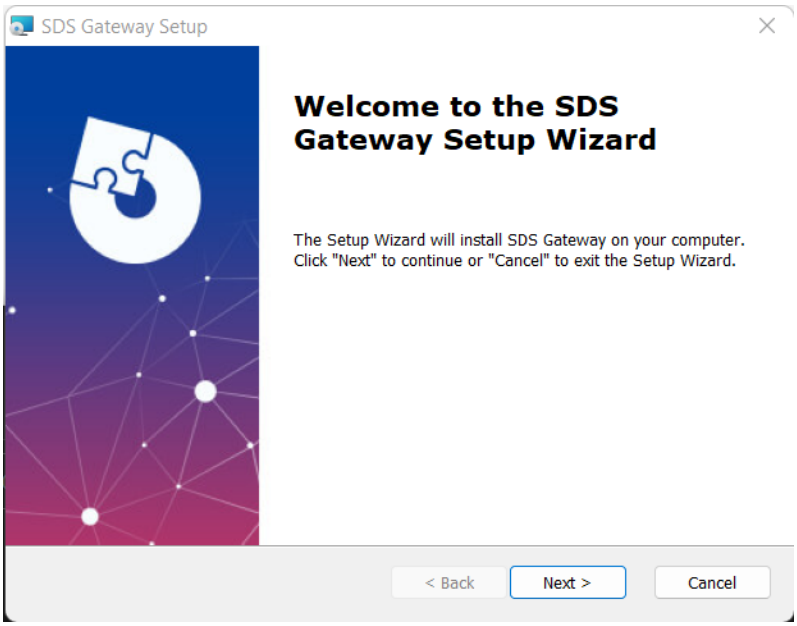


Figure 3 - Gateway Welcome Screen

Click on the “Next >” button to continue with the installation process.

3.2 End-User License Agreement

The GW Application will require you to accept the Shooter Detection Systems End-User License Agreement. As with any EULA please read and then select “I accept … Agreement”. Appendix IV is a copy of the EULA, Version 5.0.

Figure 4 - SDS EULA

Please click on the “Next >” button to continue with the installation.

3.3 Program Folder Installation Disk / Directory

During the installation of the GW Server, you will be prompted for a directory where you want to install the GW Program. Refer to the figure below. *If you are upgrading the GW Server then the location shown will be the previously selected directory, not the default location.* The default location is within **C:\Program Files\Shooter Detection Systems\SDS Gateway** and is the recommended location if you are using the “C” drive for program installations. Some organizations require all programs to be installed in a non “C” drive location and if this is the case then change the Destination Folder accordingly (e.g., D:\Programs\SDS\SDS_GW). Once selected this information will be stored in a Windows Environment variable for the system to access. Throughout this document we will refer to this program directory as ${SDS_ GW_PROG_DIR}.

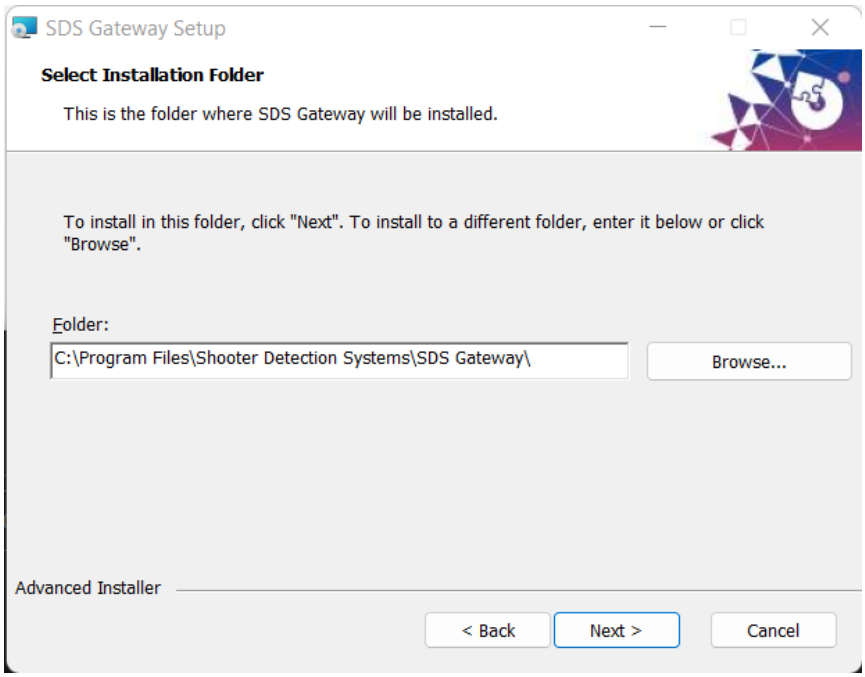


Figure 5 –GW Program Directory Selector

3.4 Data Folder Installation Disk / Directory

You will then be asked to specify a directory where the SDS Indoor Gunshot Detection System configuration files, templates, logs and other various data files will be kept.

NOTE: If you have already installed the SDS Gateway or Situational Awareness application then this directory is configured, and the GW will show as its default location. In this case DO NOT change the directory path.

If GW is the first application being installed, then you will see the dialog below. The default directory selection is **C:\SDSData** and is the recommended location if you are using the "C" drive for application data. Some organizations require all data to be maintained in a non "C" drive location and if this is the case then change the Destination Folder accordingly (e.g., D:\SDSData). Once selected this information will be stored in a Windows Environment variable for the SDS Indoor Gunshot Detection System to access. Throughout this document we will refer to this data directory as ${SDS_Data_Dir}. Select "Next" and the installer will install the GW Server and start that service as well as install the GW Admin console and add a launcher icon to the desktop. The final step in installing the GW Server / Admin console is to select Finish in the dialog shown in Figure 7.

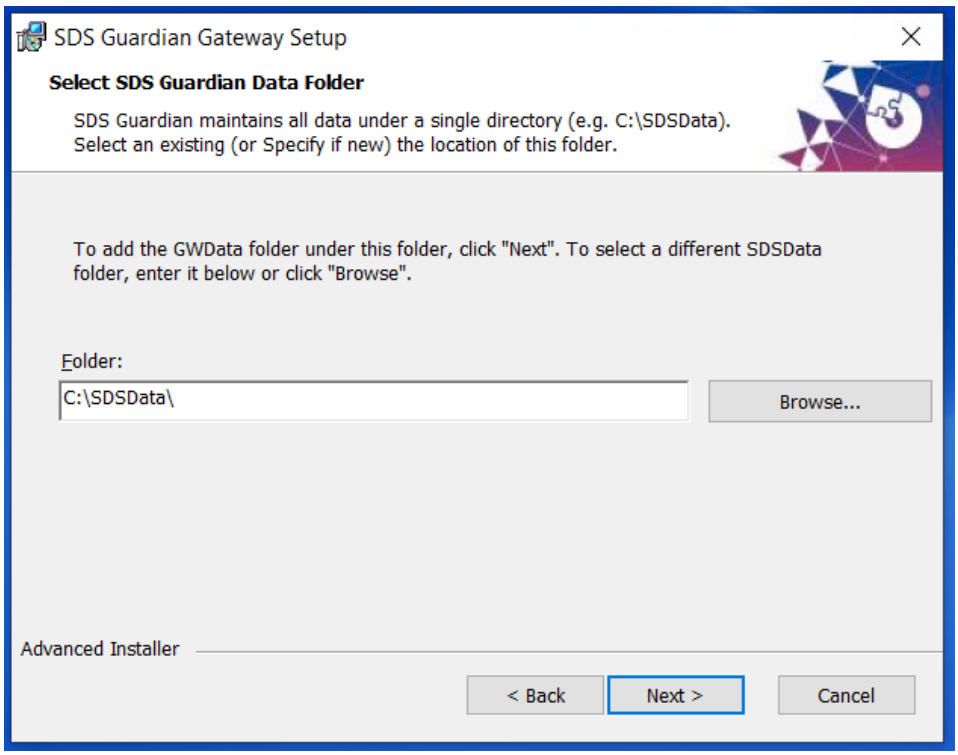


Figure 6 - GW Data Directory Selector

Figure 7 - GW Server / Admin Console Complete

3.5 Interacting with the SDS Gateway Admin GUI

At times when you need to interact with the Gateway UI you will need to launch SDS Gateway Admin GUI application. To do this simply double click on the GW Admin icon on the desktop. This will launch the GW-Admin console and give you access to licensing information, sensor information and various Server controls.

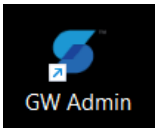


Figure 8 – GW Admin Icon

4 Licensing the SDS Indoor Gunshot Detection System

If this is the first time that the Gateway has been installed on a machine, then a 90-day trial license will be automatically initiated at the time of installation. During this trial period the system will operate normally with up to 400 sensors.

The license enables items such as the number of sensors, 3rd party integrations, and time-period (typically updated annually, but can be purchased for an extended period).

The GW will monitor the license and when issues (over-use) of a resource or when the system is nearing the end of the license the GW will report these issues via the Admin console and through the SDS SA and 3rd party integrations. The GW implements a License Request, Status and Install New set of licensing screens as described in the following sub-sections.

4.1 Licensing the GW Application

The Gateway requires a license which must be installed allowing it to operate for the duration of the license.

4.1.1 Generating a License Request

To obtain the initial license from SDS you must generate a License Request for each server machine. Refer to the SDS APP Note – **SDS GW License Request** for details on generating and sending the request to the Licensing Group at SDS.

4.1.2 Applying a new License

Once issued, the license will be emailed to the POCs on the license request. The final step is to install the license within the GW application. Refer to the instructions that are emailed along with the license file to apply it to your server.

4.1.3 License Status

The status of the license information can be shown (in detail) using the GW GUI. Select File → License → Status will show a view identifying License Contact / Computer information, maximum counts for sensors and interfaces as well as all integrations which are licensed for use. At the bottom of the screen, you will see the Expiration date and time remaining on the license. Refer to the following Figure.

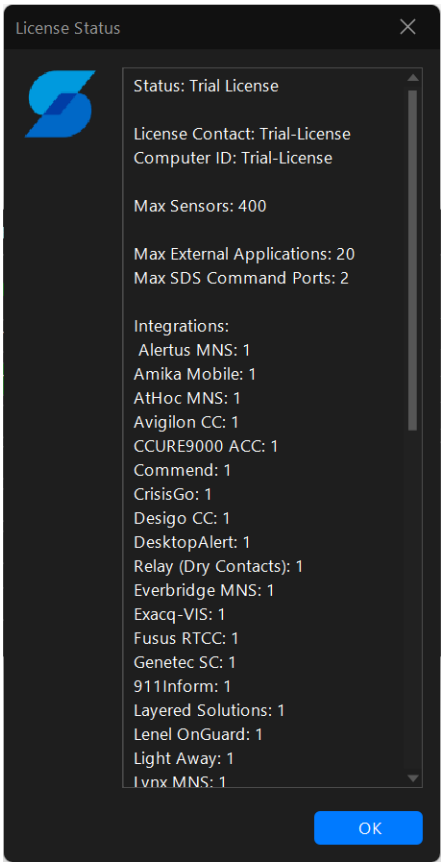


Figure 9 – License Status (Details)

4.1.4 License Alerts

The GW GUI will automatically show a License Alert (if running at the time of the alert) should any of the license values be exceeded. You can also access this view via File → License → Show License Alerts.

The licensing includes a License Period, Sensor Config (maximum number of sensors configured), FSAMonitor / FSACommand / SDSCommand (maximum number of connections supported on each of these interface types). An example of a fully licensed system is shown in the next Figure.

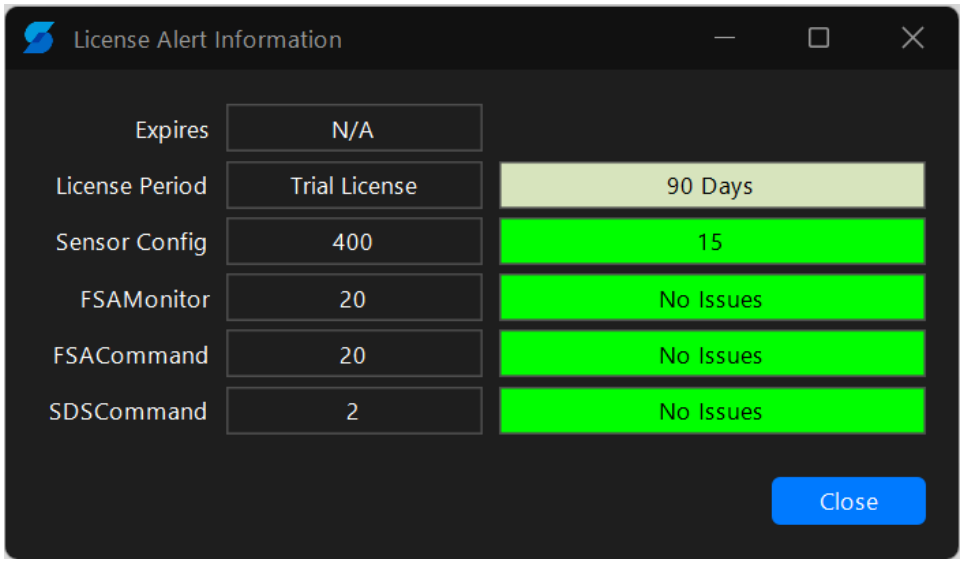


Figure 10 – License Alerts

4.2 Gateway Server (Service) Management

The Gateway Server is launched as a Windows Service. The service is shown as **SDS Gateway Server** and the actual service name (if working from the command line Windows Service tools) is SDS_GATEWAY_SERVER. The service is configured to automatically start when the server is powered on.

Within the Admin console, under the "File" menu option you have options to Stop, Start/Restart and Refresh the GW Service:

- File → GW Server Stop: Stops the Gateway Server service and leaves it not running. **NOTE:** This simply stops the service, it does not disable it and as such if the server machine is rebooted the GW Server service will automatically restart.
- File → GW Server Restart: Stops (if it is currently running) the Gateway Server service and then Starts the service. This causes the GW Server to re-read all of it settings and configuration files. It also causes all interfaces to disconnect and then reconnect after the restart.
- File → GW Server Refresh: This option does NOT stop/restart the GW Server service but rather causes it to re-read (refresh) its Sensor information (not the gateway.csv file). This can be useful if there is an issue after a sensor Add/Mod/Del was made and did not properly reflect the update in the GW.

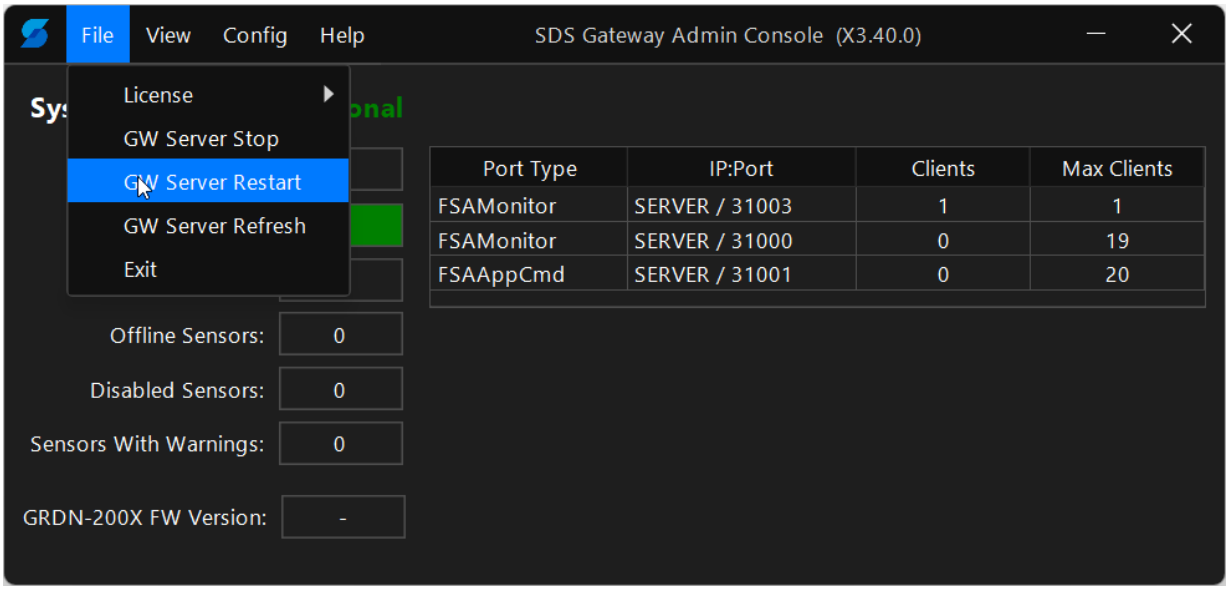


Figure 11 – SDS GW, GW Stop, Restart and Refresh

5 Gateway Interface Configuration (gateway.csv)

The GW server communicates with wireless (LoRa) access points and software platforms to integrate SDS sensors events and 3rd party applications. The configuration of these connections is managed via a configuration file (gateway.csv). The default file that is loaded during installation defines a set of connections which will meet many customer's needs.

To configure additional external connections, the configuration file can include additional TCP server ports where the GW will support connections from other applications such as the SA and many 3rd party products. The GW can also be configured to act as a TCP Client to connect out to other 3rd party products. Finally, when operating with the GRDN-300x wireless sensors the GW will be configured to connect to one or more LoRa Access points to enable the sensor information to be uplinked to the GW Server. All this configuration information is provided via the configuration file gateway.csv.

Refer to the SDS application note **SDS App Note – Configuring Gateway External Connections** for details on adding the LoRa Access Points and other integration connections which are required for this installation.

6 Sensor Configuration

The recent releases of the GW (R3.x) and the SA (R4.x) have significantly changed the method of managing the sensor configuration information. Historically the information was managed via the GW and an associated configuration file (nodes.csv). The recent releases have moved the Sensor information to the SA Database and now all sensor information is managed directly in the SDS SA. The SA then makes the information available to the GW. The sensor configuration information includes device serial numbers, IP addresses (when applicable), physical location, network location and can include information for the SDS Relay Connector and Site / Geo-Location information for each sensor.

6.1 Sensor Management (via the SA)

If the SDS server is deployed with SA Release R4.x (or newer) the sensors will be managed ONLY in the SA. Refer to the SA Admin Guide, Section 5.7 and the SDS App Note - Sensor Configuration File.

NOTE: Please use SDS Situational Awareness application to add or remove a sensor. This functionality has been removed from GW application in favor of SA application.

6.2 Sensor Management (via the GW)

If the SDS server is deploying without the SDS SA (not a likely scenario) the sensors must be managed in the GW and by directly editing the sensor configuration file. Refer to Appendix I – Sensor Management via the GW / nodes.csv file.

7 GW Admin Operations

The GW is a useful administrative tool and provides a system level summary of the sensors and application connection status. Additionally, the tool provides several detailed "views" of the sensor information. The GW supports the following functions described in detail in the following sections:

System Status

Front page of the GW, shown when the GW launches, provides a system level view of the sensor status, connection status and other information.

- System Health: System health information is shown on the top of the GW Admin Consoles. There are several states that depict the health of the system
    - **Operational:** SDS Indoor Gunshot Detection is healthy and online. There are no problems reported
    - **Degraded – Sensors Offline:** Some number of sensors are Offline
    - **Offline - All Sensors Offline:** All SDS sensors are currently not communicating with the GW.
    - **GW Server – Not Connected:** GW Server Windows service has been either stopped or failed to start
    - **GW Server - LICENSE EXPIRED:** Gateway Server License has expired and needs to be renewed

Information Views (Front screen and View menu)

- **Sensors:** Table view of the Sensors information.
- **Sensor Maintenance Issues:** Table view showing Sensors that are currently reporting an issue or are not connected.
- **Sensor Discovery Issues:** Table showing Sensors (DHCP) that are reporting their information to the GW but are not included in the nodes.csv file. *Typically represents a configuration issue/error.*

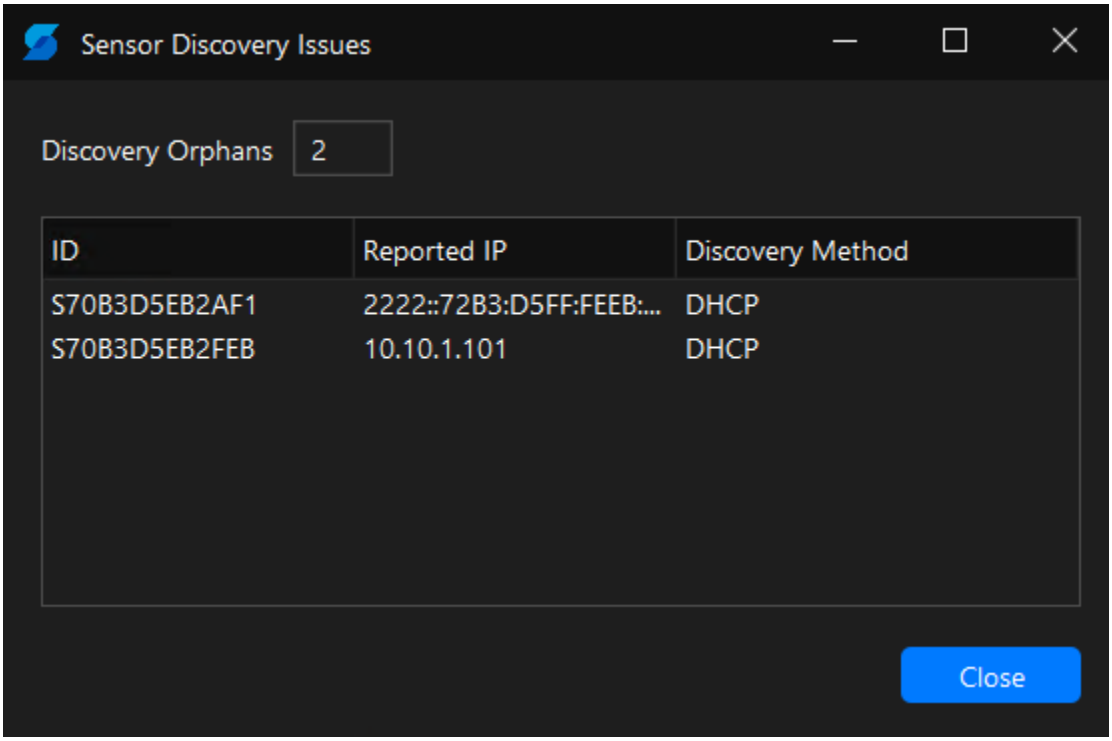


Figure 12 – System Status (Front Page)

- **External Connections:** Table view showing the status of external connections. This view is tightly coupled to the gateway.csv configuration file.

Configuration Tools (Config menu)

- **Handheld Tester Controls:** Management screen used to enable test modes for the sensors during maintenance installation and maintenance testing.
- **Sensor Firmware Upgrade:** Management and status view used when upgrading the sensor firmware.
- **Gateway Certificates:** Management and status view used when updating the gateway SSL certificate.
- **Common Sensor Certificates:** Management screen used to update SSL and 802.1x certificates for the sensors on the system.
- **Advanced Settings:** Management dialog enabling the admin to adjust advanced settings within the GW Server.

7.1 System Status (Front Page)

The GW application's front page provides system level information regarding the sensors, sensor firmware version, GW Site-ID and application connections. Depending on your configuration you may not see all these fields (e.g., Site-ID). Refer to the examples below for a running system.

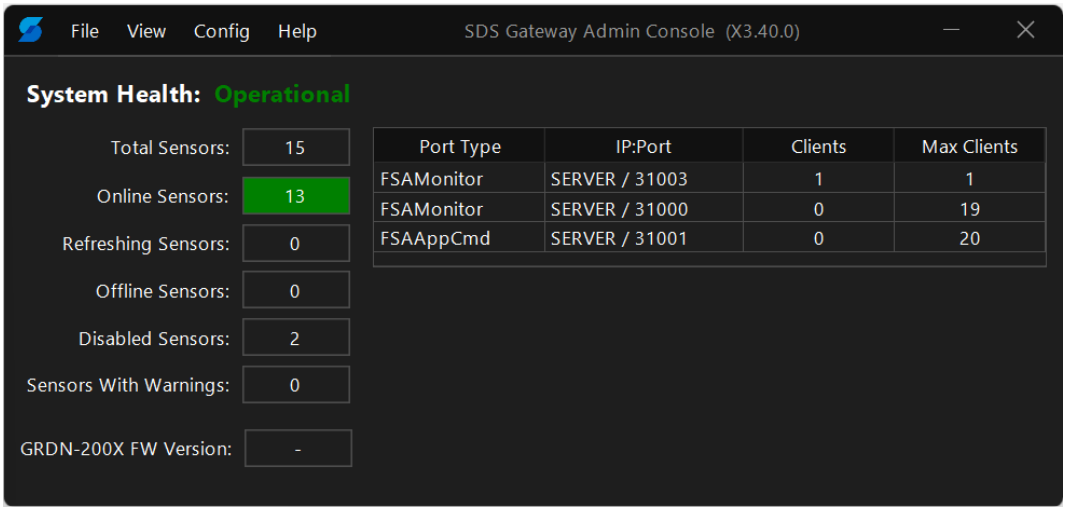


Figure 13 – System Status (Front Page)

The sensor information provided is:

- **GW SW Version** – shown in the Title bar. In this example the version is X3.40.0
- **Total Sensors** – number of sensors in the current configuration. This is the number of sensors the application expects to be connected based on the SA/GW Sensor Config List,
- **Online Sensors** – number of sensors currently online (communicating with the GW).
- **Refreshing Sensors** – Wireless sensors can take up to 10 minutes to report to the GW (battery life) and rather than consider these sensors Offline … the GUI will show them as "Refreshing" for the first 10-15 minutes following a GW Server restart. *This line will **only** be shown when there are Wireless sensors registered, and then only for the initial 15-minute period after a GW restart.*
- **Offline Sensors** – number of sensors currently not communicating with the GW.
- **Disabled Sensors** – number of sensors disabled through SA.
- **Sensors with Warnings** – number of sensors currently reporting some form of issue (built-in-test, environment or other).
- **Gen-2 (GRDN-2xxx) FW** – Shows the version of sensor FW currently available on the GW. This FW version will be downloaded to all sensors on the system to keep them up to date. **NOTE:** This line will **only** be shown if the administrator has loaded a FW Kit onto the GW, refer to Sensor Upgrade later in the document.
- **GW Site-ID** –Shows the Site-ID assigned to this GW. This Site-ID is assigned to all sensors on this GW and becomes part of their meta-data reported to external integrations. It is typically **required** for Computer Aided Dispatch (CAD) type integrations such as Central Square.

NOTE: This line will **only** be shown if the administrator has assigned a GW Site-ID in the GW Properties File.

The status of application connections (shown as "External Connections") is:

- **External Connections**
  - TCP server ports are shown with their configuration information as well as the number of clients that are currently connected.
  - *The FSAMonitor port should show one connect for the SA Server and one for each integration interface (e.g. SDS Relay Connector (RC) application.*
  - The **Max Clients** number is configured by the SDS license.
  - TCP Clients (FSAMonClient) are shown with the 3rd party systems IP address:port as well as the maximum number of connections that will be made and the current number of connections (Clients).
  - WirelessEvents and WirelessCmds will indicate the connection to a LoRa Access Point.
    NOTE: The IP address will match the IP address as indicated in the gateway.csv file.

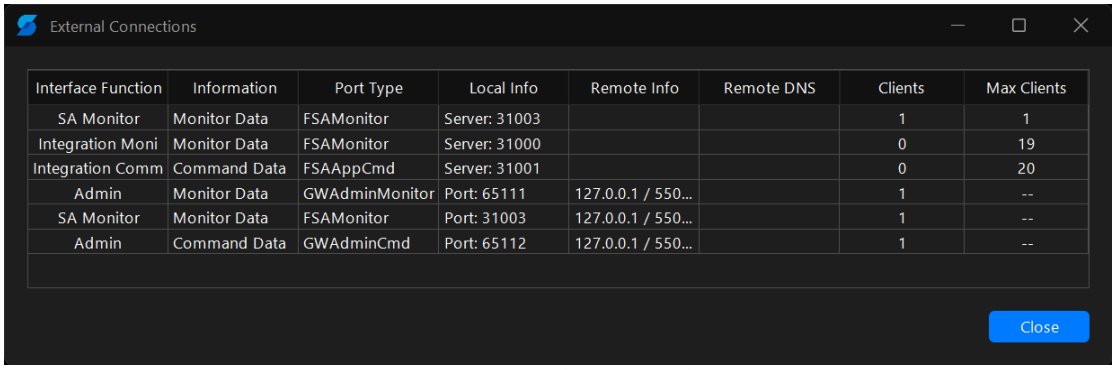


Figure 14 – System Status (Front Page)

7.1.1 Wireless Sensor Refresh

Following a GW Server start/restart - this can be done by selecting "File → GW Server Restart" the GW will reconnect to the various sensors. At this point the Wireless (GRDN-300x) sensors may take up to 10 minutes to send a status message to the GW. During this initial period the GW will show these sensors as "Refreshing Sensors". Once the GW receives a Heartbeat from the sensor it will change from refreshing to online.

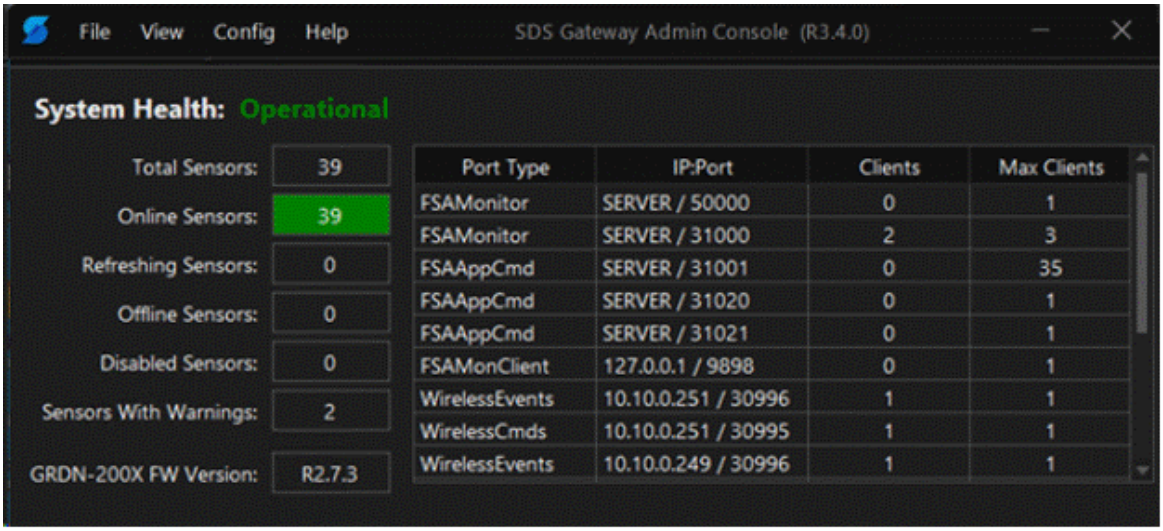


Figure 15 - System Status with Refreshing Sensors

The Wireless (300x) Statistics View which is detailed in a later section, will show any remaining refreshing sensors in gray with “Refreshing” in the “Status w/Details” column.

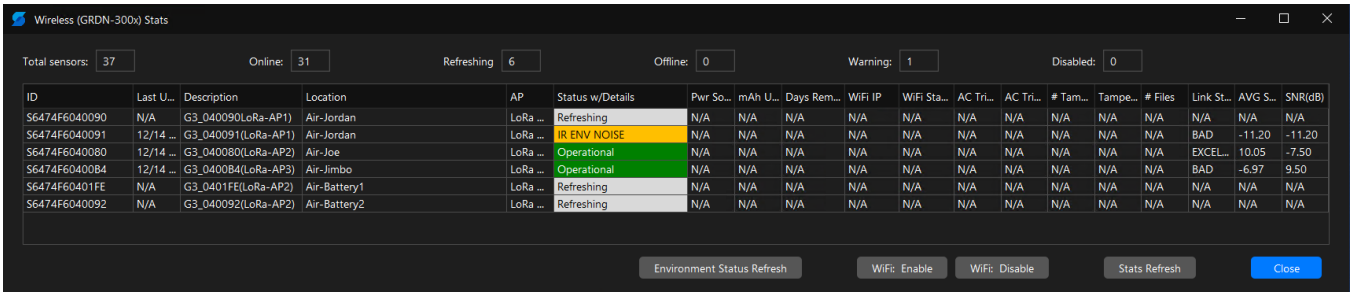


Figure 16 - Wireless (300x) Statistics with Refreshing Sensors

7.2 View Menus

The View menu contains several table views of the SDS Sensors, their configuration information, and their current operational status. Additional views show information about the external connections and their status.

7.2.1 Sensor Information View

By selecting "**View → Sensors"** a window will be displayed showing information about the sensors and the location information in the nodes.csv file.

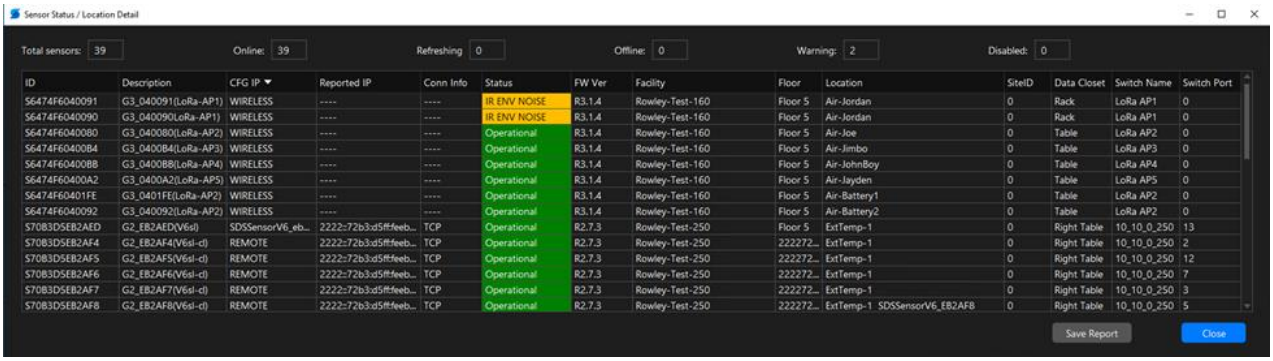


Figure 17 – Sensor Location View

The summary information provided is the same as on the front page. The table, like all GW table views, is color coded:

- **Green** – online and no issues/warnings. *This is also indicated by the Warning Info column containing no entry.*
- **Orange** – online but reporting a warning. Throughout the SDS documentation this is referred to a "Degraded" operation. *Additional warning information is displayed in the status column.*
- **Red** – offline and not communicating with the GW. *Displayed as OFFLINE in the status column.*
- **Gray** – GW Server has been restarted and sensor is refreshing, refer to previous section for more information.

The table columns are:

- **ID** – Sensor serial number
- **Description** – Sensor names, such as "S1"
- **CFG IP** – IP address.

  NOTE: SDS Wireless Sensors will be entered as "LORA" and show as "WIRELESS" in the Sensor View window.
- **Reported IP** – contains the reported IP address of a sensor. In the case of DHCP sensors, DNS configuration and some other cases the ReportedIP will not match the CFGIP but will be the correct IP address to reach the sensors.
- **Conn Info –** TLS-CT1, TLS-CT2 depending on which cert the DS Wired Power over Ethernet ("PoE") Gunshot Detection Sensor is using. For all SDS Wireless Gunshot Detection Sensors, it will show ---- since wireless sensors do not use TLS certificates. TCP for nonsecure connections.
- **Status** – contains an entry if the sensor is currently reporting an issue (Environmental, HW/SW) or is OFFLINE. The Warning information and recommended actions are defined in

- Appendix II – Sensor & License Warning Codes.
  NOTE: The Status of a sensor with a Warning will also be highlighted in Orange or Red as shown.'
    - **Operational**: Sensor is fully online and operational
    - **DISABLED**: Sensor is disabled
    - **OFFLINE:** Sensor is currently not communicating with the system
- **FW Ver** – the FW version currently running on each sensor.
- **Facility / Floor / Location / SiteID / Data Closet / Switch Name / Switch Port** – refer to the Sensor Configuration file for more details.

Window provides a way to save displayed report for archiving or future analysis.

Save Report – Creates an output report (CSV format) containing all the SDS Sensors, their configuration information and current operational status. This report can be opened in Excel or processed through a script to obtain system information and customer reports as required.

7.2.2 Sensor Maintenance Issues View

By selecting "**View → Sensor Maintenance Issues"** a window opens showing only sensors that are currently reporting an issue (degraded performance or OFFLINE). This view is useful when working with a large system and trying to find one or a few degraded sensors.

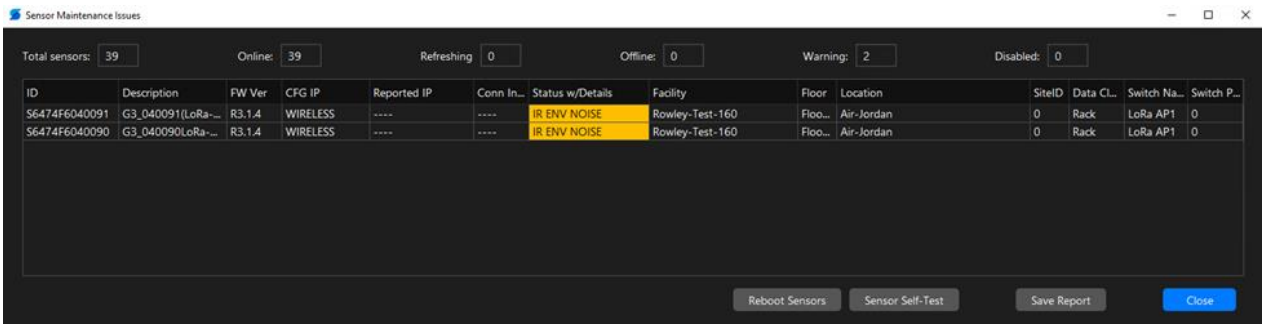


Figure 18 – Sensor Maintenance Issues

The format and buttons associated with this view are all the same as described in the prior section.

- Reboot Sensors This button will Reboot every sensor that is ONLINE (reachable). *The Admin will receive a confirmation/instruction dialog prior to sending the command.*

- Sensor Self-Test This button will send a command to all of the sensors to have them run their Self-Test (includes IR & Acoustic signal tests). *The Admin will receive a confirmation/instruction dialog prior to sending the command.*

Save Report – Creates an output report (CSV format) containing all the SDS Sensors and their maintenance issues. This report can be opened in Excel or processed through a script to obtain system information and customer reports as required.

7.2.3 Wireless (300x) Statistics View

By selecting "**View → Wireless (300x) Statistics"** a window opens showing only the SDS Wireless sensors in the sensors database. This view is useful to view the operating statistics of any SDS Wireless sensors in the system.

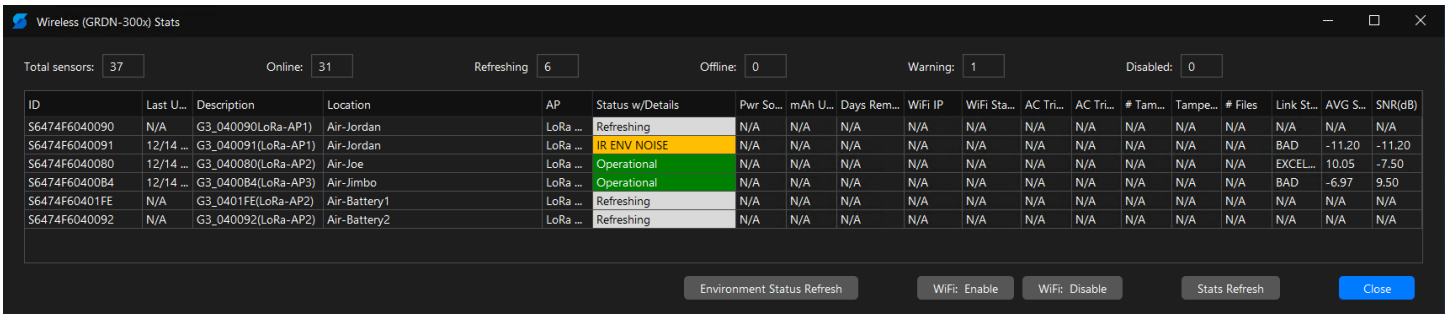


Figure 19 - Wireless (GRDN-300x) Stats

The table columns are:

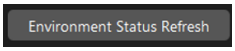
- **ID –** Sensor serial number.
- **Last Update** – Contains the time that the gateway last received a heartbeat from the sensor. **NOTE:** The SDS Wireless sensors send a Heartbeat every 10 minutes.
- **Description / Location** – Sensor Configuration "Description" and "Location"
- **AP –** Name of the LoRa AP connecting the sensor to the GW. Name comes from gateway.csv configuration file.
- **Status w/ Details** – Contains any warning information such as tamper, improper mounting orientation, temperature, noise, i.e.
- **Pwr Source** – Indicates if the sensor is powered by BAT (Battery) or EXT (External DC Supply)
- **mAh Used / Days Remaining (est)** – When powered by battery, the energy consumption and estimated remaining battery life will be shown here.
- **WiFi IP** – Contains the DHCP or static IP configuration for the sensor's WiFi IP address
- **WiFi Status** – Indicates if the sensor's WiFi is Disabled, On Network, TCP Active, or Enabled but Not Connected.
- **AC Triggers / AC Trig(24hr)** – Contains the total number of acoustic triggers and the number of acoustic triggers in the last 24hrs
- **# Tamper / Tamper(24hr)** – Contains the total number of tampers and the number of tampers in the last 24hrs.

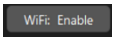
- **# Files** – Contains the total number of shot files on the sensor.

  NOTE: The max number of files a SDS Wireless can save is 50.
- **Link Status** – Contains the LoRa connection quality. Values:
  - **EXCELLENT** – Link has very strong signal strength (many bars).
  - **GOOD** – Link has good strength and should operate well.
  - **FAIR** – Link is ok but may not be reliable/robust over time. Consider moving the LoRa AP if possible.
  - **BAD** – Link is marginal and will not be reliable/robust over time. Consider moving the LoRa AP if possible.
- **AVG SNR(dB) / SNR(dB)** – Contains the most recent LoRa heartbeat signal strength as well as the average of the last 10 received messages.

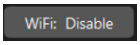
  NOTE: The average is used to indicate the Link Status above.

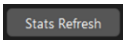
The buttons associated with this view are described below.

- 

- This button will refresh the sensor statuses by performing a quick analysis of the sensor's environment to ensure there is no external IR Source interfering with the sensor.
- 

– This button will send a WiFi Enable command to all of the sensors the next time they send a heartbeat.

  NOTE: The sensor's WiFi will be enabled for 30 minutes, and the enable will typically start within 10 minutes after the button is pressed. There are two warning dialogues that will pop up after pressing the button to warn about the decreased battery life during WiFi operation.
- 

– This button will send a WiFi Disable command to all of the sensors to disable their WiFi.
- 

– This button will send a Stats Refresh command to all of the sensors the next time they send a heartbeat. This will cause the sensors to update all of the columns in the Stats view.

  NOTE: Doing a Stats Refresh affects the sensor's battery life as it requires many LoRa messages to update the statistics. Statistics refresh over time with each heartbeat otherwise.

7.2.4 Wireless (300x) Versions View

By selecting "**View → Wireless (300x) Versions"** a window opens showing only the SDS Wireless sensors in the nodes.csv. This view is useful to view the software versions of any SDS Wireless sensors in the system.

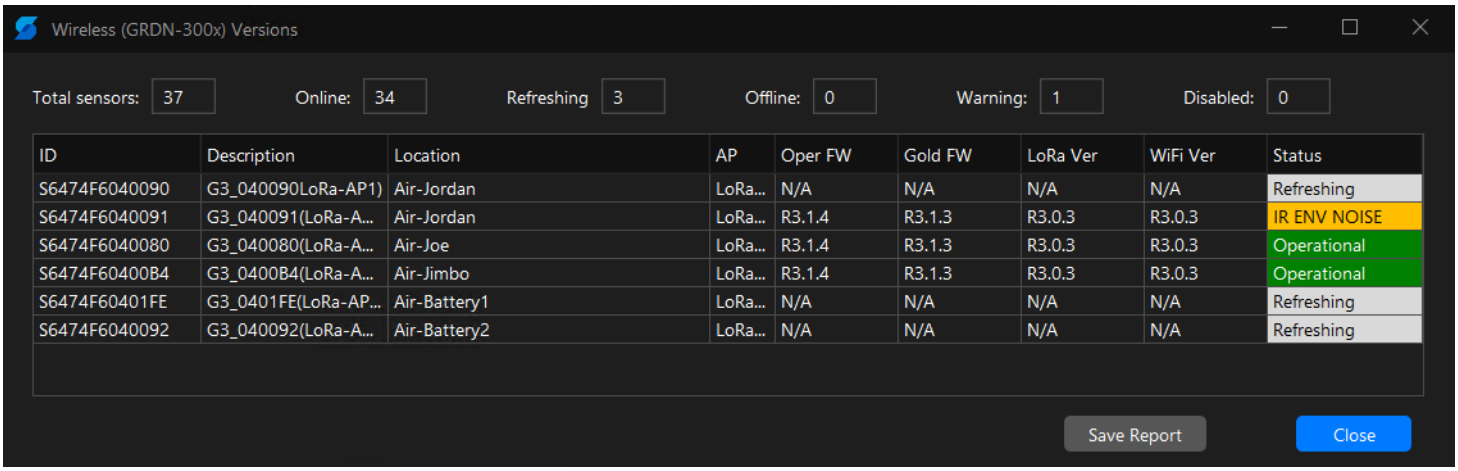
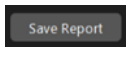


Figure 20 - Wireless (GRDN-300x) Versions

The table columns are:

- **ID –** Sensor serial number
- **Description / Location** – Sensor "Description" and "Location".
- **AP –** Name of the LoRa AP connecting the sensor to the GW. Name comes from gateway.csv configuration file.
- **Oper FW** – Contains the Operational Firmware version currently running on the sensor.
- **Gold FW** – Contains the Golden Firmware version on the sensor.
- **LoRa Ver** – Contains the LoRa Firmware version currently running on the sensor's LoRa module.
- **WiFi Ver** – Contains the WiFi Firmware version currently running on the sensor's WiFi module.
- **Status** – Contains any warning information such as tamper, improper mounting orientation, temperature, noise, i.e.

Window provides a way to save displayed report for archiving or future analysis.



– Creates an output report (CSV format) containing all the SDS Sensors and their information. This report can be opened in Excel or processed through a script to obtain system information and customer reports as required.

7.2.5 Sensors Discovery Issues View

There are several discovery methods which involve the sensors connecting into the GW (versus having the GW connect to the sensor). In the case of a DHCP sensor and the Wireless sensor the GW will receive heartbeats from the devices and if there is a configuration issue (they are not in the sensor list the GW is expecting) the issue is reported in this view.

Each issue (sensor not in configuration) will be shown along with IP information and the Discovery method – DHCP or LoRa.

At this point, to resolve each issue review the Sensor Configuration information to determine if there is a mistake in the Sensor IDs and correct the issue within the SA so that the system is up to date.

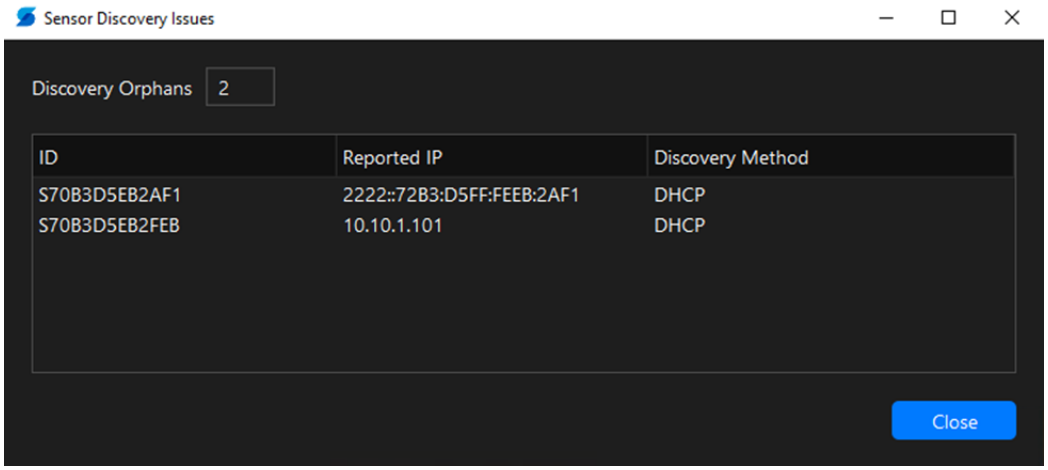


Figure 21 - Sensor Discovery Issues

7.2.6 External Connections View

This view shows the external connection information for the GW including available Server Ports, Clients and number of current connections. Additionally, each external connection is listed along with the IP information of the application connected to the GW. If the Admin has configured different ports / servers for the integrations this table will clearly identify the connections and status of the various integrations.

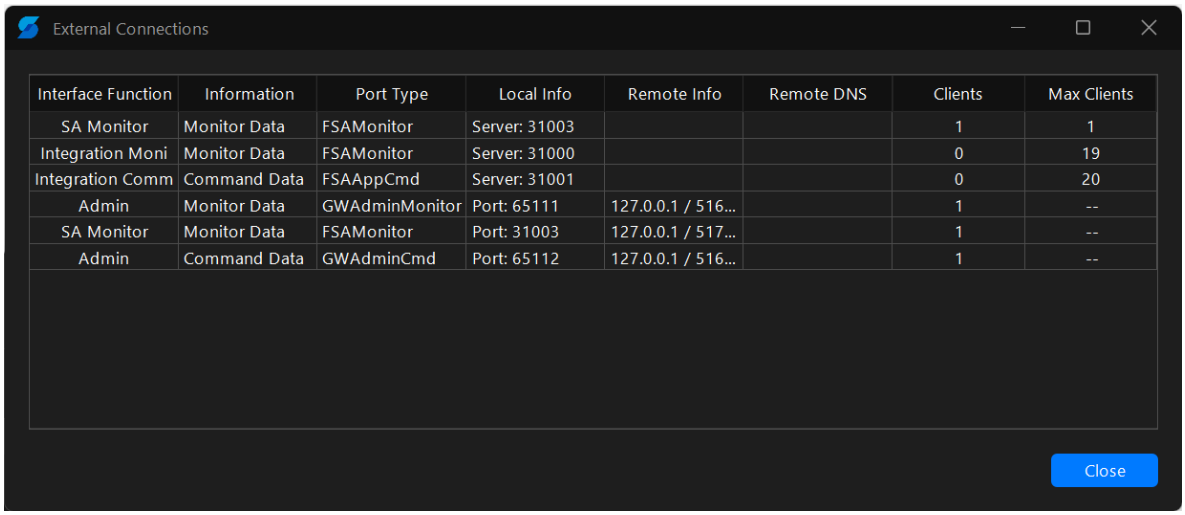


Figure 22 - External Connections Status

The columns are:

- **Interface Function** – Shows the "Label" information from the gateway.csv file.
- **Information** – Shows the type of information communicated on the interface:
  - "Monitor Data" → Sensor Event and Status information
  - "Command Data" → Command interface
- **Port Type** – Shows the type of information and level of privilege on the interface:
  - "FSAMonitor" → (Server) Sensor Event and Status information (integrations)
  - "FSAMonClient" → (Client) Sensor Event and Status information (integrations)
  - "FSAAppCmd" → Command interface (limited to sensor metadata)
  - "SDSCmd" → Command interface (extended privilege, SDS functionality)
  - "GWAdminCmd" → Command interface (extended privilege, GW Admin GUI)
  - "GWAdminMonitor" → Sensor and GW information (GW Admin GUI)
  - "WirelessEvents" → SDS Wireless Sensor Information (GW Admin GUI)
  - "WirelessCmds" → SDS Wireless Command Interface (GW Admin GUI)
- **Local Info** – Shows the IP information at the GW application
- **Remote Info** – Shows the IP information for the integration/device connecting to the GW
- **Remote DNS** – Shows and DNS (IP naming) information available for the integration/device connecting to the GW.
- **Clients** – Current number of clients connected on this interface.
- **Max Clients** – Maximum licensed clients that can be connected on this interface.

7.3 Config Menu

The Config Menu includes a window to support the testing of SDS Sensors as well as the upgrading of FW on the sensors. Additionally, an Advanced Settings page is available to configure controls on the GW Server itself.

7.3.1 Handheld Tester Controls

The SDS Sensors can be tested using the SDS Tester (**PN:GRDN-TSTR-2000**). It is **REQUIRED** to perform this test as part of the installation process and then periodically as part of ongoing maintenance.

The SDS Sensor Handheld Maintenance Tester dialog is shown in Figure 23. This dialog allows you to enable and disable the test mode, set a test period and select which sensors are involved in the testing.

Details regarding the entire Test procedure including planning, notifying, testing and after test reports are covered in the **SDS App Note: Sensor Testing.**

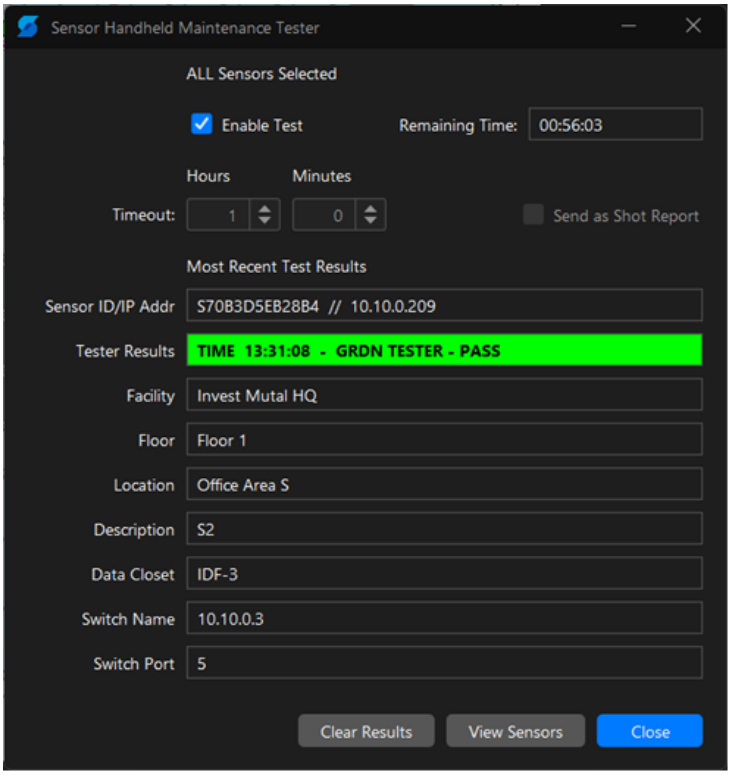


Figure 23 – Sensor Handheld Maintenenance Tester Configuration

7.3.2 SDS (GRDN-200x) Sensor Firmware Upgrade Information

The firmware in the SDS sensors may be updated periodically. These updates should be applied to all sensors during the installation process, under administrator control, and again when they are made available.

The GW provides an automated mechanism to be certain that the latest version of firmware is running on all the sensors. The upgrade process is managed via the **"Sensor Upgrade Information"** screen which is accessed via "**Config → Sensor Firmware"** and is shown in the figure below.

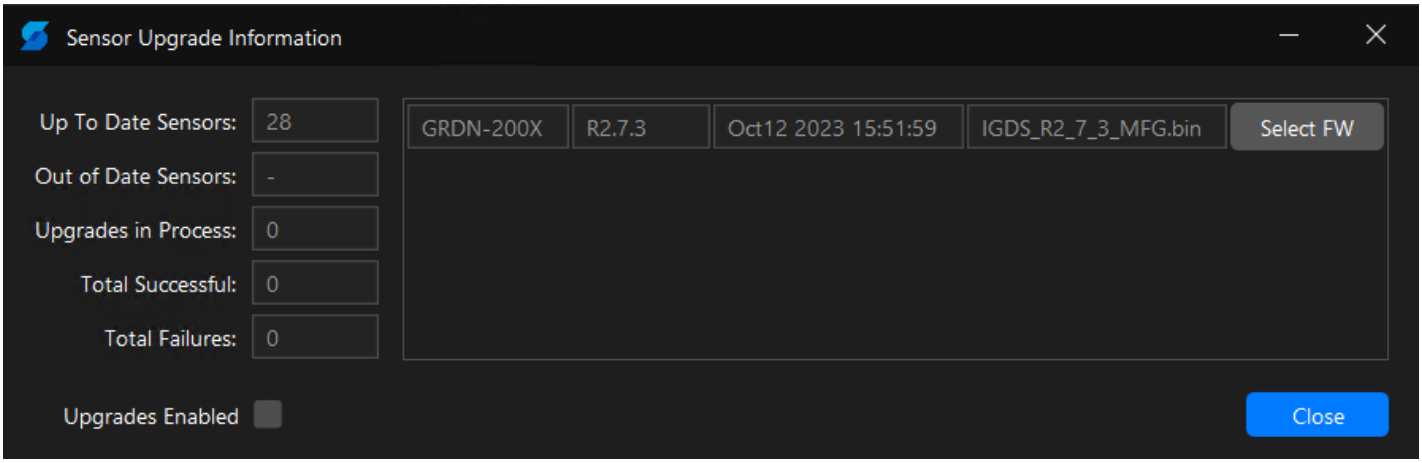


Figure 24 - Sensor Firmware Upgrade View

7.3.2.1 Sensor Firmware Upgrade Process

The procedure for the upgrade is initiated by the system administrator and then automated and managed by the GW. The administrator is provided feedback throughout the process via the upgrade information screen.

The upgrade procedure is as follows:

1. SDS will provide, via e-mail and web, information regarding the new firmware version. This will include information on any performance improvements and on any impact to system security or other issues. The firmware will be posted on a restricted access file share site for system administrators to download. A firmware kit will be named GRDN-2_XX_X_X_X_FWKIT.zip where the "Xs" are the version code.

2. System administrator will download the firmware kit. This kit is a single ZIP file containing the encrypted firmware image and firmware revision information.

3. During the upgrade process the individual sensors will be "offline" for a short period of time to reboot and reload their firmware. This will result in maintenance notifications being sent out. The administrator has several options in this regard:
    - Easiest – Inform users on the maintenance notification list to ignore notification(s) during the upgrade period.
    - If the SDS Indoor Gunshot Detection System is a standalone installation, then the SA users can be informed, and the SA Server can be closed during the upgrade period (via Windows Start Menu). This will prevent email/SMS notifications from being generated.
    - If the SDS Indoor Gunshot Detection System is monitored by external systems (e.g. 3rd Party SA, Center Station Security Monitor) notify them of the maintenance actions.

4. Using the GW application's **"Sensor Upgrade Information"** screen the administrator will, at a convenient maintenance time load, the kit into the GW. "Upgrades Enabled" toggle button can be used to initiate the actual upgrade process.

5. Loading a FW Kit – SDS sensor FW is provided as a ZIP file containing an encrypted binary file and other information. To load the FW Kit onto the GW, select "Select FW" and in the file open browser that is shown, select the FW kit provided by SDS.

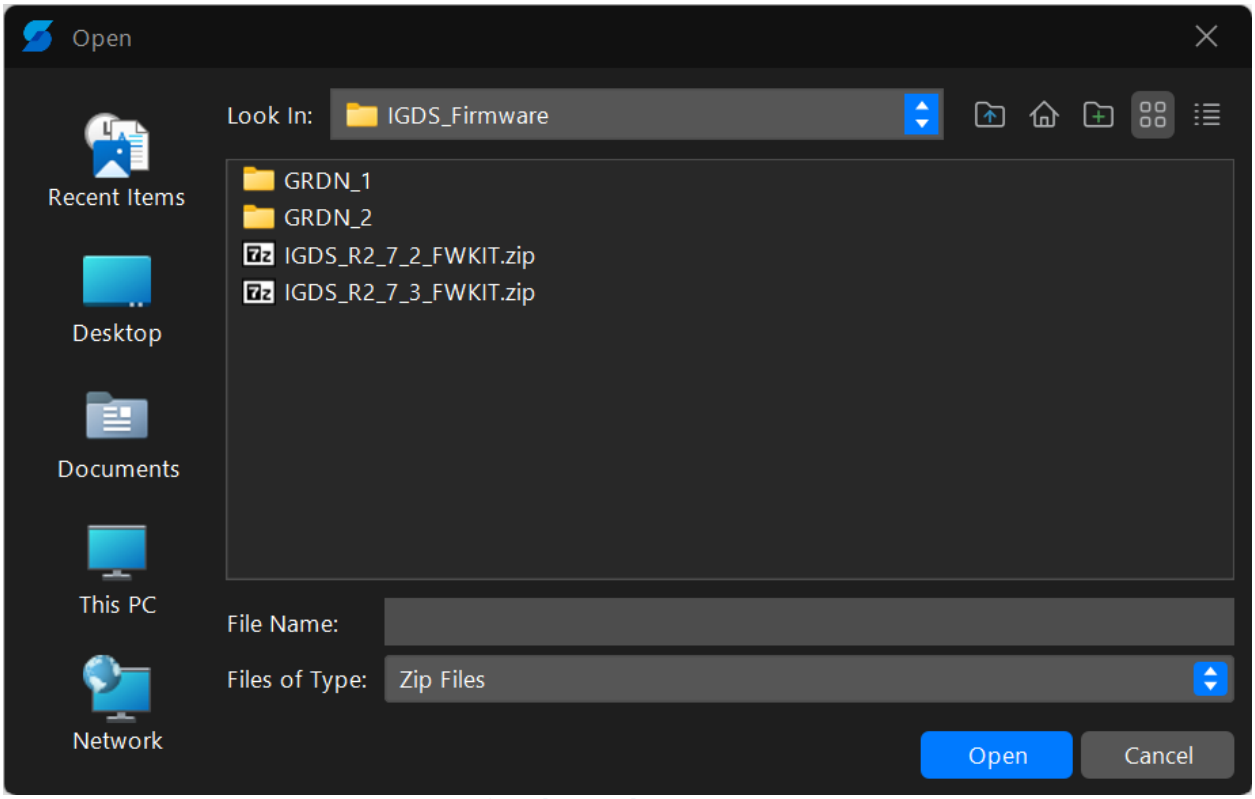


Figure 25 – Select FW kit

6. Once selected the GW will import the kit and will respond with either

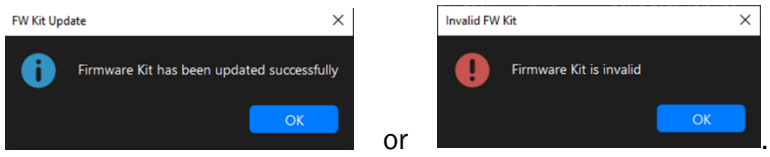


Figure 26 – Sensor Firmware Kit Status

If the kit is invalid, repeat the load process and make sure that you are selecting the correct file. If the problem continues then re-download the kit or email SDS customer support. Once a FW kit is successfully loaded the version information, build date and file name will be updated in the window as shown previously; as well as the FW version on the main screen.

7. Upgrade Process Status – The GW will upgrade groups of sensors in parallel (5-10 sensors at a time). Each sensor upgrade requires about ½ minute and includes downloading the new firmware, image validation and reboot of the sensor. As this is occurring the status information in the screen will be updated as follows:
    - **Sensor Unit Firmware Status** – this section shows the number of sensors that are running the firmware version loaded onto the GW. When running normally all sensors should be **"Up to Date"** and none should **"Need Update"**.
    - Immediately after a new kit is loaded onto the system all of the sensors will show as needing the update. As this upgrade progresses the sensor will move from **"Need Update"** to **"Up to Date"**.
    - The example below shows the status during an upgrade process. It can be seen that 10 sensors have been upgraded, 5 remain to be upgraded.
      NOTE: During the upgrade process sensors are rebooted and will go Offline during which time they will not show up in either category. As they come back online, they will all become "Up to Date".

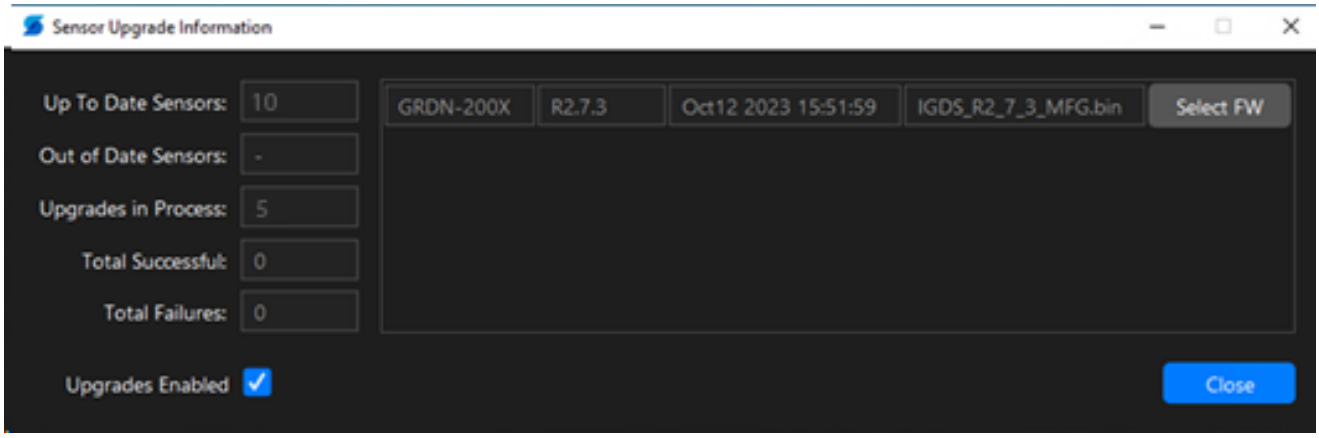


Figure 27 – Sensor Upgrade Information View

Sensor Upgrade Processing Status – This section of the window shows the status of the upgrade process including the number of upgrades currently in process, the number completed and any failed upgrades.

Referring to View Five sensors are currently in the update process and ten were already successfully upgraded. The statistics are based on all upgrades since that last time the GW software was restarted.
NOTE: It is not uncommon for an occasional upgrade failure due to network timing or other factors. The sensors will restart, and the upgrade will be run again.

7.3.2.2 SDS Wireless (GRDN-300x) Sensor Firmware Upgrade Information

The firmware in the SDS Wireless Sensors is not managed by the Gateway. To update the firmware on any SDS Wireless Sensor, please refer to the SDS Wireless Config Tool documentation. It is recommended that wireless sensors are updated via USB.

Alternately, wireless sensor FW may be updated via Wi-Fi, although this is not the preferred method. The USB function of the Wireless Config Tool is the preferred method.

For WiFi updates, additional steps are necessary and battery life will be impacted. The following step is detailed in the above-mentioned documentation but is repeated here. To update the firmware on the SDS Wireless sensors, their WiFi must first be enabled. The sensor's Wi-Fi can be enabled by connecting USB or External DC power, or by sending the "Enable Wi-Fi" command from the Gateway. The "Enable Wi-Fi" command can be sent from the "Wireless (GRDN-300x) Stats" window of the Gateway as detailed in Section 7.2.3.

7.3.3 Common Sensor Certificates

This page can be used to view and install common SSL and 802.1x certificates on the system. The dialog can be seen in the figure below. For more detailed information please refer to the **SDS App Note – PoE Sensor / Gateway – Common SSL Certificate Management.**

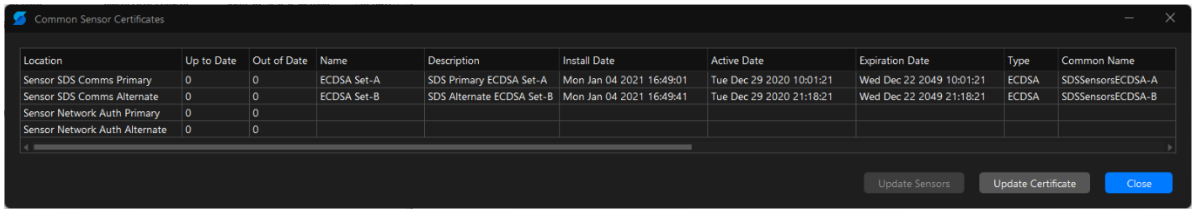


Figure 28 – Common Sensor Certificate View

7.3.4 Gateway Advanced Settings

This configuration page can be used to configure several settings in the GW Server. The dialog is shown in the figure below and the **SDS AppNote – GW Advanced Settings** provides detailed information regarding each of the parameters. *As the name implies these settings should be updated carefully as they can result in system outages and performance issues.*

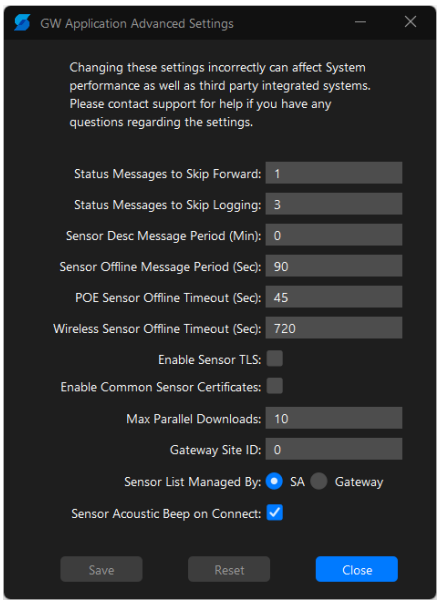


Figure 29 - GW Advanced Settings Page

7.3.5 UI Theme

Starting with GW version 3.4.0, user can select between Dark and Light color scheme for the GW application and all subsequent sub-windows.

Clicking on UI Theme, the user is provided with Dark and Light options.

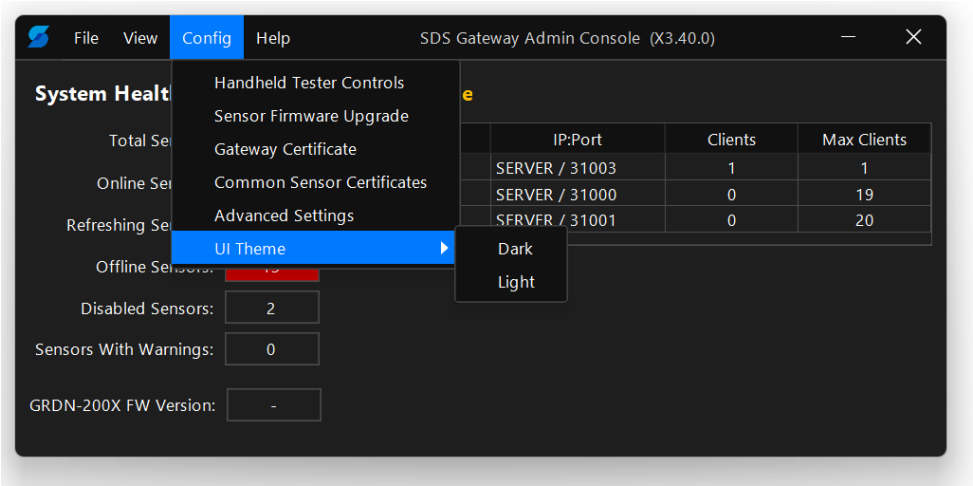


Figure 30 - GW UI Theme Settings Menu

After selecting the desired option, a restart of the GW Admin Console window is required for the new settings to take effect.

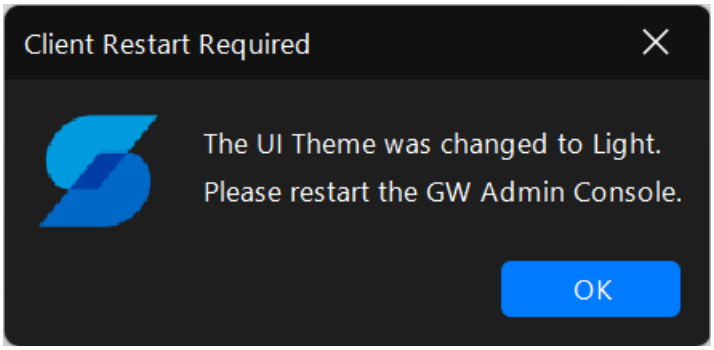


Figure 31 - GW UI Theme Restart GW Admin Console

8 SDS Gateway Maintenance

8.1 SDS Gateway Software Upgrade

The GW application will be revised periodically to add functionality and make improvements to its operation. When this occurs, SDS will provide, via email and web, information regarding the GW software upgrade. This will include information on any performance improvements and on any impact to system security or other issues. The software will be posted on an SDS provided site for system administrators to download.

The upgrade process follows the steps in Section 0 but you will be asked if you want to remove the current version. **Always allow the GW to be uninstalled** as it will not remove any of the configuration information, logs, or other data on the system.

8.2 SDS Gateway Backups (Recommended Practice)

All installation specific information for the GW is stored in ${SDS_Data_Dir}\GWData. It is suggested that either this specific directory (or the entire SDSData) folder be backed up on a regular basis.

If a Gateway configuration issue occurs with your system, follow the instructions in the next section to restore the Gateway to a functional state.

8.3 Gateway Configuration Restore (Recovering from an Issue)

The easiest method of restoring the Gateway configuration to a prior backup is to restore ${SDS_Data_Dir}\GWData from a backup. If you have only a limited backup then restore at a minimum ${SDS_Data_Dir}\GWData\config and ${SDS_Data_Dir}\GWData\.preferences.

If restoring this information in these folders does not resolve the issue then a last step is to re-install the GW application using the most recent installer. The re-install process does not affect the data folder just the program installation area.

If the GW is still not operating correctly then contact your site support personnel.

9 Appendix I – Sensor Management via the GW / nodes.csv file

THIS APPENDIX APPLIES ONLY TO SYSTEMS NOT RUNNING THE SDS SA
or RUNNING AN OLDER VERSION OF THE SA SOFTWARE (Pre R4.x)

In this deployment scenario the GW Server will be configured to manage the sensor configuration file. The first step is to enable the GW Server to manage the nodes.csv configuration file. This setting is configured in the GW Advanced Settings Dialog using the Config → Advanced Settings menu item. The "General Settings" portion near the bottom of the screen shows a selection for "Sensor List Managed By" and it is defaulted to the SA. In this specific scenario if you are running with no SA then allow the Gateway to manage the file. Once you have changed the selection and hit Save you can configure the Sensors using the nodes.csv file directly as described in the following subsections.

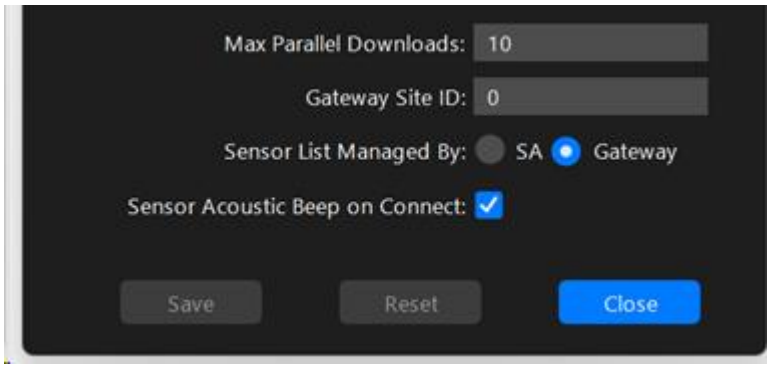


Figure 32 - Sensor Management Selection

9.1.1 Generating a Sensor Configuration File

Refer to Appendix I (**App Note – Sensor Configuration File)** for instructions in creating and managing a Sensor Configuration file. Once the sensor information has been added to the configuration file you will need to place the file in the GW's data folder {$SDS_DATA_DIR}\GWData\configuration\default\nodes.csv.

NOTE: It is always suggested to keep a current backup of this file in the case that it is corrupted or overwritten by the system or an administrator.

The figure below shows an example of a nodes.csv file that includes the Site-ID field.

Table 1 Sensor Configuration Information

Id	IP	MonitorPort	CmdPort	Facility	Floor	Location	Description	DataCloset	SwitchName	SwitchPort	Gunshot Detection	Tamper Detection	Sensor Offline	Sensor Degraded	SiteID
S6474F6000201	10.10.0.101	0	0	One Beacon Street	Floor 30	Exec - Conference Rm	F30-1	IDF-F30	10.10.30.254	1	5	3	3	4	440030
S6474F6000202	10.10.0.102	0	0	One Beacon Street	Floor 30	CEO - Elevators and Lobby	F30-2	IDF-F30	10.10.30.254	2	6	3	3	4	440030
S6474F6000203	10.10.0.103	0	0	One Beacon Street	Floor 30	CEO - Office	F30-3	IDF-F30	10.10.30.254	3	7	3	3	4	440030
S6474F6000204	10.10.0.104	0	0	One Beacon Street	Floor 30	Exec - Hall 1	F30-4	IDF-F30	10.10.30.254	4	8	3	3	4	440030
S6474F6000205	10.10.0.105	0	0	One Beacon Street	Floor 30	Exec - Hall 2	F30-5	IDF-F30	10.10.30.254	5	9	3	3	4	440030
S6474F6000206	0	0	0	One Beacon Street	Floor 7	Hall - NearRM7010 - North Side	F7-1	MDF-F7	10.10.7.254	1	10	3	3	4	440007
S6474F6000207	0	0	0	One Beacon Street	Floor 7	Hall - NearRM7015 - North Side	F7-2	MDF-F7	10.10.7.254	2	11	3	3	4	440007
S6474F6000208	0	0	0	One Beacon Street	Floor 7	Hall - NearRM7018 - North Side	F7-3	MDF-F7	10.10.7.254	3	12	3	3	4	440007
S6474F6000209	0	0	0	One Beacon Street	Floor 7	Cafeteria - Enterance	F7-4	MDF-F7	10.10.7.254	4	13	3	3	4	440007
S6474F6000210	0	0	0	One Beacon Street	Floor 7	Cafeteria - Food Court	F7-5	MDF-F7	10.10.7.254	5	14	3	3	4	440007
S6474F6000211	0	0	0	One Beacon Street	Floor 7	Cafeteria - Table Area	F7-6	MDF-F7	10.10.7.254	6	15	3	3	4	440007
S6474F6000212	0	0	0	One Beacon Street	Floor 7	Hall - Near RM7050 - East Side	F7-7	MDF-F7	10.10.7.254	7	16	3	3	4	440007
S6474F6000213	0	0	0	One Beacon Street	Floor 7	Hall - Near RM7055 - East Side	F7-8	MDF-F7	10.10.7.254	8	17	3	3	4	440007
S6474F6000214	0	0	0	One Beacon Street	Floor 7	Elevators	F7-9	MDF-F7	10.10.7.254	9	18	3	3	4	440007
S6474F6040215	WIRELESS	0	0	One Beacon Street	Floor 1	Lobby - North Entrance	F1-1	IDF-F1	10.10.1.254	3	19	3	3	4	440001
S6474F6040216	WIRELESS	0	0	One Beacon Street	Floor 1	Lobby - Main Desk	F1-2	IDF-F1	10.10.1.254	3	20	3	3	4	440001
S6474F6040217	WIRELESS	0	0	One Beacon Street	Floor 1	Lobby - South Entrance	F1-3	IDF-F1	10.10.1.254	3	21	3	3	4	440001
S6474F6040218	WIRELESS	0	0	One Beacon Street	Floor 1	Lobby - East Entrance	F1-4	IDF-F1	10.10.1.254	3	22	3	3	4	440001
S6474F6040219	WIRELESS	0	0	One Beacon Street	Floor 1	Lobby - Elevator	F1-5	IDF-F1	10.10.1.254	3	23	3	3	4	440001
S6474F6040220	WIRELESS	0	0	One Beacon Street	Floor 1	Lobby - West Entrance	F1-6	IDF-F1	10.10.1.254	3	24	3	3	4	440001

Once the file is in place restart the GW Server to update the sensor information. Verify that the proper number of sensors show up on the front screen and using "**View → Sensors"** menu option.

9.1.2 Maintaining the Nodes Configuration File

Each time additional sensors are added to the system or sensors are replaced for maintenance the nodes.csv file must be updated accordingly.

- Adding Sensors: Additional sensors will require rows be added with the appropriate serial numbers, IP address, and installation information.
    - Adding SDS Wireless Sensors: SDS Wireless (GRDN-300x) sensors are added similarly to GRDN-200x sensors; however, the IP address field must be entered as "WIRELESS".
- Replacing Sensors: If a sensor is replaced (and maintains the same IP address) then the only modification required to the file is to change the first column (Id) to match the new sensor's serial number. *Modifications are made by editing the file in Excel (or similar tool).*

Once you have updated the file and saved it, **stop and restart the GW application to update the settings**. Refer to Section 7.3.5 for information regarding backing up and restoring the GW application.

The figure below shows an example nodes.csv file for a system with multiple facilities and floors. In the table you can see how the RC interface is uniquely defining the Gunshot Detection events (separate relays) but using a common relay for each of the other notifications.

Table 2 Sensor Configuration Information

Id	IP	MonitorPort	CmdPort	Facility	Floor	Location	Description	DataCloset	SwitchName	SwitchPort	Gunshot Detection	Tamper Detection	Sensor Offline	Sensor Degraded	SiteID
S6474F6000201	10.10.0.101	0	0	One Beacon Street	Floor 30	Exec - Conference Rm	F30-1	IDF-F30	10.10.30.254	1	5	3	3	4	440030
S6474F6000202	10.10.0.102	0	0	One Beacon Street	Floor 30	CEO - Elevators and Lobby	F30-2	IDF-F30	10.10.30.254	2	6	3	3	4	440030
S6474F6000203	10.10.0.103	0	0	One Beacon Street	Floor 30	CEO - Office	F30-3	IDF-F30	10.10.30.254	3	7	3	3	4	440030
S6474F6000204	10.10.0.104	0	0	One Beacon Street	Floor 30	Exec - Hall 1	F30-4	IDF-F30	10.10.30.254	4	8	3	3	4	440030
S6474F6000205	10.10.0.105	0	0	One Beacon Street	Floor 30	Exec - Hall 2	F30-5	IDF-F30	10.10.30.254	5	9	3	3	4	440030
S6474F6000206	0	0	0	One Beacon Street	Floor 7	Hall - NearRM7010 - North Side	F7-1	MDF-F7	10.10.7.254	1	10	3	3	4	440007
S6474F6000207	0	0	0	One Beacon Street	Floor 7	Hall - NearRM7015 - North Side	F7-2	MDF-F7	10.10.7.254	2	11	3	3	4	440007
S6474F6000208	0	0	0	One Beacon Street	Floor 7	Hall - NearRM7018 - North Side	F7-3	MDF-F7	10.10.7.254	3	12	3	3	4	440007
S6474F6000209	0	0	0	One Beacon Street	Floor 7	Cafeteria - Enterance	F7-4	MDF-F7	10.10.7.254	4	13	3	3	4	440007
S6474F6000210	0	0	0	One Beacon Street	Floor 7	Cafeteria - Food Court	F7-5	MDF-F7	10.10.7.254	5	14	3	3	4	440007
S6474F6000211	0	0	0	One Beacon Street	Floor 7	Cafeteria - Table Area	F7-6	MDF-F7	10.10.7.254	6	15	3	3	4	440007
S6474F6000212	0	0	0	One Beacon Street	Floor 7	Hall - Near RM7050 - East Side	F7-7	MDF-F7	10.10.7.254	7	16	3	3	4	440007
S6474F6000213	0	0	0	One Beacon Street	Floor 7	Hall - Near RM7055 - East Side	F7-8	MDF-F7	10.10.7.254	8	17	3	3	4	440007
S6474F6000214	0	0	0	One Beacon Street	Floor 7	Elevators	F7-9	MDF-F7	10.10.7.254	9	18	3	3	4	440007
S6474F6040215	WIRELESS	0	0	One Beacon Street	Floor 1	Lobby - North Entrance	F1-1	IDF-F1	10.10.1.254	3	19	3	3	4	440001
S6474F6040216	WIRELESS	0	0	One Beacon Street	Floor 1	Lobby - Main Desk	F1-2	IDF-F1	10.10.1.254	3	20	3	3	4	440001
S6474F6040217	WIRELESS	0	0	One Beacon Street	Floor 1	Lobby - South Entrance	F1-3	IDF-F1	10.10.1.254	3	21	3	3	4	440001
S6474F6040218	WIRELESS	0	0	One Beacon Street	Floor 1	Lobby - East Entrance	F1-4	IDF-F1	10.10.1.254	3	22	3	3	4	440001
S6474F6040219	WIRELESS	0	0	One Beacon Street	Floor 1	Lobby - Elevator	F1-5	IDF-F1	10.10.1.254	3	23	3	3	4	440001
S6474F6040220	WIRELESS	0	0	One Beacon Street	Floor 1	Lobby - West Entrance	F1-6	IDF-F1	10.10.1.254	3	24	3	3	4	440001

10 Appendix II – Sensor & License Warning Codes

SDS Sensors run Built-In-Test functions to verify hardware performance and continuously monitor their environment to ensure that they are operating correctly and, in an environment, where they will meet their performance specifications. When an issue is detected this information is communicated to the GW and other connected applications via a Warning Code (WC) and other information. This WC is shown in the GW Sensor Views and the table below provides a mapping between the WC, its meaning and suggested action.

"TEMPERATURE" - Sensor Over/Under Temperature (WC = 10)

Solution: If it is determined that the sensor is experiencing extreme temperatures then you will need to correct the problem or move the sensor. If the environment is found to be a normal temperature then reset the sensor (power-cycle) and if the issue remains the sensor will need to be replaced.

"VOICE MIC" - Monitor Microphone Not Operational (GRDN-200x Only) (WC = 15)

Solution: Reset (power-cycle) the sensor. If the problem persists then the sensor will need to be replaced.

NOTE: The sensor is operational – but the "Listen" after shot event may not work on this sensor.

"ACOUSTIC ENV. NOISE TOO HIGH" - Acoustic Environmental Noise Too High (WC = 20)

Solution: The sensor is indicating that its performance is degraded due to a loud noise source(s) in the area. If a noise source is found then the noise source (or sensor) will need to be moved. If there is no noise source then reset (power-cycle) the sensor and if the issue remains this could indicate a hardware issue and the sensor will need to be serviced.

"ACOUSTIC SENSOR NOISE TOO HIGH" - Acoustic Sensor Noise Too High (WC = 25)

Solution: The sensor is indicating that its performance is degraded due to sensor noise (likely internal) found during BIT.

"IR ENV. NOISE TOO HIGH" - IR Environmental Noise Too High (WC = 30)

Solution: The sensor is indicating that its performance is degraded due to an IR/Lighting source(s) in the area. At the sensor look for bright lighting, direct sunlight or other lighting sources that might be the issue. If a source is found then the source (or sensor) will need to be repositioned. If there is no noise source then reset (power-cycle) the sensor and if the issue remains this could indicate a hardware issue and the sensor will need to be serviced.

"IR SENSOR NOISE TOO HIGH" - IR Sensor Noise Too High (WC = 35)

Solution: The sensor is indicating that its performance is degraded due to sensor noise (likely internal) found during BIT.

"ACOUSTIC SENSOR BIT" - Acoustic Sensor Degraded (WC = 40)

Solution: The sensor is indicating that one or both acoustic sensors are not fully functional. Reset (power-cycle) the sensor and if the issue persists then the sensor will need to be serviced.

"IR SENSOR BIT" - Infrared Sensor Degraded (WC = 50)

Solution: The sensor is indicating that one or both infrared sensors are not fully functional. Reset (power-cycle) the sensor and if the issue persists then the sensor will need to be serviced.

"ORIENTATION" – Sensor Orientation Warning (WC = 60)

Solution: The sensor is indicating that it is not installed in the proper wall or ceiling mount orientation. Please refer to the Installation Guide for proper mounting instruction.
NOTE: If the sensor is installed in a non-typical orientation (e.g. slanted roof-line) contact SDS Customer Support for help disabling the warning for this sensor.

"TAMPER" – Sensor Tamper Warning (WC = 61)

Solution: Indicates the sensor was moved very recently. Note this will be the WC for a period after Sensor Motion Detected (200) was detected and reported. If this is re-occurring and it is known that the sensor has not been moving, then the sensor will need to be replaced.

WC = 100 to 160 Hardware Test Failure

Solution: The sensor is indicating an internal hardware test failure. Reset (power-cycle) the sensor and if the issue persists then the sensor will need to be replaced.

"LOW BATTERY" – Sensor Low Battery (GRDN-300x Only) (WC = 185)

Solution: The SDS Wireless (GRDN-300x) sensor is indicating that the battery life is critically low. Perform the yearly maintenance on the sensor and replace the battery.

"TAMPER" – Sensor Motion Detected (WC = 200)

Solution: The sensor is indicating that it has recently detected motion. Ensure that the sensor is operational and still properly installed with no indications of tampering.

WC = 210 to 225 Maintenance Tester Codes

These warning codes are utilized when the sensor is operating in TESTER mode and do not immediately indicate an issue. They are used to allow the notification software in the SA to determine the results of detecting the SDS Tester Signal and to send the installer/admin an email denoting proper operation or issues detected by the sensor. The WC are just used to signal the test results and do not remain asserted; thus, they will not appear in the Sensor View tables.

WC = 230 to 240 License Issue Codes

These warning codes indicate a SDS License Violation (or Warning – e.g. Expiration in < 90 days). Licensed features include the Annual Operating License (period of time), Number of Sensors, and Integrations / Integration connections.

11 Appendix III – Troubleshooting & FAQs

Listed below are frequently asked questions you may come across while installing and configuring the Gateway Application or interfacing with the Situational Awareness application.

Q1) I made a change to the nodes.csv, how do I refresh the data within the Gateway application?

Solution: Starting with GW R3.x and SA R4.x the sensors are NOT managed/updated via the nodes.csv file. A separate Sensor Configuration file (can be a copy of nodes.csv) needs to be updated and imported into the SA. Alternatively, the sensor can be edited in the SA GUI and this will update the SA and GW.

Note that this file is a .csv, not an .xls file, and must be saved as such.

Q2) I made a change in the nodes.csv. Why don't I see the change reflected in the Situational Awareness (SA) application?

Solution: Refer to the question above and SDS App Note – Sensor Configuration.

Q3) I added a row in the Sensor Configuration file for a new sensor and imported it into the SA. Why does it report as "offline" in the Gateway application?

Solution: Verify the following:

- ✓ Select **"View"** → "**Show Sensors with Issues View"**. Sensors which have an issue which is detectable by the Gateway application will be displayed here.

  In the example below the reported ID (Read from the sensor) does not match the ID located in the nodes.csv file.
  Example: SID Mismatch, Reported: S70B3D5ED20AB

- ✓ Ensure that there are no additional spaces or incorrect characters in the Id or IP fields.

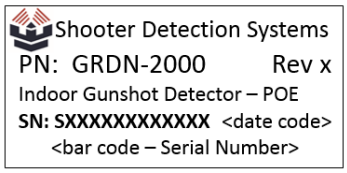
- ✓ Each Id field MUST contain **uppercase** characters only.
  Example:

  S70B3D5ED20AB [Correct]

  s70b3d5eb20ab [**Incorrect**]

- ✓ Ensure that the Id (also called the Serial Number or MAC address) matches the label on the top/rear of the SDS sensor. Also confirm that the Id and IP are paired correctly.

  Serial Number Label Example:



- ✓ Verify that the SDS sensor is connected to a Power Over Ethernet (POE) switch and that the switch is connected to the gateway hardware. On the switch side the Ethernet Link should be lit as well as the POE indicator. On a Smart or Managed POE switch ensure power is enabled and that the sensor is drawing power.
  When the SDS is powered and has link the sensor will beep once. The sensor plays a two-tone beep (High – Low) when a connection is successfully opened from the Gateway.

- ✓ Ensure that the SDS sensor has been configured with the correct IP address. This can be determined by first pinging the sensor at the IP address that you believe has been programmed. A SDS unit will have a factory default IP address of 10.10.0.10.

  As a second level of debug can be provided by the SDS IP Address tool (SDS Explorer) application using the "Refresh IP List" button. This will display all SDS sensors on the subnet specified under the **"Network"** field of the SDS Explorer application.

- ✓ The default Monitor and Cmd Ports should be set to "0" in the Sensor Configuration file – verify this is the case.

Q4) Why don't I see the number of "Total Sensors" reported in the Gateway application that I would expect?

Solution: Verify the following:

- ✓ Verify that a row has been added to the Sensor Configuration file for each sensor.

- ✓ Confirm that you have imported this file into the SA Server – which will synchronize it on the GW Server.

Q5) Why do I see a SDS sensor reporting a warning?

Solution: The sensor may report a warning for a variety of reasons. The following steps can be used to determine the specific issue:

- ✓ Select “View” → “Sensor Maintenance Issues”. Sensors with warning will be displayed here. The Warning Info column will contain a brief description of the cause of the warning. Contact SDS support for more information on the warning.

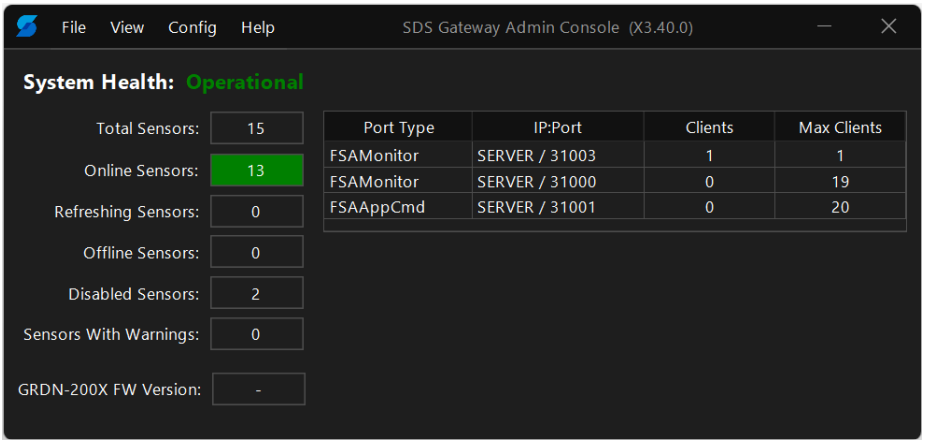
- ✓ A more common warning is due to high levels of IR Noise. This noise may be generated by intense lighting sources or ambient IR from outside a building. Ensure the sensor is position properly and not in the path of a direct IR source.

Q6) Why won’t the Situational Awareness application connect to the Gateway?

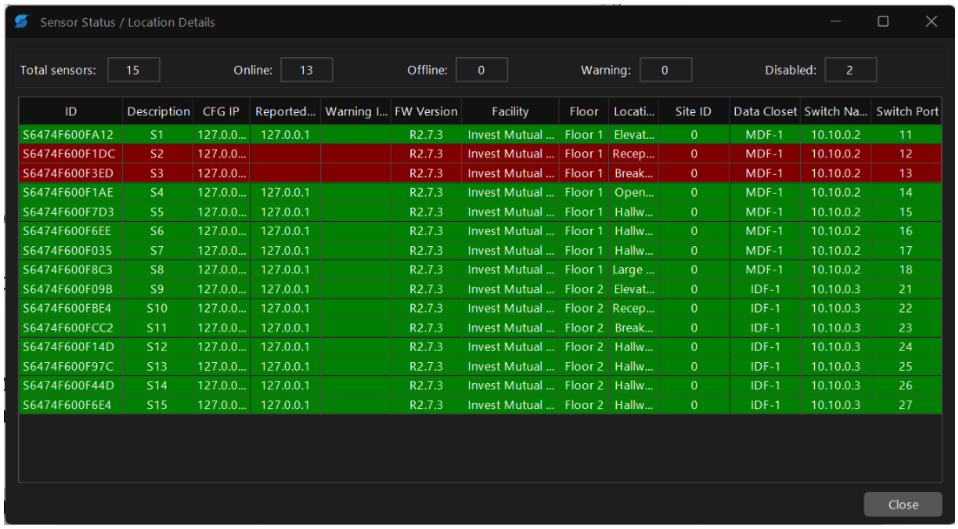
Solution: Verify the following:

- ✓ Confirm that the IP and Ports configured within the SA application match those configured in the Gateway application. The SA Server, when running on the Gateway, may have the localhost address of 127.0.0.1, otherwise it must match the static IP of the Gateway machine. The Gateway ports are configured in the gateway.csv file.

  Gateway Application:



Situational Awareness Application: "File" → "Sensors"



- ✓ Ensure that the following range of ports is not blocked on the Gateway firewall: 31000 – 31006[1] . This range of ports should be configured to allow inbound traffic.

- ✓ Verify that any Anti-virus application is not interfering. This can be confirmed by temporarily disabling features within the anti-virus program.

Q7) Why do I see the SDS SA disconnecting and then reconnection from the GW a few minutes later?

Solution: It has been observed that Anti-Virus programs can lock the SDSData folder and prevent the GW from being able to log information for an extended period of time (2-10 minutes). When this occurs, the GW can become blocked and stop processing sensor information – resulting in the SA and 3rd party applications disconnecting and reconnecting until the problem clears:

- ✓ If you are running an Anti-Virus program you **MUST** exclude the SDSData folder and all subfolders.

Q8) Why do I see SDS Sensors disconnecting and reconnecting a few seconds later?

Solution: There are several possibilities in this case. If you are not running GW Release R3.1.1 then as a first step upgrade to that version (or more recent) and see if the issue is resolved. If not then consider the solution offered for the prior question.

[1] Ports: 31000-31006 assume the system is operating with default ports. If you have configured different ports for the GW connections, verify those are enabled for input through the firewall.

12 Appendix IV – SDS License Agreement

SHOOTER DETECTION SYSTEMS, LLC

CLICK WRAP LICENSE AGREEMENT

Version 5.0

Note: As a user of the **EMBEDDED SOFTWARE**, you are required to accept the terms and conditions of the Agreement below. Before you click on the "Accept" button, you should carefully read the terms and conditions as set forth below.

By downloading the software or otherwise using the software, you, on behalf of yourself or your company ("SUBSCRIBER") agree to the following terms and conditions.

SHOOTER DETECTION SYSTEMS CLICKWRAP LICENSE AGREEMENT

SHOOTER DETECTION SYSTEMS, LLC ("SDS" OR "WE") IS WILLING TO PROVIDE CERTAIN HARDWARE, SOFTWARE AND DOCUMENTATION TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY (REFERENCED BELOW AS "YOU" OR "SUBSCRIBER") THAT EITHER ACCEPTS THIS AGREEMENT OR THAT ENTERS INTO AN ORDER OR SIMILAR DOCUMENT WITH SDS THAT REFERENCES THIS AGREEMENT ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS CLICK WRAP LICENSE AGREEMENT ("AGREEMENT"). READ THE TERMS AND CONDITIONS OF THIS AGREEMENT CAREFULLY BEFORE PURCHASING ANY HARDWARE OR SOFTWARE FROM SDS. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SDS. BY ACCEPTING THIS AGREEMENT (INCLUDING ELECTRONICALLY OR VIA CLICKWRAP) OR ENTERING INTO A WRITTEN ORDER OR SIMILAR DOCUMENT WITH SDS THAT REFERENCES THE AGREEMENT BELOW, YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE WITH THE TERMS AND CONDITIONS STATED HEREIN ALL HARDWARE, SOFTWARE AND DOCUMENTATION ASSOCIATED WITH THIS AGREEMENT MUST BE RETURNED TO SDS OR ITS APPROVED RESELLER WITHIN FIFTEEN (15) DAYS FROM THE DATE OF RECEIPT BY YOU.

IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF (AND FOR USE ON BEHALF OF) A COMPANY OR OTHER ENTITY (A "CORPORATE ENTITY"), YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH CORPORATE ENTITY TO THE TERMS OF THIS AGREEMENT AND YOU ACKNOWLEDGE THAT THE TERM "YOU" OR "SUBSCRIBER" REFERENCED BELOW REFERS TO SUCH CORPORATE ENTITY.

DEFINITIONS

Documentation means the documentation for the SOFTWARE generally supplied by SDS to assist its customers in the use of the SOFTWARE, including user and system administrator guides and manuals and other written materials, including the software functional specifications.

Fees means the fees set forth and described on the Order to be paid by SUBSCRIBER to SDS or its authorized dealer or reseller, as the case may be, for use of the SOFTWARE.

Hardware means that equipment provided by SDS set forth and described on an Order and may include sensors, computers, servers, cameras and similar equipment.

Order means each ordering document signed by SDS or one of its authorized dealers or resellers and SUBSCRIBER which references this Agreement, identifies the specific SOFTWARE ordered by SUBSCRIBER from SDS, sets forth the prices to be paid by SUBSCRIBER for the SOFTWARE, lists the Subscription Term and sets forth any other applicable terms and conditions.

Permitted Capacity means system resource limitations of SUBSCRIBER's subscription license to the SOFTWARE and may include but is not limited to number of hardware sensors, hardware devices, number and type of supported external applications, number and type of supported users.

SOFTWARE means the software products provided by SDS to SUBSCRIBER and which are listed on an Order and all updates, enhancements, bug fixes and new releases thereto that SDS makes available to SUBSCRIBER hereunder during the Subscription Term.

Subscription Term means the specific term of SUBSCRIBER's subscription license to the SOFTWARE. The Subscription Term

shall be set forth on the Order.

GRANT OF LICENSE.

Subject to the provisions contained in this Agreement, and timely payment of the applicable Fees, SDS hereby grants to SUBSCRIBER a limited, non-exclusive, non-sublicensable, non-transferable license, solely during the applicable Subscription Term, to use the SOFTWARE identified in the Order, solely in object code as embedded in the Hardware and solely for SUBSCRIBER's internal business purposes up to the Permitted Capacity set forth in the Order. Subject to compliance with the terms and conditions of this Agreement, SUBSCRIBER may relocate or transfer the SOFTWARE for use on a different server within its location. SUBSCRIBER shall not, and shall not permit, anyone else to copy the SOFTWARE, other than copies authorized in this Agreement. SUBSCRIBER understands that its right to use the SOFTWARE is limited by the Permitted Capacity purchased, and SUBSCRIBER'S use may in no event exceed the Permitted Capacity authorized under the applicable Order. If SUBSCRIBER's use exceeds the Permitted Capacity, SUBSCRIBER must purchase additional Permitted Capacity sufficient for the balance of the then-current Subscription Term to cover the excess use.

FEES.

SUBSCRIBER agrees to pay SDS (or if applicable its authorized dealer or reseller as set forth on the Order) the Fees in the amounts specified in the Order. Such FEES are not refundable and cannot be applied towards the purchase of other products or services. SDS reserves the right to change FEES and terms of this Agreement for any renewal Subscription Term, and will give the SUBSCRIBER prior written notice of any such changes.

OWNERSHIP OF SOFTWARE.

SDS shall at all times retain title to and ownership of the SOFTWARE, including any derivative works, improvements, adaptations or copies of the SOFTWARE, regardless of the form or media in or on which the original and other copies may exist. The SOFTWARE is protected by copyright laws and international copyright treaties and SDS may incorporate certain measures in the SOFTWARE to prevent unauthorized use. SUBSCRIBER acknowledges and agrees that any and all suggestions regarding features, functionality or performance that SDS may elect to adopt for any of its products including the SOFTWARE (expressly excluding SUBSCRIBER Confidential Information), such features, functionality and performance shall be deemed to be automatically assigned to SDS under this Agreement, and shall become the sole and exclusive property of SDS.

RESTRICTIONS.

SUBSCRIBER will not and will not allow any third party to: (a) copy or use the SOFTWARE in any manner except as expressly permitted in this Agreement; (b) use or deploy the SOFTWARE in excess of the Permitted Capacity number for which SUBSCRIBER has paid the applicable Fee; (c) transfer, sell, rent, lease, lend, distribute, or sublicense the SOFTWARE to any third party; (d) use the SOFTWARE for providing time-sharing services, service bureau services or as part of an application services provider or as a service offering primarily designed to offer the functionality of the SOFTWARE; (e) reverse engineer, disassemble, or decompile the SOFTWARE or otherwise attempt to reduce the SOFTWARE from object code to source code or reconstruct or discover any source code, underlying ideas, algorithms, file formats or programming interfaces of the SOFTWARE by any means whatsoever; (f) alter, modify, enhance or prepare any derivative work from or of the SOFTWARE; (g) use the SOFTWARE to develop any works which are functionally compatible or competitive to the SOFTWARE or create any works which are derived from the SOFTWARE (using the SOFTWARE to produce reports or other tasks permitted by the SOFTWARE are not deemed to be works derived from the SOFTWARE) (h) alter or remove any proprietary notices in the SOFTWARE; (i) utilize any equipment, device, software, or other means designed to circumvent or remove any security mechanisms or form of copy or usage protection used by SDS in connection with the SOFTWARE; or publicly disseminate or disclose performance information or analysis on the SOFTWARE, including any results of benchmark tests run on the SOFTWARE; or (j) use the SOFTWARE in any manner that violates any applicable law or regulation, including, without limitation, any third party copyright, intellectual property or proprietary right law, or U.S. Department of Commerce export administration rules. If SUBSCRIBER does not comply with the license terms or the foregoing restrictions, SDS may immediately terminate or suspend SUBSCRIBER'S license to the SOFTWARE (without refund or credit) until SUBSCRIBER comes into compliance with such terms and restrictions in accordance with the terms of this Agreement. SDS reserves all rights not expressly granted to SUBSCRIBER in this Agreement.

SUBSCRIBER agrees to use the SOFTWARE only on the SUBSCRIBER'S computer(s). SUBSCRIBER may, subject to any applicable export requirements, change the computer(s) on which SUBSCRIBER is authorized to use the SOFTWARE to other computer(s) within SUBSCRIBER'S organization. If SUBSCRIBER changes the computer(s) on which SUBSCRIBER is using the SOFTWARE, SUBSCRIBER may no longer use the SOFTWARE on the former computer(s).

THIRD PARTY SOFTWARE

If the Software licensed under this Agreement contains open source software, the terms and conditions governing the use of such open source software are in the open source software licenses of the copyright owner and not this Agreement. If there is a conflict between the terms and conditions of this Agreement and the terms and conditions of the open source software licenses governing SUBSCRIBER's

use of the open source software, the terms and conditions of the license grant of the applicable Open Source Software Licenses will take precedence over the license grants in this Agreement. If requested by SUBSCRIBER, SDS will use commercially reasonable efforts to: (i) determine whether any open source software is provided under this Agreement; and (ii) identify the Open Source Software and provide SUBSCRIBER with a copy of the applicable open source software license (or specify where that license may be found).

CONTACT INFORMATION.

SUBSCRIBER shall be responsible for ensuring SDS has the most current SUBSCRIBER contact and billing information as it pertains to this Agreement.

VERIFICATION.

SUBSCRIBER acknowledges and agrees that SDS may, upon reasonable notice to SUBSCRIBER and no more than once per year, request records to verify SUBSCRIBER'S use of the SOFTWARE complies with the terms of this Agreement. If SDS, on a reasonable basis, believes that such report is not correctly disclosing information of SUBSCRIBER'S SOFTWARE usage, SDS will conduct an audit at SUBSCRIBER'S business premises to verify that SUBSCRIBER'S use of the SOFTWARE complies with this Agreement. Such audit will be carried out during business hours and in accordance with SUBSCRIBER'S reasonable site security requirements. If the audit shows that SUBSCRIBER is in violation of this Agreement, SUBSCRIBER will reimburse SDS for its reasonable expenses related to the audit and will pay any appropriate additional fees.

DISASTER RECOVERY AND FAILOVER.

SUBSCRIBER may install additional copies of the SOFTWARE on one or more non-production servers designated for disaster recovery or failover purposes. Such additional copies may only be run on non-production server(s) and may only be used to carry out the designated purpose associated with the non-production server(s).

DELIVERY; SOFTWARE SUBSCRIPTION KEYS AND USE MANAGER.

The SOFTWARE is only available electronically via download and, unless specifically agreed to by SDS, will not be available in any other format. The SOFTWARE shall be deemed delivered to SUBSCRIBER upon SDS making available to SUBSCRIBER the SOFTWARE Subscription Key. SUBSCRIBER understands and agrees that a SOFTWARE Subscription Key provided by SDS is required to enable the SOFTWARE and that SOFTWARE Subscription Keys are valid only during the applicable Subscription Term. SUBSCRIBER further understands and agrees that: (i) SUBSCRIBER will be provided with a temporary SOFTWARE Subscription Key upon invoicing, and upon receipt by SDS (or its authorized dealer or reseller, as the case may be) of payment in full for the then-current Subscription Term, SUBSCRIBER will be provided with a SOFTWARE Subscription Key that is effective for the duration of such Subscription Term; (ii) in case of breach by SUBSCRIBER of the payment terms stipulated in this Agreement, SDS will have the right to suspend the SOFTWARE subscription and such suspension will not give rise to any modification of the amount of the SOFTWARE subscription fee or to any extension of the Subscription Term; (iii) the SOFTWARE will, in the absence of any renewal of the Subscription Term, be disabled automatically upon the termination or expiration of the Subscription Term or due to non-payment of the Fees during the Subscription Term; and (iv) the SOFTWARE Subscription Key will automatically prevent the use of the SOFTWARE in violation of the applicable restrictions, as set forth in the Order. SUBSCRIBER understands and agrees that activation of the SOFTWARE will include providing certain information to SDS regarding the system environment in which the SOFTWARE is operating. Information will include SUBSCRIBER name, license type, license resource limitations, Operating System, amount of RAM, MAC address and other machine resource information. Upon activation of the SOFTWARE a software module ("Use Manager") will monitor and limit resources to the levels in the Subscription. The Use Manager will provide SUBSCRIBER with information and notifications including the remaining duration of the Subscription period, usage statistics and attempts to exceed resource limitations. SUBSCRIBER can enable these notifications to be provided to SDS for external monitoring of Subscription, but external monitoring is not required.

ACTIVATION.

SUBSCRIBER is required to take certain steps to activate the SOFTWARE or validate SUBSCRIBER'S subscription. Failure to activate or register the SOFTWARE, validate the subscription, or a determination by SDS of fraudulent or unauthorized use of the SOFTWARE may result in reduced functionality, inoperability of the SOFTWARE, or a termination or suspension of the SOFTWARE Subscription.

UPDATES:

At any time during the Subscription Term, SDS may provide SOFTWARE upgrades, subject to SUBSCRIBER having paid the then-applicable Subscription Fee. From time to time, SDS may make improvements to the SOFTWARE. In SDS's sole discretion, releases containing minor improvements to the SOFTWARE will be provided to SUBSCRIBER at no additional charge. However, releases that incorporate major performance improvements or additional functionality not found in the original SOFTWARE may be offered to SUBSCRIBER at an additional charge. The additional charge will be separately quoted to SUBSCRIBER.

SUBSCRIPTION TERM.

This Agreement will become effective upon your acceptance of this Agreement. Unless otherwise specified in the Order, the Subscription Term will be for the time period specified in the Order (e.g., twelve (12) months). The Subscription Term will automatically renew thereafter for successive periods of twelve (12) months each unless either party notifies the other party in writing at least sixty (60) days prior to the then-current expiration date of the Subscription Term that such party has elected not to renew the Order. In addition, to the foregoing, SDS may terminate this Agreement upon breach of the terms of this Agreement by SUBSCRIBER, including failure to make full payment of the Fees when due.

THE SOFTWARE CONTAINS TECHNOLOGY THAT ALLOWS SDS TO TERMINATE SUBSCRIBER'S USE OF THE SOFTWARE IN THE EVENT SUBSCRIBER MATERIALLY BREACHES THE TERMS OF THIS AGREEMENT, INCLUDING BUT NOT LIMITED TO SUBSCRIBER'S FAILURE TO PAY FEES WHEN DUE. SUBSCRIBER SHALL BE SOLELY AND EXCLUSIVELY LIABLE FOR ANY ACT OR FAILURE TO ACT OR ANY OTHER RESULT DUE TO SUBSCRIBER'S BREACH OF THIS AGREEMENT AND TERMINATION OF SUBSCRIBER'S USE OF THE SOFTWARE.

Upon expiration of the Subscription Term or the termination of the Agreement as provided above, SUBSCRIBER shall promptly destroy the SOFTWARE and any back-up copy of the SOFTWARE. SUBSCRIBER shall also promptly return all materials provided by SDS in connection with the SOFTWARE. Except as expressly provided herein, termination of this Agreement by SDS will be a nonexclusive remedy for breach and will be without prejudice to any other right or remedy of SDS. All rights and obligations of the parties which by their nature are reasonably intended to survive such termination or expiration will survive termination or expiration of this Agreement and each Order.

PAYMENT TERMS.

Unless otherwise specified in an Order, all FEES due hereunder shall be paid annually in advance. FEES will be due in full within thirty (30) days after the date of invoice. The first annual Subscription Fee will be invoiced promptly after the effective date of such Order. Subsequent annual Subscription Fees will be invoiced at least thirty (30) days prior to the anniversary of the Subscription Term, and are due in full no later than the anniversary of the Subscription Term. All payments shall be in US Dollars and shall be made to SDS or, if applicable, the authorized SDS dealer or reseller as set forth on the applicable Order. Any amount not paid when due shall bear a late payment charge, until paid, at the rate of 1.5% per month or the maximum amount permitted by law, whichever is less. SUBSCRIBER agrees to reimburse SDS for all costs (including attorneys' fees) incurred in collecting late payments.

TAXES.

All payments required by the Order and Agreement are exclusive of federal, state, local and foreign taxes, duties, tariffs, levies, withholdings and similar assessments (including without limitation, sales taxes, use taxes and value added taxes), and SUBSCRIBER agrees to bear and be responsible for the payment of all such charges, excluding taxes based upon SDS's or its dealer's or reseller's net income.

CONFIDENTIAL INFORMATION.

SUBSCRIBER will protect any information provided to it by SDS that is marked confidential or that by its nature should be reasonably understood to be confidential or proprietary in nature (collectively, "Confidential Information"). SUBSCRIBER shall hold in confidence, and shall not disclose (or permit or suffer its personnel to disclose) any Confidential Information to any person or entity except to a director, officer, employee, outside consultant, or advisor (collectively "Representatives") who have a need to know such Confidential Information in the course of the performance of their duties for SUBSCRIBER and who are bound by a duty of confidentiality no less protective of SDS's Confidential Information than this Agreement. SUBSCRIBER and its Representatives shall use such Confidential Information only for the purpose for which it was disclosed and shall not use or exploit such Confidential Information for its own benefit or the benefit of another without the prior written consent of SDS. SUBSCRIBER accepts full responsibility for the actions of its Representatives and shall protect SDS Confidential Information in the same manner as it protects its own valuable confidential information, but in no event shall less than reasonable care be used. The parties expressly agree that the terms of this Agreement and any associated pricing and Fees are Confidential Information and the SOFTWARE is SDS's Confidential Information. SUBSCRIBER shall promptly notify SDS upon becoming aware of a breach or threatened breach hereunder, and shall cooperate with any reasonable request of SDS in enforcing its rights.

Information will not be deemed Confidential Information hereunder if such information: (i) is known prior to SUBSCRIBER receipt from SDS, without any obligation of confidentiality, as proven by SUBSCRIBER's written records; (ii) becomes known to SUBSCRIBER directly or indirectly from a source other than one having an obligation of confidentiality to SDS or a third party; (iii) becomes publicly known or otherwise publicly available, except through a breach of this Agreement; or (iv) is independently developed by SUBSCRIBER without use of SDS's Confidential Information, as proven by SUBSCRIBER's written records. SUBSCRIBER may disclose Confidential Information pursuant to the requirements of applicable law, legal process or government regulation, provided that it gives SDS reasonable prior written notice to permit SDS to contest such disclosure, and such disclosure is otherwise limited to the required disclosure.

Notwithstanding any other provision of this Agreement, SUBSCRIBER acknowledges that any use of the SDS Confidential Information in a manner inconsistent with the provisions of this Agreement may cause SDS irreparable and immediate damage for which remedies other than injunctive relief may be inadequate. Therefore, SUBSCRIBER agrees that, in addition to any other remedy to which SDS may be entitled hereunder, at law or equity, SDS shall be entitled to an injunction or injunctions (without the posting of any bond and without proof of actual damages) to restrain such use in addition to other appropriate remedies available under applicable law.

NO IMPLIED LICENSE.

Except for the limited rights and licenses expressly granted hereunder, no other license is granted by implication, estoppel or otherwise and no other use is permitted.

PURCHASE THROUGH RESELLERS.

In the event that SUBSCRIBER purchases a license to the SOFTWARE through an authorized dealer or reseller of SDS, the terms and conditions of this Agreement shall apply and supersede any other agreements except for any terms and conditions related to pricing, payment (if less than 30 days) or taxes. Such terms and conditions shall be negotiated solely by and between SUBSCRIBER and such authorized dealer or reseller. In the event that SUBSCRIBER ceases to pay the applicable dealer or reseller any applicable Fees, or terminates its agreement with the dealer or reseller, SDS shall have the right to (a) terminate SUBSCRIBER's access to the SOFTWARE at any time upon thirty (30) days' prior written notice to SUBSCRIBER or (b) mutually agree otherwise with SUBSCRIBER.

SOFTWARE WARRANTY.

SDS HEREBY GRANTS TO SUBSCRIBER A NINETY (90) DAY LIMITED SOFTWARE WARRANTY, AS DEFINED BELOW, COMMENCING ON THE INITIAL DATE THE SOFTWARE IS FIRST DELIVERED TO SUBSCRIBER BY SDS (THE "WARRANTY PERIOD"). SDS WARRANTS THAT DURING THE WARRANTY PERIOD THE SOFTWARE WILL PERFORM IN ACCORDANCE WITH THE THEN-CURRENT DOCUMENTATION IN ALL MATERIAL RESPECTS (THE "SOFTWARE WARRANTY"). THIS SOFTWARE WARRANTY DOES NOT COVER ANY COPY OF THE SOFTWARE, WHICH HAS BEEN ALTERED OR CHANGED IN ANY WAY BY A PARTY OTHER THAN SDS.

SOFTWARE WARRANTY REMEDY.

SUBSCRIBER'S SOLE AND EXCLUSIVE REMEDY FOR ANY BREACH OF THE SOFTWARE WARRANTY SHALL BE TO HAVE SDS OR ITS AUTHORIZED REPRESENTATIVES, AT SDS'S OR ITS AUTHORIZED REPRESENTATIVES' OPTION, MODIFY SUCH SOFTWARE TO CORRECT THE DEFECT GIVING RISE TO SUCH BREACH WITHIN A REASONABLE PERIOD, NOT TO EXCEED THIRTY (30) DAYS FROM SDS'S RECEIPT OF WRITTEN NOTIFICATION OF SUCH DEFECT FROM SUBSCRIBER (THE "CURE PERIOD"). IF, WITHIN THE CURE PERIOD AS DEFINED ABOVE, SDS IS UNABLE TO MODIFY THE DEFECTIVE SOFTWARE IN SUCH A WAY AS TO CORRECT SUCH DEFECT, THEN, UNLESS SDS IS ABLE TO PROVIDE SUBSCRIBER WITH ANOTHER METHOD OF ACHIEVING THE DESIRED EFFECT, SUBSCRIBER SHALL BE ENTITLED TO TERMINATE THIS AGREEMENT AND RETURN THE SOFTWARE TO SDS WITHIN TEN (10) DAYS FOLLOWING THE END OF THE CURE PERIOD. IN SUCH EVENT, SUBSCRIBER SHALL BE ENTITLED TO A PRO RATA REFUND, OF ANY PREPAID FEES PAID BY SUBSCRIBER AND RECEIVED BY SDS FOR SUCH DEFECTIVE SOFTWARE.

EXCLUSIONS AND CONTINGENCIES.

SUBSCRIBER'S remedy and SDS's liability under this Section are expressly contingent upon: (i) SUBSCRIBER notifying SDS in writing of the claim within the warranty period and furnishing SDS with adequate supporting documentation and details to substantiate the claim and to assist SDS with the identification and detection of the cause of the problem, and (ii) the problem being capable of reproduction on properly functioning equipment by SDS; (iii) the SOFTWARE has not been altered or changed in any way by a party other than SDS; (iv) the SOFTWARE has been properly installed and operated in accordance with the Documentation; and (v) the SOFTWARE has not experienced interference from products, applications, or configurations provided by SUBSCRIBER.

SDS IS NOT RESPONSIBLE FOR PROBLEMS CAUSED BY CHANGES IN, OR MODIFICATIONS TO, THE OPERATING CHARACTERISTICS OF ANY COMPUTER HARDWARE OR OPERATING SYSTEM FOR WHICH THE SOFTWARE IS PROCURED, NOR IS SDS RESPONSIBLE FOR PROBLEMS WHICH RESULT FROM THE USE OF THE SOFTWARE IN CONJUNCTION WITH SOFTWARE OF THIRD PARTIES OR WITH HARDWARE WHICH IS INCOMPATIBLE WITH THE OPERATING SYSTEM FOR WHICH THE SOFTWARE IS BEING PROCURED. THIS LIMITED WARRANTY SHALL NOT APPLY TO (A) SOFTWARE USED IN VIOLATION OF THIS AGREEMENT, (B) USED, HANDLED, OPERATED, MAINTAINED OR STORED IMPROPERLY, OR IN ANY MANNER NOT IN ACCORD WITH THE DOCUMENTATION, INDUSTRY STANDARD PRACTICE OR SUBSCRIBER INSTRUCTIONS OR RECOMMENDATIONS; (C) SOFTWARE INSTALLATION, CONFIGURATION, OR SUPPORT PROVIDED BY SUBSCRIBER OR A THIRD-PARTY SERVICE PROVIDER NOT PERFORMING SERVICES ON SDS'S BEHALF, (D) ANY MODIFICATION OR DAMAGE TO THE SOFTWARE BY SUBSCRIBER OR ANY THIRD PARTY, OR (E) USE OF THE SOFTWARE IN COMBINATION WITH ANY THIRD-PARTY SOFTWARE, THIRD-PARTY DATABASE, OR OPERATING SYSTEM NOT AUTHORIZED OR CERTIFIED IN THE DOCUMENTATION OR WITH HARDWARE OR SOFTWARE SPECIFICALLY FORBIDDEN BY THE DOCUMENTATION.

SDS DOES NOT REPRESENT THAT THE SOFTWARE WILL BE ERROR-FREE OR THAT THE SOFTWARE WILL MEET SUBSCRIBER'S

REQUIREMENTS OR THAT ALL ERRORS IN THE SOFTWARE WILL BE CORRECTED OR THAT THE OVERALL SYSTEM THAT MAKES THE SDS SOFTWARE AVAILABLE (INCLUDING BUT NOT LIMITED TO THE INTERNET, OTHER TRANSMISSION NETWORKS, AND SUBSCRIBER'S LOCAL NETWORK AND EQUIPMENT) WILL BE FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS. THE WARRANTIES STATED ABOVE ARE THE SOLE AND EXCLUSIVE WARRANTIES OFFERED BY SDS. THERE ARE NO OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY RIGHTS. SUBSCRIBER ASSUMES ALL RESPONSIBILITY FOR DETERMINING WHETHER THE SOFTWARE IS SUFFICIENT FOR SUBSCRIBER'S PURPOSES. ANY AND ALL WARRANTIES, EXPRESS OR IMPLIED, OF FITNESS FOR HIGH RISK PURPOSES REQUIRING FAIL-SAFE PERFORMANCE ARE HEREBY EXPRESSLY DISCLAIMED.

WITHOUT LIMITING THE GENERALITY OF THE FOREGOING DISCLAIMERS, WHILE THE SOFTWARE IS NOT DESIGNED, SOLD, OR INTENDED TO BE USED TO DETECT, INTERCEPT, TRANSMIT OR RECORD ORAL OR OTHER COMMUNICATIONS OF ANY KIND, SDS CANNOT CONTROL HOW THE SOFTWARE IS USED, AND, ACCORDINGLY, SDS DOES NOT WARRANT OR REPRESENT, EXPRESSLY OR IMPLICITLY, THAT USE OF THE SOFTWARE WILL COMPLY OR CONFORM TO THE REQUIREMENTS OF FEDERAL, STATE OR LOCAL STATUTES, ORDINANCES AND LAWS, OR THAT USE OF THE SOFTWARE WILL NOT VIOLATE THE PRIVACY RIGHTS OF THIRD PARTIES. SUBSCRIBER SHALL BE SOLELY RESPONSIBLE FOR USING THE SOFTWARE IN FULL COMPLIANCE WITH APPLICABLE LAW AND THE RIGHTS OF THIRD PERSONS. SUBSCRIBER ACKNOWLEDGES AND AGREES THAT THE SOFTWARE IS NOT A CONSUMER GOOD, AND IS NOT INTENDED FOR SALE TO OR USE BY OR FOR PERSONAL, FAMILY OR HOUSEHOLD USE.

FURTHER, REGARDLESS OF ANY PRIOR STATEMENTS, REPRESENTATIONS, OR COURSE OF DEALINGS BY ANY SDS REPRESENTATIVES, SDS DOES NOT WARRANT OR REPRESENT, EXPRESSLY OR IMPLICITLY, THAT THE SDS SOFTWARE OR ITS USE WILL: RESULT IN THE PREVENTION OF CRIME OR HOSTILE ENEMY ACTION, APPREHENSION OR CONVICTION OF ANY PERPETRATOR OF ANY CRIME, MILITARY PROSECUTION OF ANY ENEMY FORCE, OR DETECTION OR NEUTRALIZATION OF ANY CRIMINAL, COMBATANT OR THREAT; PREVENT ANY LOSS, DEATH, INJURY, OR DAMAGE TO PROPERTY DUE TO THE DISCHARGE OF A FIREARM OR OTHER WEAPON; OR THAT THE SOFTWARE WILL REMAIN IN OPERATION AT ALL TIMES OR UNDER ALL CONDITIONS. THE SDS SOFTWARE IS PROVIDED TO HELP WITH PERSONAL SAFETY, BUT SUBSCRIBER SHOULD ALWAYS USE COMMON SENSE AND SEEK HELP WHEN IT IS NEEDED. SDS CANNOT AND DOES NOT GUARANTEE THAT ANY EMERGENCY PERSONNEL WILL RESPOND IN A TIMELY MANNER OR AT ALL, OR THAT THE MOST APPROPRIATE PERSONNEL WILL RESPOND. ADDITIONALLY, EMERGENCY RESPONSE PERSONNEL MAY NOT RESPOND BECAUSE OF LOCAL LAWS, REGULATIONS OR POLICIES. SUBSCRIBER SHOULD VERIFY THAT APPROPRIATE EMERGENCY PERSONNEL HAVE BEEN CONTACTED AND HAVE ALL INFORMATION NEEDED TO RESPOND TO THE EMERGENCY.

SDS, ITS AFFILIATES, SUBSIDIARIES, OFFICERS, DIRECTORS, EMPLOYEES, CONSULTANTS, AGENTS, SUPPLIERS, LICENSORS, RESELLERS, AND/OR DISTRIBUTORS EXPRESSLY DISCLAIM, AND DO NOT UNDERTAKE OR ASSUME ANY DUTY, OBLIGATION OR RESPONSIBILITY FOR ANY DECISIONS, ACTIONS, REACTIONS, RESPONSES, FAILURE TO ACT, OR INACTION, BY SUBSCRIBER AS A RESULT OF OR IN RELIANCE ON, IN WHOLE OR IN PART, THE SOFTWARE PROVIDED BY SDS, OR FOR ANY CONSEQUENCES OR OUTCOMES, INCLUDING ANY DEATH, INJURY, OR LOSS OR DAMAGE TO ANY PROPERTY, ARISING FROM OR CAUSED BY ANY SUCH DECISIONS, ACTIONS, REACTIONS, RESPONSES, FAILURE TO ACT, OR INACTION. IT SHALL BE THE SOLE AND EXCLUSIVE RESPONSIBILITY OF SUBSCRIBER TO DETERMINE APPROPRIATE DECISIONS, ACTIONS, REACTIONS OR RESPONSES, INCLUDING WHETHER OR NOT TO DISPATCH EMERGENCY RESPONDER RESOURCES. SUBSCRIBER HEREBY EXPRESSLY ASSUMES ALL RISKS AND LIABILITY ASSOCIATED WITH ANY AND ALL ACTION, REACTION, RESPONSE, AND DISPATCH DECISIONS, AND FOR ALL CONSEQUENCES AND OUTCOMES ARISING FROM OR CAUSED BY ANY DECISIONS MADE OR NOT MADE BY SUBSCRIBER IN RELIANCE, IN WHOLE OR IN PART, ON THE SOFTWARE, INCLUDING ANY DEATH, INJURY, OR LOSS OR DAMAGE TO ANY PROPERTY.

SDS MAKES NO WARRANTIES THAT ANY MESSAGES, ALERTS OR TEXTS SENT VIA THE SOFTWARE WILL BE ACCURATE, TIMELY OR SUCCESSFULLY SENT, DELIVERED OR RECEIVED.

SUBSCRIBER CONTENT.

SUBSCRIBER acknowledges and understands that the SOFTWARE relies on the information provided by the SUBSCRIBER including, without limitation, contact information, location address, floorplans and other information used to configure the SOFTWARE (collectively, the "SUBSCRIBER Content"). SUBSCRIBER Content is SUBSCRIBER'S sole and exclusive responsibility including but not limited to accuracy, and making and keeping back-up copies of SUBSCRIBER Content. SUBSCRIBER shall be solely responsible for any claims or causes of action that may arise in connection with such use, reliance upon, and distribution of SUBSCRIBER Content. Notwithstanding anything to the contrary herein, SDS has no responsibility or liability for the accuracy or deletion of SUBSCRIBER Content or any other content, the failure to store, transmit or receive transmission of SUBSCRIBER Content or any other content, or the security, privacy, storage, or transmission of other communications originating with or involving use of the SOFTWARE.

LIMITATION OF LIABILITY.

IN NO EVENT WILL SDS, ITS AFFILIATES, SUBSIDIARIES, OFFICERS, DIRECTORS, EMPLOYEES, CONSULTANTS, AGENTS, SUPPLIERS, LICENSORS, DEALERS, RESELLERS, AND/OR DISTRIBUTORS BE LIABLE FOR ANY LOST PROFITS OR FOR ANY CONSEQUENTIAL, INDIRECT, EXEMPLARY, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES, INCLUDING ANY LOST DATA, ARISING FROM OR RELATING TO

THE SOFTWARE OR THIS AGREEMENT, EVEN IF SDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SDS'S AND ITS AFFILIATES' TOTAL CUMULATIVE LIABILITY IN CONNECTION WITH THIS AGREEMENT AND THE SOFTWARE, WHETHER IN CONTRACT OR TORT OR OTHERWISE, WILL NOT EXCEED 10|% OF THE PURCHASE PRICE OF THE PRODUCT GIVING RISE TO THE CLAIM; PROVIDED THAT IN NO EVENT WILL SDS'S AND ITS AFFILIATES' TOTAL CUMULATIVE LIABILITY FOR ALL CLAIMS EXCEED $2,000. SUBSCRIBER ACKNOWLEDGES THAT THIS PROVISION REFLECTS THE AGREED UPON ALLOCATION OF RISK FOR THIS AGREEMENT AND THAT SDS WOULD NOT ENTER INTO THIS AGREEMENT WITHOUT THESE LIMITATIONS ON ITS LIABILITY.

INDEMNIFICATION.

SUBSCRIBER hereby agrees to indemnify SDS, its affiliates, assignees, dealers and resellers and hold them harmless, and to defend SDS, its affiliates, assignees, dealers and resellers, at SDS's, its affiliates', assignees' dealers' and resellers' request, against any loss, damage or expense (including, without limitation, reasonable attorney's fees) that may be suffered or incurred by SDS, its affiliates and assignees, and claims that may be made against SDS, its affiliates, assignees, dealers and resellers by any person, as a direct or indirect result of use of the SOFTWARE by SUBSCRIBER or its agents, any negligence or misconduct by SUBSCRIBER or its agents, any breach of SUBSCRIBER'S covenants contained herein, the infringement of any trademark or other proprietary rights claimed by a third party (other than the Software), the violation of any laws, directives or standards applicable to the SOFTWARE, the insolvency of SUBSCRIBER or any act or omission of SUBSCRIBER or its agents. The provisions of this Section shall survive any termination or expiration of this Agreement.

COMPLIANCE WITH LAWS.

SUBSCRIBER shall comply with all laws, regulations, rules, ordinances and orders applicable to its use of the Software.

U.S. GOVERNMENT SUBSCRIBERS.

The SOFTWARE is a "commercial item" as that term is defined at 48 C.F.R. 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in 48 C.F.R. 12.212. Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4, all U.S. Government Subscribers acquire the Software with only those rights set forth therein.

ENTIRE AGREEMENT AND CONTROLLING DOCUMENTS.

This Agreement along with the applicable Order contains the entire agreement between the parties with respect to the subject matter hereof, and supersedes all proposals, understandings, representations, warranties, covenants, and any other communications (whether written or oral) between the parties relating thereto and is binding upon the parties and their permitted successors and assigns. Only a written instrument that refers to this Agreement or the applicable Order and is duly signed by both authorized representatives of both parties may amend this Agreement or the applicable Order. The terms and conditions contained in any purchase order issued by SUBSCRIBER shall be of no force or effect, even if the order is accepted. In the event of a conflict in terms among the Agreement and any ordering instrument, the Agreement shall control. This Agreement shall apply to all SOFTWARE ordered by SUBSCRIBER or delivered to SUBSCRIBER, except for services which are explicitly supplied under a separate written services agreement between the parties.

CONSENT TO ELECTRONIC SIGNATURES.

Each party agrees that any electronic signatures, whether digital or encrypted, of the parties included in this Agreement are intended to authenticate this writing and to have the same force and effect as manual signatures. Electronic signature means any electronic sound, symbol or process attached to or logically associated with a record and executed and adopted by a party with the intent to sign such record. By clicking on the "Accept" button, SUBSCRIBER is consenting to the use of SUBSCRIBER's electronic signature in lieu of an original signature on paper.

ASSIGNMENT.

This Agreement shall be binding upon and for the benefit of SDS and SUBSCRIBER and their respective legal representatives, successors, and assigns; provided, that SUBSCRIBER shall not assign or otherwise transfer any of its rights or obligations under this Agreement without SDS's prior written consent. SDS shall have the right to assign this Agreement, or any right or obligation hereunder, without SUBSCRIBER's consent.

DISPUTE RESOLUTION, WAIVER OF COLLECTIVE OR CLASS ACTION, CHOICE OF LAW, STATUTE OF LIMITATIONS.

Any cause of action or claim arising out of or relating to this Agreement or the breach thereof, including without limitation, the validity, enforceability, or scope of this Agreement, shall be settled by binding arbitration in Boston, Massachusetts pursuant to this section and the applicable rules of either J.A.M.S/Endispute (Boston, Massachusetts) or the National Arbitration Forum in effect at the time the claim is filed. Judgment upon the award rendered by the arbitrator may be entered into any court having jurisdiction thereof. The

parties expressly agree that the arbitrator shall have the authority to provide injunctive relief or equitable remedies as necessary including, without limitation, in the event of a breach affecting the non-breaching party's intellectual property or proprietary rights, Confidential Information or business reputation. In addition, SUBSCRIBER agrees that any cause of action or claim will be arbitrated individually and that SUBSCRIBER will not consolidate or seek class treatment for any claims, unless previously agreed to by the parties. This Agreement shall be governed by the laws of the Commonwealth of Massachusetts without regard to (i) its conflict of law provisions, and (ii) the applicability, if any, of the United Nations Convention on Contracts for the International Sale of Goods. ANY CLAIM OR CAUSE OF ACTION, REGARDLESS OF FORM, MUST BE BROUGHT NO MORE THAN ONE (1) YEAR AFTER IT AROSE. OTHERWISE THE CLAIM OR CAUSE OF ACTION SHALL BE BARRED, EXCEPT THAT THE FOREGOING LIMITATION AND THE ARBITRATION PROVISION SHALL NOT APPLY TO THE ENFORCEMENT BY SDS OF SUBSCRIBER PAYMENT OBLIGATIONS OR ANY SDS INTELLECTUAL PROPERTY RIGHTS.

HEADINGS.

The headings to the sections of this Agreement are for ease of reference only and shall not affect the interpretation or construction of this Agreement.

RELATIONSHIP OF THE PARTIES.

SDS and SUBSCRIBER are independent contractors, and nothing in this Agreement shall be construed as making them partners or as creating the relationships of employer and employee, master and servant, or principal and agent between them, for any purpose whatsoever. Neither party shall make any contracts, warranties or representations or assume or create any other obligations, express or implied, in the other party's name or on its behalf.

FORCE MAJEURE.

Neither SDS nor any of its affiliates or providers shall have any liability for any nonperformance or deficiency of performance resulting from the negligence or willful act of SUBSCRIBER or any other person, any act of God, fire, explosion, unusually severe weather, natural disaster, epidemic, pandemic, war, terrorism, riots, governmental entities, default of supplier, damage to machinery or equipment, any disruption in transportation, communications, electric power or other utilities, or other vital infrastructure, any means of disrupting or damaging internet or other computer networks or facilities or any other cause beyond the control of SDS, its affiliates or providers.

NOTICES.

Any demand, notice, consent, or other communication required by this Agreement to be given in writing shall be given either (i) by being hand-delivered to the receiving party, or (ii) by being deposited in the mail (registered or certified) or delivered to a recognized private express common carrier, postage or freight prepaid, addressed to the receiving party at its common address. Electronic mail may be acceptance, if agreed upon in advance by both parties.

WAIVER AND SEVERABILITY.

The waiver or failure of either party to exercise in any respect any right provided for in this Agreement shall not be deemed a waiver of the subject right or any further right under this Agreement. If any provision of this Agreement or the application thereof to any party or circumstances shall be declared void, illegal or unenforceable, the remainder of this Agreement shall be valid and enforceable to the extent permitted by applicable law. In such event the parties shall use their best efforts to replace the invalid or unenforceable provision by a provision that, to the extent permitted by applicable law, achieves the purposes intended under the invalid or unenforceable provision.

13 Support Resources

Email:	support@shooterdetectionsystems.com
Tel:	1-844-746-8911, Option 2
Website Contact Form:	https://shooterdetectionsystems.com/technical-support/
SDS Authorized Dealer Portal:	https://secure.shooterdetectionsystems.com
SDS Learning Management System:	https://training.shooterdetectionsystems.com/