



# SA SERVER INSTALL AND CONFIG

---

SDS INDOOR GUNSHOT DETECTION SYSTEM

Version R5.7.1 Dated 1/03/2024

Change / Rev	Date	Description of Change	Author	Pages Affected
5.6.1	15 Oct 23	Updated per version 5.6.1 of SA application	SSHJ	All
4.2	20 Oct 21	Add Feature table in front, remove references to nodes.csv, add some questions to be answered / filled it. Move detailed setup to Appendix references to APPNotes.	RE / RaF	All
4.1	26 Aug 21	Update for Audit Logging, AD, LDAP, LDAPS, Sensor Config File & Secure SQL Connection	RE	All
3.0	27 Oct 18	Update for R3.0 modifications. SQL, Multi-Server, Remote Admin, new MNS integrations.	RaF	
2.2	20 Jun 18	Update to include SDS License file as an Appendix. Update SW Release to R2.1.4	RaF	Appendix III
2.1	4 Aug 17	Updated for V2.1.1/2/3 modifications. Floorplan Manager, Shot History List, SDS Tester Events.	RaF	All
2.0	28 Nov 16	Update Version and release	RaF	Version only
1.7	26 Jan 16	Updates for standalone server configuration, email notification, mass notification and maintenance.	RaF	All
1.6	6 Jan 16	Added Voice Monitor Configuration and Usage	RTO	Section 4 and 7
1.5	7 Jul 15	Initial Release	RaF	All

Shooter Detection Systems, LLC (SDS) – The SDS Indoor Active Shooter Detection System is a Commercial-Off-The-Shelf (COTS) Product developed entirely at the private expense of SDS. The information contained in this document is proprietary to SDS and shall not be disclosed except as explicitly allowed by SDS. All rights reserved.

Shooter Detection Systems, LLC

300 Newburyport Turnpike

Rowley, Massachusetts 01969

844-SHOT911

[sales@shooterdetectionsystems.com](mailto:sales@shooterdetectionsystems.com)

[support@shooterdetectionsystems.com](mailto:support@shooterdetectionsystems.com)

# Contents

Contents .....	3
List of Figures .....	6
List of Tables .....	8
1 Product Overview .....	9
1.1 Architecture .....	9
1.2 Features .....	10
2 Situational Awareness (SA) Architecture .....	13
3 Installing the SA Server .....	14
3.1 Welcome Screen .....	14
3.2 End User License Agreement .....	14
3.3 Directory and Disc Drive Selection .....	15
3.4 Upgrade Email Templates .....	17
3.5 Database Selection and Configuration .....	18
3.5.1 <i>Configuring a Mongo Database Connection</i> .....	18
3.5.2 <i>Configuring a SQL Database Connection</i> .....	19
3.6 Configuring Firewall Rules for the SA Server .....	19
4 Installing the SA Client .....	20
4.1 Configuring the SA Client .....	20
5 Configuring the SA System .....	21
5.1 Configuring Active Directory (AD) .....	21
5.2 Configuring the “Server Name” .....	21
5.3 SA Server / Gateway Connection (Admin → Gateway Settings) Screen .....	22
5.4 SA Client Appearance Preferences .....	23
5.4.1 <i>Show / Hide Sensor Name on the Floorplan</i> .....	24
5.4.2 <i>Shot Icon Timing Controls</i> .....	24
5.4.3 <i>Clearing Detection History</i> .....	24
5.4.4 <i>Tester Event Icon Timing Controls</i> .....	25
5.4.5 <i>SA Server Communication</i> .....	25
5.5 Floorplans – Configuring and Managing .....	25
5.6 Sites – Creating and Managing .....	26
5.6.1 <i>Creating Floorplans</i> .....	26
5.6.2 <i>Loading New Floorplans</i> .....	27

5.6.3	Deleting Floorplans .....	28
5.7	Sensors - Configuring and Managing .....	28
5.7.1	Add New Sensor: .....	28
5.7.2	Generating a Sensor Configuration File .....	30
5.7.3	Importing Sensors – Initial Import .....	32
5.7.4	Sensor Configuration File – SiteID and Geo Location .....	33
5.7.5	Sensors Window .....	33
5.7.6	Sensor Placement .....	37
5.8	Email Notification – Configuring and Managing .....	38
5.8.1	E-mail Server Configuration .....	38
5.8.2	Notification List Setup .....	39
5.8.3	3 <sup>rd</sup> Party Mass Notification .....	41
5.8.4	Tailoring Notification Message Formats .....	41
5.9	Audit Logs .....	44
5.9.1	Audit Trails in Local Log File (AllEvents.log) .....	44
5.9.2	Audit Trails in SQL Database .....	44
5.10	Managing “Information Pages” .....	44
6	Database Management Tools .....	45
6.1	Database Management .....	45
6.1.1	Database Export ( <b>Mongo DB Only</b> ) .....	45
6.1.2	Database Import ( <b>Mongo DB Only</b> ) .....	46
6.1.3	Write Gateway File .....	46
6.2	Database Backup (Mongo DB Only) .....	46
6.3	Database Connection .....	47
7	Configuring SA Client Access Control .....	48
7.1	Client (Read Only) Access Control .....	48
8	Configuring 3 <sup>rd</sup> Party Mass Notification Systems .....	50
8.1	Everbridge MNS .....	50
8.2	LynxGuide MNS .....	50
8.3	Desktop Alert .....	51
9	Noonlight Emergency Response .....	53
9.1	Configuration .....	53
9.1.1	Enable/Disable and Status Display .....	54
9.1.2	Operation Mode - Active Monitoring .....	55

9.1.3	<i>Operation Mode – Test Modes</i>	57
9.1.4	<i>Noonlight Authentication Token</i>	58
9.1.5	<i>Customer Information</i>	59
9.1.6	<i>Contact Person Information</i>	59
9.2	<b>Status Display</b>	61
9.2.1	<i>“Disabled” Status</i>	61
9.2.2	<i>Active “Alarm” Status</i>	62
9.2.3	<i>“Monitoring Active – Immediate Dispatch” Status</i>	62
9.2.4	<i>“Monitoring Active – Confirmation Prior to Dispatch” Status</i>	62
9.2.5	<i>“Test Mode – SMS Only” Status</i>	62
9.2.6	<i>“Test Mode – Callback / SMS” Status</i>	63
9.2.7	<i>Active “Test Alarm” Status</i>	63
9.2.8	<i>“Connection Issue” Status</i>	63
10	<b>Alertus Mass Notification</b>	64
10.1	<b>Configuration</b>	64
10.2	<b>Testing</b>	65
11	<b>SA Client (Normal Operation)</b>	68
12	<b>SA Server Maintenance</b>	69
12.1	<b>SDS SA Software Upgrade</b>	69
12.2	<b>SDS Server Backups (Recommended Practice)</b>	69
12.2.1	<i>SA Database Backup</i>	69
12.2.2	<i>SDS Indoor Gunshot Detection System Backup</i>	69
12.3	<b>Recovering from an Issue</b>	70
12.3.1	<i>Restoring from a Backup</i>	70
12.3.2	<i>Reinstall the SA Software</i>	71
13	<b>Appendix I – SA SQL Server Database Setup</b>	72
14	<b>Appendix II – Windows Active Directory Setup</b>	73
15	<b>Appendix III – Azure Active Directory Setup</b>	74
16	<b>Appendix IV – SA Audit Reporting Setup</b>	75
17	<b>Appendix V – Monitoring the SA Server</b>	76
18	<b>Appendix VI – Troubleshooting &amp; FAQs</b>	77
19	<b>Support Resources</b>	79

## List of Figures

Figure 1 – SDS Indoor Gunshot Detection System Architecture.....	9
Figure 2 – SA Opening Screen (Floorplan view) .....	13
Figure 3 – SA Welcome Screen.....	14
Figure 4 – SA License Agreement.....	15
Figure 5 – SA Program Directory Selector.....	16
Figure 6 – SA Data Directory Selector.....	17
Figure 7 – Email Notification Templates .....	17
Figure 8 – Database Selection.....	18
Figure 9 – Database Selection.....	19
Figure 10 – Mongo Configuration .....	19
Figure 11 – SA Client / Server Connection Successful .....	20
Figure 12 – SDS SA Server Name .....	22
Figure 13 – Gateway Settings.....	22
Figure 14 – Gateway Restart.....	23
Figure 15 – SDS Gateway Connection Error .....	23
Figure 16 – SA Client Appearance Settings Dialog.....	24
Figure 17 – SA Main Screen.....	25
Figure 18 – Floorplan Manager (Site Management).....	26
Figure 19 – Adding / Selecting Floorplans .....	28
Figure 20 – Adding a new sensor .....	29
Figure 21 – Importing Sensors .....	33
Figure 22 – Manage Sensors .....	34
Figure 23 - Group Select (Group Edit) .....	35
Figure 24 – Selecting a Floorplan for a Sensor .....	35
Figure 25 – Adding a new sensor .....	37
Figure 26 – Sensor Placement.....	38
Figure 27 – Email Server Configuration .....	39
Figure 28 – Email Notification List Management.....	41
Figure 29 – Database Management Dialog.....	45
Figure 30 – Database Backup Dialog.....	46
Figure 31 – Database Configurations .....	47
Figure 32 – Client Management Dialog.....	48
Figure 33 – Password Changed Popup.....	49

Figure 34 – Everbridge Configuration Dialog .....	50
Figure 35 – LynxGuide Configuration Dialog .....	51
Figure 36 – Enable and Configure Remote Admin .....	52
Figure 37 – Noonlight Emergency Response Configuration Menu Option.....	54
Figure 38 – Noonlight – Enable/Disable and Status Display .....	55
Figure 39 – Noonlight – Active Monitor Operation Modes.....	56
Figure 40 – Noonlight – Test Mode Operation Modes.....	57
Figure 41 – Noonlight – Authentication Token .....	58
Figure 42 – Noonlight – Test Mode Operation Modes.....	59
Figure 43 – Noonlight – Test Mode Operation Modes.....	60
Figure 44 – Noonlight – Status Display .....	61
Figure 45 – Noonlight – Disabled Status Display .....	61
Figure 46 – Noonlight – Active “Alarm” Status Display .....	62
Figure 47 – Noonlight – “Monitoring Active Immediate Dispatch” Status Display .....	62
Figure 48 – Noonlight – “Monitoring Active – Confirmation Prior to Dispatch” Status Display .....	62
Figure 49 – Noonlight – “Test Mode – SMS Only” Status Display.....	62
Figure 50 – Noonlight – “Test Mode – Callback / SMS” Status Display .....	63
Figure 51 – Noonlight – Active “Test Alarm” Status Display .....	63
Figure 52 – Noonlight – “Connection Issue” Status Display.....	63
Figure 53 – 3 <sup>rd</sup> Party Mass Notification setting.....	64
Figure 54 – Alertus Configuration Window .....	65
Figure 55 – Alertus Configuration Error – URL and Credentials .....	65
Figure 56 – SDS Trainer Application.....	66
Figure 57 – Alertus Event Dashboard .....	66
Figure 58 – Alertus Event Details .....	67



# List of Tables

Table 1 - SDS Indoor Gunshot Detection System Server Features .....10

Table 2 Sensor Configuration Information.....30

Table 3 - Email/SMS Notification Templates .....42

Table 4 – Email/SMS Notification Template Keys.....43

# 1 Product Overview

## 1.1 Architecture

The SDS Indoor Gunshot Detection system features the world's finest acoustic and IR gunshot detection software. The System includes some number of SDS sensors to provide full coverage of the space to be protected. Via a standard Local-Area-Network (LAN), the SDS 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 **Error! Reference source not found..**

The **Situational Awareness (SA) Tool** consists of two SW components: the SA-Server which is installed on a computer (referred to as the SDS Gateway) and the SA-Client which can be installed on multiple computers. The server supports several different databases and authentication models as discussed below.

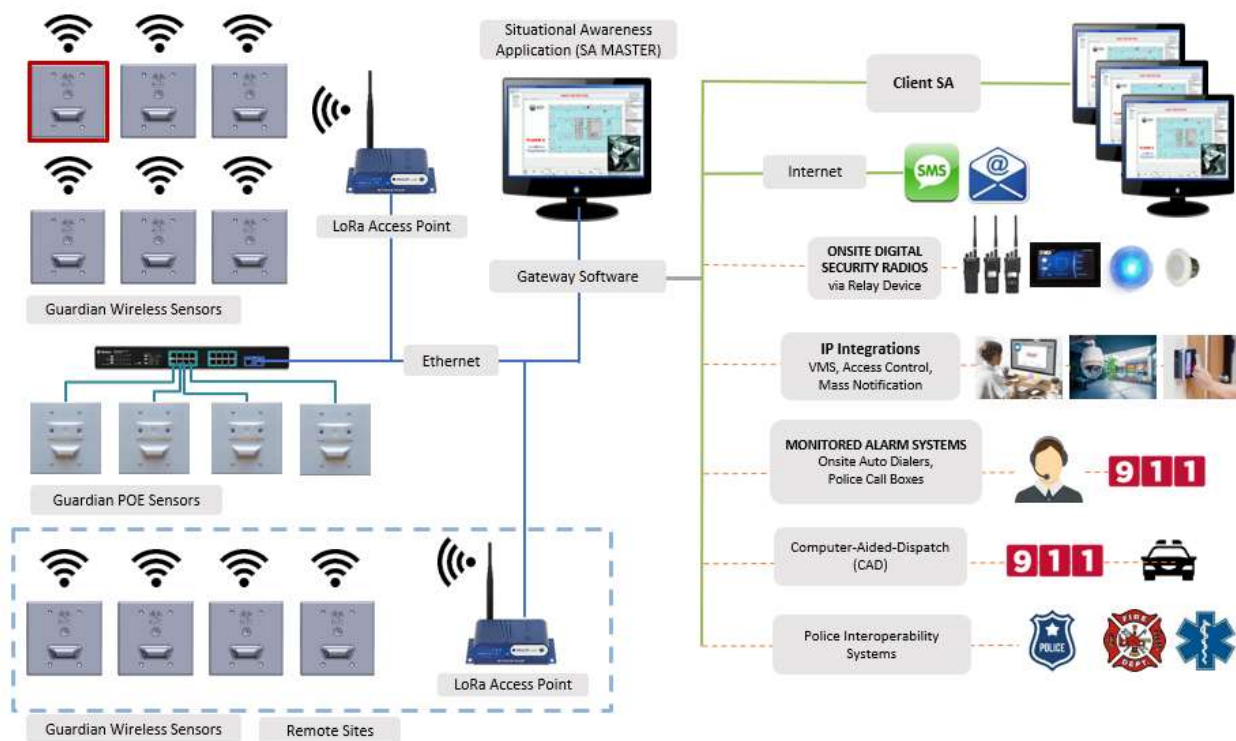


Figure 1 – SDS Indoor Gunshot Detection System Architecture

## 1.2 Features

The SA-Server provides the management portal to the SDS Indoor Gunshot Detection System and includes database and authentication options.

The default server installation installs with a local database (MongoDB) and will allow admin access only for a user logged onto the server.

For larger installations or customers with specific database and authentication requirements, the server software also supports Microsoft SQL DB and either Windows or Azure based Active Directory (AD) authentication.

The table below provides a high-level set of server features and the configuration requirements to support them. This guide provides the details to select and configure all these features as well as the general configuration of sensors, floorplans, and notifications, etc.

Database selection must be made at time of installation. Authentication should be made at time of first system configuration.

**Table 1 - SDS Indoor Gunshot Detection System Server Features**

Feature	Database (Note 1)	Authentication (Note 2)	Comment
SA Client GUI	MongoDB or SQL	Local Admin or Windows / Azure based Active Directory	
Sensor Add/Mod/Del	MongoDB or SQL	Local Admin or Windows / Azure based Active Directory	
GRDN-2000 (PoE)	MongoDB or SQL	Local Admin or Windows / Azure based Active Directory	

GRDN-3000 (Wireless)	MongoDB or SQL	Local Admin or Windows / Azure based Active Directory	
Email / Text Notification	MongoDB or SQL	Local Admin or Windows / Azure based Active Directory	
3 <sup>rd</sup> Party Mass Notification Systems	MongoDB or SQL	Local Admin or Windows / Azure based Active Directory	
Virtual Machine Support	MongoDB or SQL	Local Admin or Windows / Azure based Active Directory	
Non-C drive Program &/or Data Directory	MongoDB or SQL	Local Admin or Windows / Azure based Active Directory	SA Server & Client can be installed in a non-C drive location.
Remote Database	SQL	Local Admin or Windows / Azure based Active Directory	Only SQL (not MongoDB) is supported on a separate machine.
Automatic DB Backups	MongoDB	Local Admin or Windows / Azure based Active Directory	MongoDB is backed up nightly by the SA Server software.
Active Directory Authentication	MongoDB or SQL	Windows / Azure based	Active Directory is available only when using the SQL DB

		Active Directory	
Remote Management	MongoDB or SQL	Windows / Azure based Active Directory	Logging in as an Admin from a separate computer (not server) is limited to Active /Directory & SQL
Audit Logs (Local File)	MongoDB or SQL	Local Admin or Windows / Azure based Active Directory	To log user/admin actions into a local log file any DB/Auth can be utilized.
Audit Logs (in DB)	SQL	Local Admin or Windows / Azure based Active Directory	To log user/admin actions into the DB you must be using SQL.

## **NOTES**

- 1) Admin can select either MongoDB (installed automatically if selected) or SQL (customer must provide) at the time of installing the SW.

**NOTE:** SDS will provide support if converting an existing database from MongoDB to SQL.

- 2) Admin can select the default authentication (Server machine is always Admin), Windows Active Directory or Azure Active Directory. Windows and Azure AD provide the same functionality within the SA Server.

## 2 Situational Awareness (SA) Architecture

The SA is based on a Server-Client architecture in which both the SA Server and a SA Client reside on the Gateway computer. For a standard (default) SA installation, the Client installed on the Gateway computer provides a full Admin (R/W) Console for SA configuration. As of release R4.2 the SA application can be configured to use Active Directory (either Windows or Azure) and this allows users on other machines to also be Admin level access. This remote administration capability is limited to systems with AD enabled.

An SA Client with Admin privileges can load and manage the SDS sensors, floorplans, sensor placement as well as the definition of the notification databases and 3<sup>rd</sup> party integrations. This information is maintained by the SA Server database which can be either a local MongoDB or a SQL database.

The SA Clients provide a graphical display of the floorplans and sensor locations within the installation. Figure 2 (below) shows a map with 15 sensors active (light green icon). This installation includes an additional floorplan which is visible in the floorplan navigation panel to the left.

In the toolbar at the top of the window the “Admin” drop-down menu identifies this as the Admin client. A User client does not have this menu or several other functions. Additionally, at the right top of the screen the user’s access level will be displayed.

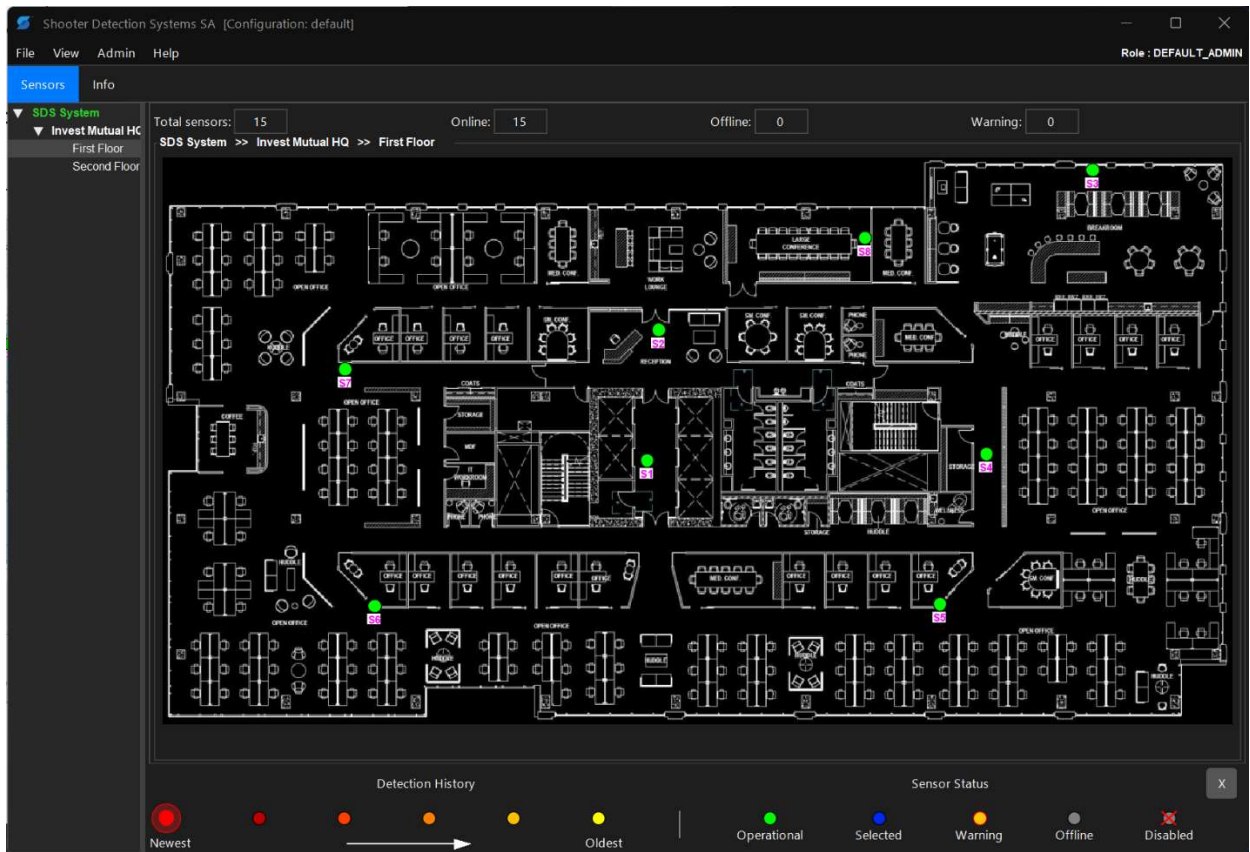


Figure 2 – SA Opening Screen (Floorplan view)

## 3 Installing the SA Server

If the SA Server is to be installed on a machine other than an SDS Gateway PC, load the installation file onto the machine's Desktop. The installation file is named `Installer_GuardianSAServer_XXX.exe` where XXX is the current version.

### 3.1 Welcome Screen

As the installation file is double clicked to launch the install application, the following welcome screen displays application name, version number, and other information.

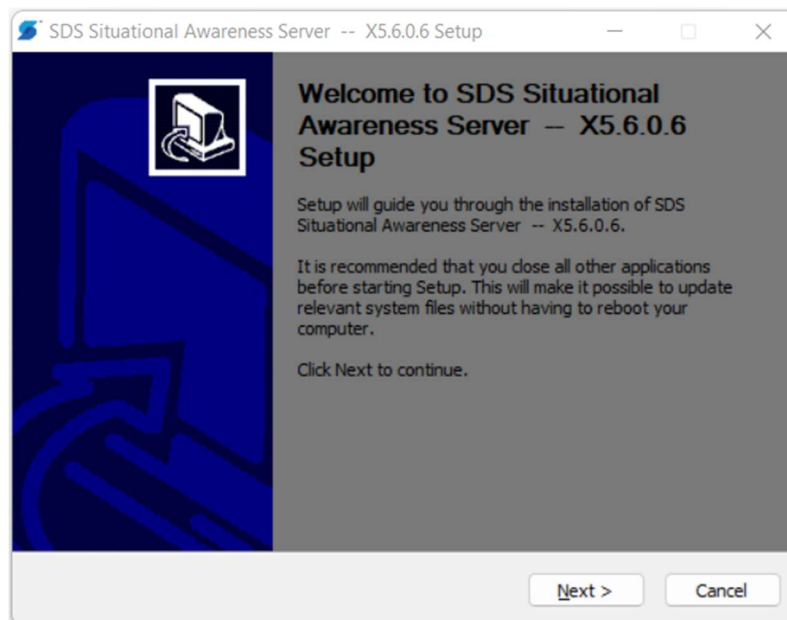


Figure 3 – SA Welcome Screen

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

### 3.2 End User License Agreement

Progressing with installation of the SA Server requires accepting SDS's End User License Agreement presented on the License Agreement screen.

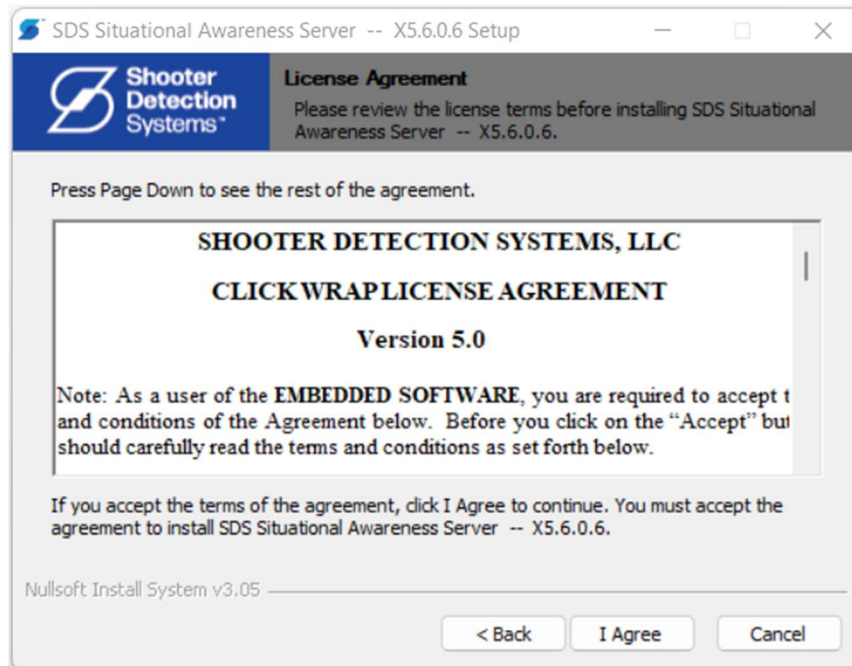


Figure 4 – SA License Agreement

Please click on the “I Agree” button to continue with the installation.

Appendix VII is a copy of the EULA, Version 5.0.

### 3.3 Directory and Disc Drive Selection

During the initial installation of the SA Server you will be prompted for a directory where you want to install the SA Program, refer to the figure below. Once selected this directory will be used for both the SA Server and SA Client programs. The default location is C:\Program Files (x86)\Shooter Detection Systems\SDS Situational Awareness 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\_SA). 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 program directory as \${SDS\_PROG\_DIR}.



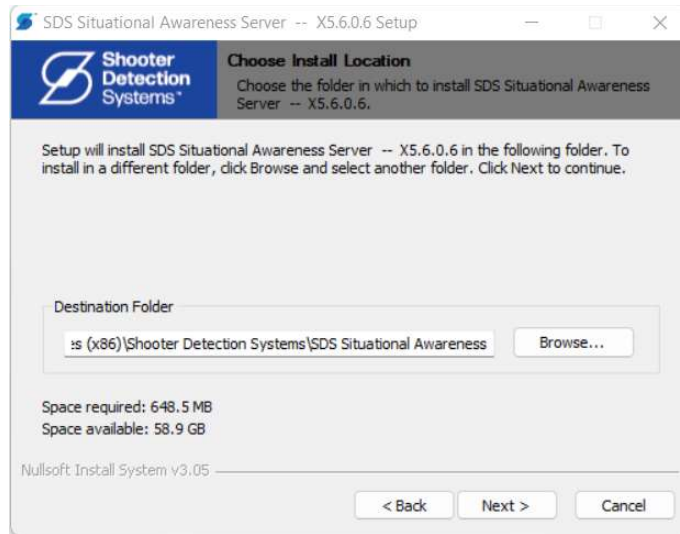


Figure 5 – SA Program Directory Selector

During the initial installation process, you can specify a directory where the SDS configuration files, templates, logs, and other various data files will be kept.

**NOTE:** If you have already installed the SDS Gateway application then this directory is configured, and the SA **will not** ask for a new location. If the SA is the first application being installed, then you will see the dialog below. The default directory is C:\SDSData and it 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 \${SDSData}.

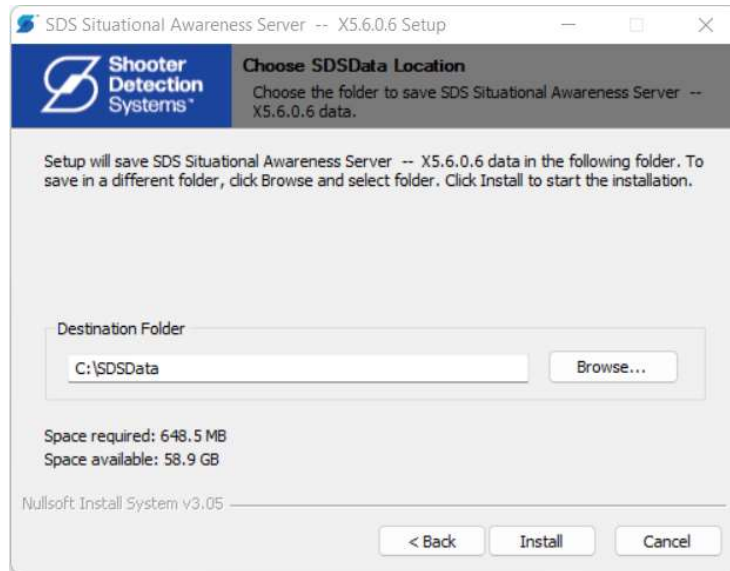


Figure 6 – SA Data Directory Selector

### 3.4 Upgrade Email Templates

Next user is presented with an option to update or keep email notification templates. Email notification templates have been enhanced from the previous versions.

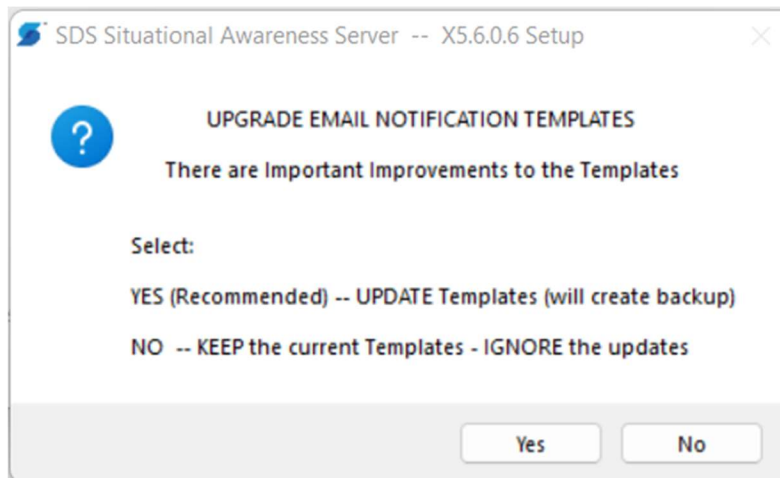


Figure 7 – Email Notification Templates

Select “Yes” or “No” to upgrade or not to upgrade the email templates. SDS recommends selecting “Yes” unless you have previously created custom SMS/Email templates for your organization.

The installation process will proceed with copying application and data files to the chosen directories.

## 3.5 Database Selection and Configuration

### 1. Database Selection (Figure 8)

- a. The SA supports both MongoDB (default) as well as SQL (e.g., SQL Express) databases to manage the system information.
- b. **MongoDB (Local – Self Installing)** – The default configuration (and easiest to configure and manage) is a local MongoDB database. If this meets your needs, then simply select **Next** and the installer will install MongoDB and a database on this machine (refer to Section 3.5.1)
- c. **SQL DB (Local or Remote)** If your requirements are to use a SQL database then select **ADVANCED**, click **Next** and continue with the instructions in Section 3.5.2.

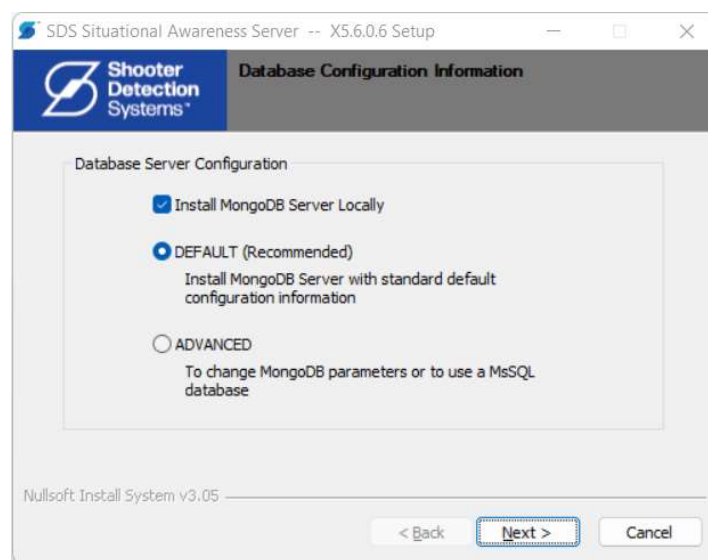


Figure 8 – Database Selection

### 3.5.1 Configuring a Mongo Database Connection

#### 3.5.1.1 Local Mongo Database Server

If you are going to run a Mongo Database hosted on this machine, then the SA installer will manage the installation on the local server as well as configure the connection. In this scenario you will see the installation proceed and when complete you will receive a dialog as you see below. At this point the SA Server database installation and configuration is complete.

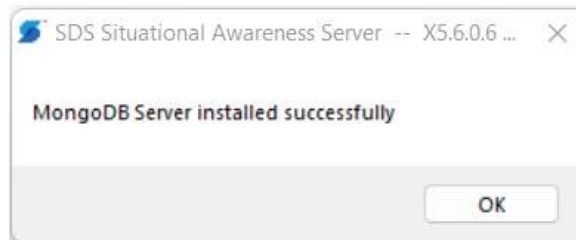


Figure 9 – Database Selection

### 3.5.1.2 Mongo Database Server Advanced Settings

When installing a Mongo database, the end user has the option to change default database setting using the ADVANCED database configuration option. The ADVANCED option gives the end user the ability to change the default DB Name, Username, and Password. The SA Server will then create and connect to the database based on the new settings.

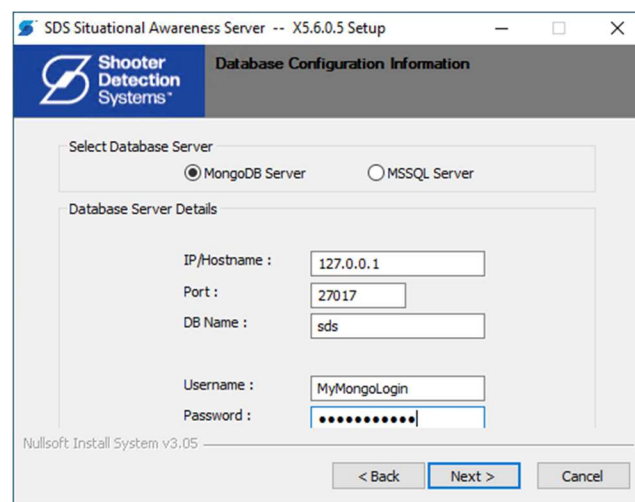


Figure 10 – Mongo Configuration

## 3.5.2 Configuring a SQL Database Connection

It is recommended, for larger systems and/or customers utilizing SQL for other applications, to connect the SDS SA to a SQL Database rather than the default MongoDB. If you are going to use SQL, refer to Appendix I (**APP Note – SA SQL Server Setup**) for instructions to connect to and configure your SQL database.

## 3.6 Configuring Firewall Rules for the SA Server

The SDS SA Server supports the SA Clients on other machines to make “Inbound” TCP connections on a single port: 31006 for TLS. You must enable the Server Firewall to allow these Inbound requests for proper operation.

## 4 Installing the SA Client

The SA Client installer only requires you to read and accept the License Agreement. There are no installation time configuration options. *The SA Server connection parameters will be specified the first time you launch the client.*

**IMPORTANT:** The SA Client is an application, not a service, and does not automatically launch at Windows startup or user login. To configure the SA Client to launch on user login add the SA Client launcher into your Startup Directory.

### 4.1 Configuring the SA Client

The first time the SA Client is launched it will prompt you for a connection to the SA Server, which in this scenario is on the same machine. Simply select **OK** and the Client will proceed by connecting to the Server and synchronizing with the default database (2 empty floorplans) and no sensors. Once the client has connected you will see a Connection Established Successfully dialog.

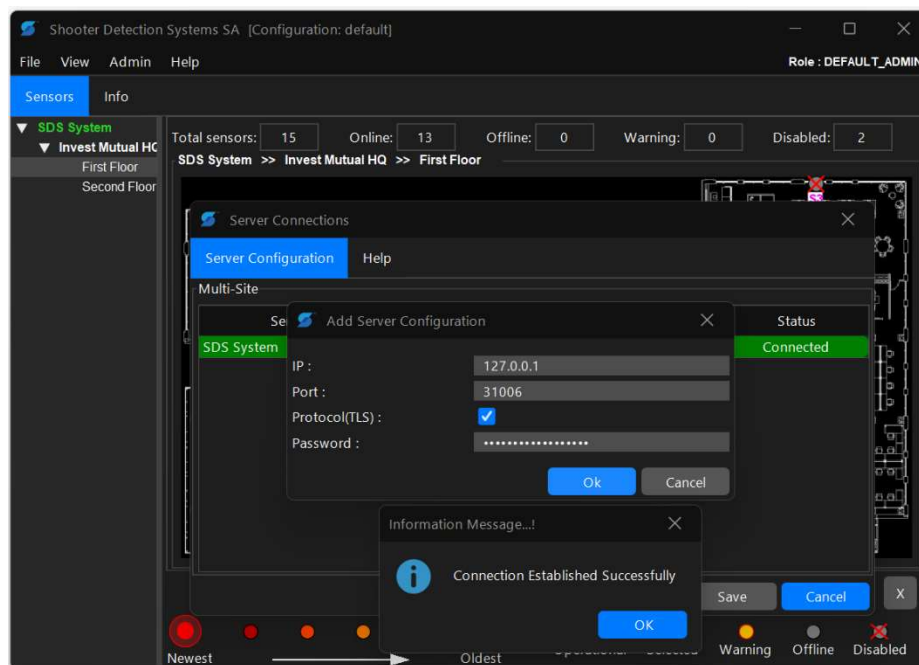


Figure 11 – SA Client / Server Connection Successful

## 5 Configuring the SA System

When the SA Server machine is booted the SA Server services are automatically started. Once configured, the SA server is responsible for communicating Sensor events and information to the SA Clients, Email/SMS notification, 3<sup>rd</sup> Party Mass Notification System integrations as well as user authentication for all SA Client connections. All this functionality is available at Windows startup and requires no admin/user interaction to enable.

### 5.1 Configuring Active Directory (AD)

By default, the SA Server will allow ONLY the SA Client installed directly on the server to have Admin rights. All other SA Clients will be considered User rights which are essentially read/view only.

Starting with Release R4.2 authentication can now be configured to be managed via Active Directory using either the Windows AD or Azure AD services. Using AD does allow you to establish not only the full Admin and the User (view only) but as well you will have privilege levels between these two endpoints. Once configure to use AD all SA Client access will be authenticated via your AD server.

**IMPORTANT:** An important constraint is that when deploying the system using an Active Directory authentication you must use a SQL Database as the MongoDB solution does **NOT** support our Active Directory configuration.

Refer to Appendix II (**APP Note – SA Active Directory Setup**) for detailed information on configuring the SA to work with a Windows Active Directory Server.

Refer to Appendix III (**APP Note – SA Azure Active Directory Setup**) for detailed information on configuring the SA to work with an Azure Active Directory Server.

### 5.2 Configuring the “Server Name”

The SA Client can support multiple SDS Server connections. The default name for a Server is SDS System. It is strongly recommended that you configure a unique meaningful name for each Server based on its coverage or other sever related attributes. If you are deploying a single Server then utilize a recognizable name (New York Public Schools, Invest Mutual, Enterprise Incorporated etc.). The reasoning is that as you configure notifications and communicate event information outside of your organization this Server Name will be included in most of these notifications.

**“Admin” → “Server Name”** will open a dialog and allow you to enter a name for this Server as shown below.

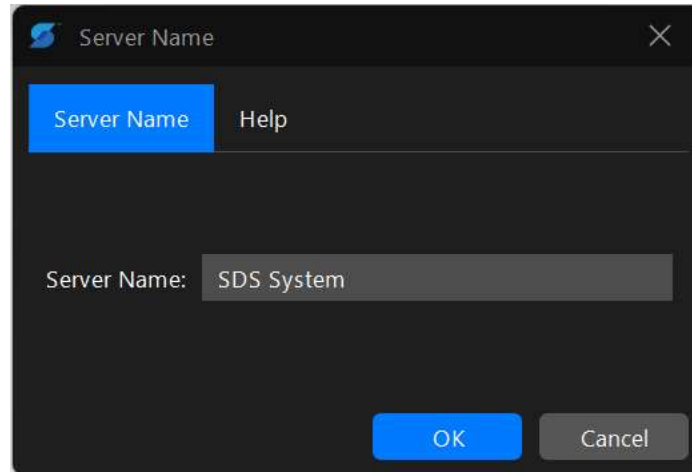


Figure 12 – SDS SA Server Name

### 5.3 SA Server / Gateway Connection (Admin → Gateway Settings) Screen

The SA Server connects to the SDS Gateway application to communicate with the sensors. If the Gateway is installed on the same machine, then there is no configuration required.

If your architecture has the SDS GW and SA Server on separate machines, then you will need to configure the connection using the Client. **Admin → Gateway Settings** will show the Gateway Settings dialog below. Enter the IP information to specify the connection to the Gateway. Do not change the Ports unless you have reconfigured the Gateway defaults.

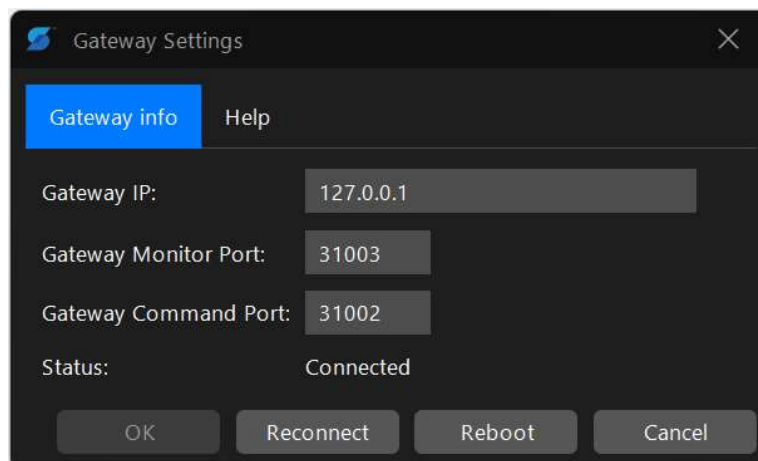


Figure 13 – Gateway Settings

Select OK and the information will be updated, and the system will immediately attempt to connect to the specified Gateway.

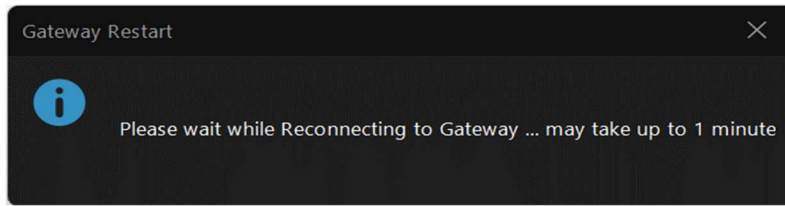


Figure 14 – Gateway Restart

If the Server cannot reach the Gateway (incorrect IP information or Firewall issues) then you will receive the following error dialog. Correct the issue and reconnect to the Gateway.

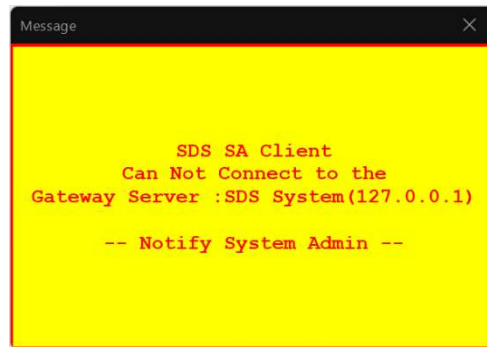


Figure 15 – SDS Gateway Connection Error

## 5.4 SA Client Appearance Preferences

There are several features that can be configured regarding the local SA Client display and operation including whether sensors are shown with a name, the timing of the Shot icons during an event, the timing of the Tester Event icons and the amount of time to wait before informing the user that the Client has lost its connection to the SA Server. The settings are reached by **"File" → "Preferences"**.



The figure below shows the appearance settings available.

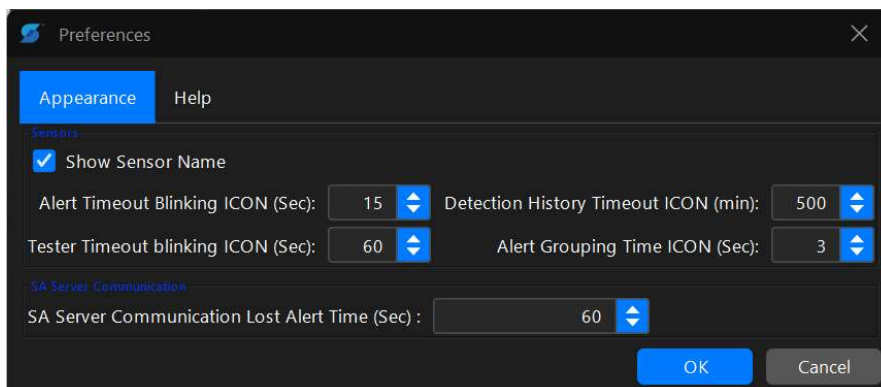


Figure 16 – SA Client Appearance Settings Dialog

#### 5.4.1 Show / Hide Sensor Name on the Floorplan

Each sensor can be shown with a name under it on the floorplan (or shown with no name).

Enable “**Show Sensor Name**” to show the sensor name below the ICON or Disable to show just the icon; Choose “**OK**” when done.

#### 5.4.2 Shot Icon Timing Controls

At the time when a shot is detected on a sensor it is shown as a “blinking” icon. This period of time is referred to as the “Alert” period. After the Alert period, the icon is shown as an enlarged icon with a color denoting its age/sequence and this period is referred to as the “Shot History” period.

- **Alert Timeout Blinking Icon:** SDS suggests using a period of ~10 seconds so that the icon stands out for a period long enough to draw your attention but not too long as to be confused with future shots.
- **Detection History Timeout:** SDS suggest using an extended period (500 minutes → 8+ hours) so that the icon remains visible to show the shooter’s path through a facility while the situation is active.
- **Alert Grouping Time Icon:** Adjustable time for color grouping of sensor icons and shot event window. Shots that fall within the same group will have matching grey bars in the SAs scrolling event window. It is recommended that a value of 3 seconds be set for POE sensors and 8 seconds be set if the system contains wireless sensors.

#### 5.4.3 Clearing Detection History

Detection History can be cleared manually if the event is over or if a “clean” view is needed. *To clear all Shot icons ... click the “Clear All Shots” button in the top right corner just above the shot history panel or right click on the Floorplan pane and select Clear All Alerts.*

**IMPORTANT NOTE:** Once an icon ages out (Shot History Timeout) it cannot be recalled on the Client.

#### 5.4.4 Tester Event Icon Timing Controls

The SA will respond to the SDS Handheld Tester events by displaying a test result banner at the top of the screen as well as showing the tested sensor as a “blinking” icon. The period that the sensor continues to blink is controlled by the Tester Timeout Blinking icon setting. Typically, the default value of 30 seconds will work well with the testing process.

#### 5.4.5 SA Server Communication

When an SA Client loses communication with the SA Server (network or software issue) the user is informed via a pop-up dialog, refer to the SA Client User Guide for more details. The setting on this tab controls the length of time prior to the pop-up being shown. It is suggested that this be set to between 30 and 120 seconds to allow for brief network events but not allow an extended period to occur prior to the notification.

### 5.5 Floorplans – Configuring and Managing

Once connected to the server the SA “Admin” Client is used to configure and manage the Floorplans with your installation. The first step in the process is to create “Sites” which can be thought of as groups of floorplans. Once that is complete you can then create and install floorplans and import the SDS sensor information. The main SA screen is shown in Figure 17.

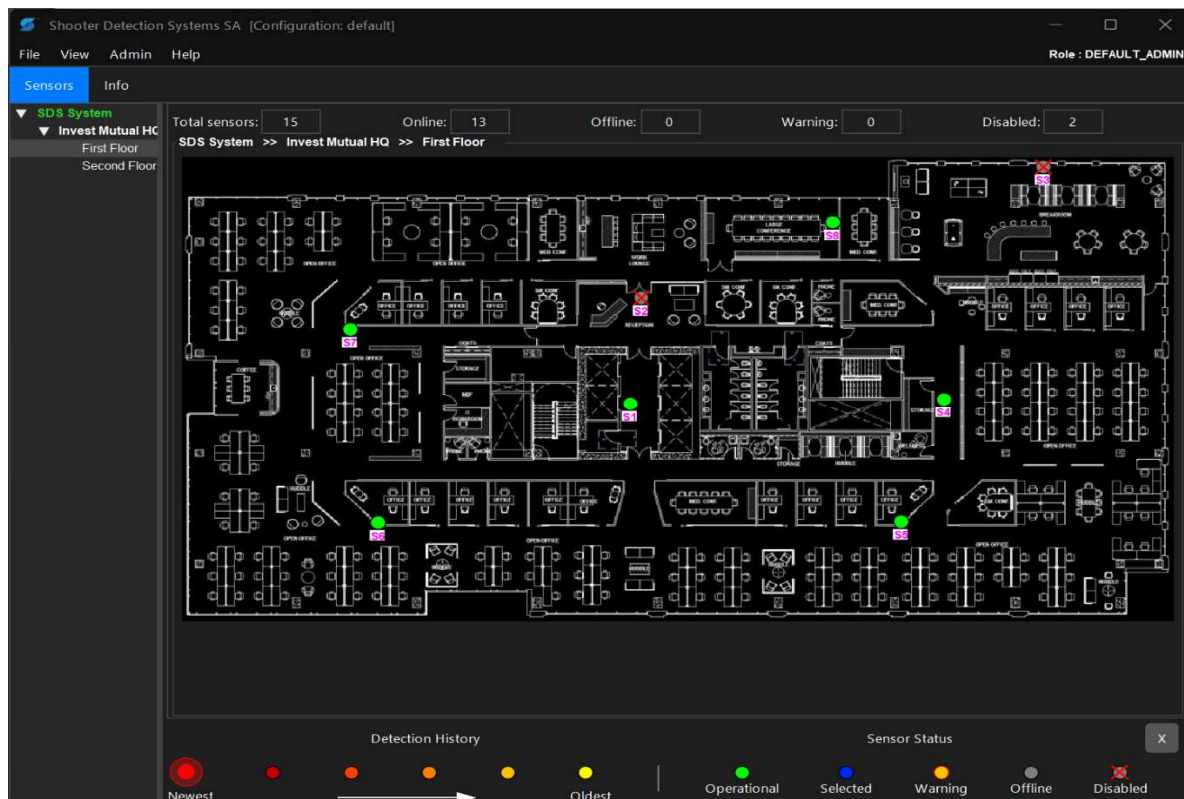


Figure 17 – SA Main Screen

## 5.6 Sites – Creating and Managing

The SA allows for Sites (Sites in this context are **Groups** of floorplans) which can be assigned by the user based on a specific building, portion of a building, or geographic location such as a campus. Individual floorplans are then assigned to each site, building a tree structure of sites with corresponding floorplans as shown in the floorplan navigation panel below. The figure below shows a system with 50 floorplans organized into 10 sites. For this example, the sites are simply named by the floors contained ... but could as easily have been “Capital Building”, “Governors Wing”, “State House Chambers” etc.

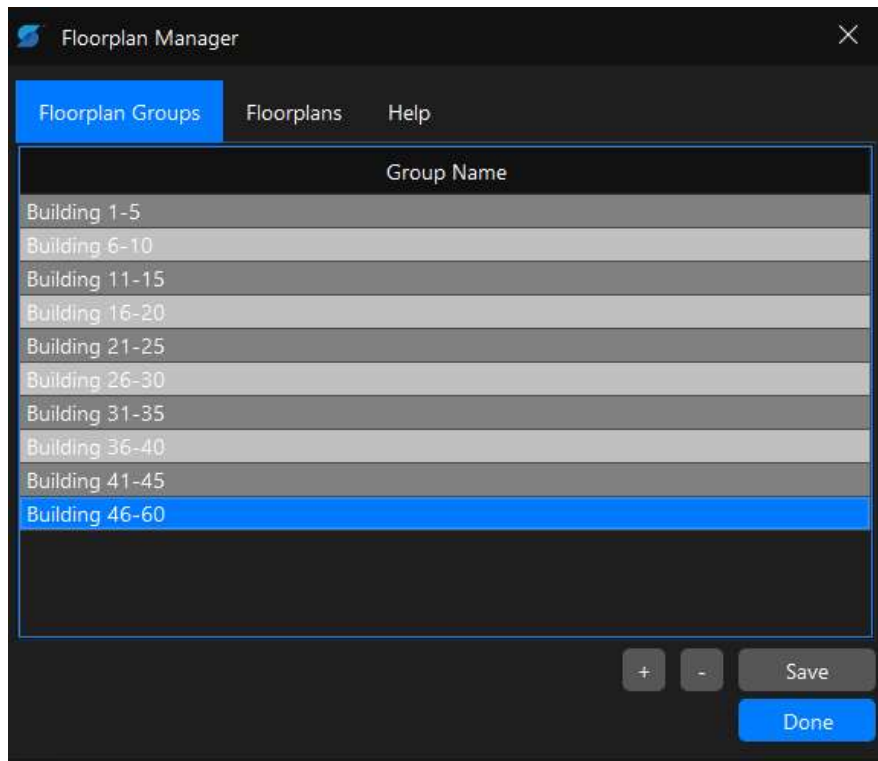


Figure 18 – Floorplan Manager (Site Management)

1. Select “Admin” → “Floorplan Manager” → “Site Management” Tab
2. The default site is named main. This can be renamed by double clicking the site name.
3. Additional sites may be added by clicking the “+” button and adding a name for this site.
4. Add as many sites as required. In the next step floorplans can be added to each specific site
5. Sites may be renamed at any time by double clicking the site name.
6. Sites may be removed by selecting the “-” button however any associated floorplans must first be removed using the **Floorplan Management** tab.

### 5.6.1 Creating Floorplans

Once Sites (if you are using them) have been created the next step is to create and install floorplans representing the installation. The SA utilizes **PNG** (preferred) files as floorplans. The following suggestions are useful when creating a floorplan:

1. Start with an existing floorplan drawing, if available. Open the file (PDF, PPT or other) and display on the screen as large as possible being careful to have all required areas showing.
2. Use the Windows Snipping Tool to capture the required portion of the available plan. Save as a PNG file naming it appropriately.
3. Open the PNG file with an editing tool such as Paint or more advance editor. Clear (delete) notations and information which are too detailed, just leaving enough information to clearly identify key “landmarks” within the building. *A floorplan which is too congested can slow down visual response time / information gathering.*
4. Add annotations to the floorplan as necessary to improve the landmarks.

**NOTE:** PNG File Size – It is recommended that the PNG file size be in the 100-200kB range. Much larger files do not improve usability and can slow down the SA response to an event.

The editing process can be iterative as the SDS SA re-reads the floorplans each time the SA Server is launched. Thus, if the floorplan does not display well, once seen on the SA, it can be modified and then updated by restarting the server (Start Menu).

## 5.6.2 Loading New Floorplans

To add new floorplans first copy the PNG files to \$SDSData\SADData\Server\floorplans with a meaningful name. In the SA tool use the following steps:

1. Select “Admin” → “Floorplan Manager” → “Floorplan Management Tab” and choose “+”.
2. In the Group Selection column select the appropriate site from the drop-down menu. If additional sites/buildings are required add this using the process described above. The default site is named “main”.
3. Enter Floor Name in **Floorplan Name** field. (See Figure 19 (l))
4. Double Click the **Floorplan Image Path** field and browse to floorplan location - \$SDSData\SADData\Server\floorplans (All floorplans must be placed in this location); select corresponding file.
5. Repeat for all floorplans.
6. Choose “OK” when done.
7. The SA will verify that the floorplan file size is OK and if the file is found to be too large will require you to reduce the file size. It has been found that the file-size depends on the file source as much as its content. If the file is too large, then try to generate it as a screen capture or from a different tool.
8. If successful, the floorplans will display on the Start page as shown in Figure 19 (r).

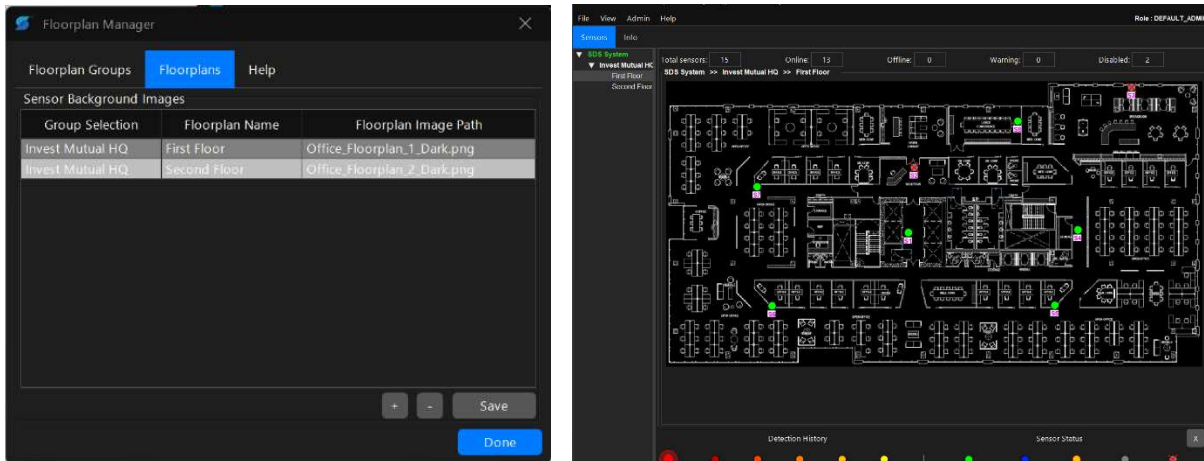


Figure 19 – Adding / Selecting Floorplans

### 5.6.3 Deleting Floorplans

If you need to delete a floorplan then you should remove it from the SA tool (first) and then delete it from the floorplan directory<sup>1</sup> (refer to previous section for directory path).

- Select “Admin” → “Floorplan Manager” → “Floorplan Management” Tab; Highlight the floorplan to delete and choose “-”. Choose “OK” when done.
- Delete the source file in the floorplan directory (\$SDSData\SAData\Server\floorplans).

**NOTE:** It is recommended that you delete extra/unused floorplan files, as they increase backup and DB synchronization time.

## 5.7 Sensors - Configuring and Managing

As of SA version R4.2, all configuration/management (add, modify, and delete) of sensors is controlled from the SA Client using a Sensor Configuration File for large/bulk updates and the SA GUI for individual Add/Modify/Delete.

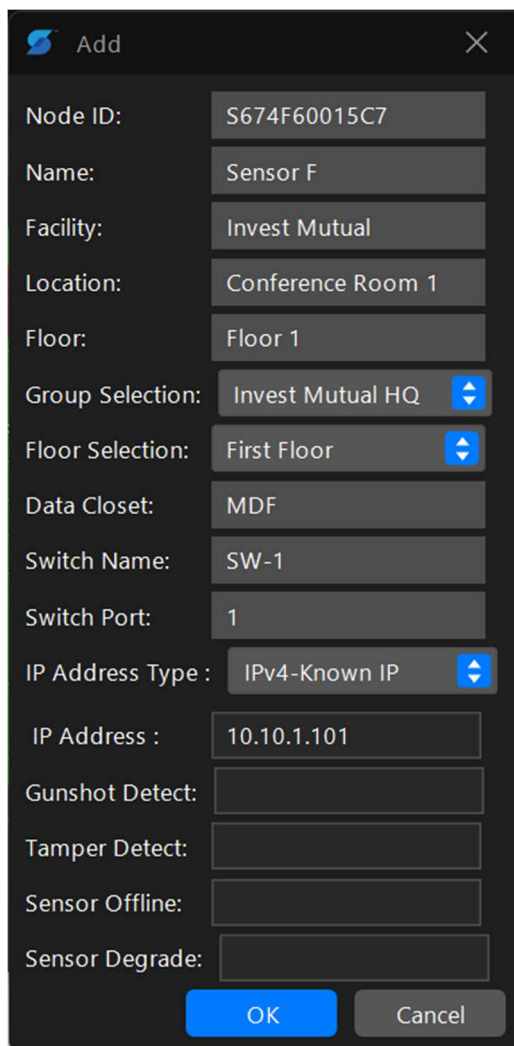
**IMPORTANT:** Historically the sensors were managed via manual editing of the Gateway configuration file, however, starting with SA version R4.0 it is **IMPORTANT** that all sensor adds/deletes/changes be managed via the SA Client UI (either Import, Add/Modify/Delete).

### 5.7.1 Add New Sensor:

Sensors can be manually added to the SDS Server using the “Add New Sensor” button. Adding a sensor with this option will write the new sensor info to Gateway’s configuration file and SA Server

DB. The sensor new sensors will appear on the right side of the opened floorplan as Icon and in the Gateway UI when addition is completed.

Data Closet and Switch names are for reference and troubleshooting only. The last four entries are associated with the optional relay controller. The number added to these fields will correspond with a physical relay on the external relay controller module. Be aware that these relay numbers will be defaulted when installing a new sensor. The Site-ID and sensor Geo Location cannot be entered individually using this method and must use the Bulk method as described earlier.



The screenshot shows a dark-themed 'Add' dialog box with a close button (X) in the top right corner. The dialog contains the following fields and values:

- Node ID: S674F60015C7
- Name: Sensor F
- Facility: Invest Mutual
- Location: Conference Room 1
- Floor: Floor 1
- Group Selection: Invest Mutual HQ (dropdown menu)
- Floor Selection: First Floor (dropdown menu)
- Data Closet: MDF
- Switch Name: SW-1
- Switch Port: 1
- IP Address Type: IPv4-Known IP (dropdown menu)
- IP Address: 10.10.1.101
- Gunshot Detect: (empty field)
- Tamper Detect: (empty field)
- Sensor Offline: (empty field)
- Sensor Degrade: (empty field)

At the bottom of the dialog are two buttons: 'OK' (highlighted in blue) and 'Cancel' (greyed out).

Figure 20 – Adding a new sensor

## 5.7.2 Generating a Sensor Configuration File

The initial importing of sensor configuration information as well as bulk Add/Modify/Delete of sensor information is best accomplished by creating or updating a CSV file.

In the SDS system, it is named as the nodes.csv file and resides in \${SDSData} folder.

**IMPORTANT NOTE:** All header Names are required to be spelled exactly (with exact case) in the spreadsheet. Here is how it should be exactly added as the first row of the nodes.csv file

"Id","IP","MonitorPort","CmdPort","Facility","Floor","Location","Description","DataCloset","SwitchName","SwitchPort","Gunshot Detection","Tamper Detection","Sensor Offline","Sensor Degraded","SiteID"

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

**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
86474F6000201	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
86474F6000202	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
86474F6000203	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
86474F6000204	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
86474F6000205	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
86474F6000206	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
86474F6000207	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
86474F6000208	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
86474F6000209	0	0	0	One Beacon Street	Floor 7	Cafeteria - Entrance	F7-4	MDF-F7	10.10.7.254	4	13	3	3	4	440007
86474F6000210	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
86474F6000211	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
86474F6000212	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
86474F6000213	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
86474F6000214	0	0	0	One Beacon Street	Floor 7	Elevators	F7-9	MDF-F7	10.10.7.254	9	18	3	3	4	440007
86474F6040215	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
86474F6040216	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
86474F6040217	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
86474F6040218	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
86474F6040219	WIRELESS	0	0	One Beacon Street	Floor 1	Lobby - Elevator	F1-5	IDF-F1	10.10.1.254	3	23	3	3	4	440001
86474F6040220	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

Various fields from the Sensor Configuration File are defined below:

- **Id:** This field identification contains the unique 13-characters alpha-numeric serial number of the sensor as identification number of the sensor.
- **IP:** IP address as reported by the sensor.
- **MonitorPort:** Network port for communications with the SDS Gateway application. All communications between the sensor and the SDS Gateway go through this network port.
- **CmdPort:** Network port for communications with the FSA Command interface.
- **Facility:** Facility is intended to include information about the building or area in which the sensor is mounted. Typically, this could include a wing or section of a building. In a scenario where the system spans multiple campuses and buildings this might be extended to include the campus, building, wing etc. as part of the information.
- **Floor:** Floor is exactly as it sounds and indicates the floor where the sensor is installed.

**NOTE:** Currently “floor” is independent of the SA GUI Floorplan configuration but may be replaced by that information in a future SW Release.



- **Location:** Location is intended to provide specific information regarding where in the building the sensor is installed. Depending on the customer's normal building nomenclature this can vary from a simple text label (EG: Main Cafeteria, West Gym, etc.) to a coded location such as Pole M7-3. The information must be selected to be a format that the First Responders and others receiving the notification can quickly understand.
- **Description:** Description is intended to be a short (typically less than 6 characters) description of the sensor which can be shown on the SDS SA Floorplan views below the sensor. As such, if the Description is too long it will clutter/cover the SA Floorplan information. Some examples of useful Descriptions might be a building Pole/Station number, last octet of the IP address or some other easily recognized label.

**NOTE:** If the information is not going to be shown on the SDS SA (or other Floorplan type displays) then Description can be used to carry other information important to the Notifications or 3rd Party integrations.

- **DataCloset:** DataCloset is intended to provide the administrator the name/location of the data closet where the SDS Sensor is plugging into the network. In the case of wired sensors this will typically be the location of the Power-Over-Ethernet switch providing it power and network access. In the case of the battery-operated wireless sensors this can be the location of the Multitech Conduit LoRa Access Point.
- **SwitchName:** SwitchName is intended to provide the administrator the specific Power-Over-Ethernet switch providing a wired sensor its power and network access. In the case of the battery-operated wireless sensors this can be the name of the Multitech Conduit that the sensor is sending LoRa messages to.
- **SwitchPort:** SwitchPort is intended to provide the administrator the specific Power-Over-Ethernet switch port number providing a wired sensor its power and network access. In the case of the battery-operated wireless sensors this can be **NA**.
- **Gunshot Detection:** The number of gunshot incidents detected by this sensor.
- **Tamper Detection:** The number of tamper detection incidents detected by this sensor. Tamper is defined as someone physically tampering with the sensor, moving, uninstalling, orientation, rotating or any other manual operation that would physically alter its position.
- **Sensor Offline:** The number of sensor offline incidents detected by this sensor. An offline incident is defined by the failure of the sensor to communicate with SDS Gateway service. This could denote network issue or SDS Gateway service being down.
- **Sensor Degraded:** The number of incidents where sensor detected a degraded operation either due to hardware failure of IR and/or acoustic sensors, orientation, or tamper issues. A degraded sensor requires human intervention to remove this condition.
- **SiteID:** SiteID must be a numeric integer value (e.g. 4, 332, 231178, etc.) and was added as an optional field to support 3rd Party systems which must perform a data record lookup for the sensor's location. The main example of this is the SDS System integration with Computer Aided Dispatch (CAD) systems where the SiteID is tied to a data record in CAD that identifies the Street Address, Response Action Plan etc. Each sensor can have a unique SiteID allowing very granular record lookup within the 3rd Party System.



Example use case: An example of how the SiteID might be used in a corporate environment would be to encode the campus, building, floor and location as a numeric value and use this (instead of the Sensor ID) to lookup the sensor's location, display and activation information which might be unique to the 3rd Party application. Remembering that the value must be integer an encoding scheme might be:

- Campus – 2-digit code
- Building – 2-digit code
- Floor – 2-digit code
- Location – 3-digit code
- Sensor at
  - Campus 4, Building 12, Floor 8, Location=32,
  - → SiteID 41208032

SiteID column is required in the Sensor Configuration File, even if no values are added in there and it is left blank.

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.

### 5.7.3 Importing Sensors – Initial Import

1. Select **“Admin” → “Import Sensors”**. See Figure 21.
2. Browse to location where Sensor Config File is stored.
3. Select **Sensor Config File** and Choose **“Import”**.
4. Sensors will appear on the right side of the opened floorplan as Icons (green if installed and connected, gray if not).
5. The imported sensors will also be written to the Gateway configuration file and the sensor will be displayed in the Gateway UI.

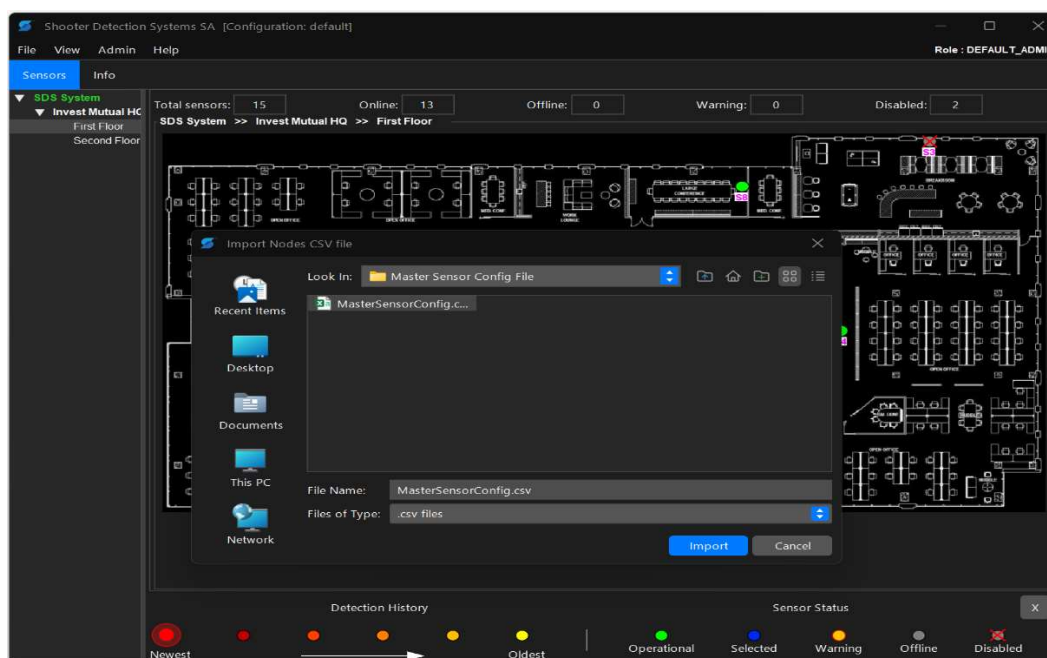


Figure 21 – Importing Sensors

#### 5.7.4 Sensor Configuration File – SiteID and Geo Location

Once the initial sensor information import is completed the Add/Modify/Delete process can be managed within the SA Client GUI. There are a few exceptions to this approach, some just issues of scale (e.g., manually updating 25 sensors within the GUI is time-consuming and error prone) and some are limitations of the GUI as of Release R4.2 (e.g., the GUI currently does not support editing the Site-ID field or any of the Geo Location information).

#### 5.7.5 Sensors Window

This window allows a SA Client User with Admin level privileges to Edit, Add and Delete sensors on the SDS Server. To access it, select File → Sensors.

- **Edit:** Modifying a sensor using this option will update the Gateway configuration file and SA Server DB with the configured parameter changes.
- **Add New Sensor:** Used to add a new sensor to the SDS Server configuration. Adding a sensor with this option will write the new sensor info to Gateway's configuration file and SA Server DB
- **Delete:** If a sensor is deleted or replaced then you will need to use this function to remove it from the SA database and Gateway configuration file.

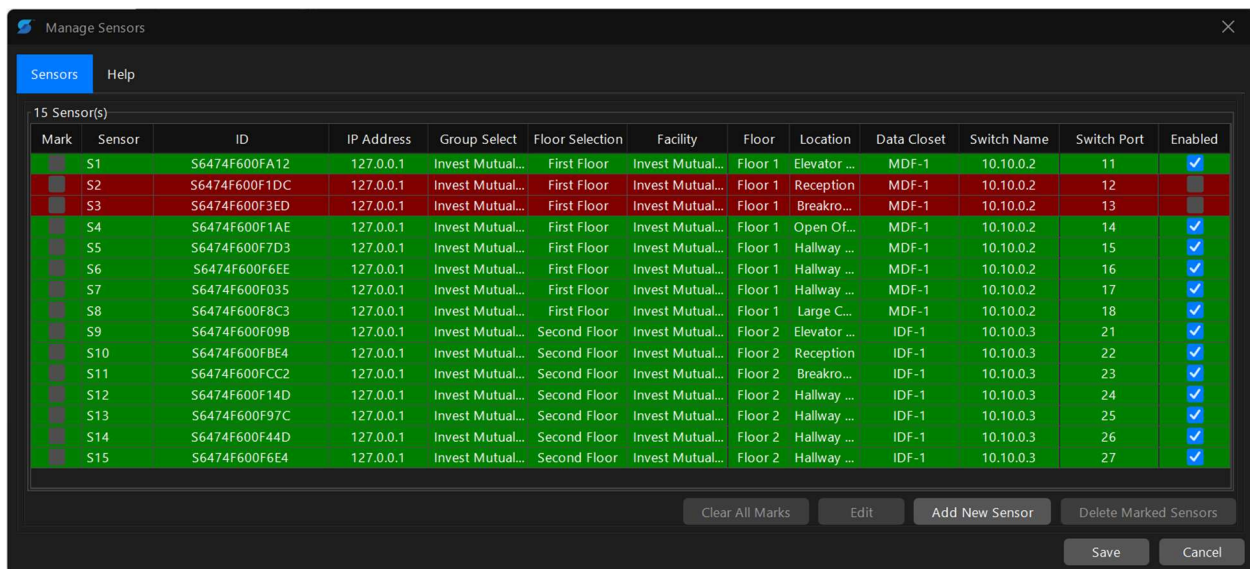


Figure 22 – Manage Sensors

#### 5.7.5.1 Edit a Sensor:

From the Sensors Window, an Admin can select a sensor (or a group of sensors) and then edit the information associated with that sensor(s). All sensor configuration information except “Group Selection”, “Floor Selection” and “Enable” (last column) come from the database.

- Changing the “Group Select”: The Group Selection specifies which SA Site the sensor belongs to. As such, this setting is unique to the SA tool.
  - To change the Group Selection for a single sensor, simply click on the Group Select cell and select the Group from the drop-down list that is provided.
  - To change the Group Selection for a group of sensors, “Mark” each sensor (as shown in the figure) and then change the Group Selection for one of the marked sensors and all marked sensors will be updated.
  - If only one site is required, the default “main” site may be used.

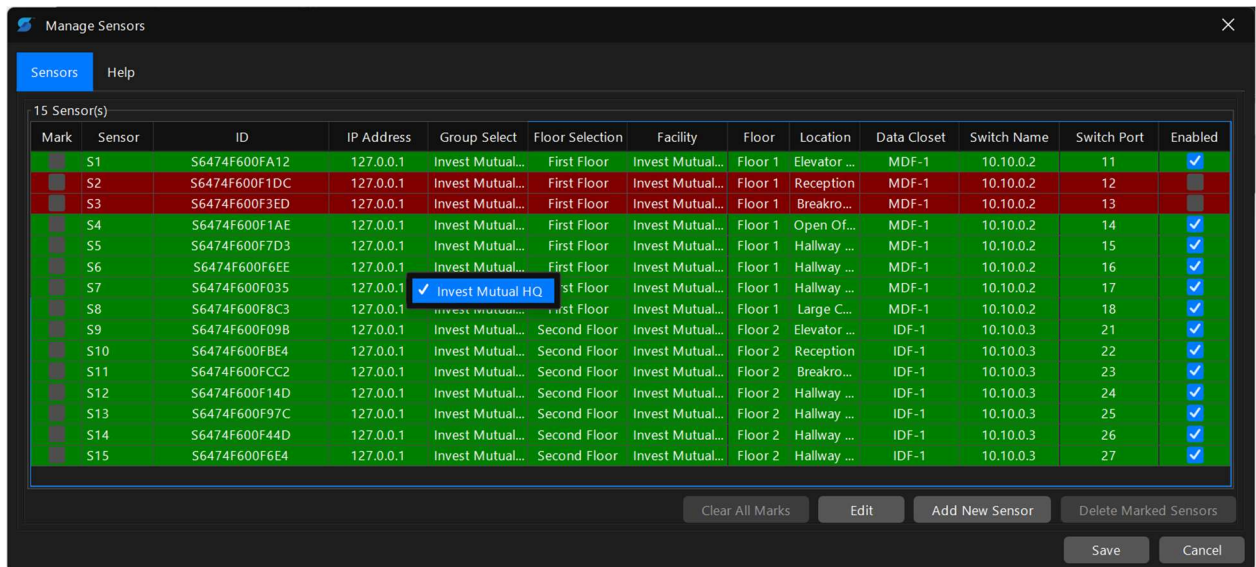


Figure 23 - Group Select (Group Edit)

- Changing the “Floor Selection”: The Floor Selection specifies which SA Floorplan the sensor belongs to. As such, this setting is unique to the SA tool.
  - To change the Floor Selection for a single sensor, simply click on the Floor Selection cell and select the floorplan from the drop-down list that is provided.
  - To change the Floor Selection for a group of sensors, “Mark” each sensor and then change the Floor Selection for one of the marked sensors and all marked sensors will be updated.

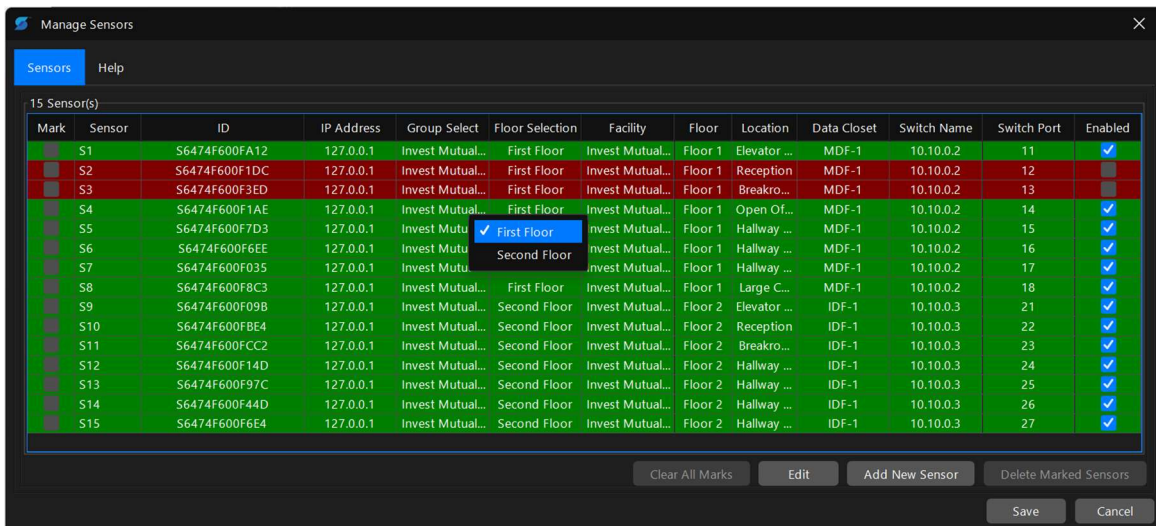


Figure 24 – Selecting a Floorplan for a Sensor

#### 5.7.5.2 Enabling/Disabling a Sensor

A sensor can be disabled when it is not available (e.g. has not been installed or is being replaced). The purpose of disabling the sensor is so that it will not cause Maintenance Notifications to be sent and to show the sensor as not operational on the Gateway and SA UI. ***Due to concerns with leaving a sensor in this state and forgetting to correct the issue – this is not recommended unless it is known that the sensor will not be ONLINE for an extended period.*** To disable a sensor, Uncheck the Enable/Disable box (last column). The Sensor will now be ignored as to its status and the GUI will display the sensor with an “X” through the ICON.

#### 5.7.5.3 Add New Sensor:

Sensors can be manually added to the SDS Server using the “Add New Sensor” button. Adding a sensor with this option will write the new sensor info to Gateway’s configuration file and SA Server DB. The sensor new sensors will appear on the right side of the opened floorplan as Icon and in the Gateway UI when addition is completed.

Data Closet and Switch names are for reference and troubleshooting only. The last four entries are associated with the optional relay controller. The number added to this fields will correspond with a physical relay on the external relay controller module. Be aware that these relay numbers will be defaulted when installing a new sensor. The Site-ID and sensor Geo Location cannot be entered individually using this method and must use the Bulk method as described earlier.

Node ID:	S674F60015C7
Name:	Sensor F
Facility:	Invest Mutual
Location:	Conference Room 1
Floor:	Floor 1
Group Selection:	Invest Mutual HQ
Floor Selection:	First Floor
Data Closet:	MDF
Switch Name:	SW-1
Switch Port:	1
IP Address Type :	IPv4-Known IP
IP Address :	10.10.1.101
Gunshot Detect:	
Tamper Detect:	
Sensor Offline:	
Sensor Degrade:	

OK Cancel

Figure 25 – Adding a new sensor

#### 5.7.5.4 Delete Marked Sensors:

Typically, sensors are not deleted from a system however if you need to delete a sensor(s) then the required steps are:

- In the SA go to, File → Sensors mark the sensor (or sensors) which will cause the Delete button to be enabled.
- Click on “Delete Marked Sensors” - the sensors will be removed from the screen, as well as from the Gateway configuration file.

#### 5.7.6 Sensor Placement

1. Select a Floorplan to place sensors – single click on a floorplan in left pane.

2. Single click (and release) on the sensor icon. The icon will turn blue. Click and hold, drag and drop the icon into its location. See Figure 26 (l). When released the icon will automatically be de-selected, repeat the process if you need to move it again.
3. Repeat for all floorplans and sensors. See Figure 26 (r).

**NOTE:** It is suggested that periodically during this process you run a Database Backup, see Section 12.2.1.

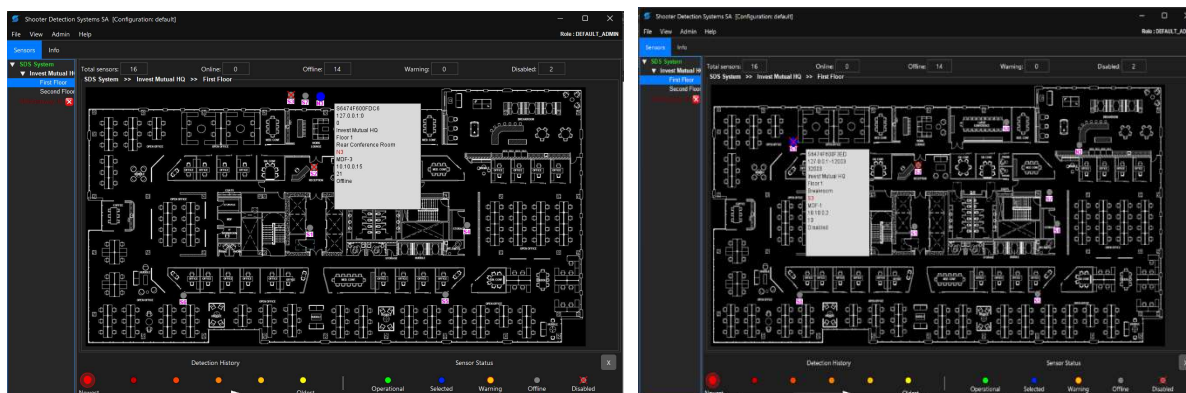


Figure 26 – Sensor Placement

## 5.8 Email Notification – Configuring and Managing

The SDS SA can be configured to send emails/SMS immediately upon the detection of a Gunshot event as well as maintenance required events. To enable this functionality an email server and notification list must be configured.

### 5.8.1 E-mail Server Configuration

1. Select **“Admin” → “Email Server Configuration”**.
2. Enter the email server (smtp server) which will be used for the system. See Figure 27 (l).
3. **“SMTP Server”**: Enter the name (or IP Address) of the email server – for example smtp.gmail.com
4. **“SMTP Port”**: Enter the port number for the server. This setting is typically related to the Security Protocol selected (see next setting). As an example, for the gmail server, TLS is on Port 587 and SSL is on 465.
5. **“TLS”, “SSL”**: Select the Security Protocol used to communicate to the email server. Disable both for plain-text.
6. **“Sending Address (From)”**: This is the email sender’s address shown with the email. This can be any text string – for example AcmeCorp\_SDSSystem.
7. **“Require Authentication”** – Depending on the Email server there are several authentication options: Account required w/ password, Account w/o password, no Account required. If at least an account is required then select this checkbox.



8. **“Email Login Account”**: Enter the account configured for the SA. Can be omitted if the email server has automatic authentication for this computer (make sure that the Require Authentication is not checked).
9. **“Email Login Password”**: Enter the Account’s login password. Can be omitted if the email server has automatic authentication for this account/ machine.
10. **“Maintenance re-notify time”**: Enter the desired number of hours between Maintenance emails. This setting can be set from 1 to 24 hours and has the purpose of controlling the system from sending out a constant stream of emails if, for example, several of the sensors are not connected “OFFLINE”.

**NOTE:** The system will automatically send a “re-notify” about 3 minutes after a problem is first reported – to identify if the issue is a single sensor ... or if other sensors are now being identified as having issues. After this first update, the next update will be sent after the specified re-notify period.

11. **“GGW Lost Connection Notify:”** Enter the number of seconds to allow Gateway communications to be down prior to sending out a Maintenance email. *Recommend 30 – 120 seconds for a typical installation.*
12. Choose **“Configure”** and **“OK”**. See Figure 27 (r).

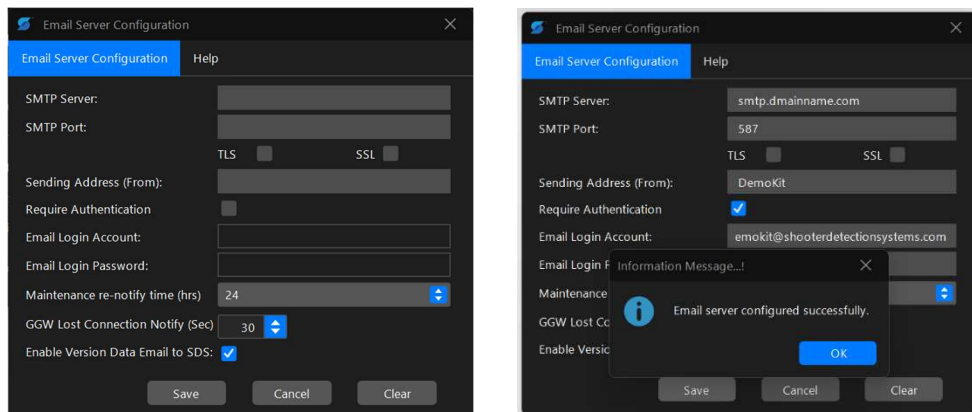


Figure 27 – Email Server Configuration

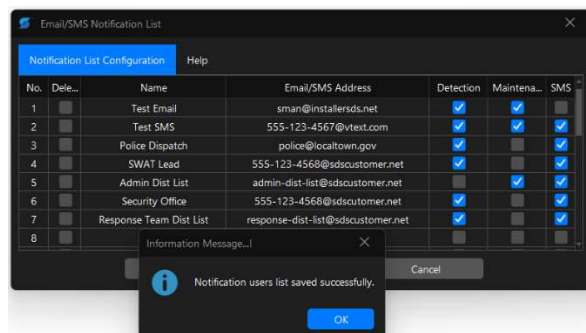
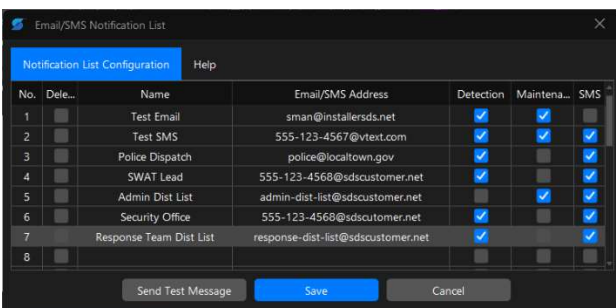
## 5.8.2 Notification List Setup

1. Select **“Admin”** → **“Email/SMS Notification List”**.
2. Entering Email/SMS addresses into the Notification List (enter a test email/SMS and verify setup prior to entering customer’s information):
  - a. The term email/SMS address refers to the fact that cellphone carriers provide the ability to send a phone an SMS message by entering the phone number as part of the email address (for example Verizon uses [9781234567@vtext.com](mailto:9781234567@vtext.com), AT&T uses [9781234567@mms.att.net](mailto:9781234567@mms.att.net)).
  - b. **Select the notification categories:** Each email address must be specified to receive either **“Detection”**, or **“Maintenance”** messages or both using the selection checkboxes.



**NOTE:** To temporarily “disable” a user you can deselect both the Shot and Maintenance messages ... sometimes useful when testing the system.

- c. **Selecting email or SMS:** Additionally, if the address is for an SMS destination, select the “**SMS**” checkbox. Selecting SMS will cause the proper notification template (next section) to be used whereas SMS templates are character limited and standard email templates are more verbose.
  3. Testing the Email Server Configuration (See Figure 28 (l)).
    - a. To test the configuration, enter at least one email and one email/SMS address into the Notification list.
    - b. Choose “Save”.
    - c. Choose “Send Test Message”.
    - d. Each addressee should receive an email or SMS as shown in Figure 28
    - e. If the email configuration information is not correct or the customer’s Firewall rules prevents the email from sending then the SA tool will attempt to send the email for about 30-60 seconds after which you will receive an Error dialogue. If this occurs, correct the configuration and repeat the “Send Test Message”.
  4. Removing a Notification recipient:
    - a. To remove a notification list entry, select the “Delete” checkbox for that entry. Choose “Save”.
    - b. To temporarily disable a recipient, uncheck both Shot and Maintenance, “Save”.
    - c. To close the window, choose “Cancel”.
    - d. Select “Admin” -> “Notification List” to re-open the window and verify the deleted recipient has been removed.
- NOTE:** If the email/SMS addresses used to test the configuration are not intended for the final list then remove them now.
5. **Notification List:** Up to 25 email addresses may be added to this list with proper message category and SMS selections for each. Choose “**Save**” when complete. See Figure 28 (r). Alternatively, the customer can choose to set up mailing distribution lists on their own server and enter just the email addresses for these lists. In this case it is recommended that a total of 4 distributions lists be created and referenced: a) Shot detection email, b) Shot detection SMS, c) Maintenance email, d) Maintenance SMS.
  6. Open the Notification List Configuration window and select the **Send Test Message** to verify that all the addresses and information is correct. *Each time the email configuration or notification lists are changed it is strongly recommended to test the changes in this manner.*



### 5.8.3 3<sup>rd</sup> Party Mass Notification

The SDS SA has been integrated with several 3<sup>rd</sup> Party Mass Notification systems. Refer to [Section 8](#) for configuration information.

### 5.8.4 Tailoring Notification Message Formats

The SA System will automatically send either email or SMS messages to those addresses listed in the Notification list. The message templates are contained in `$SDSData\SADData\Server\notification_templates`. The templates are generally unique between email and SMS to allow for more information in the email and less to be SMS compatible.

These may be customized per company policy or company specification. Currently there are nine default templates – Shot detections (2), Maintenance (2), Test Message (2), Normal Operation / All Clear (2) and GW Connection (1). Their file names are given in the following table.

Table 3 - Email/SMS Notification Templates

Template File Name	Email or SMS	Template Description / Use
det-email-template.ftl	Email	Shot Detection
det-sms-template.ftl	SMS	Shot Detection
license-email-template.ftl	Email	Application License Issue
license-sms-template.ftl	SMS	Application License Issue
main-email-template.ftl	Email	Maintenance/Admin Issue
main-sms-template.ftl	SMS	Maintenance/Admin Issue
mns-configuration-error-template.ftl	Both	Everbridge Account Configuration Issue
mns-connectivity-template.ftl	Both	Everbridge Account Connectivity Issue
normaloperation-email.ftl	Email	Maintenance – All Clear
normaloperation-sms.ftl	SMS	Maintenance – All Clear
test-email-template.ftl	Email	Test Message – Verify notification list
test-sms-template.ftl	SMS	Test Message – Verify notification list
connectivity-template.ftl	Both	Gateway Connection Lost
sds-email-support.ftl	Email	SDS Support Contact

There are several KEYS whose information is taken from various entries in the SA Server's database such as the Sensor information, Server Name, Email configuration dialog and the Server's system clock. Note that email's "Send From" field is configured in the Email Server Configuration dialog.

When customizing any of these templates ensure that you include the information you need, include any valid KEYS (see below) and then overwrite the original file, saving the edited file in the same folder with the original name.

Refer to Table 3 below for all the KEYS and their information source.

**Table 4 – Email/SMS Notification Template Keys**

KEY	KEY Source	Where Used (see notes)	Description
\${DATETIME}	SW	All	Date and time from SA Server computer clock
\${FACILITY}	DB-Sensors	Group 1	Data from <b>Facility</b> field
\${FLOOR}	DB-Sensors	Group 1	Data from <b>Floor</b> field in nodes.csv.
\${LOCATION}	DB-Sensors	Group 1	Data from <b>Location</b> field in nodes.csv
\${MESSAGE}	SW	Group 2	SW generated information
\${NAME}	DB-Sensors	Group 1	Data from <b>Description</b> field in nodes.csv.
\${SENSORID}	Sensors	Group 1	Data from <b>Id</b> field in nodes.csv.
\${SENSORIP}	Sensors	Group 1	Data from <b>IP</b> field in nodes.csv.
\${SEN_DEGRADED}	SW	Group 2	# of Sensors currently reporting a maintenance issue.
\${SEN_ENABLED}	SW	Group 2	# of Sensors enabled in the system. Unless admin has disabled 1 or more this is the total sensor count.
\${SEN_OFFLINE}	SW	Group 2	# of Sensors currently not communicating with the SA.
\${SHOT_SOURCE}	SW	Shot Detect	Data from the sensor message ... reports as a shot detection or a simulated shot.
\${SYSTEM_NAME}	See desc	All	SA Server name configured in Admin GUI.
\${WARN_DESC}	SW	Group 2	Data from the SA Server software.

**Testing your changes.** It is critical that you verify any changes made to the Template(s) to ensure that there are no issues with the Keys or formatting. While verifying the templates, be sure to test both email and SMS notifications. The templates can be tested using the following steps:

- Using the Notification List management page – send a Test message.

- Active Shooter Trainer tool: a) Test shots, b) Maintenance events. Tests “detection templates, “maintenance templates, and “normal-operation” templates.
- Close the SDS GW application and after the configured amount of time (default is 60 seconds) the connectivity notification will be sent.

## 5.9 Audit Logs

The SA Server supports the capability to record system configuration changes and information regarding the source of the change. By default, the logging will be added to a local log file, however, it can also be configured to be written into a SQL database.

### 5.9.1 Audit Trails in Local Log File (AllEvents.log)

By default, audit information will be written to a local SA log file (AllEvents.log). The audit information is clearly identified by the tag “AUDIT” within that file. The information will include the User (Windows Login), the time and the action taken to change the SDS Indoor Gunshot Detection System configuration.

### 5.9.2 Audit Trails in SQL Database

If it is a requirement to provide the Audit Logging information within a SQL Database environment and your SDS Indoor Gunshot Detection System is configured using a SQL Database then you can build a separate database on the server to store Audit information from the SA. If you are going to configure your Audit information to be stored in SQL, refer to Appendix V (**APP Note – SA Audit Reporting Setup**) for instructions to connect to and configure your SQL database.

## 5.10 Managing “Information Pages”

The SA tool provides an area where the admin can locate “Information Pages” so that they are easily accessed during critical events (such as an Active Shooter situation). To see an example of an Information page in the main GUI window Click on the “Info” tab and you will see the default Information Page that is loaded with the SA tool. This is intended to be a way to quickly locate some key contact or action plan information. Likewise, information such as Sys-Admin contact information can be stored here.

To add or delete Information Pages, “Admin” → “Info Page Manager”. Using the dialog, you can add / delete pages as well as name/re-name them. The files must be PNG files (refer to Floorplan section regarding creating PNG files) and they should be placed in the \$SDSData\SAData\Server\resources directory. The easiest way of “adding” a single sheet is to replace the InfoPage1.png file that is in that directory and restart the system.

## 6 Database Management Tools

The Admin has several tools which can be useful in configuring, managing and updating the SDS SA Database. *In addition to these built-in tools you should also follow the instructions regarding Server Maintenance, Section 12.*

### 6.1 Database Management

“Admin” → “Database Management” will open the dialog shown below, providing the details regarding the current database. Additionally, the Database Import/Export buttons will be available.

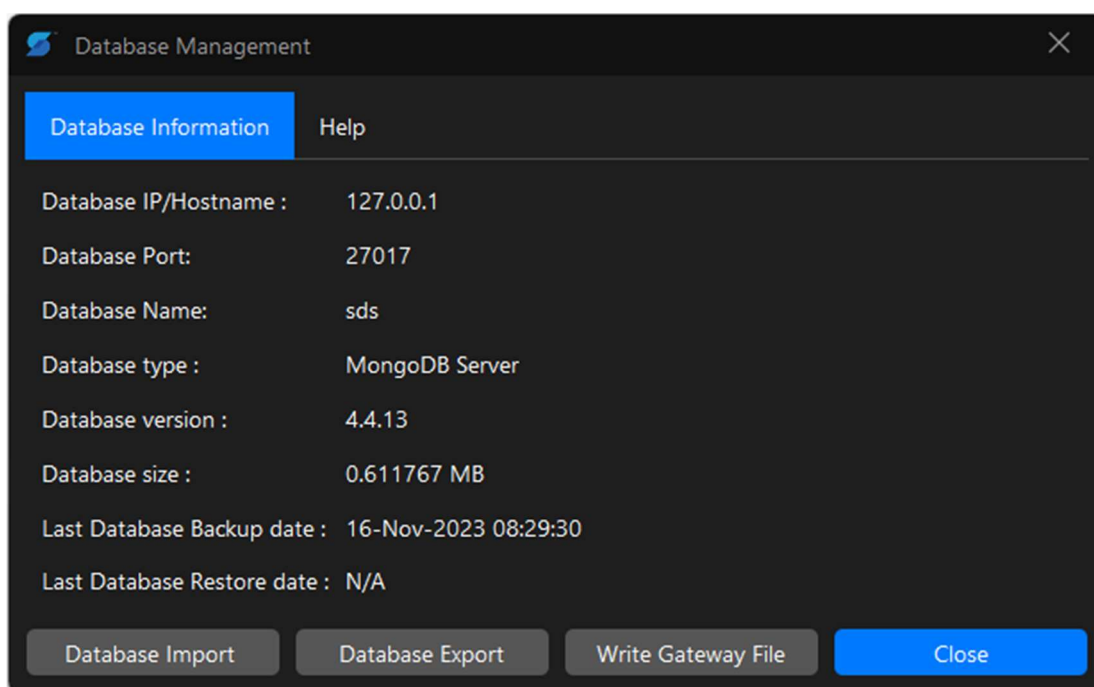


Figure 29 – Database Management Dialog

#### 6.1.1 Database Export (Mongo DB Only)

Selecting **Database Export** will open a file dialog (default location is \$SDSData\backup) and allow you to export the current database as a compressed file. The generated filename includes the database type and the current date and time.

The exported database contains all information necessary to recover the SA Server and local client should an issue occur in the future. *The export does **not** contain the SDS Gateway information ... it is limited to the SA.*

### 6.1.2 Database Import (Mongo DB Only)

Selecting **Database Import** will open a file dialog (default location is \$SDSData\backup) and will show prior Export files. Select the file which you want to import, and the system will import the prior database, stop and restart the SA Server and synchronize all clients to the restored database.

**NOTE:** You will likely see a pop-up from the Client regarding being disconnected from the Server due to the restart process.

### 6.1.3 Write Gateway File

Updates the Gateway configuration file to ensure it is synchronized with any Database changes which were made (e.g., Database Import).

## 6.2 Database Backup (Mongo DB Only)

“Admin” → “Database Backup” will open the dialog shown below, providing a configuration page to setup automatic backups.

By default, the SA Server will be configured to take a daily backup at 2AM (Time is 24hr clock) and to use no more than 250MB of disc space for the backup. The disc space will be managed by removing the oldest backup if this limit is reached.

Each of the parameters can be adjusted to meet your requirements.

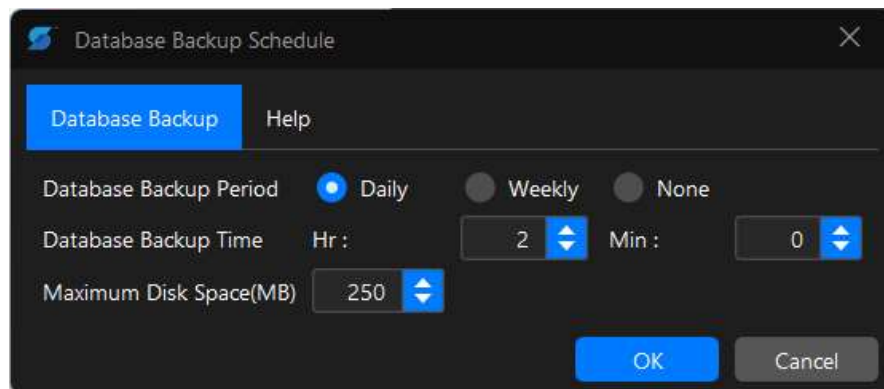
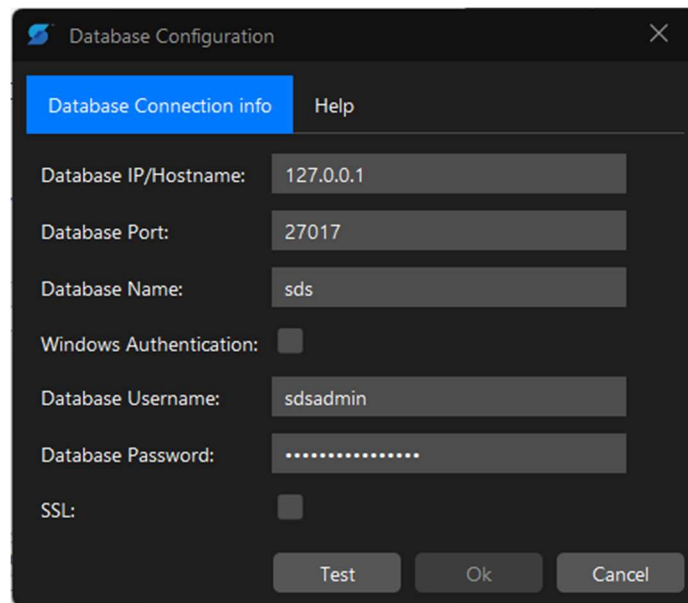


Figure 30 – Database Backup Dialog

## 6.3 Database Connection

“Admin” → “Database Configurations” will open the dialog box shown below. This window provides information regarding the current (**Mongo or SQL**) Database Connection. Database connection parameters can be edited to update the database connection if a change is required.



The screenshot shows a 'Database Configuration' dialog box with a dark theme. It has a title bar with a blue icon and a close button. Below the title bar are two tabs: 'Database Connection info' (selected) and 'Help'. The main area contains several configuration fields: 'Database IP/Hostname' with the value '127.0.0.1', 'Database Port' with '27017', 'Database Name' with 'sds', 'Windows Authentication' with an unchecked checkbox, 'Database Username' with 'sdsadmin', 'Database Password' with masked characters '.....', and 'SSL' with an unchecked checkbox. At the bottom are three buttons: 'Test', 'Ok', and 'Cancel'.

Field	Value
Database IP/Hostname	127.0.0.1
Database Port	27017
Database Name	sds
Windows Authentication	<input type="checkbox"/>
Database Username	sdsadmin
Database Password	.....
SSL	<input type="checkbox"/>

Figure 31 – Database Configurations



## 7 Configuring SA Client Access Control

The SA Server can be configured with a customer specified password for SA Client connections.

“Admin” → “Client Management” will open the dialog shown below.

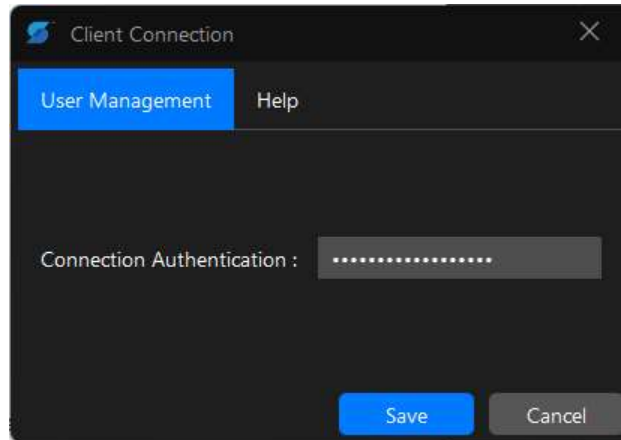


Figure 32 – Client Management Dialog

### 7.1 Client (Read Only) Access Control

“**Client Password:**” is the connection authentication that is used to authenticate any SA Client attempting to connect to the Server.

*There are several items to be aware of when changing this Password:*

1. All of the SA Clients, when they attempt to reconnect to the Server, **will** show the Server as Disconnected and/or will show a “password has been changed” dialog, Figure 33. Each user will have to go into the “File” → “Server Connect Configuration”, select the affected Server and re-enter the Client Password.
2. If you are remotely managing the Server, and you change the Client Password from this remote client you will have to close and re-open the Client and then follow the instructions above to reconnect to the Server. *If you have made a mistake when changing the password ... refer to the next bullet.*
3. The SA Client installed on the SA Server machine is **always** able to connect to the Server. If you make a mistake and/or forget the Client Password for the Server, you can access the server through this client and change the password to a known setting.

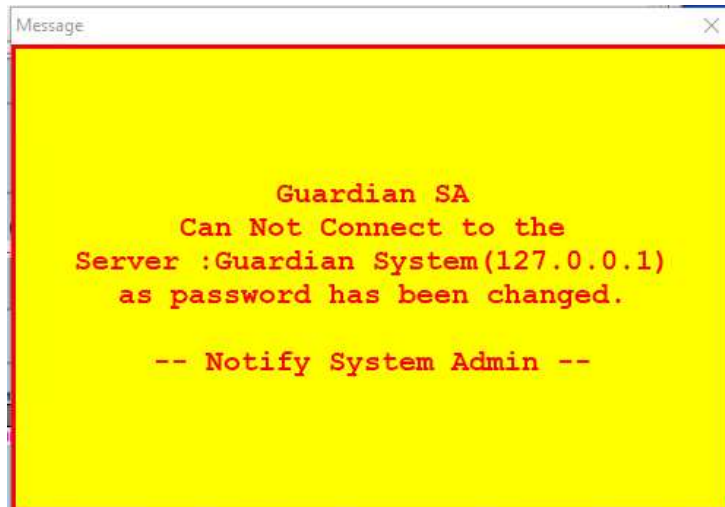


Figure 33 – Password Changed Popup

**NOTE:** Default SA Client password is: **SDSGuardianGateway**

## 8 Configuring 3<sup>rd</sup> Party Mass Notification Systems

Many of SDS Indoor Gunshot Detection System integrations are connected directly to the SDS Gateway application. In addition to those integrations currently three Mass Notification Systems (MNS) are integrated with the SDS SA. These are Everbridge, LynxGuide and Desktop Alert.

### 8.1 Everbridge MNS

SDS Indoor Gunshot Detection System provides a direct data integration with Everbridge. This integration requires you to configure several connection parameters in the SA 3<sup>rd</sup> Party MNS configuration as well as configure variables and templates within your Everbridge account. Please refer to the **Guide\_GuardianEverbridge** integration guide for details. *The document is posted to the SDS Partner Portal. If you do not have access to the Portal, please contact SDS Support.*

NOTE: Everbridge is a licensed integration – you must install the proper license on the SDS Gateway to enable this integration.

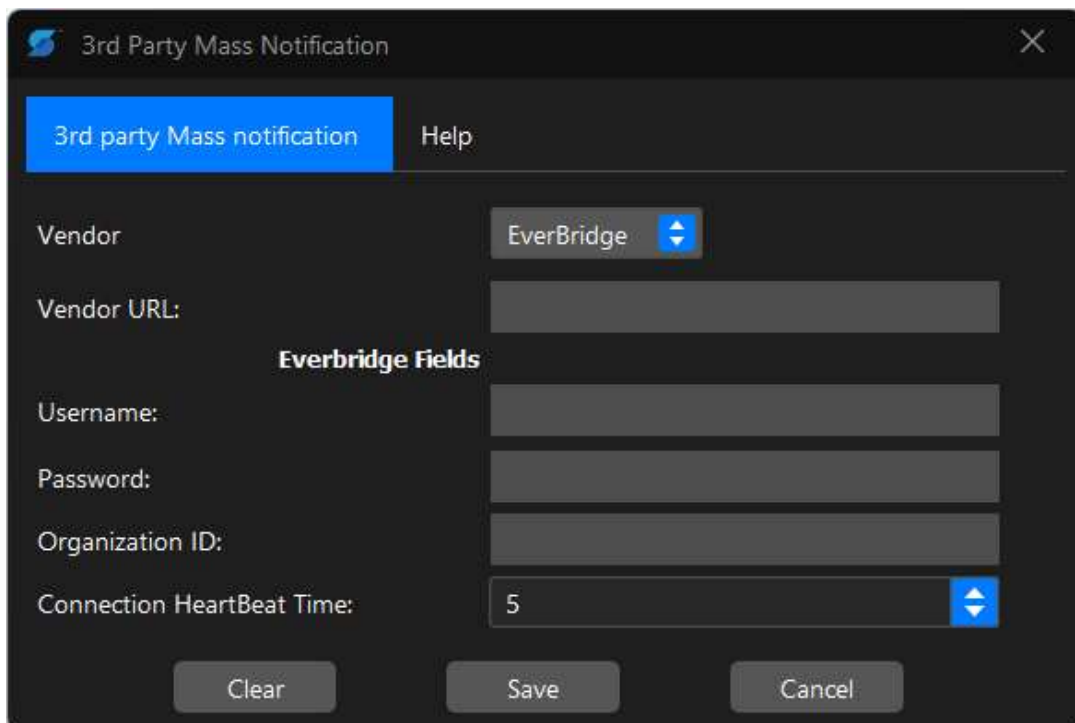
The image shows a software dialog box titled "3rd Party Mass Notification" with a close button (X) in the top right corner. Inside the dialog, there is a tab labeled "3rd party Mass notification" and a "Help" link. The "Vendor" field is set to "EverBridge" with a dropdown arrow. Below it is a "Vendor URL:" field. A section titled "Everbridge Fields" contains four input fields: "Username:", "Password:", "Organization ID:", and "Connection HeartBeat Time:". The "Connection HeartBeat Time:" field has the value "5" and a dropdown arrow. At the bottom of the dialog are three buttons: "Clear", "Save", and "Cancel".

Figure 34 – Everbridge Configuration Dialog

### 8.2 LynxGuide MNS

SDS Indoor Gunshot Detection System provides a direct data integration with the LynxGuide server. This integration requires you to configure several connection parameters in the SA 3<sup>rd</sup> Party MNS configuration as well as configure variables and templates within your LynxGuide server. Please refer

to the **Guide\_GuardianLynxGuide** integration guide for details. *The document is posted to the SDS Partner Portal. If you do not have access to this Portal, please contact SDS Support.*

**NOTE:** LynxGuide is a licensed integration – you must install the proper license on the SDS Gateway to enable this integration.

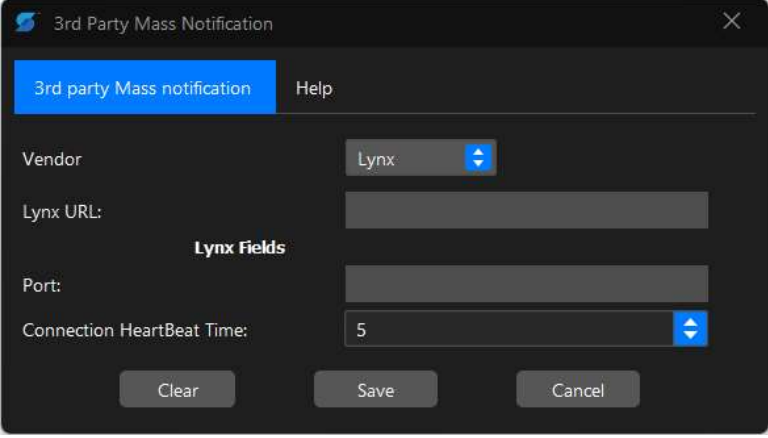


Figure 35 – LynxGuide Configuration Dialog

### 8.3 Desktop Alert

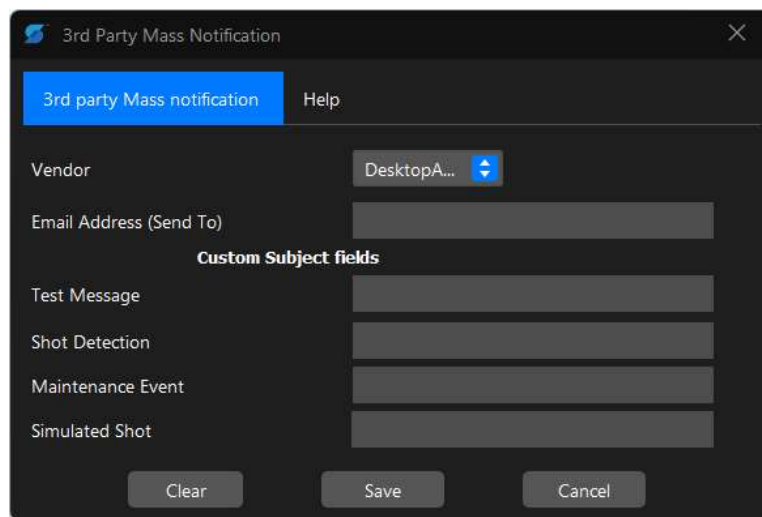
SDS Indoor Gunshot Detection System provides an interface to DesktopAlert, a 3<sup>rd</sup> Party Mass Notification system. This interface is implemented by providing a customized notification email to the DesktopAlert application. *This integration REQUIRES SDS Indoor Gunshot Detection System to be configured to be able to send Emails.*

The SA interfaces to DesktopAlert by sending custom subject fields within an email message. These expected message fields are configured by the user within DesktopAlert. The DesktopAlert application can be programmed to take specific actions based on the receipt of emails from the SA with these subject fields. The SA allows for four custom subject fields based on the following events: Test Message, Shot Detection, Maintenance Event and Simulated Shot.

Configuration of this integration within the SA is accomplished through the SA Email Server configuration page as described below:

1. Select **“Admin”** → **“Email Server Configuration”**. The Email Server should be configured prior. Please see the Email Server Configuration section for more details.
2. Select **“3<sup>rd</sup> Party Mass Notification Configuration”** at the bottom left of the dialog.
3. Select DesktopAlert from the **“Vendor”** dropdown menu.
4. In the **“Email Address (Send To)”** field enter the email address which has been configured within DesktopAlert to receive emails.

5. DesktopAlert should be preconfigured to receive emails from **“Sending Address (From)”** which is configured in the **“Email Server Configuration”** section. This entails creating a user with DesktopAlert with a matching username.
6. Enter a scenario name for each **“Custom Subject Field”** including **“Test Message”**, **“Shot Detection”**, **“Maintenance Event”** and **“Simulated Shot”**. Scenario subject fields are not required to be unique but must match the expected value configured within DesktopAlert.
7. When configuration is complete select **“Apply”**. A **“3<sup>rd</sup> Party Mass Notification”** configuration may be removed at any time by selecting the **“Clear”** button.
8. Once configured, an email will be sent to the **“Email Address (Send To)”** from **“Sending Address (From)”** with a subject matching the **“Custom Subject Field”** for that event and a body containing information based on the Email Template for that event.



The screenshot shows a software window titled "3rd Party Mass Notification" with a close button (X) in the top right corner. The window has a dark theme. At the top, there is a blue tab labeled "3rd party Mass notification" and a "Help" link. Below the tab, the "Vendor" field is set to "DesktopA..." with a dropdown arrow. The "Email Address (Send To)" field is an empty text box. Under the heading "Custom Subject fields", there are four text input fields labeled "Test Message", "Shot Detection", "Maintenance Event", and "Simulated Shot". At the bottom of the window, there are three buttons: "Clear", "Save", and "Cancel".

Figure 36 – Enable and Configure Remote Admin

## 9 Noonlight Emergency Response

**WARNING:** The Noonlight Emergency Response system should remain in “Noonlight Emergency response: Disabled” status until the system is fully set up and ready to be used.

Noonlight Emergency Response feature provides provisioning capabilities for automatically calling 911 dispatch in case of an active shooting event, in addition to normal an SDS Enterprise Solution features, saving valuable time at very critical moments.

To use the Noonlight Emergency Response feature the following are required:

- Noonlight feature enabled
- Mode of operation selected
- Digital token entered
- Accurate address information entered
- Accurate contact information entered

Noonlight Emergency Response feature is included in your subscription fee. This feature is supported in Situational Awareness version R5.1.1 and higher.

### 9.1 Configuration

Noonlight Emergency Response configuration dialog box can be opened by selecting menu item **Admin→Noonlight Emergency Response Configuration**

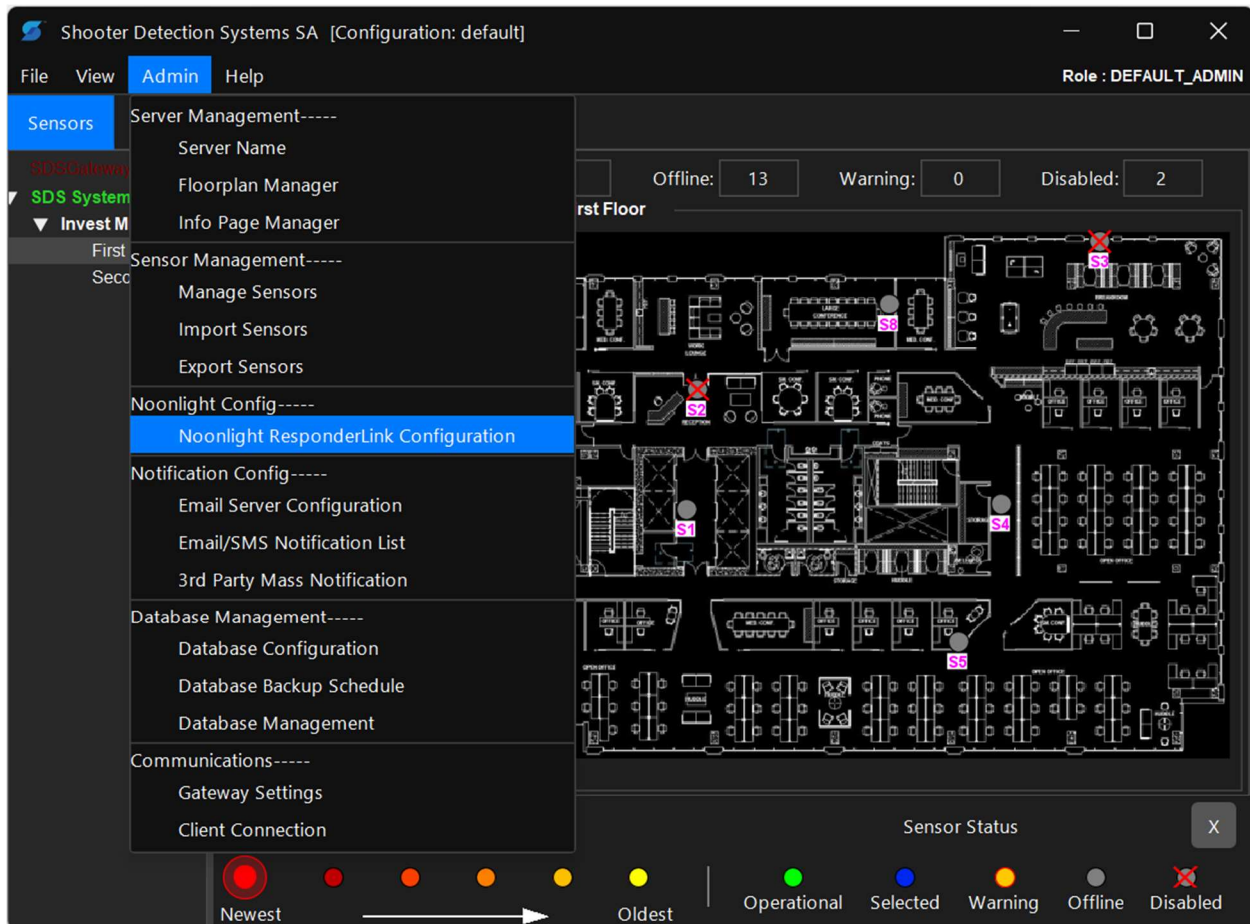


Figure 37 – Noonlight Emergency Response Configuration Menu Option

### 9.1.1 Enable/Disable and Status Display

Noonlight Emergency Response feature can be enabled by clicking on the “**Enable Noonlight Monitoring**” box.

Noonlight ResponderLink Configuration

Enable Noonlight Monitoring: ☒

Show Noonlight Status on Client: ☒

Operation Mode:

Active Monitor (Immediate Dispatch): ☐ ID : 9f7d4dc1-943b-43df-918e-d5baa8883ae5

Active Monitor (Confirmation Prior to Dispatch): ☐ ID : 6e405e13-9716-41a0-8aa0-c03c25b2d306

Test Mode (Callback / SMS): ☐ ID : 2617bab3-950d-4a38-8555-a0ea77e0c620

Test Mode (SMS Only): ☒ ID : 30874da5-e64c-469a-86e5-398232fbed8a

Noonlight Token (Authentication) :

Customer Information :

Name/Description :

Address Line 1:

Address Line 2:

City :

State : Select ZipCode :

Contact Person Information:

	Name :	Phone :	Notify :
Customer Primary Contact:			<input type="checkbox"/>
Customer Secondary Contact:			<input type="checkbox"/>
Integrator Primary Contact:			<input type="checkbox"/>
Integrator Secondary Contact:			<input type="checkbox"/>

Select Primary Contact: Customer Primary Contact

Save Cancel Clear

Figure 38 – Noonlight – Enable/Disable and Status Display

**NOTE:** The default state when this version of the SA is installed will be “Noonlight Emergency response: Disabled”.

**NOTE:** Once the Enable option is selected, Noonlight Emergency Response feature is enabled, and any detected gunshot will be dispatched according to the current feature settings

Displaying status of **Noonlight Emergency Response status** on the Shooter Detection Systems SA can be enabled or disabled by selecting “Show Noonlight Status on Client.” This option allows convenient verification of the feature’s operational status.

## 9.1.2 Operation Mode - Active Monitoring

Operation Mode settings control the desired feature behavior in case of a gunshot detection event.

Noonlight Emergency Response feature provides two types of Active Monitoring.



Noonlight ResponderLink Configuration

Enable Noonlight Monitoring: ☒

Show Noonlight Status on Client: ☒

Operation Mode:

Active Monitor (Immediate Dispatch): ☐ ID : 9f7d4dc1-943b-43df-918e-d5baa8883ae5

Active Monitor (Confirmation Prior to Dispatch): ☐ ID : 6e405e13-9716-41a0-8aa0-c03c25b2d306

Test Mode (Callback / SMS): ☐ ID : 2617bab3-950d-4a38-8555-a0ea77e0c620

Test Mode (SMS Only): ☒ ID : 30874da5-e64c-469a-86e5-398232fbed8a

Noonlight Token (Authentication) :

Customer Information :

Name/Description :

Address Line 1:

Address Line 2:

City :

State :  ZipCode :

Contact Person Information:

	Name :	Phone :	Notify :
Customer Primary Contact:	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
Customer Secondary Contact:	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
Integrator Primary Contact:	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
Integrator Secondary Contact:	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Select Primary Contact:

Save Cancel Clear

Figure 39 – Noonlight – Active Monitor Operation Modes

The two Active Monitoring modes are described as:

- **Active Monitor (Immediate Dispatch):** Selecting this option results in the Noonlight agent immediately contacting the 911 dispatch center. Emergency responses will be sent to the specified address. An automated SMS message will be sent to the contacts. A follow-up call with the primary contact will then follow.
- **Active Monitor (Confirmation Prior to Dispatch):** Selecting this option will result in an automated SMS message to the contacts as well as a call from a Noonlight Agent to the primary contact. Unless the contact confirms that and Emergency Response is not needed, the agent will then contact the 911 dispatch center.

**NOTE:** Emergency Response will be contacted in these modes. If Emergency Response is not desired, such as a test or drill, the Noonlight Monitoring service should be disabled or switched to Test Mode.

### 9.1.3 Operation Mode – Test Modes

The Noonlight Emergency Response feature provides two modes for testing the feature.

The screenshot shows the 'Noonlight ResponderLink Configuration' window. The 'Operation Mode' section is highlighted with a red box. It contains four radio button options: 'Active Monitor (Immediate Dispatch)', 'Active Monitor (Confirmation Prior to Dispatch)', 'Test Mode (Callback / SMS)', and 'Test Mode (SMS Only)'. The 'Test Mode (SMS Only)' option is selected. To the right of these options are four IDs: '9f7d4dc1-943b-43df-918e-d5baa8883ae5', '6e405e13-9716-41a0-8aa0-c03c25b2d306', '2617bab3-950d-4a38-8555-a0ea77e0c620', and '30874da5-e64c-469a-86e5-398232fbed8a'. Below the 'Operation Mode' section are fields for 'Noonlight Token (Authentication)', 'Customer Information' (Name/Description, Address Line 1, Address Line 2, City, State, ZipCode), and 'Contact Person Information' (Customer Primary Contact, Customer Secondary Contact, Integrator Primary Contact, Integrator Secondary Contact, Select Primary Contact). At the bottom right are 'Save', 'Cancel', and 'Clear' buttons.

Figure 40 – Noonlight - Test Mode Operation Modes

- **Test Mode (SMS Only):** Selecting this **TEST ONLY** option will have the system send automated SMS message to the selected contacts(s).
- **Test Mode (Callback / SMS):** Selecting this **TEST ONLY** option generates an automated SMS message as well as a callback from a Noonlight agent to the selected contacts(s).

**NOTE:** Test Modes are only used for testing the feature through callback or SMS and shouldn't be left enabled in a production environment since these modes will NOT DISPATCH authorities to the site in case of any gunshot detection.

Gunshots can be simulated in SA application to test the Noonlight Emergency Response feature.

### 9.1.4 Noonlight Authentication Token

Noonlight Emergency Response requires an authentication token to function. The authentication token is validated by Noonlight systems and must be entered in for the feature to be operational.

Noonlight ResponderLink Configuration

Enable Noonlight Monitoring: ☒

Show Noonlight Status on Client: ☒

Operation Mode:

Active Monitor (Immediate Dispatch): ☐ ID : 9f7d4dc1-943b-43df-918e-d5baa8883ae5

Active Monitor (Confirmation Prior to Dispatch): ☐ ID : 6e405e13-9716-41a0-8aa0-c03c25b2d306

Test Mode (Callback / SMS): ☐ ID : 2617bab3-950d-4a38-8555-a0ea77e0c620

Test Mode (SMS Only): ☒ ID : 30874da5-e64c-469a-86e5-398232fbed8a

Noonlight Token (Authentication) :

Customer Information :

Name/Description :

Address Line 1:

Address Line 2:

City :

State : Select ZipCode :

Contact Person Information:

	Name :	Phone :	Notify :
Customer Primary Contact:			<input type="checkbox"/>
Customer Secondary Contact:			<input type="checkbox"/>
Integrator Primary Contact:			<input type="checkbox"/>
Integrator Secondary Contact:			<input type="checkbox"/>

Select Primary Contact: Customer Primary Contact

Save Cancel Clear

Figure 41 – Noonlight – Authentication Token

- Each customer is assigned a unique Noonlight Token for authentication and verification purposes.
- The token is provided by SDS in a text document as a 32-character string. It can be copied and pasted into this field.
- The Noonlight Token doesn't expire and is part of SDS system licensing.
- If not already provided, the Noonlight Token can be obtained by emailing: [license@shooterdetectionsystems.com](mailto:license@shooterdetectionsystems.com)
- Each customer is required to obtain their own Token and it cannot be shared with another organization.

There is no additional configuration or account setup required with SDS or Noonlight.

### 9.1.5 Customer Information

The Customer Information section contains the customer facility address the 911 dispatch will use to send the Emergency Response.

Noonlight ResponderLink Configuration

Enable Noonlight Monitoring: ☒

Show Noonlight Status on Client: ☒

Operation Mode:

Active Monitor (Immediate Dispatch): ☐ ID : 9f7d4dc1-943b-43df-918e-d5baa8883ae5

Active Monitor (Confirmation Prior to Dispatch): ☐ ID : 6e405e13-9716-41a0-8aa0-c03c25b2d306

Test Mode (Callback / SMS): ☐ ID : 2617bab3-950d-4a38-8555-a0ea77e0c620

Test Mode (SMS Only): ☒ ID : 30874da5-e64c-469a-86e5-398232fbed8a

Noonlight Token (Authentication) :

Customer Information :

Name/Description :

Address Line 1:

Address Line 2:

City :

State :  ZipCode :

Contact Person Information:

	Name :	Phone :	Notify :
Customer Primary Contact:	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
Customer Secondary Contact:	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
Integrator Primary Contact:	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
Integrator Secondary Contact:	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Select Primary Contact:

Save Cancel Clear

Figure 42 – Noonlight - Test Mode Operation Modes

**NOTE:** It is critical that this information is complete and accurate.

### 9.1.6 Contact Person Information

This section contains contact information for individuals to be informed in case of a gunshot detection or testing, as specified in the Operation Modes section.

Noonlight ResponderLink Configuration

Enable Noonlight Monitoring: ☒

Show Noonlight Status on Client: ☒

Operation Mode:

Active Monitor (Immediate Dispatch): ☐ ID : 9f7d4dc1-943b-43df-918e-d5baa8883ae5

Active Monitor (Confirmation Prior to Dispatch): ☐ ID : 6e405e13-9716-41a0-8aa0-c03c25b2d306

Test Mode (Callback / SMS): ☐ ID : 2617bab3-950d-4a38-8555-a0ea77e0c620

Test Mode (SMS Only): ☒ ID : 30874da5-e64c-469a-86e5-398232fbed8a

Noonlight Token (Authentication) :

Customer Information :

Name/Description :

Address Line 1:

Address Line 2:

City :

State :  ZipCode :

Contact Person Information:

	Name :	Phone :	Notify :
Customer Primary Contact:	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
Customer Secondary Contact:	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
Integrator Primary Contact:	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
Integrator Secondary Contact:	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Select Primary Contact:

Save Cancel Clear

Figure 43 – Noonlight - Test Mode Operation Modes

- **Customer Primary Contact:** This is the principal contact's information; Name, Phone number.
- **Customer Secondary Contact:** This is the secondary contact's information; Name, Phone number.
- When the **Notify checkbox** is selected this contact will be notified.
- **Integrator Primary Contact:** This is the principal integrator contact's information; Name, Phone number.
- **Integrator Secondary Contact:** This is the secondary integrator contact's information; Name, Phone number.
- When the **Notify checkbox** is selected this contact will be notified.
- **Select Primary Contact:** This dropdown selects the contact (Customer Primary/Secondary, Integrator Primary/Secondary) that will be contacted first when Noonlight is activated.

## 9.2 Status Display

Current status of the Noonlight feature is displayed on top of the SA screen.

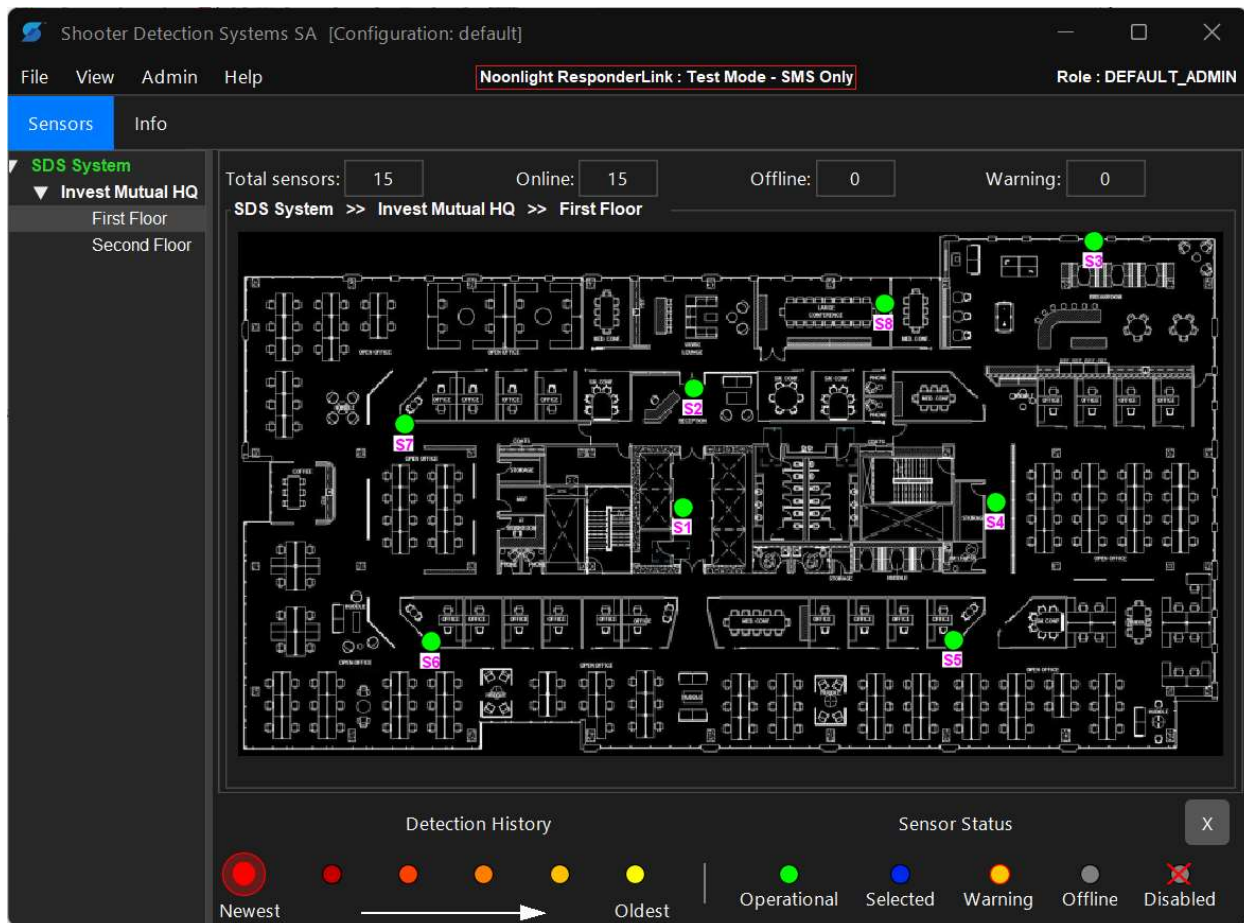


Figure 44 – Noonlight - Status Display

### 9.2.1 “Disabled” Status

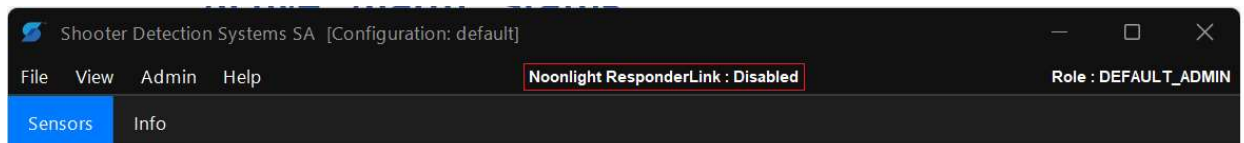


Figure 45 – Noonlight - Disabled Status Display

### 9.2.2 Active “Alarm” Status



Figure 46 – Noonlight - Active “Alarm” Status Display

### 9.2.3 “Monitoring Active – Immediate Dispatch” Status

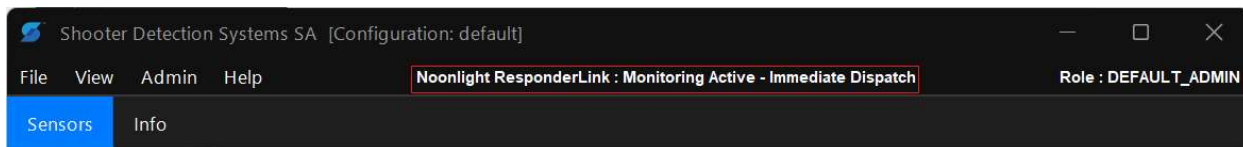


Figure 47 – Noonlight – “Monitoring Active Immediate Dispatch” Status Display

### 9.2.4 “Monitoring Active – Confirmation Prior to Dispatch” Status

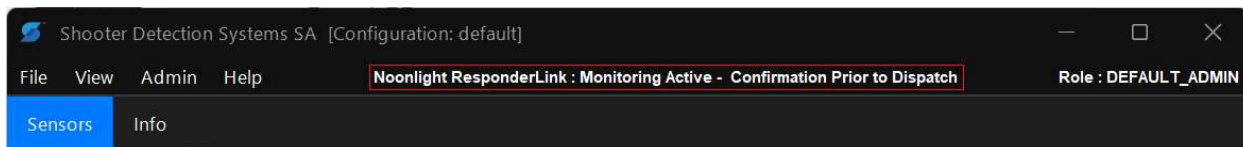


Figure 48 – Noonlight – “Monitoring Active – Confirmation Prior to Dispatch” Status Display

### 9.2.5 “Test Mode – SMS Only” Status



Figure 49 – Noonlight - “Test Mode – SMS Only” Status Display



### 9.2.6 “Test Mode – Callback / SMS” Status



Figure 50 – Noonlight - “Test Mode – Callback / SMS” Status Display

### 9.2.7 Active “Test Alarm” Status

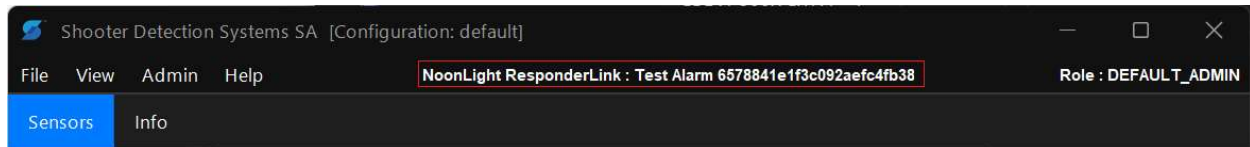


Figure 51 – Noonlight - Active “Test Alarm” Status Display

### 9.2.8 “Connection Issue” Status

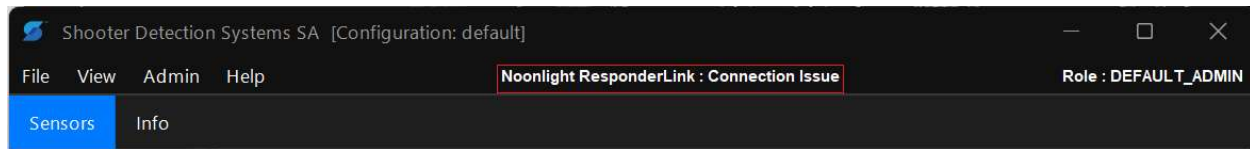


Figure 52 – Noonlight - “Connection Issue” Status Display



## 10 Alertus Mass Notification

The SDS Situational Awareness application now integrates with Alertus allowing shot detection messages to be sent to the platform. The document describes the license and minimum release requirements as well as configuration steps for integrating with Alertus.

### 10.1 Configuration

Within the Situational Awareness (SA) Client, navigate to Admin à 3rd Party Mass Notification

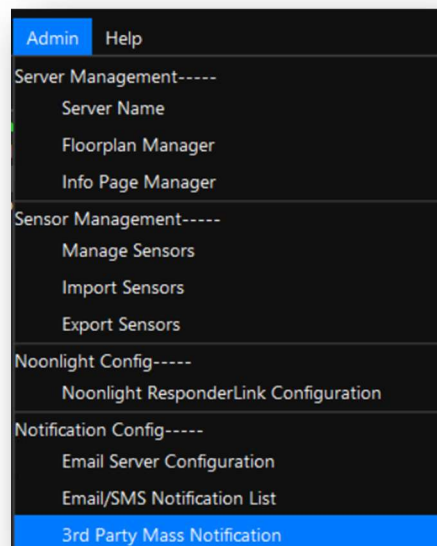


Figure 53 – 3<sup>rd</sup> Party Mass Notification setting

From the 3rd Party Mass Notification configuration window select the Vendor dropdown menu and then select Alertus. Enter the URL to your Alertus installation and your account credentials. You may leave the heartbeat/health-check time at 5 minutes or adjust as needed.

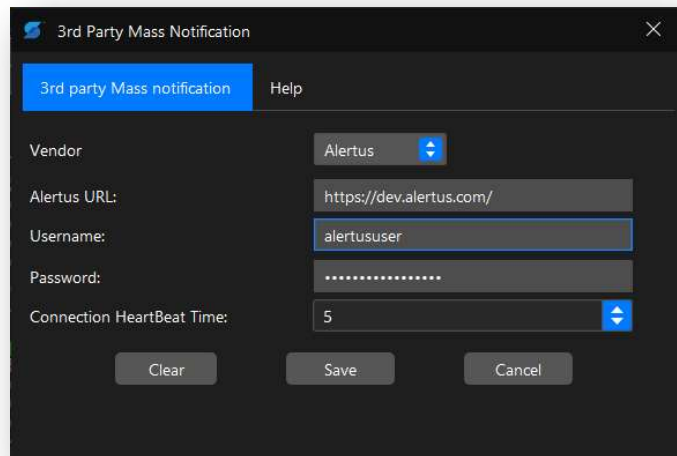


Figure 54 – Alertus Configuration Window

Select the Save button. The account credentials will be verified upon saving and status reported.

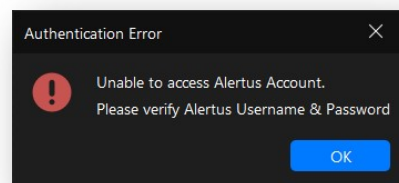
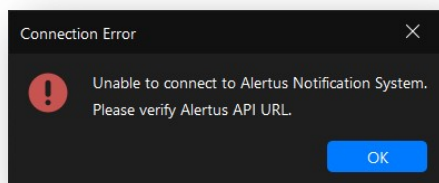
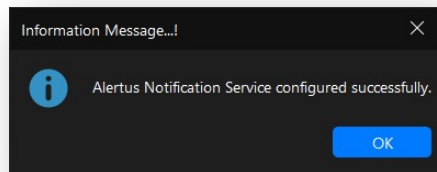


Figure 55 – Alertus Configuration Error – URL and Credentials

## 10.2 Testing

To verify that detection messages are being received by the Alertus platform you may send a test shot from SDS Active Shooter Trainer Application. Be aware that other

integrations, SA clients, SMS/Email users and the SDS ResponderLink service will also receive this message. Disable these features as necessary.

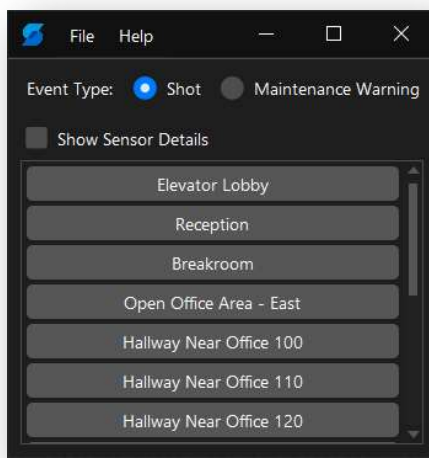
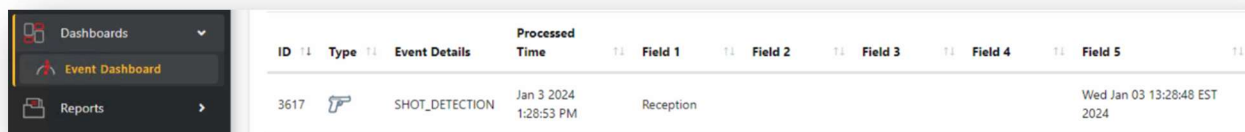


Figure 56 – SDS Trainer Application

After sending a test shot from the SDS trainer validate that the message is received within the Alertus platform. Log into your Alertus account and navigate to Dashboards à Event Dashboard. Event details will be displayed for the detection event as shown below.




ID	Type	Event Details	Processed Time	Field 1	Field 2	Field 3	Field 4	Field 5
3617		SHOT_DETECTION	Jan 3 2024 1:28:53 PM	Reception				Wed Jan 03 13:28:48 EST 2024

Figure 57 – Alertus Event Dashboard

To view additional event details, select the gun or magnifying glass icons from that event row.

Dashboards
Event Dashboard
Processed Event

**Event #3617 - Sensor Event**

### Event Details

Expand All
Collapse All

<b>Abnormal:</b>	true
<b>Client Name:</b>	Shooter Detection Systems
<b>Event Time:</b>	2024-01-03T13:28:48-05:00
<b>Facility:</b>	Invest Mutual HQ
<b>Floor:</b>	Floor 1
<b>Icon:</b>	gun.png
<b>Location:</b>	Reception
<b>Message:</b>	SHOT_DETECTION
<b>Priority:</b>	1
<b>Sensor Name:</b>	S2
<b>Sensor Type:</b>	Gunshot
<b>System Name:</b>	SDS System - Alertus Demo

Raw XML

```

1 <?xml version="1.0" encoding="UTF-8"?><sensorEvent>
2   <abnormal>true</abnormal>
3   <clientName>Shooter Detection Systems</clientName>
4   <eventTime>2024-01-03T13:28:48-05:00</eventTime>
5   <facility>Invest Mutual HQ</facility>
6   <floor>Floor 1</floor>
7   <icon>gun.png</icon>
8   <location>Reception</location>
9   <message>SHOT_DETECTION</message>
10  <priority>1</priority>
11  <sensorName>S2</sensorName>
12  <sensorType>Gunshot</sensorType>
13  <systemName>SDS System - Alertus Demo</systemName>
14 </sensorEvent>
15

```

Figure 58 – Alertus Event Details

## **11 SA Client (Normal Operation)**

The SA Client provides Situational Awareness during normal operation of the system. This includes Sensor Status icons, Shot icons, Shot History Lists and information as well as Tester Events and Sensor Status information.

As this functionality is the same for User and Admin level privileges you are referred to the SA Client User's manual (Section 4 and above) for information regarding use of these features.

## 12 SA Server Maintenance

### 12.1 SDS SA Software Upgrade

The SA tool (Server and/or Client) may 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 SA software upgrade. This will include information on any performance improvements and include any impact to system security or other issues. The software will be posted on a private site for system administrators to download.

The upgrade information will include information as to whether the SA Server and Clients must both be upgraded during this process. SDS tries to maintain interoperability to the extent possible to simplify the upgrade requirements and constraints.

The upgrade process follows the steps in Section 3 but you will be asked if you want to remove the current version. **Always allow the previous version to be uninstalled** as it will not remove any of the configuration information, logs or other data on the system.

**IMPORTANT:** It is strongly recommended that prior to upgrading any of your SDS SW products you make a SDS Indoor Gunshot Detection System Backup as described in Section 12.2.2

### 12.2 SDS Server Backups (Recommended Practice)

There are two methods of backing up the SDS Indoor Gunshot Detection System Information. The first is specific to the SA Database and is supported directly through the SA Admin console. The second allows an admin to backup, the entire SDS Indoor Gunshot Detection System configuration.

#### 12.2.1 SA Database Backup

Backing up the SA Database is easily accomplished from within the SA Admin console. Select **File → Database Export** and provide a backup location for the database file. This file can be restored later using **File → Database Import**.

As the description implies this backup is limited specifically to the SA Database and does not include the SDS Gateway or any tools or Integration (Connector) Services. See the next section for a full system Backup.

#### 12.2.2 SDS Indoor Gunshot Detection System Backup

All installation specific information for the SDS Indoor Gunshot Detection System (including the SA) is stored in \$SDSData. It is suggested that this folder be backed up on a regular basis. If a configuration issue occurs, follow the instructions in the next section to restore the system to a functional state.

Prior to making a backup copy of the SDSData folder the SA and other Services must be stopped.

- Stopping the SA prior to making a backup: Use the **Windows Start menu → Shooter Detection Systems → SDS Situational Awareness → Server → Stop SA Server** to stop both the SA and Mongo services.
- Stopping the GW prior to making a backup: Use the **Windows Start menu → Shooter Detection Systems → SDS Gateway → Stop GW Task** to stop the GW task.
- If you are running other SDS Integration (Connector) Services refer to those manuals for information on stopping and restarting the services.

Once the services have been stopped you will be able to make a backup of the \$SDSData folder.

*Note that the "UploadFiles" folder can contain a large amount of logging data and you may want to either not copy it ... or delete it from your backups to save disk space.*

Once the backup has completed restart the Services by using the Restart menu items or rebooting the server.

## 12.3 Recovering from an Issue

If a severe configuration issue occurs, then there are options for restoring the database from a prior backup. Prior to any of these steps it is **strongly** recommended that you make a complete copy of the \$SDSData folder (as described in the prior section – SDS Indoor Gunshot Detection System Backup).

### 12.3.1 Restoring from a Backup

Depending on your backup procedures, and most recent backup available, you can restore either the SA Database or the entire SDS Indoor Gunshot Detection System as described below.

#### 12.3.1.1 Restoring from an SA Database Backup

The SA Database can be restored from the most recent database export, Section 12.2.1. To restore this database, select File → Database Import and then select the most recent backup. The restore process can take 1-2 minutes.

Once the restore process has completed determine if the system is back to normal operation.

#### 12.3.1.2 Restoring from a SDS Indoor Gunshot Detection System Backup

The SDS Indoor Gunshot Detection System (all components) can be restored from the most recent backup of the \$SDSData folder. To restore a folder backup, follow the instructions to stop the ongoing Services, Section 12.2.2 and then rename the current SDSData folder. Copy (do NOT RENAME) your backup to be \$SDSData and then restart the system to ensure that the system is operating correctly.

### 12.3.2 Reinstall the SA Software

In the situation that a system restore has not corrected the issue then the possibility is that the SA software installation has been corrupted. In this case it is suggested that you uninstall the SA Server and SA Client (this does not affect your system data) and then re-install both tools.

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



## 13 Appendix I – SA SQL Server Database Setup

SDS APP Note – SA SQL Server Setup which documents this setup is posted to the SDS DropBox account:

- < [https://secure.shooterdetectionsystems.com/wp-content/uploads/sites/6/2022/05/AppNote\\_GuardianSA\\_SQL\\_Server\\_Setup\\_1.0.pdf](https://secure.shooterdetectionsystems.com/wp-content/uploads/sites/6/2022/05/AppNote_GuardianSA_SQL_Server_Setup_1.0.pdf) >

## 14 Appendix II – Windows Active Directory Setup

SDS APP Note – SA Active Directory Setup which covers this setup is posted to the SDS DropBox account:

- < [https://secure.shooterdetectionsystems.com/wp-content/uploads/sites/6/2022/05/AppNote\\_GuardianSA\\_ActiveDirectory\\_Setup\\_1.0.pdf](https://secure.shooterdetectionsystems.com/wp-content/uploads/sites/6/2022/05/AppNote_GuardianSA_ActiveDirectory_Setup_1.0.pdf) >

## 15 Appendix III – Azure Active Directory Setup

SDS APP Note – SA Azure Active Directory Setup which covers this setup is posted to the SDS DropBox account:

- *<TBD – Link>*

## 16 Appendix IV – SA Audit Reporting Setup

SDS APP Note – SA Audit Reporting Setup is posted to the SDS DropBox account:

- <TBD – Link>

## 17 Appendix V – Monitoring the SA Server

The SA Server is a critical component of your SDS Indoor Gunshot Detection System protection. It monitors the other components and notifies users (visually and through its Email/SMS notifications) when a problem is detected with a Sensor or with the SDS GW application.

The final component of providing a robust installation is to provide a monitoring capability for the SA Server itself. If the SA Server is installed with a Mongo DB, the server runs as two Windows Services: SDS\_SA\_SERVER and SDS\_MONGODB\_SERVER. If the server is installed using a SQL DB, it runs a single Windows Service SDS\_SA\_SERVER. It is strongly recommended that a 3<sup>rd</sup> party monitoring software package be used to verify that the SA Services are, operational at all times. SDS does not recommend a specific approach as the “best” approach will be to use tools that you are familiar with and are part of the existing server / computing environment.

## 18 Appendix VI – Troubleshooting & FAQs

Listed below are frequent questions you may come across while installing and configuring the Gateway and/or Situational Awareness tools.

**Q1)** I see a square icon “□” in the Sensor information but when I check the nodes.csv file it looks fine.

**Solution:** The csv file must not contain special characters. Some spreadsheet editor utilities auto-correct certain character such as a dash “-” to a larger, or double, dash “-”. This will be misinterpreted in the SA application and displayed as a box icon.

**Q2)** Why do I see a SDS sensor reporting a warning?

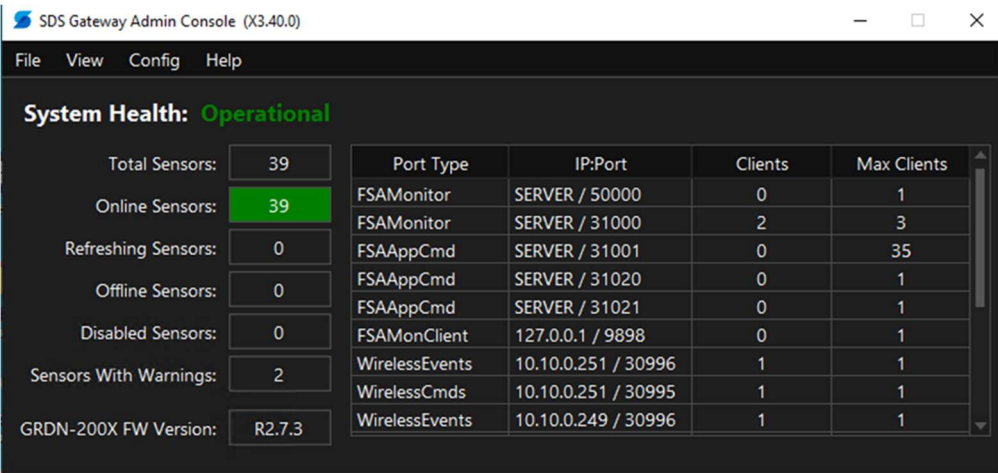
**Solution:** The sensor may report a warning for a variety of reasons. Refer the SDS GW manual for help in identifying potential causes and solutions.

**Q3)** 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.

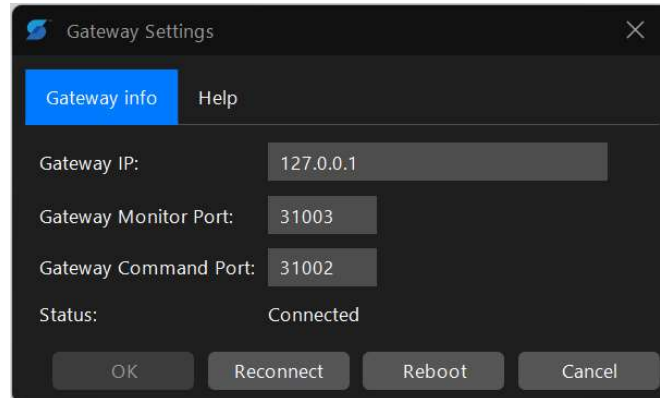
**Gateway Application:**



System Health: <span>Operational</span>	
Total Sensors:	39
Online Sensors:	39
Refreshing Sensors:	0
Offline Sensors:	0
Disabled Sensors:	0
Sensors With Warnings:	2
GRDN-200X FW Version:	R2.7.3

Port Type	IP:Port	Clients	Max Clients
FSAMonitor	SERVER / 50000	0	1
FSAMonitor	SERVER / 31000	2	3
FSAppCmd	SERVER / 31001	0	35
FSAppCmd	SERVER / 31020	0	1
FSAppCmd	SERVER / 31021	0	1
FSAMonClient	127.0.0.1 / 9898	0	1
WirelessEvents	10.10.0.251 / 30996	1	1
WirelessCmds	10.10.0.251 / 30995	1	1
WirelessEvents	10.10.0.249 / 30996	1	1

### Situational Awareness Application: “Admin” → “Gateway Settings”



- ✓ Ensure that the following range of ports is not blocked on the Gateway firewall: 31000 – 31001<sup>2</sup>. 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.

#### Q4) Why won't the SA Client Connect to the SA Server?

**Solution:** Verify the following:

- ✓ Confirm that the IP and Ports configured within the SA Client application are correct. Unless modified, the connection will be either TLS (Port 31006) or Plaintext (no TLS) (Port 31005).
- ✓ Ensure that the selected Port is not blocked (Inbound requests are enabled) on the SA Server machine firewall.
- ✓ Verify that any Anti-virus application is not interfering. This can be confirmed by temporarily disabling features within the anti-virus program.

---

<sup>2</sup> Ports: 31000-31002 assumes 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.

## 19 Support Resources

Email: [support@shooterdetectionsystems.com](mailto: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/>

© Shooter Detection Systems, LLC, an Alarm.com Company