SDS Gateway – Release Notes

The Gunshot Detection System utilizes sensors distributed throughout a facility to detect and report active shooter events immediately as they occur. The SDS Gateway connects to all configured SDS Sensors on a system to provide their status as well as provide access to their control and monitor ports. The SDS system is developed and maintained by Shooter Detection Systems, LLC.

Software Installation:

The provided installer (Installer_SDSGWServer_xxxxx.exe) will uninstall the currently installed Gateway version and go through all the steps to install the software in the selected computer. The installer will also create a configuration directory (C:\SDSData by default but user configurable), which will hold all configuration files for the Gateway. This directory will be persistent through installs.

R3.4.0b Release

New Features:

Issues / Improvements:

- Change the GW Client to have a more modern Look and Feel
- Change images on GW screens/installers to match new SDS branding
- Change "Guardian Gateway" to "SDS Gateway" throughout GW Client
- Use "Sensors" instead of "Nodes" where possible on GW Client screens
- Move to 2.7.4 FW Kit
- GW Certificate: Description of Updated Cert not Shown
- Add License Support for:
    - Titan HST Mass Notification
    - Alertus Mass Notification
    - SDS Notification Service

R3.3.1 Release

New Features:

Issues / Improvements:

- GW messages forwarded from wireless sensors have a blank NIP field
- Wireless sensors are not displayed in the Admin client windows

R3.3.0 Release

New Features:

- Update EULA for GW Server and Client applications

Issues / Improvements:

- Moved to OpenJDK 11.0.14.1 to fix TLS1.3 issue
- GW does not use HB's NIP value for data in "Reported IP" column on sensor screen(s)
- Jackson DataBind vulnerabilities in GW Server and GW Client
- Bump max value of NODE_POWERED_OFFLINE_TIMEOUT_SEC to 5 min in settings screen
- Add License Support for Noonlight Emergency Response

SDS Gateway – Release Notes

R3.2.5 Release

Issues / Improvements:

- HB and CMD timeouts preempted when socket is reset on sensor side
- Bump max value of NODE_POWERED_OFFLINE_TIMEOUT_SEC to 5 min in settings screen

R3.2.3 Release

New Features:

- Noonlight Emergency Response – Licensing supported added to the SDS system. Noonlight is enabled for all customers by default.
- Certificate Logic (Customer Cert Insertion) – Support https on API for Customer Cert generation.

R3.2.0 Release

New Features:

- GRDN-2000 FW is updated to the latest R2.7.2 release.
- SSL Certificate management – added GUI and server features to support updating the GW's certificate as well as the sensor certificates. *If you have advanced certificate management requirements, contact Customer Support.*
- SSL Certificate management – added support for "chained" certificates (multiple CAs). Changes included handling of both the GW and Sensor certificates during import and activation.
- License Support: Added support for the Singlewire (Informacast) and Lightaway integrations (current) as well as OpenEye, Raptor, and Sureview (future integrations).
- GW GUI previously limited the Wireless Sensor timeout period to be no more than 12 minutes. In some installations the sensors need to be slowed down to send a HB at 30 mins (default is 10 minutes). The GUI now supports the 30 minute HBs.

Issues / Improvements:

- Runtime Environment – Updated the Java Runtime environment from the 1.8 release path to the OpenJDK 11.0 path.
- Sensor OFFLINE/ONLINE issues – Several edge cases were causing sensors to be declared OFFLINE prematurely and, in some cases, preventing them from coming back ONLINE. These issues have been resolved.
- Sensor Warning Codes – updated based on the latest Sensor FW capabilities.

R3.1.8 Release

New Features:

- None.

Issues / Improvements:

- Prior releases had an issue (edge case) where the GW might send out a sensor OFFLINE message and then follow with normal ONLINE messaging. In this case the SA might send out a maintenance message incorrectly calling the Sensor OFFLINE for a short period of time. This issue (along with a correction in the SA R4.5.0) resolves this issue.

Security Issues Addressed:

- None

R3.1.7 / R3.1.6 Release

New Features:

- None.

Issues / Improvements:

- R3.1.5 introduced an issue which resulted in some OFFLINE sensors being shown as ONLINE. This issue is resolved in the R3.1.6 release
- R3.1.5/6 introduced an issue which can cause a sensor to temporarily be marked off-line during the sensor's nightly maintenance activity. R3.1.7 fixes this issue.
- R3.1.5/6 introduced an issue which can cause WIRELESS sensors to be marked OFFLINE incorrectly. This is due to their 10-minute Heartbeat timing. This issue is resolved in the R3.1.7 release.

- The GW can produce a Description message for each sensor, repeated periodically (MT:DESC). Most systems do not require this message and in R3.1.6 setting the timeperiod to "0" will completely disable the messages.

Security Issues Addressed:

- None

R3.1.5 / … R3.1.2 Release

Security Issues Addressed:

- Addresses CVE-2021-44832 identified for Apache Log4j2.
- Addresses CVE-2021-45105 identified for Apache Log4j2.
- Addresses CVE-2021-45046 identified for Apache Log4j2.
- Addresses CVE-2021-44228 identified for Apache Log4j2.

SDS Gateway – Release Notes

R3.1.1 (Release)

Release R3.1.1 incorporates a single issue-resolution as a minor update to R3.1.0.

New Features:

- None.

Issues / Improvements:

- Sensor TLS Connection/Handshake – An issue was detected in the R3.1.0 release where (as an edge case) if the establishment of a Sensor TLS Connection (referred to as the Handshake) was interrupted and didn't complete the GW would not try to reconnect to that sensor, leaving it OFFLINE. *This has been corrected and the GW will connect to the sensor once it is available and the network is stable.*

R3.1.0 (Release)

Release R3.1.0 incorporates several new features as well as product improvements. Updates have been made to the management of LoRa Access Point connections, Enterprise testing using the SDS Handheld Tester as well as various management interfaces including sensor communications, SSL Certificates, an Advanced management GUI and others.

New Features:

- LoRa Access Point (AP) Support – "N" LoRa APs can be connected to the GW directly. *Prior release supported a single LoRa AP connection. When using multiple LoRa APs they had to be daisy chained as a single network.*
- Handheld Tester Controls – GW now supports selecting subsets (groups or individual sensors) and enabling them for Test Mode. Allows larger installations to test sensors in a specific building, floor etc. while leaving the remaining sensors in normal operation. The GUI provides several methods to filter and clearly understand the sensors selected as well as their recent test success and failure.
- Failover Improvement – DHCP Sensor Config. GW will "forget" any sensor reported IP information (DHCP configuration) when sensor becomes not-available for > 1 minute. This reduces issues with both GWs trying to connect to the sensor
- SSL Certificate Management – GW now provides a GUI to manage a "common" certificate which is distributed from the GW to all Sensors to secure their connection to the GW. Alternatively, this common certificate approach can be disabled, and the customer can configure each sensor with its own certificate via a command line API (scriptable). The system supports up to 4K byte private keys. *NOTE: As of this release of GW R3.1 and Sensor FW R2.7.1 Chained Certificates are **not** supported. The certificates are limited to a depth of one (one root CA machine signing all the certificates directly).*
- Advanced Config Dialog added – Admin can select this dialog and has control of parameters previously manipulated via the property file.
- Sensor DHCP Operation (expanded to IPv6) – Support added to allow IPv6 sensors to report their address information to the GW. *Prior releases required IPv6 sensors to have a known (typically static) IP in the configuration file.*

- Sensor Configuration File – GW now supports the entries of "DHCP" (previously required "0") and "REMOTE" (previously required "-1") for these special IP addressing modes.
- GUI Improvements:
  - External connection labels shown – The External Connections View shows the Label assigned by the Admin within the gateway.csv configuration file.
  - PoE Sensor connection – Sensor views show the protocol TCP / TLS being used to communicate with each sensor.
  - Wireless Sensor AP – Sensor views show the LoRa AP name associated with each connected sensor.
- Sensor Description Message Control – Advanced dialog enables admin to reduce or eliminate these messages (MT:DESC) as they are not typically utilized by 3rd party integrations.
- Sensor Geo-Location Support – R3.1 provides support for specifying a geo-location (Latitude / Longitude) for each sensor. This information is provided to 3rd party systems such as our Fusus integration. *CURRENT LIMITATION: Currently the Lat/Lon must be overloaded in the Relay columns to be compatible with the SA Server and as such Geo-Location and the Dry Contact output module are NOT compatible.*
- GW Log Format – R3.0 introduced a default format based on UTC (rather than server time-zone) as the 1st field and this increases the file size and can introduce confusion when investigating issues. R3.1 returns the default format to the prior state, removing the UTC timestamp. *If UTC logs are required for an application SDS Customer Support can provide instructions to enable that feature.*

License Additions (3rd Party):

- Desigo CC, Fusus, Rave Mobile, ReadyOP.

Issues / Improvements:

- Sensor Enable/Disable state – When refreshing the GW configuration file changes in the Sensor Ena/Dis state was not always properly updated. This has been corrected.
- GW communicated too often with the Wireless (Battery) sensors which reduces battery life. This is corrected.
- GUI Issues Resolved:
  - Wireless Sensor Last Update Time – Statistics page did not change the "Last Update Time" when a WARN or DET message was received. Now all these message types cause the new time to be shown. Date is now included in this Last Update field as well.
  - WiFi Ena/Dis dialogs – Prior release treated an "X" out of the dialog as a "Yes" response. This has been corrected – treated as a No.
  - FW Update screen – Prior release showed the date information in the filename box. This has been corrected.
  - External interface labels – Labels longer than 16 characters were not truncated properly. This has been corrected.
  - License Screen – Amika Mobile license was shown missing the "A". This has been corrected.

- Sensors reporting an "Unknown" WARNing code (one the GW didn't understand) were shown as GREEN/Healthy. This has been corrected – they are now shown as ORANGE/Degraded.
- Multi-Server Systems: Prior versions of the GW did not clear out the Sensor IP once it had been learned from the Sensor Announcement (DHCP). This caused the GW to continue connection attempts. In a multi-server environment, the better behavior is to clear the sensor IP and then re-learn it if a new Sensor Announcement is received.
- Sensor static IP address in configuration file ignored – GW changed the sensor static IP address (internally – not in file) when a new one was received in the Sensor Announcement message. Admin entered Static IP should never be changes. This has been corrected.
- Sensor static IP = 0.0.0.0 – R3.0 stopped recognizing this address as DHCP (prior build had). R3.1 (this release) corrects this and treats a static IP of 0.0.0.0 as DHCP.

R3.0.0 (Release)

New Features:

- Sensor Secure Communications – GW can now be configured to connect to the Sensors using TLS 1.2. *Requires Sensor FW R2.7.0.2 or newer.*
- Sensor Communication Channels reduced – GW can now connect to each Sensor using a single communication channel. Improves performance and GW capacity.
- Sensor Configuration – Sensors can now be configured using their DNS name or IPv6 address information.
- Maximum Sensor Increased – Improvements were incorporated to allow further scaling of the SDS GW. The SDS system now supports up to 5000 sensors on a single GW instance.
- Firewall Rules – GW Installer configures a basic set of Firewall Rules to enable integration connections as well as incoming SA Client connections.
- Audit Logging – GW Admin Client logs now include audit log entries which can be extracted for Audit reporting. Logs include updates to settings and to

Bug Fix:

- 3rd Party Integration Issue
  - Prior versions of the GW did not properly handle input messages from 3rd Party connections (none are expected – but may occur in some scenarios). R3.0.0 properly discards these messages eliminating the memory issues that were occurring.
- Windows Time Updates
  - GW did not properly manage Windows Time Updates which was causing sensor "OFFLINE" and other issues to occur. R3.0.0 properly handles changes in the PC time.
- GUI Improvements
  - Certain windows allowed (but didn't properly scale with) Maximum. Windows which cannot maximize have this feature removed.
  - Selecting windows from main screen did not bring them to forefront if they were Minimized. This has been corrected.

SDS Gateway – Release Notes

R2.1.1 (Release)

New Features:

- Wireless AP Info – Only show the Wireless AP (LoRa AP) information when there is at least one Wireless sensor in the configuration file.
- SDSUtilities – folder now has a CMD file **getGWDebugInfo.cmd** which will cause the GW to collect some diagnostic information.

Bug Fix:

- Nodes.csv File handler
  - GW was not properly handling leading/trailing spaces in the fields such as SID, IP etc. This has been corrected.
  - GW did not handle lower case letters in the ID. This has been corrected.

R2.1.0 (Release)

New Features:

- The major driver for the GW R2.1.0 release is its support of the new SDS Wireless-Battery operated sensor (GRDN-3000). R2.1.0 provides the sensor management functions and screens necessary to operate with this new class of SDS Sensors. *Refer to the "SDS Gateway What's new" document for an explanation of the new features and screens associated with this sensor.*
- Support for the new GRDN-3000 (Generation 3 Wireless/Battery operated sensors).
- DNS Support for Sensor Configuration (nodes.csv).

Bug Fix:

- Maintenance Screen issues
  - Sensor Reboot and Sensor BIT buttons were not operating correctly. *This issue is resolved.*

- License SW crashes when running with an expired license.
  - Prior GW version R2.0.0/1 will crash (often) when trying to review or upgrade an expired license. *This issue is resolved.*

- Locating the SDSData folder when not at its default location C:\SDSData
  - Prior versions required the user to browse to find the SDSData folder when not located at the default location C:\SDSData. This included firmware upgrades, report storage and license request file (TEM) storage. These issues have been resolved in this release

Improvements:

- GW Server Restart
  - Prior versions required the Admin to use Windows utilities to Stop/Start the GW Server. The GW Admin GUI allows the Admin to Stop/Restart the GW Server from within the application. File→GWServer

- GW GUI Screen Activation
  - Prior versions of the GW Admin Client did not activate (bring to focus) screens which has been minimized when they were selected again. The new release will automatically repaint the screens when selected (after being minimized).

R2.0.2 (Minor Release)

New Features:

- None.

Bug Fix:

- License SW crashes when running Trial license (not permanent)
  - Prior GW version R2.0.0/1 will not run correctly with a Trial license. When powering-up the system will crash due to licensing issue. *This issue is resolved.*

- License SW crashes when running with an expired license.
  - Prior GW version R2.0.0/1 will crash (often) when trying to review or upgrade an expired license. *This issue is resolved.*

Improvements:

- License Installation Dialog
  - Prior release said to restart the GW Server. This dialog was updated to include the directions to perform the GW Server Restart.

- License Status GUI
  - Prior releases showed License Status information even when the GW Server was not running. This result in incorrect / out-dated license information being shown. *This issue is resolved*.

R2.0.1 (Minor Release)

Note that there were NO GW code modifications in this release. The R2.0.1 release was a FW Kit Upgrade (installer change only).

New Features:

- None

Bug Fix:

- None

Improvements:

- SDS Sensor FW Kit (Updated)
  - The SDS Sensor FW Kit installed with the SDS GW is now R2.6.2 (Prior R2.6.1). Refer to the Sensor release notes regarding the modifications in R2.6.2.

R2.0.0

Baseline release of the SDS Gateway Server / Client implementation.