INTRADO SAFETY SUITE SERVICE GUIDE

Ver. 2023.04.19

Table of Contents

Introduction

This Service Guide describes the products and services that together constitute Intrado's Safety Suite. Safety Suite includes the three elements defined below:

1. **Safety Shield** is a cloud-based web and mobile application creating an incident and safety management platform which includes a soft panic button that transmits the user location and incident details to the correct 911 Emergency Communications Center ("ECC") while simultaneously triggering a workflow response and notifying administrators and staff.
2. **Intrado Wearable Panic Button** (optional) is a hardware panic button which transmits the device location and incident details to the correct 911 ECC while simultaneously notifying administrators and staff.
3. **Revolution Notification Management Platform** (optional) is a premise-based mass notification software solution that unites fragmented on-premise systems and processes into a centralized platform to help people notify staff and communicate critical information more efficiently.

Safety Shield

The Safety Shield web portal is available through standard web browsers with Internet connection. The mobile phone application is available for download for users to access its features. It is available for iOS and Android devices through the Apple App Store and Google Play store. The mobile application is supported on the latest operating systems.

The Safety Shield service provides a hub for emergency response with a single operational view and integration with critical systems. All documentation, data, safety information, and incident management efforts are managed via the Emergency Response Hub. The hub's features currently include:

- A digital document library for document storage to support event response workflows, and situational data such as floor plans; Emergency Response Plans (ERPs), and emergency contacts;
- Geographical view of campuses, events occurring on them and the response protocols status in a single dashboard
- Role-specific action checklists to provide specific guidance on how to respond to emergencies;
- Safety drill management to launch, schedule, and manage safety drills, provide training, and identify opportunities for improvement;
- Reunification process to account for staff and/or students in near real time
- Event metrics can be tracked and monitored in real time and can be reviewed post-event to evaluate response efficiency and processes. Detailed event reports are available for emergency response review and to assist with compliance reporting; and,
- Staff communication that includes real time, one- and two-way communication among users via the web portal and the mobile application, as well as the wellness check notifications, and post-crisis check-ins.

Additional features include: event history; broadcast notifications; in-building notifications; floor plans; emergency response plans (ERPs); checklists; library; users; emergency contacts; chat; staff check; user groups; visitor logs (this feature requires integration with the visitor management platform); event summary reports; drill summary reports; drill comparison reports; general reports; event types; event gateway; map editor; operational roles; user permissions; and security desk support.

The Safety Shield service can integrate with the following third party or Intrado tools for enhanced emergency response features.

- Mass Notification – external notification capabilities
  - Broadcast Notification through integration with Customer's mass notification system's REST API. Enables messaging via pre-defined repeating broadcast notifications sent to a pre-defined list of recipients.
- School Information System (SIS)
  - Student Attendance – mobile users can take attendance when an emergency event is activated to determine who is present or absent at the time of the event.
  - Student Attendance – mobile users can take attendance when an emergency event is activated to determine who is present or absent at the time of the event.
  - Guardian Reunification – matching parent/guardian ID information on file to reunite students following an emergency event.
    - Intrado is currently able to pull information from the third-party SchoolMessenger solution if the Customer has a current subscription. The Customer must notify Intrado if this subscription lapses, or if another platform is utilized.
- Intrado Revolution – unified web-based platform that allows management of communication or security technology from a single, simple interface.
  - In-building notification and alarms
- Visitor Management System
  - Visitor Logs – a searchable list of currently signed-in visitors.
- Intrado Emergency Data Broker platform
  - An additional way to share safety information with 9-1-1 PSAPs/first responders at time of the emergency call. Secure, two-way texting enables situational awareness.

Intrado Wearable Panic Button

This wearable panic button is a small, wearable device configured through Safety Shield which, when activated:

- Sends a wireless signal to alert on-site staff and administrators in the event of an emergency;
- Triggers events in Safety Shield;
- Can send an alert to 9-1-1; and
- Can relay critical information (such as device location and incident details) to emergency responders.

The Intrado wearable panic button offers triple redundancy, operating on Bluetooth Low Energy, WiFi, and Cellular/LTE connections. Health checks on the panic buttons occur daily, and can be monitored by customer administrators.

Wearable panic buttons are powered by a rechargeable, commercial-grade battery, and when activated, light up with two LED lights. The lights are configurable within the Safety Shield application.

Each of the Intrado wearable panic buttons has two buttons: one on the front, and one on the side of the device, and the button press sequence is configurable in the Safety Shield application, which allows for configuration of multiple event types, each with its own unique press sequence.

Each purchase of the Intrado wearable panic button includes a charger and two Intrado Beacons, which are small, battery-powered Bluetooth radio transmitters that transmit Bluetooth Low Energy (BLE) signals. Beacons can be detected in the Safety Shield application to ensure area coverage during implementation and registration. Beacons are replaced every two years for customers under a current subscription agreement.

Beacons can be placed in and registered to a static location. Panic buttons are registered to individual users and can be activated and deactivated as necessary. Configuration of device behavior occurs in the Safety Shield application.

Offered on a Hardware-as-a-Service subscription basis, or upfront purchase. The Safety Shield application is required for use of the Intrado wearable panic button.

Each purchase includes the following:

- 1 device;
- 2 Bluetooth low energy beacons;
- 1 charging cable and charger;
- 1 silicone sleeve in the color selected by the school district; and
- 1 logo per school district.

Revolution Notification Management Platform

The Revolution software platform enables the customer to deliver information and alerts to people on or off-premises. Communications can include live or scheduled notifications with text, audio, and graphics delivered to cell phones, computers, IP phones, overhead IP and analog speakers, loud horns, digital signs, and more. Revolution can also be used to alert people located off-premises using tools like mobile alerts, SMS, email, collaboration chat tools, and social media using the organization's own integrated systems or third-party platforms. Notifications are customizable and support text, audio, and visual information, as well as optional responses for recipients to report on their status (i.e., "Yes, I am safe" or "No, please send help") and can be broadcast or targeted to a select set of endpoints, devices, and contacts.

Revolution Desktop Notification Client

The Revolution Desktop Notification Client (DNC) is a client-side application for Windows and Apple operating systems to become notification endpoints. As an endpoint, user desktops may receive and broadcast emergency alerts, weather alerts, live or pre-recorded audio broadcasts, and text messages.

- Audio / text / visual alerts directly to software installed on users' Windows and Apple computers.
- Notification priority levels determine whether the DNC takes over the computer with a full-screen override or utilizes a less intrusive corner pop-up.
- Recipients can respond to notifications using custom acknowledge buttons.
- Trigger notifications directly from the desktop.

Revolution Mobile Application

The mobile application is available for iOS and Android devices via the Apple App and Google Play stores and is supported on the latest operating systems. The App is licensed as an individual Mobile Endpoint.

- Authorized senders can activate alerts directly from the Revolution mobile app.
- Notifications and alerts received can include predefined text, image, and audio. The sender can also share additional information using the mobile app.
- Audible + Visual alerts delivered to users within the facility or off-premises. Geolocation enables targeted alerts only to those users on-premises.

Implementation

Intrado will provide implementation services by providing the Customer with an assigned specialist who will determine the implementation process and configuration of the environment. The Customer will primarily communicate with the assigned specialist throughout this phase. However, there will be additional coordinators who will continue to be available to assist and provide guidance and suggestions.

The specialist will use information provided by the Customer to construct the organizational hierarchy and will work with Customer to configure any additional features (if applicable).

If applicable, the specialist will configure Lightweight Directory Access Protocol (LDAP) integration with the Customer, as well as provide example files of contacts that will be brought over into the Safety Shield system from the Customer's current Active Directory file.

Intrado will provide configuration support for the Intrado Wearable Panic Button as part of implementation.

Maintenance and Technical Support

What is included:

- 24x7x365 telephone and email support
- Product use guidelines and available configurations
- Resolution of software defects, usage and configuration
- Documentation irregularities
- Customer-owned Intrado hardware fault diagnosis and resolution

What is excluded:

The following are not covered by technical support services. However, many of the services can be purchased as professional services.

- Configuration change request or software enhancement request.
- Incidents traced back to faulty third-party components (firewalls, third party software, network issues).
- Support for third-party platforms, such as the Customer's notification tool or School Information System (SIS).
- Software or hardware not officially supported, validated or approved as specified in the applicable Intrado product documentation
- Repair any issue or support any product that: (a) has been altered, except by Intrado or an Intrado designated representative or in accordance with Intrado's written instructions, (b) has not been installed, configured, operated, repaired, or maintained in accordance with Intrado's instructions, (c) has been subjected to abnormal physical or electrical stress, extreme temperatures, misuse, negligence or accident, or intentional damage, including damage to hardware components from spills, drops, power surge, or improper voltage selection on system's power supply, (d) has been operated outside of the environmental specifications for the product, or (e) when such malfunction, damage or other problem is caused by use with software or hardware that is not recommended by Intrado or that does not conform to the system requirements or specifications made available by Intrado.

How to reach Intrado:

- Customers can obtain support from Intrado through telephone and email support for any Intrado product for which the Customer is entitled to support services. Support is available 24/7 for all emergency issues by phone and five days per week, 9:00 am-6:00 pm EST for all other issues and inquiries.

Email	24x7support@intrado.com
Phone	1-800-988-6228

- Customers should be prepared to supply as much information as possible including:
  - Description (description of the problem or perceived symptoms);
  - Attachments (logs, traces, screenshots); and,
  - Date/time the problem/disruption was detected.

- If the Customer calls the support desk, the support technician will create a trouble ticket, analyze the problem, and attempt to achieve problem resolution as quickly as possible.
- When sending an email, a trouble ticket/request is automatically created in the Support System. Customer can continue to correspond with Customer's Intrado support representative via email or a phone call. Either way, a seamless communications trail is applied to the request.

Severity Levels and Escalation Guidelines

Severity levels are used to manage support resources and to resolve important issues as quickly as possible. The severity assigned to the ticket may be later updated (increased or decreased) after analysis. Severity changes are preceded by a Customer consultation.

Error Severity Level	Severity Level Description	Response	Time for Response
1	**FATAL**: Reported problems preventing all useful work from being done or potential data loss or corruption, or service (including any associated client Hardware or Software) functionality is inoperative; inability to use has a critical impact to Customer's operations; impairment or failure of security systems relating to the service or any applicable data center.	• Acknowledgment • Work Around, temporary fix • Final fix, update, or new release • Communications	• Less than 4 hours - constant effort until fixed • No more than 24 hours • No more than 72 hours • Daily
2	**SEVERE IMPACT**: Problems disable major functions required to do productive work or services (including any associated client Hardware or Software) is partially inoperative and is considered as severely restrictive Customer's.	• Acknowledgment • Work around, temporary fix • Final fix, update, or new release • Communications	• Less than 8 hours • No more than 72 hours • Less than 30 days • Every 48 hours
3	**MINOR** A problem that involves partial, non-critical loss of use of the software in a production environment or development environment. For production environments, there is a medium-to-low impact on the business, but business continues to function, including by using a procedural workaround. For development environments, where the situation is causing testing and/or trial impacts	• Acknowledgment • Work around, temporary fix • Update, or new release • Communications	• Less than 24 hours • No more than 5 days • Over 30 days

4	**Query/Request** A general usage question, reporting of a documentation error, or recommendation for a future product enhancement or modification. For production environments, there is low-to-no impact on the business or the performance or functionality of the system. For development environments, there is a medium-to-low impact on the business, but business continues to function, including by using a procedural workaround.	• Acknowledgment • Update • Communications	• Less than 1 week • No more than 2 weeks

- "Time for Response" means Intrado's acknowledgement that Customer has reported an issue. A support engineer will engage and be in contact with the Customer via various means depending on the severity level.
- Intrado will provide a support engineer to work with the customer on issues on a severity priority basis.
- Intrado will provide troubleshooting support for the Intrado Wearable Panic Button and may request the button to be shipped back if a warranty replacement or deeper troubleshooting is needed.

Customer Responsibilities

Safety Shield:

- The Customer will gather and upload any existing Emergency Response Plans, Actions Plans, Checklists, and Floor Plans for use with Safety Shield.
- The Customer must provide name and contact details for a specific data contact for Intrado Application Specialist to work with on building the Safety Shield environment.
- The Customer will ensure all deliverables are provided on or before the date required, as any delays in the return of completed forms, signoffs, deliverables, and revisions may affect overall timelines and deadlines.
- Customer is responsible for interaction with the ECC and coordination of test calls with the local ECC.
- The Customer will conduct User Acceptance Testing (UAT) on the completed configuration of the Environment, Organizational Hierarchy, and User Accounts. Any issues discovered by the Customer must be reported to the assigned Application Specialist for remediation.

Panic Buttons:

- The Customer is responsible for the following within the Safety Shield application:
  - Intrado (BLE) Beacon placement
  - Intrado (BLE) Beacon registration
  - Intrado Wearable Panic Button assignment

    - Intrado Wearable Panic Button registration
- Any LTE carrier SIM cards that are not provided by Intrado are the responsibility of the customer.

Revolution:

- Intrado is not responsible for the monitoring or management of customer's endpoints.
- The Customer is responsible for server maintenance.
- The Customer is required to provide complete user and organizational information.

Twilio Terms

The Safety Shield application currently utilizes SMS short code for messaging between users of the Safety Shield application. The following terms are required by Intrado's third-party provider of such codes, Twilio:

- Intrado Safety Shield is a program that will send critical event information.
- You can cancel the SMS service at any time. Just text "STOP" to the short code. After you send the SMS message "STOP" to us, we will send you an SMS message to confirm that you have been unsubscribed. After this, you will no longer receive SMS messages from us. If you want to join again, just sign up as you did the first time, and we will start sending SMS messages to you again.
- If you are experiencing issues with the messaging program, you can reply with the keyword HELP for more assistance, or you can get help directly at 24x7support@intrado.com or 1-800-988-6228.
- Carriers are not liable for delayed or undelivered messages.
- Message frequency varies. If you have any questions about your text plan or data plan, it is best to contact your wireless provider.
- If you have any questions regarding privacy, please read our privacy policy at https://www.intrado.com/legal-privacy.

Limitations and Disclaimers

The following limitations and disclaimers apply:

- For Safety Shield, Intrado is not responsible for any third-party platform used in connection with the Services, such as the Customer's notification tool or School Information System. The Customer is solely responsible for the content of information and delivery of any messaging through such systems.
- Intrado may temporarily suspend services, if any abuse of the system is detected or at the request of any federal, state, and local law enforcement agency. Intrado will promptly notify Customer on any suspension of services.
- Intrado may provide reports and other pertinent information or audit Customer's usage at the request of any federal, state or law enforcement agency.

- The Safety Shield services currently operate on geographically diverse Amazon Web Services (AWS) platforms. Intrado is not responsible for any failure or interruption in Services due to a failure of such AWS platforms.
- The Panic Button does not replace other emergency reporting methods. In case of fire, medical, police or other types of emergencies, calls to emergency agencies such as 911 must still be made in addition to activating the Panic Button.
- The Intrado Wearable Panic Button must be properly cared for.
    - Do not submerge the panic button in water. Panic buttons are water resistant but not waterproof.
    - Do not subject the panic button to extreme temperatures.
    - Intrado is not responsible if any intentional damage is inflicted on the device.

Warranty and Returns

Product or Service	Warranty	Returns
Safety Shield	Covered by warranty during the term of any active subscription. Warranty claims will be handled as part of maintenance and support services, as referenced in this Service Guide.	n/a
Wearable Panic Button	Covered for up to five years under an active subscription	Wearable panic button returns: Minimum 15% restocking fee with original packaging. A minimum ground shipping charge of $15 per box will apply to all returns
Revolution	Software covered by warranty during the term of any active subscription. Revolution server hardware is covered by a one-year warranty for parts and labor. Revolution paging relay hardware is covered by a one-year warranty with optional “for fee” extended protection available (purchased by year).	Intrado New in Box Hardware Returns Paging Relay and Server: Minimum 15% restocking fee with original packaging. No returns accepted after 30 days from invoice date. A minimum ground shipping charge of $15 per unit will apply to all hardware. Third-party hardware (devices and accessories) ordered through Intrado and drop shipped from the manufacturer or reseller are subject to the manufacturer's

		policies. All warranty claims and returns should be processed through the manufacturer.

License Terms:

- Customer receives a personal, nonexclusive, nontransferable, non-sublicensable, license to use the Safety Shield or Revolution software delivered or made available to Customer, at the location and on the number of servers, workstations and users or other applicable metric set forth in Customer's applicable order, for the duration of Customer's purchased subscription. All right, title and interest in and to the software, including updates or upgrades, will remain vested with Intrado and its licensors. Customer's rights to use the software will terminate on notice of breach or upon termination of Customer's subscription term. On termination, Customer will destroy all copies of software and associated documentation in its possession or control.
- Customer will not itself, or through any affiliate, agent or other third party: (a) sell, lease or sublicense or otherwise transfer the software; (b) decompile, disassemble, reverse engineer or otherwise attempt to derive source code from the software; (c) modify or enhance the software or write or develop any derivative software or any other functionally compatible, substantially similar or competitive products; (d) network the software or use the software to provide processing services to third parties, commercial timesharing, rental or sharing arrangements or otherwise use the software on a service bureau basis; or (f) provide, disclose, divulge or make available to, or permit use of the software by any third party without Intrado's prior written consent.