ONE PLATFORM, TOTAL CONTROL: INTEGRATING SECURITY WITH WAVESYS

One Platform, Total Control: Integrating Security with Wavesys

As modern security ecosystems become more interconnected, the ability to integrate multiple systems efficiently and securely is no longer optional—it is essential for effective operations. While current advancements address several integration challenges, the diversity of security systems continues to grow. The good news is that with the latest updates in the Wavesys platform, system integration has become more streamlined than ever.

Introducing the dedicated **"Security Systems API"**—a powerful and flexible interface designed to enable seamless connectivity between Wavesys and third-party systems such as access control solutions, security panels, fire alarm systems, and more.

This document provides an overview of the integration framework using this API, along with supporting developer resources that simplify implementation, testing, and deployment.

Why Integrate Security Systems with Wavesys?

Connecting your safety and security infrastructure directly with Wavesys is more than just a technical enhancement—it's a strategic upgrade that strengthens overall operational control. Key advantages include:

Unified Real-Time Visibility: Monitor all security and safety events through a single interface within Wavesys, eliminating the need to switch between systems.

Centralized Command & Control: Manage doors, partitions, alarms, and sensors efficiently from one platform.

Future-Ready Scalability: The Wavesys ecosystem is designed to evolve with your infrastructure, supporting expansion without complexity.

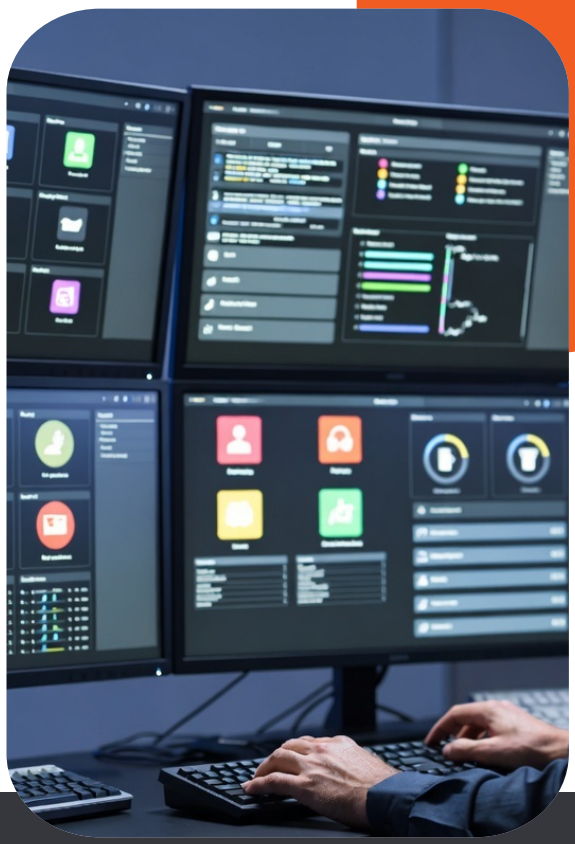
Interoperability Across Systems: The API supports integration with diverse hardware and protocols, provided they align with defined endpoints.

Developer Resources: Tools to Accelerate Integration

To support developers and system integrators, Wavesys provides a set of resources aimed at reducing development effort and ensuring smooth implementation:

Access Control Adapter API Documentation:
Detailed technical documentation covering API architecture, endpoints, request/response structures, and implementation guidelines—helping teams get started quickly and efficiently.

Sample Access Control Adapter:
A ready-to-use reference implementation demonstrating how software-to-software integration can be achieved. This serves as a foundation for building customized solutions while following best practices



Access Control Emulator:
A lightweight simulation tool that mimics real-world system behavior, including event generation. This allows developers to test integrations in a controlled and realistic environment before deployment.

Together, these resources are designed to simplify onboarding, reduce development time, and ensure reliable, scalable integrations within the Wavesys ecosystem.

From Setup to Deployment: A Practical Integration Workflow

Getting started with the Wavesys Security Systems API is designed to be simple and developer-friendly. Follow the steps below to move from initial setup to a fully functional integration:

Access the Codebase:
Begin by downloading the available resources from the Wavesys repository, which include documentation, sample implementations, and testing tools.

Initialize the Emulator:
Use the Access Control Emulator to simulate a real-world environment. This allows you to validate system responses and test integration behavior without requiring live hardware.

Customize the Adapter:
Adapt the sample Access Control Adapter to align with your specific system architecture, workflows, and operational requirements.

Validate Your Implementation:
Conduct extensive testing using real-world scenarios. Simulate common use cases, evaluate system performance under load, and ensure reliability across expected operational conditions.

Integration Fundamentals: Core API Structure

To establish full compatibility with the Wavesys platform, integration begins with a base endpoint that exposes system capabilities:

/info – Provides essential system details, supported functionalities, and the unique integrator identifier.

The response from this endpoint outlines additional endpoints that can be implemented. While the suggested structure can be followed, it can also be adapted to suit your system design.

Key API Endpoints

- /v1/users
  Manages user or cardholder data, with optional support for images. (Custom paths such as /custom/v1/users can also be used.)
- /v1/events
  Streams event data for real-time monitoring and analysis.
- /v1/actions
  Enables execution of commands such as locking/unlocking doors or bypassing alarms.
- /v1/parameters
  Allows configuration of system settings like access rights or PIN codes.
- /v1/items
  Provides control and monitoring of system components such as doors, zones, and outputs.
- /v1/states
  Displays the current operational status of all connected components.
- /v1/notifications
  Uses Server-Sent Events (SSE) to deliver real-time updates from the system.

If the external system operates on a closed architecture or relies on low-level protocols, an intermediate adapter (proxy service) will be required to bridge communication between Wavesys and the target system.

API Response Structure

All responses from the API follow a standardized JSON format to ensure consistency and ease of processing:

```
{ "page":null,

 "nextPage":null,

 "error":null,

 "errorMessage":null,

 "data":{}}
```

This uniform structure simplifies parsing, error handling, and integration across different systems.

Ensuring Secure Integration

For a successful and secure connection between Wavesys and third-party systems, the following requirements must be met:

1. Unique Integrator ID (GUID)

Each integration must include a unique identifier issued by Wavesys (subject to NDA approval). This GUID must be embedded within the adapter or third-party system. Without it, Wavesys will not authorize the connection.

This identifier acts as a secure authentication mechanism, ensuring that only verified systems can interact with the platform.

To obtain your Integrator ID, connect with the Wavesys team or your designated account representative.

2. Enable Integration Licensing

The "Security System Integration" feature must be activated within your Wavesys license. This applies to both live deployments and testing environments.

Without the appropriate license configuration, integration attempts—even if technically correct—will not be accepted by the system. Ensure this requirement is addressed during procurement or setup.

Be Part of the Integration Ecosystem

We encourage developers and integrators to leverage Wavesys API capabilities to connect access control systems, fire panels, security systems, and more into a unified platform.

Whether you're working with a single entry point or an enterprise-level infrastructure, Wavesys provides the tools and support needed to build reliable integrations.

Explore the available resources, experiment with the emulator, and contribute to a growing network of professionals focused on creating connected, intelligent security environments.

Follow us on

Wavesys Global | 16192 Coastal Highway | Lewes, DL-19958, County Of Sussex, |United States of America
www.wavesysglobal.com | sales.americas@wavesysglobal.com