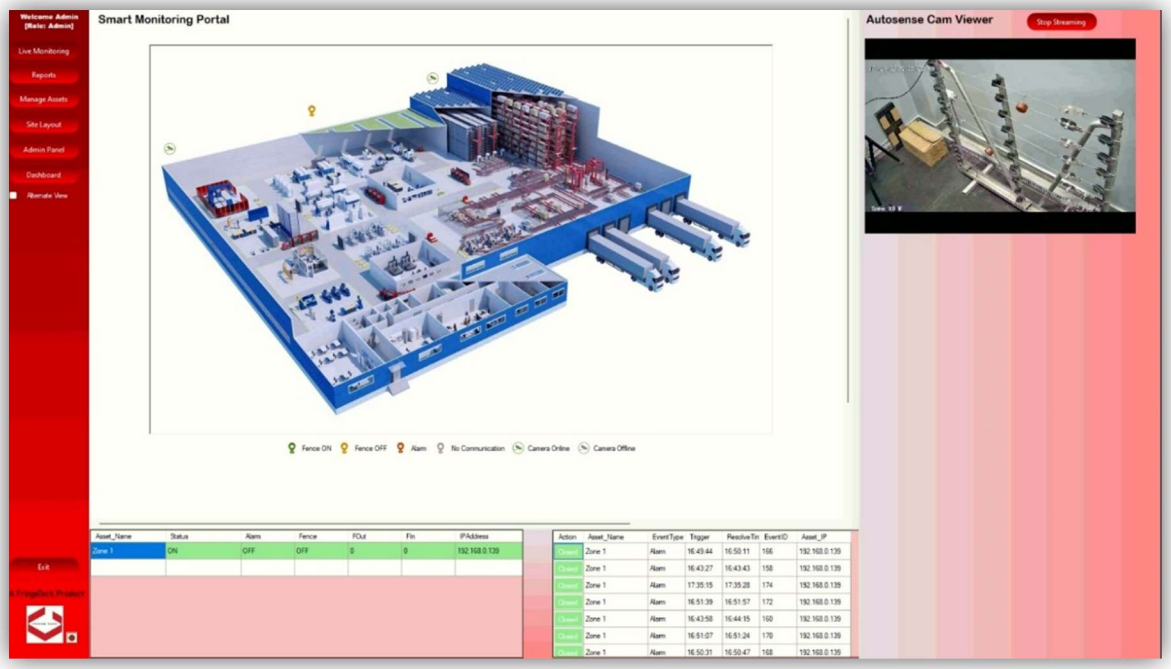
PIDS Software

Interactive Graphical User Interface

The software must feature an intuitive and user-friendly graphical interface that allows users to easily navigate, monitor, and control all connected devices and security systems. The interface should be visually rich with real-time data representation.



Facility to monitor different security Zones

The system should allow the user to configure, monitor, and manage multiple predefined security zones independently, offering zone-specific status, alarms, and controls.

Complete control of the Fence

Users should be able to arm or disarm the fence, monitor fence voltage levels, acknowledge alarms, and configure automated actions all from the software interface.

Multi User Interface

Support for multiple users with customizable access levels. Each user can have individual dashboards, access rights, and control permissions.

User Authentication

Only authorized personnel should be allowed access via strong authentication methods such as username/password or biometric login.

Password Protected Operations and Logging

Every security operation such as configuration change, arming/disarming, etc., should be password protected and the activities logged with timestamp and user details for audit purposes.

Administrative Full System Control

Administrators should have complete control over the system including user management, permission settings, device configuration, and event override.

Database Encryption

All stored data, including logs and configuration files, must be encrypted to prevent unauthorized access or tampering.

Customised Site Layouts

Users should be able to import site maps and overlay device placements for a clear visual understanding of device positions and event locations.

Drag & Drop Device Mapping

The interface should support simple drag-and-drop functionality for mapping devices onto the layout, making system setup and changes easier.

Support for Various Layout Formats

Compatibility with multiple layout file types such as JPG, PNG, BMP, or CAD formats for flexible system visualization.

Audio Video Alarms

The system must generate real-time audio and video alerts for intrusion, malfunction, or any anomaly to ensure rapid response.

Dedicated Reporting Dashboard

A robust dashboard that allows filtering, viewing, and downloading reports in Excel and PDF format. Should include summaries, detailed event lists, and graphs.

Dedicated Event Window

A specialized window showing all system events with classification such as open, in progress, or closed, along with timestamps and relevant device information.

Dedicated Camera Viewing Window

A live view section to monitor camera feeds, allowing users to visually verify incidents in real-time.

Dedicated Health Monitoring Dashboard

A separate interface section that shows system health metrics such as device status, connectivity status, and performance indicators.

Event Type Segregation

Ability to categorize and filter events based on type – intrusion, fault, tampering, etc., for easier analysis and response.

Event Log Archive

Historical event data should be archived and accessible for future analysis, compliance, and auditing.

Smart Scheduling Feature

Allows users to schedule security actions like arming/disarming or maintenance routines at specific times or intervals.

High Level Interface API

Support for APIs that allow integration with third-party applications, central management systems, or government monitoring systems.

Full Screen Mode

A mode where the software occupies the entire screen, disabling access to other applications to prevent tampering or distraction.

TCP/IP Communication

Communication between system components should use standard TCP/IP protocol ensuring secure and reliable connectivity.

Integrated Camera View

Unified view of all surveillance feeds integrated directly into the software, eliminating the need for a separate video monitoring system.

Instant Camera Pop-up

When an event occurs, the corresponding camera feed should automatically pop up to provide immediate visual confirmation.

Instant Camera Screenshot

System should automatically take a snapshot from relevant camera feed at the moment an event is triggered for documentation.

Smart Rack Integration

System should integrate with smart racks for automated control and environmental monitoring of server or equipment enclosures.

Temperature Monitoring with Alerts

Real-time monitoring of system and environment temperature. Alerts should be generated if values exceed safe thresholds.

AI-powered Temperature Management

Use of AI to learn and predict temperature trends and automate response actions like fan activation or system shutdowns to prevent damage.

Certifications

The software OEM should be certified under CMMI Level 3 and ISO 9001:2015, ensuring quality standards. Certifications must be current (less than 6 months old at time of bid).

Techroots Intelliprojects

info@intelliprojects.in

C-1175, Ground Floor, Ansal Esencia, Sector-67, Gurugram - 122101