OnGuard® Access

Overview

OnGuard Access is an integrated access control and alarm monitoring system that delivers maximum protection, versatility, simple operation and cost efficiency. OnGuard Access incorporates the most advanced technologies available, including modern object-oriented software, an advanced client/server database architecture and Microsoft's multitasking, multithreading 32-bit Windows 2000/XP/2003 operating system. Solid technology and an intuitive graphical user interface combine to make OnGuard Access the most powerful yet easiest to use integrated security management system on the market.

Unlimited Handling Capacity

OnGuard Access offers unlimited scalability within a single, seamlessly integrated software solution. It has been designed to meet the needs of any size organization, from one that requires an entry-level, two-reader system to a large corporation with numerous facilities and thousands of card readers located around the world. OnGuard Access supports an unlimited number of card readers, alarm points and cardholders.

Segmentation

Segmentation is an optional feature that provides a logical way to group database components. System administrators define segments within the database, then assign each system user or object (access levels, card formats, badge types, etc.) to one or more of those segments. Segmentation is beneficial in environments where not every cardholder needs access to every area within a facility. A user sees only those objects that are in his segment(s) and those objects that are system-wide. In a segmented system, only those records associated with a particular segment are downloaded to the Intelligent System Controllers and associated field hardware in that segment. By minimizing the number of records that must be stored in a given device, segmentation provides more efficient utilization of the limited memory contained in access control hardware.

Scheduler

OnGuard's scheduling utility allows system administrators to coordinate and plan system actions to be performed in the future. Many system operations can and are often anticipated to occur on certain dates at certain times. To reduce the risk of error in performing these functions manually, administrators can set rules of execution for actions such as starting guard tour, archiving, firmware or database downloads, and DataExchange scripts. Scheduler can also be configured to repeat security actions such as arming/disarming areas or masking/unmasking specific alarms. For any Scheduler action, the iterations can be one-time-only, or repeated at the administrator's desired frequency. Such actions may occur once every hour, at a specific time every day, on a specific day of the week, or on a specific day of the month, recurring as often as the system requires.

Applications to Integrate

- OnGuard Area Access Manager
- OnGuard Biometrics & Smart Cards
- OnGuard ID CredentialCenter
- OnGuard Fire & Intrusion
- OnGuard VideoManager
- OnGuard Visitor

Integration Toolkits and Standards to Enable

- OnGuard DataExchange
- OnGuard OpenAccess Alliance Program
- OnGuard DataCondulT
- OPC Server/Client
- SNMP Agent/Manager
- WebSphere MQ Adapter

Support

- Intelligent System Controller (ISC) Communications
  - Ethernet
  - RS-232
  - Multidrop (RS-485)
  - Modem
  - Dual-Path
- FIPS 197 128-bit AES encrypted ISC Communications
- FIPS 140-2 Validation Pending
- Industry Standard Card Reader Technologies

Features

Flexible Programming Functions

- First Card Unlock
- Elevator Control
- (Selective) System Downloads
- Import/Export Utility
- Occupancy Limit
- Local and Global Anti-Passback

Flexible Monitoring Functions

- Alarm Masking Groups
- Graphical Maps and System Overview Tree
- Monitor Zones
- Alarm/Event Mappings and Routings
- Customizable Voice Instructions and Annunciation

Flexible Cardholder Commands

- Escort Control
- Use Limits
- Extended Individual Strike Times and (On-Demand) Door Held Open Times
- Destination Assurance (with Elevator Control)

Flexible Card Reader Commands

- Time Zone Overrides
- Cipher Mode
- Multiple Card Formats
- Denied Access Attempts Counter

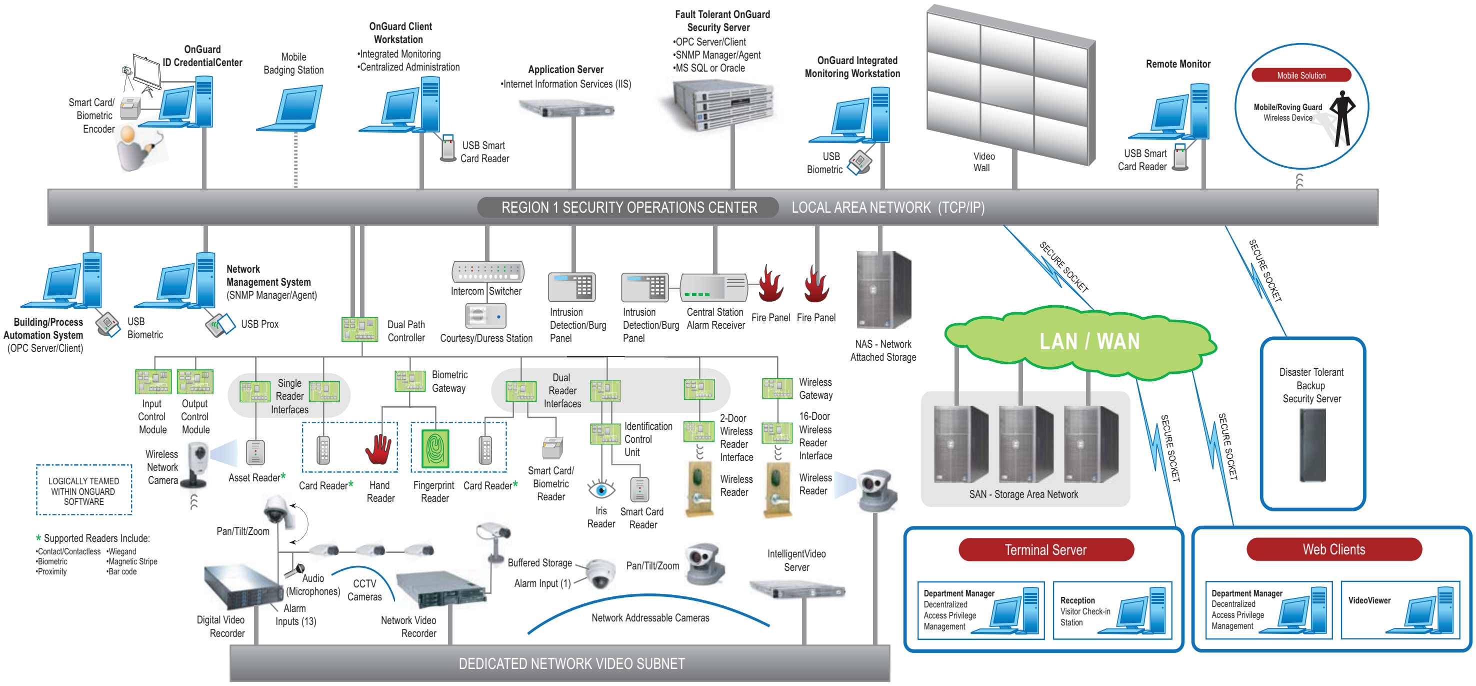
Options

- CCTV Interface
- Paging/E-mail Interface
- Video Verification
- Mustering
- Guard Tour

Lenel

A UTC Fire & Security Company

OnGuard System Architecture



Area Control

■ **Global Hard Anti-passback** allows administrators to require that cardholders present credentials to both enter and exit an area. This prevents the same credentials from simultaneously being used elsewhere in the area, while reporting an alarm to the Alarm Monitoring workstation(s).

■ **Global Soft Anti-passback** allows administrators to require that cardholders present credentials to both enter and exit an area. This rule would allow the same credentials to be simultaneously used elsewhere in the area, accompanied by an alarm will be reported to the Alarm Monitoring workstation(s).

■ **Timed Anti-passback (across readers)** allows administrators to determine how long after an accepted card-read before the same credential may be allowed at the same card reader. This rule can also be applied across a group of readers, a valuable feature for turnstile applications where multiple readers are in close, open proximity and credentials have a chance of being passed back for additional use.

■ **Two Person Control** allows administrators to require that two individuals be present before being able to access high-security areas and both credentials be presented upon exit of those areas. In between entry and exit of the first two and last two cardholders, individual access may be allowed as the two-cardholder minimum is in effect.

■ **Occupancy Limit** allows administrators to restrict the amount of cardholders in a specific area at any given time. Once the Occupancy Limit has been reached, a cardholder must use the exit reader before another card read will be accepted at the entry reader. This is a valuable instrument in managing access to parking areas which are at capacity.

Global Input/Output Event Linkage

OnGuard allows administrators to configure linkages where any input/output/event can be linked to any other input/output/event in the system. These linkages can be derived from any OnGuard application and associated hardware. Events such as invalid access level, valid card read, or motion detection might trigger such outputs as unmasking an alarm masking group, open an area or set the active mode of a card reader. With Global I/O, OnGuard is easily automated to ensure rules execute properly and security can be engaged instantly as necessary.

Lenel Systems International, Inc.
1212 Pittsford-Victor Road
Pittsford, New York 14534
Tel 585.248.9720 Fax 585.248.9185
www.lenel.com

A UTC Fire & Security Company