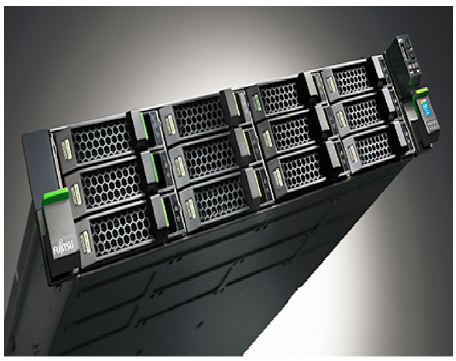
SECUREALL SECURITY REINVENTED℠

Guardian Software SA-GSW

(comes installed on a SecureALL supplied server)



Server specifications

Package	Laptop, rack mount w/single power supply, or rack mount with dual power supply
Rack Mount Dimensions	19.85" x 17.2" x 1.7"
Rack Mount Power Supply	100-240 VAC / 400W
CPU	1 - 2 Intel Xeon E5-2600
Memory	32 - 128 GB
Mass Storage	SSD and HDD: RAID-1
Remote Management	IPMI 1.5/2.0 dedicated LAN
LAN Interfaces	2 x 1000BASE-T, RJ45
Operating Temperature	+10° C to +35° C
Operating Humidity	8 - 90%, non-condensing
Operating System	Linux/CentOS
Application Server	JBoss
Application Software	SA *Guardian*

Features & Benefits

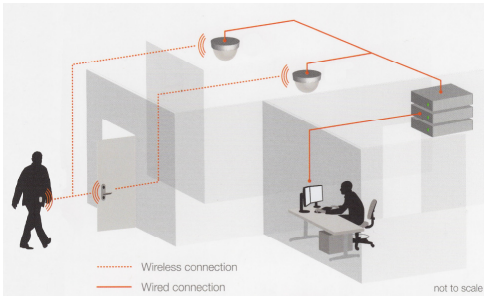
- **Turn key - ready to use system**
- **End-to-end hard encryption**
- **No backdoor - customer owns the encryption keys**
- **Easy to set up and maintain**
- **Server is data repository only; locks have autonomous control over accessibility**
- **No risk of compromised site encryption key**
- **Domains allow flexible and cooperative multi-department use**
- **Lowest Total Cost of Ownership**
- **Multi-featured, not simple access control**
- **System capability can be expanded as users and requirements grow**

System specifications

Size	1K, 5K, 10K, 20K, 70K doors
U-Key™ Users	Up to 70,000
Concurrent GUI Users	≤ 12
Access Groups	Up to 10,000, each with up to 500 room schedules
User Membership of Access Groups	Up to 100 memberships/user
U-Key™ Access Levels	5 levels available. The highest level is assigned to "first responders," who have access even during lockdown
GUI Encryption	SSL
Device Communication	PKI and AES
Audit Trail	3 months of data stored
Door Activation Distance	Programmable from 20% to 300% of standard opening distance (3')
Client Operating System	Windows

Guardian Software SA-GSW

How it works



System functionality

New Device Join	PKI cryptographic acceptance
Encryption Keys	Each device has separate PKI and AES encryption key; user controlled
U-Key™ Encryption	Separate key per door
Remote Lockdown	By room, floor, building, campus, or pre-defined door set
Local Lockdown	At a door
"Reflex" Lockdown	Automatically locks down a building when multiple local lockdowns are initiated within a defined time period
Partitioning of Campus	Each administrator controls only a specific part of the campus
Role Management	Collection of user defined action privileges. User can have multiple roles
Support Isolated Secured Network	Router connected to server via VLAN
Door Unlock	Local (with U-Key™) and remote
Asset and People Tracking	Utilizes door locks and/or tracker
Integration With Other Enterprise Systems	Web-services compliant interface
Security Watch Window	Puts U-Key™ user's picture on a monitor for extra validation

Frequently asked questions

1. **Do customers have to purchase server hardware?** SecureALL provides a turnkey, prebuilt server with the *Guardian* software ready to use. Servers are sized for a customer's specific needs. The server can be field upgraded as capacity requirements increase.
2. **Where does access control information reside in the system?** The server automatically downloads this information to each applicable lock. The lock is then fully capable of making access control decisions without going back to the server. As locks are battery operated, doors will continue to function, even in the event of a power failure.
3. **Does SecureALL have a master account for access into a deployed server?** No, customers are in complete control of users who can log into the system and their operational and domain privileges. Customers have the option of creating their own private PKI keys, not known to SecureALL, thus ensuring no backdoor entry.
4. **Can one server handle multiple campuses?** Yes, the only requisite is that the LAN connecting the SecureALL routers be configured to provide a low latency communication link with the server. Client PCs can also be deployed across multiple campuses.
5. **Can the server be located in the "cloud?"** For security and logistics reasons, customers should resist the urge to place their security system server outside their physical control. However, as long as a customer has the necessary network tunneling (quality of service and firewall protection connecting the server, routers and client PC), the *Guardian* system can be deployed in many different topologies.