

IEI eMerge CSI Spec 1 **IEI eMerge™**

Access Control System Specifications

Software version 3.2

Specifier's Guide Release 3.2 and above - December 2008

For use by Specifiers and Application Engineers. IEI eMerge CSI Spec 2

28 13 16 ACCESS CONTROL SYSTEM AND DATABASE MANAGEMENT PART 2 - PRODUCTS

2.01 GENERAL

A. The system shall be implemented through network appliance architecture with a three-tiered modular hardware hierarchy and embedded three-tier software architecture.

B. The system shall integrate, in a browser interface, access control, alarm monitoring, video monitoring, and temperature monitoring applications.

C. All equipment and materials used shall be standard components, regularly manufactured, regularly utilized in the manufacturer's system.

D. All systems and components shall have been thoroughly tested and proven in actual use.

E. All systems and components shall be provided with an explicit manufacturer warranty.

2.02 OVERALL SYSTEM CAPABILITY

A. The Access Control System shall meet the requirements of business and government access control systems. The system shall monitor and control facility access as well as alarm monitoring, camera and video monitoring, communications loss monitoring, and temperature monitoring applications. The system shall also maintain a database of system activity, personnel access control information, and system user passwords and user role permissions. Virtual inputs such as video loss and building occupancy limits exceeded shall also be supported. The system shall be controlled from a web browser and require no software installation or client licenses. The system shall provide control and access to users on Local Area Networks (LAN), Wide Area Networks (WAN), wireless networks, and the Internet. The system shall provide email and/or text message alerts for all alarm conditions and threats.

B. The system shall provide the following Access Control capabilities:

1. Integrated photo ID creation capability with video verification.
2. User interface secured access under encrypted password control.
3. System-wide timed anti-passback function.
4. Regional anti-passback with mustering and roll call functions.
5. Region occupancy counting and control.
6. Dual reader and keypad support.
7. "First-in-unlock" rule enforcement.

8. Multiple access levels and cards per person.
 9. 128-bit card support.
 10. Detailed time specifications.
 11. Simultaneous support for multiple card data formats.
 12. Elevator control.
 13. Access privileges variable by threat level.
 14. Schedule portal unlock by time and threat level.
 15. Card format decoder quickly discovers unknown card formats.
 16. Card enrollment by reader or keyboard.
 17. Compatibility with various input devices including biometric readers.
 18. Activation/expiration date/time by person with one minute resolution.
- IEI eMerge CSI Spec 3

19. Access level disable for immediate lockdown.
20. Use of Threat Levels to alter security system behavior globally.
21. Multiple holiday schedules.
22. Timed unlock schedules.
23. Scheduled actions for arming inputs, activating outputs, locking and unlocking portals.
24. Card enrollment reader support.
25. Counted-use access control.
26. Dual-reader portal support.
27. Wiegand keypad PIN support.
28. 8-bit and 4-bit burst keypad support
29. Integration with supported alarm panels.
30. Optional storage and recall of ID photos and personal/emergency data.

C. The system shall provide the following Alarm Monitoring capabilities:

1. Common alarm panel integration for disarm on access, and arm on egress.
2. Integrated alarm monitoring and event management with alarm panels.
3. Provide alarms on video loss, and video motion detection.
4. Provide for alarms on communication loss and temperature variation.
5. Support the creation of custom sets of alarm event actions.
6. Provide the ability to record video for alarm events.
7. Provide the ability to assign threat levels to various alarms according to severity.
8. Provide system generated email or text message alerts.
9. Support electronic supervision of alarm inputs.
10. Support the use of output relays for enabling circuits under alarm event control.
11. A monitoring desktop that integrates video, system activity logs, floor plans, ID photos, and alarm notifications.
12. Graphic floor plans with active icons of security system resources.

13. System user permissions to grant whole or partial access to system resources, commands, and personal data.

14. Delivery of alerts via browsers, email, and text messages.

D. The system shall provide the following Video Management capabilities:

1. Real-time video monitoring displays, including multiple cameras simultaneously.
2. Playback of access-related video.
3. Video switching based on access activity or event activation.
4. Integrated alarm inputs from the video management system.
5. Digital recording of events.
6. Support for multiple DVR and NVR systems.
7. Multiple supported cameras.
8. Recall of photo ID and real-time image for comparison.
9. Full monitoring through a web browser interface.
10. System user permissions to grant whole or partial access to system cameras and video resources.

E. The system shall provide the following Security Database capabilities:

1. Maintain data of system activity, personnel access control information, system user passwords and custom user role permissions for whole or partial access to system resources and data.
2. Built-in Open Database Connectivity (ODBC) compliant database for personal data.
3. Up to 60,000 person records.
4. Network-secure API for external application integration.
5. Extensive and easy to use custom report generator.
6. User-defined data fields in personnel records.

IEI eMerge CSI Spec 4

7. Record recall by vehicle tag, name, or card.
8. SQL capability and ODBC compliance.
9. Storage of system user passwords and permissions.
10. Storage and recall of ID photos and emergency personal information.
11. Pre-defined reports on system configuration, system activity history, and people.
12. English-based query language for instant custom reports.
13. Custom report writer interface that allows the interactive creation of custom reports. Reports may be saved for later reuse. No third party software (such as Crystal Reports) shall be necessary.
14. Periodic backup to onboard flash ROM and optional network attached storage (NAS), including FTP servers.
15. Email and text messaging (SMS) text messaging alert notifications.

2.03 HARDWARE REQUIREMENTS

A. The system shall employ a modular hardware concept that enables simple system expansion and utilizes a three-tiered hardware hierarchy:

At the top tier is the network controller, which shall contain the database engine, web server, application software, and configuration data. It is at this level that System Users, through a browser interface, shall interact with the System, set configurations, monitor activities, run reports, and manage alarms.

At the second tier is the network node, an intelligent device with native TCP/IP support, which shall make and manage access control decisions.

At the third tier are the application extension blades. Each of these blades shall connect to and manage a set of inputs, outputs, readers, cameras, or temperature monitoring points.

The network device shall run on existing building TCP/IP networks and shall be configurable for access from separate subnets, through gateways and routers, and from the internet. A MicroNode shall also be available that combines an Access Control blade and Network Node.

B. The Network Controller shall contain the operating system, database engine, web server, application software and configuration data. The Network Controller shall be available in three configurations to support small to medium, large and ultra-large systems. Those systems shall be identified respectively as: a basic Network Controller, an Enterprise Network Controller and an Enterprise Ultra Network Controller.

C. A basic Network Controller shall consist of a blade-style, circuit card that also combines a Network Node on the card. The Network Controller portion of the card shall contain a processor, flash memory and network switch. The Network Node portion shall contain a serial port for communication with the Application blades and a network interface port. A basic Network Controller shall have the following capabilities:

1. Nodes/MicroNodes: 32
2. Access control readers: 140 certified

3. Access cards: 60,000
 4. Card formats: 32
 5. Alarm input points: 500
 6. Control point outputs: 500
 7. Temperature monitor points: 500
 8. Elevators 20
 9. Floors 100
- IEI eMerge CSI Spec 5

10. IP, DVR, and NVR cameras: Limited only by license
11. Online event history log: 4 to 10 million records (depending upon configuration and transaction types)
12. Ethernet switch ports: 2
13. Time specifications 512
14. Time spec groups 64
15. Time specs per group 8
16. Threat Levels 8
17. Threat Level Groups 32
18. Holidays 30
19. Access levels per person 16
20. Cards per person 100
21. Report Groups 50
22. Camera Groups 50
23. Concurrent system users 5 (when using the Monitoring Desktop or Camera Views)
10 (when performing administrative tasks)

D. The Enterprise Network Controller shall consist of a 1U rack-mounted Controller with additional processing power and memory, disk drive, serial port and network connections. The Enterprise Ultra Network Controller shall consist of a 2U rack-mounted controller with additional processing power and memory, RAID-1 disk drive array, serial port and network connections. The Enterprise and Enterprise Ultra Network Controllers shall have the following capabilities:

1. Nodes/MicroNodes 64 (256 for Enterprise Ultra)
2. Access control readers 1792 (3584 for Enterprise Ultra)
3. Access cards unlimited
4. Concurrent system users 35
5. Alarm input points 2000 (4000 for Enterprise Ultra)
6. Control point outputs 2000 (4000 for Enterprise Ultra)
7. Temperature monitor points: 500
8. IP, DVR, and NVR cameras: Limited only by license
9. Online event history log: 4 to 10 million records (depending upon configuration and transaction types)

10. Ethernet switch ports: 2
11. Time specifications 512
12. Time spec groups 64
13. Time specs per group 8
14. Threat Levels 8
15. Threat Level Groups 32
16. Holidays 30
17. Access levels per person 16
18. Cards per person 100
19. Report Groups 50
20. Camera Groups 50

E. The Network Node shall make and manage access control decisions with data provided by the Network Controller, and it shall manage the communication between the Network Controller and Application blades connected to the system's inputs, outputs, and readers. The Network Node shall be available in three configurations: a combined Network Controller/Network Node blade; a standalone Network Node blade, and a MicroNode with included Access Control blade. Each Network Node shall support up to seven Application blades except for the MicroNodes. Communications between the node and network controller shall be encrypted (SSL 128-bit) and authenticated (SHA-1), if desired. Each Network Node shall have the following capabilities:

1. Application blades 7
2. Access control readers 14
IEI eMerge CSI Spec 6

3. Access levels 512
4. Portals 14
5. Portal Groups 64
6. Readers 14
7. Reader Groups 128
8. Supervised Inputs 56
9. Input Groups 64
10. Relay Outputs 56
11. Output Groups 64
12. Temperature Monitor Inputs 56
13. Elevators 14
14. Floors 52
15. Floor Groups 64
16. Credential storage 20,000
17. Activity log records 27,000

F. The Application blades shall interface with the Network Controller through the Network Node. The Application blades shall be blade-style circuit cards. There shall be four types of Application blades:

1. Access Control blade: shall support 2 readers (input devices such as keypads, RFID devices or Biometric readers), 4 supervised inputs and 4 relay outputs.
2. Supervised Input blade: shall support 8 supervised inputs.
3. Relay Output blade: shall support 8 relay outputs.
4. Temperature blade: shall support 8 analog temperature sensor inputs. Temperature precision shall be 32.9° F (0.5° C). Temperature range shall be 32° to 158° F (0° to 70° C).

G. The MicroNode shall combine a Network Node and an Application blade capability in one enclosure. The Access Control blade portion of the MicroNode shall support two readers, one temperature input, four supervised inputs and four relay outputs. A MicroNode shall utilize 12VDC power at 3 Amps or Power over Ethernet (PoE) at the 802.3AF standard and be capable of supplying direct power to 2 readers, 2 motion REXs, and 2 door strikes.

2.04 HARDWARE PACKAGING REQUIREMENTS

A. The system shall have various hardware enclosures and configurations available to support different installation requirements. Enclosures shall be available for wall or rack mounting. The wall-mount enclosures shall have a lock requiring a key, and a cabinet door tamper switch.

B. The Wall-Mount enclosure supports one Network Controller/Node blade or a standalone Network Node blade and seven Application blades. The dimensions are: 17" (432 mm) H x 15" (381 mm) W x 6.75" (171.5 mm) D.

C. The Rack-Mount enclosure supports one Network Controller/Node blade or a standalone Network Node blade and seven Application blades. The dimensions are: 19" (483 mm) W x 7" (178 mm) H (4U) x 15" (381 mm) D.

D. Enterprise Network Controllers shall be housed in a 1U rack-mount enclosure with dimensions of 19" (483 mm) W (including the mounting brackets) x 1.75" (0.7 mm) H x 16.75" (425 mm) D.

E. Enterprise Ultra Network Controllers shall be housed in a 2U rack-mount enclosure with dimensions of 19" (483 mm) W (including the mounting brackets) x 3.5" (1.4 mm) H x 16.75" (425 mm) D.
IEI eMerge CSI Spec 7

F. The MicroNode enclosure shall support a Node and its Access Control blade. It shall be a wall-mount enclosure with dimensions of 7" (178 mm) H x 7" (178 mm) W x 3.5" (89 mm) D.

G. The system shall be powered by either 100-240V AC at 50-60 Hz, or by 12VDC at 3 amps. Power must come from a separate circuit with an isolated earth ground. If AC power is supplied it must be connected to the internal power supply. If DC power is supplied the internal power supply shall be bypassed. It shall be possible to backup power supplied to the system with an Uninterruptible Power Supply (UPS). It shall also be possible to place within the wall-mount enclosure an SLA battery backup sufficient for an orderly shutdown in case of external power loss.

2.05 NETWORK CONTROLLER and APPLICATION BLADE HARDWARE SPECIFICATIONS

A. Basic Network Controller

1. Network Nodes Supported: 32
2. Processor: Intel® IXP425
3. RAM: 128 MB
4. Flash ROM: 48 MB
5. Compact Flash Memory: 2 GB (8 GB maximum)

B. Enterprise Network Controller

1. Network Nodes Supported: 64
2. Processor: Intel® Celeron® 2.0 GHz
3. RAM: 1 GB, 2GB maximum.
4. IDE Hard Disk Drive: 80 GB
5. CDRW/DVD-R: Optional, external USB
6. Ethernet Ports: 2 (10/100)
7. Operating Temperature: 32° to 104° F (0° to 40° C)
8. Humidity: 10 to 80 % relative humidity
9. Power Supply: 200 W, 100 to 200 VAC
10. MTBF: 52,560 hrs (calculated)
11. Weight: 16 lbs. (7.28 kg)

C. Enterprise Ultra Network Controller

1. Network Nodes Supported: 256
2. Processor: Intel® Pentium® 4 @ 2.8 GHz
3. RAM: 2 GB, 4GB maximum.
4. IDE Hard Disk Drive: 2 x 80 GB SATA in RAID-1 configuration
5. CDRW/DVD-R: Internal
6. Ethernet Ports: 2 (10/100)
7. Operating Temperature: 32° to 104° F (0° to 40° C)
8. Humidity: 10 to 80 % relative humidity
9. Power Supply: 300 W, 100 to 200 VAC
10. MTBF: 52,560 hrs (calculated)
11. Weight: 30 lbs. (13.57 kg)

D. Access Control blade

1. 7-pin reader connectors 2
2. Maximum reader wire length 500 feet (152 m) (18 AWG twisted, shielded)
300 feet (91 m) (22 AWG twisted shielded)
3. Power available to readers 400 milliamps
4. 2-pin supervised input connectors 4
IEI eMerge CSI Spec 8

5. Maximum input wire length 2000 feet (610 m)
6. 3-pin relay output connectors 4
7. Maximum output wire length 2000 feet (610 m)

E. Input blade

1. 2-pin supervised input connectors 8
2. Maximum input wire length 2000 feet (610 m)

F. Output blade

1. 3-pin relay output connectors 8
2. Maximum output wire length 2000 feet (610 m)

G. Temperature blade

1. 2-pin analog temperature inputs 8
2. Using 18 AWG twisted, shielded 1000 feet (305 m)

NOTES:

All application blades shall receive power via the ribbon cable bus directly from the Node blade.

Relay output connectors: Both normally-open circuit and normally-closed circuit output devices shall be supported. The relay outputs shall support any output devices that operate on the following maximum electrical ratings: 30 Volts DC or AC, 2.5 Amps inductive or 5.0 Amps non-inductive.

Supervised input connectors: Shall support a wide variety of input supervision types including normally-open circuit and normally-closed circuits, and zero, one or two resistor configurations.

2.06 SOFTWARE REQUIREMENTS

A. Operating System and Application Software

The embedded operating system for the solid-state Network Controller shall be Linux®. The disk-based Enterprise and Enterprise Ultra Network Controllers shall use FreeBSD® UNIX as the operating platform. The operating system kernel shall be open-source and no operating system training or certification shall be necessary.

The system application software shall be embedded in the system. The database shall be an embedded PostgreSQL relational database requiring a small footprint and provides high reliability. The web server shall be based on an embedded GoAhead™ web server enabling users to access and operate the system using a standard web browser.

B. Software Licensing

Software licensing shall be based upon the number of readers and cameras for one network controller board only. Software license upgrades shall be available if system reader and camera capacity must be raised. The user license shall be valid in perpetuity and shall include one year of software updates from the date of shipment from the factory IEI eMerge CSI Spec 9

C. Software Upgrades

Software upgrades shall be possible from a browser on any network-connected PC, by uploading a software update to the Controller. Controllers shall automatically upgrade all connected nodes. No client software installation shall be necessary.

D. Online Help and Documentation

The system shall be provided with complete embedded documentation. The documentation shall include:

1. Context-sensitive online Help. (The Help displayed is specifically relevant to the current screen.)

2. Technical Support Notes (PDF format)

3. Installation Guides (PDF format)

4. Video Integration Guides (PDF format)

5. System Administration Guide (PDF format)

In addition, it shall be possible to print any Help topic, or any PDF document, to provide users with paper documentation.

E. Support Collaboration

It shall be possible, by the use of a network Support Collaboration Tool, for a technical support specialist to connect to the system and assist on-site technicians from remote network-connected locations. It shall only be possible for an on-site system administrator or technician to initiate this connection. There shall be no way to initiate this connection from outside the secure network.

F. Language Support

The system shall be provided with multiple language support. The ability to switch from one language to another shall be accomplished through the user interface. Translation of the user interface, online help and documentation into other languages shall be available. The languages supported shall include:

6. English

7. Spanish

8. Portuguese

9. Thai

10. Chinese

11. Japanese

G. Date Formats

The system shall support global date formats as follows:

12. mm/dd/yyyy

13. dd/mm/yyyy

14.yyyy/mm/dd

H.Floor Plans

The system shall provide graphic floor plan capability including graphic display of links to other floorplans, alarms, system resources such as portals, IP video cameras, inputs, outputs, and temperature monitoring points. The Network Administrator shall be able to graphically configure device icons onto the floor plan images. JPEG images shall be supported.

IEI eMerge CSI Spec IEI eMerge CSI Spec 10

I. Personnel Data

The system shall maintain person data relating to access control, system user privileges, photo identification, system activity, and contact information. All person data in the system shall be integrated onto one tabbed page for viewing, editing, and deletion by system users.

J. Data Import and Export

A Data Management Tool shall be provided that supports, via an API, the import and export of personnel data. This tool shall make possible the pre-populating, and ongoing populating, of cardholders into the system database. Data that shall be importable shall include:

1. LASTNAME
2. FIRSTNAME
3. MIDDLENAME
4. NOTES
5. EXPDATE (expiration date)
6. ACTDATE (activation date)
7. TEXT1...TEXT20 (user defined fields 1 through 20)
8. ACCESSLEVEL1...ACCESSLEVEL32
9. PERSONID
10. PIN
11. ENCODEDNUM1...ENCODEDNUM10
12. HOTSTAMPNUM1...HOTSTAMPNUM10
13. CARDFORMAT1...CARDFORMAT10
14. BADGELAYOUT
15. JPEG ID PHOTO

K. Data Security

Communication between the network controller and the browser shall be secured using SSL. In addition, administrative access to the security management application and the personnel data shall be password protected and controlled by roles-based authorizations.

Communication between the Network Controller and Network Nodes shall be encrypted and authentication/tamper detection shall be done using the SHA-1 algorithm.

Communication between the network controller and other systems (when using the API) shall be secured using SSL and authentication/tamper detection shall be done using the SHA-1 algorithm.

L. Data Backups

It shall be possible to configure regular automatic database backups to on-board ROM (basic Network Controller), on-board compact flash (basic Network Controller), built-in hard drive (Enterprise and Enterprise Ultra Network Controller) and to save backups to separate network attached storage (NAS) and FTP servers. It shall also be possible to setup regular automatic creation of database archive files.

M. On-board Data Management

Each night the system shall truncate a sufficient number of the oldest records held on-board to reduce the database to its set limit, if required. This shall create the needed storage space for additional system activity records. Truncation will be performed on a First-in, First-out (FIFO) basis. IEI eMerge CSI
Spec 11

N. System User Roles and Permissions

There shall be three pre-programmed levels of User Roles, and a total of 16 possible user roles in the system with different permissions for each user:

1. Monitor: These users may only use the functions in the Monitor menu. Monitor functions shall include viewing the activity log, cameras, and floor plans.
2. Administer: These users may use the functions of both the Administration and Monitor menus. Administrative functions shall include adding and editing person information in the enrollment database, issuing and revoking cards, generating reports, and performing database backups.
3. Setup: These users may use the functions of the Setup, Administration, and Monitor menus. Setup functions shall include defining access control, alarm event behavior, camera settings, floor plan images and configurations, holiday and time specifications. Setup functions shall also include: designation of network resources such as time and DNS servers, email and network storage settings; performance of system maintenance such as database backup and restore, software updates and file cleanups; designation of time zone, daily backup schedule and enrollment readers.
4. Custom User Roles: In addition to the roles above custom user roles can be created for other security application users.

O. Alarm Panels

The system shall be capable of integrating with alarm panels, arming the panels, disarming the panels, and triggering events based upon alarm panel status

P. Alarm Events

The system shall be capable of managing alarm events. It shall be possible to associate specific actions with each alarm event. These actions may include but are not limited to sending pages and emails, energizing outputs to activate lights, locks, or alarms, switching to an appropriate video monitor, recording video, displaying ID photos, changing the system threat level, making entries in a log file, and flashing device icons on a graphic floor plan.

Q. Activity Monitoring

The system shall support a monitoring desktop that integrates video, system activity logs, floor plans, ID photos, and alarm notifications. It shall also be possible to view cameras, activity logs, and floor plans on separate monitoring pages within the application.

R. Access Control

The system shall be able to make access control decisions, define a variety of access levels and time specifications, write system activity into a log file, maintain a personnel enrollment database, receive signals from input devices such as door switch monitors, card readers and motion detectors, energize devices such as door locks and alarms via outputs.

It shall be possible to configure holidays, scheduled actions, anti-passback behavior, and elevator control.

A System user holding a "Setup" user role shall be able to create, delete, and edit access control specifications. IEL eMerge CSI Spec 12

S. Threat Levels

It shall be possible to configure up to eight threat levels. It shall be possible to alter security system behavior through the use of threat levels. Groups of threat levels may be created and assigned to portal groups, access levels, input groups, output groups, floor groups, and event actions. The behavior of groups, access levels, and event actions with assigned threat level groups shall change based upon the current system threat level.

The system shall support 32 threat level groups. It shall also be possible to change the system threat level in response to an alarm event.

The current system threat level shall display in the title bar of the security application interface and on floor plans.

T. Reports

The system shall be capable of producing a variety of predefined reports regarding software and security hardware configuration, event history, and the administration of people within the system. In addition, an easy-to-use query language shall be included to create ad hoc reports. The query language shall be documented in the online help system. Alternatively, it shall be possible to specify a query by use of point-and-click.

It shall also be possible to produce reports directly from the Network Controller based on data in archive files on FTP servers, network attached storage, or the controller-attached compact flash.

The system shall support a graphic interface for interactively building custom reports from either historical or personnel data. These reports shall be savable for later reuse. Parameters can be inserted into reports to prompt for data input at report runtime. Report results can be printed, output to a PDF file or put into a spreadsheet.

It shall also be possible to group reports for assignment to custom user roles. Any reports not grouped and assigned to a custom user role shall not be viewable by that system user.

Report generation shall not affect the real-time operation of the system.

The specific reports provided shall include the following:

1. Configuration Reports

a. As Built: A graphical report that documents all resource connections to the system.

b. Cameras: Displays all camera configuration information including control address, IP port, and camera type.

c. Camera Presets: Displays configured presets for each camera in the system.

d. Elevators: Displays elevator configuration information including Node, Reader, and Floor to output mappings.

e. Floor Groups: Displays all configured floor groups for use in elevator control.

f. Holidays: Displays holiday specification information.

g. Portals: Displays portal definition information including reader, DSM input, REX input, alarm outputs, and events.

h. Portal Groups: Displays a list of all defined portal groups.

i. Reader Groups: Displays defined groups of readers.

j. Resources: Displays all configured system resources including readers, inputs, outputs, elevators, and temperature points.

k. Threat Level Groups: Displays all configured threat level groups and the threat levels assigned to them.

l. Threat Levels: Displays all configured threat levels including the description and color assignment.

IEI eMerge CSI Spec IEI eMerge CSI Spec 13

2. History Reports

- a. Access History: Displays access history based on an entered query. The system user can specify the query using either the keyboard or point-and-click selection.
- b. Custom Report: This provides the capability to create custom reports of historical data. A graphic interface provides the user with the ability to interactively create and save reports for later use. Parameters can be inserted into reports to prompt for data input at report runtime. Report results can be printed, output to a PDF file or put into a spreadsheet.
- c. General Event History: Displays time, type of activity, and activity details for a variety of event types. The system user can select the specific event types for the report.
- d. Portal Access Count: Display how many times users have used a portal.

3. People Reports

- a. Access Levels: Displays all access levels entered into the system including time specification, reader/reader group, and floor group.
- b. Current Users: Displays a list of all security system users currently logged in to the security system website.
- c. Custom Report: This provides the capability to create custom reports of personnel data. A graphic interface provides the user with the ability to interactively create and save reports for later use. Parameters can be inserted into reports to prompt for data input at report runtime. Report results can be printed, output to a PDF file or put into a spreadsheet
- d. Occupancy: Displays a list of defined regions with the number of people currently occupying each region and the maximum number of occupants allowed, if a maximum has been specified.
- e. Photo ID Gallery: Displays all the photo ID pictures in the system and the person's name.
- f. Photo ID Requests: Displays all outstanding badge print requests and lists ID, name, badge layout, activation date, request date.
- g. Portal Access: Lists people with access for a selected portal.
- h. Roll Call: Allows you to select a defined Region from the drop-down and see a list of people currently in that region.
- i. Roster: Displays every person entered into the system and it lists name, ID photo, expiration date, username, and access level.
- j. Time Specifications: Displays all defined time specifications currently in the system.

U. System Administration

The system shall provide for the performance of system administration tasks from any network-connected computer with a browser. These administrative tasks shall include but not be limited to:

1. Database backups

2. System restore
3. Software updates
4. File cleanup
5. File upload
6. Setting system time and time zones
7. Changing passwords
8. Issuing and revoking cards
9. Enrolling new people
10. Creating badges
11. Generating reports
12. Configuring network resources

Most of the administrative, maintenance, and configuration utilities and functions shall require a system user with at least a "Setup" user role. Information from the network administrator shall, in many cases, also be required. IEI eMerge CSI Spec 14

2.07 CERTIFICATIONS

A. UL 294 listed.

B. ISO 9000 listed.

2.08 APPROVED MANUFACTURERS