C-CURE 9000 System

Version 2.50

UL Addendum

8200-1188-01
Revision A0

SOFTWARE HOUSE

From Tyco Security Products

6 Technology Park Drive
Westford, MA 01886-3140
[redacted]
Fax: 978-577-4392   Phone: 978-577-4000

Product offerings and specifications are subject to change without notice. Actual products may vary from photos. Not all products include all features. Availability varies by region; contact your sales representative.

C•CURE 9000 System Version 2.50
Part Number: 8200-1188-01
Revision Number: A0
Release Date: December 2015

This manual is proprietary information of Software House. Unauthorized reproduction of any portion of this manual is prohibited. The material in this manual is for information purposes only. It is subject to change without notice. Software House assumes no responsibility for incorrect information this manual may contain.

OVERVIEW

This addendum provides UL requirements for C•CURE 9000 system components. All other C•CURE 9000 documentation is supplemental only and has not been evaluated by UL.

GENERAL REQUIREMENTS

UL approved installations must conform to the following general requirements:

- The System must be installed indoors within the protected premise, wired in accordance with the National Electrical Code (NFPA70) and the local authorities having jurisdiction.
- All devices must be UL Listed and, where applicable, powered by UL Listed access control or burglar alarm power-limited power supplies capable of up to 24 hours of standby power or 4 hours backup power with notification.
- All cabling and wiring used must be UL Listed and/or Recognized and suitable for the application.
- Unless otherwise noted, all external connections used (relays, battery wires, power supply wires, etc.) must be connected to power limited circuits only.
- The following features **MUST** be **disabled** for UL installations: suppress read misread, suppress reader misread and non alarm input report flag.
- The following features **MUST** be **enabled** for UL installations: event beep.

NOTE: System components, functions, and features not specifically included in this addendum are untested or do not conform to UL requirements.

HARDWARE CONFIGURATION REQUIREMENTS

Supply Line Transient Protection

All supply lines must be protected by a transient protection device that complies with the Standard for Transient Voltage Surge Suppressors, UL 1449, with a maximum marked rating of 330V. This includes the AC power lines for all C•CURE 9000 equipment such as client and server computers; network hubs, routers, and bridges; terminal servers; leased-line modems; and protocol converters. Excluded from this requirement are apC/8X panels, iSTAR controllers, DMP panels and periphery equipment such as RM Readers, RM-4, RM-4E, R8, I8 and I/8 CSI boards.

Signal Line Transient Protection

Shall comply with the standard for protectors for data communications and fire alarm circuits UL 497B, with a marked rating of 50 volts.

Signal line transient protection devices are not required for readers or input devices connected to an apC/8X panel, iSTAR controller, DMP panel, RM Readers, RM-4, RM-4E, R8, I8 and I/8 CSI boards.

Communication Circuits and Network Components

All communication circuits and network components connected to the telecommunications network must be protected by a transient protection device that complies with the Standard for Secondary Protectors for Data Communication Circuits, UL 497A. These protectors shall be used only on the protected side of the telecommunications network. This includes the TCP/IP network and serial data lines for all C•CURE 9000 equipment, such as client and server computers, network ports and server serial ports. Excluded from this requirement are the data lines that feed directly into apC/8X panels, iSTAR controllers and DMP panels.

Temperature Controlled Environment

The C•CURE 9000 server computer must be installed in a temperature-controlled environment that is maintained by the HVAC system to be in the range of 13-35°C (55-95°F). The HVAC system must be provided with at least 24 hours of standby power supplied by an engine-driven generator or standby battery. Excluded from this requirement are apC/8X panels, iSTAR controllers, DMP panels and periphery equipment, such as RMs and I/8 boards.

Backup System

The C•CURE 9000 server computer must be completely duplicated with provision for switchover to the backup system within 30 seconds. The backup system shall be fully operational within 6 minutes of the loss of the primary system. This allows 30 seconds for the backup system to be fully energized and connected to necessary communication lines and other devices, followed by 5-1/2 minutes for the system to boot up, conduct memory tests, file system check, security verifications and prepare for full system operation. The backup computer shall have the capabilities of the primary, such as memory, speed and the like.

The backup system may be provided by a second computer that meets C•CURE 9000 UL 1076 Listing requirements or by using a redundant computer.

Uninterruptible Power Supply (UPS)

In addition to the standby power required for the HVAC system, all system components must be provided with UPS with sufficient capacity to operate the equipment for a minimum of 15 minutes. If more than 15 minutes is required for HVAC standby power to come on-line and stabilize, the UPS must be capable of providing input for at least that amount of time. When the UPS is installed, there must be a means for disconnecting the input to the UPS while maintaining continuity of power to the system components so that maintenance and repair can be performed. All UPS devices must comply with the Standard for Uninterruptible Power Supply Equipment, UL 1778, or the Standard for Fire Protective Signaling Devices, UL 1481.

GROUNDING

All equipment shall be properly grounded according to the hardware's installation instructions.

Cabinet Tamper Detection Inputs

The C•CURE 9000 supports inputs that detect cabinet tamper for apCs, iSTARs, DMP panels and RM readers. All apCs, iSTARs, DMP panels and RM readers must be configured to detect cabinet tamper. Each tamper input must specify that an event be triggered when the device is tampered. This event must be configured to always be armed, on-line, annunciated, and require acknowledgement.

AC Power Fail Inputs

The C•CURE 9000 supports inputs that detect AC power fail for apCs, iSTARs and DMP panels. All apCs, iSTARs, and DMP panels must be configured to detect AC power fail. Each AC power fail input must specify that an event be triggered when the controller loses AC power. This event must be configured to always be armed, on-line, annunciated, and require acknowledgement.

Event Association with Communications Failure

The C•CURE 9000 supports the association of events with controller and reader communications failure. Each apC, iSTAR, and RM reader must be configured to trigger an event when the device goes into communications failure. This event must be configured to always be armed, on-line, annunciated, and require acknowledgement.

Supervised Inputs

Supervised inputs must be used for UL1076 applications. The C•CURE 9000 supports supervised inputs located on apCs, iSTARs, DMP panels and I/8 boards.

Each supervised input must be configured to trigger an event when the input is activated and a supervision error is detected for the input. These events must be configured to always be armed, on-line, annunciated, and require acknowledgement.

NOTE: See individual panel installation instructions for panel-specific End of Line (EOL) supervision requirements and specification.

MONITOR POINTS

Description

Monitor points are alarm devices connected to input circuits.

Each monitor point functions independently and does not interfere with operation of the others. The hardware modules monitor the supervised inputs. The following states are reported:

- Secure, Alert, Shorted, Open, and Line Fault

The configuration in the host computer determines how the hardware module and the reporting software will respond to the various conditions that are detected.

UL Compliant Supervision

The indication of whether a monitor point is Normally Closed (NC) or Normally Open (NO) is done by how the resistor network is wired in conjunction with the alarm device to form a supervised End Of Line (EOL) resistor alarm zone. The host system views monitor points as being either logically true or false. Software House wires NO and NC supervised input circuits two ways because it makes the software implementation more logical.

The two different methods result in an alarm loop resistance of 1K ohms being the Secure supervised state whether the monitor point is connected as a NO or NC alarm loop. Since the hardware wiring defines NO and NC, the software works with inputs that are simply either logically true or false.

Wiring for Alarm Zones

To wire a NO alarm loop to an input circuit, connect a 1 K Ω EOL resistor across the input and another EOL in series with the switch, as shown below. This circuit will provide 5-state supervision.

Assignment of Priorities to Events

The C•CURE 9000 supports assigning priorities to events. If this feature is used, the order of priority must be as follows — from highest to lowest:

1. Industrial supervision where a risk of injury to person or damage or destruction of property may be involved

2. Hold-up (Robbery) or panic alarm

3. Burglar alarm

4. Watchman tour

5. Fire alarm supervision error

6. Burglar alarm supervision error

7. Industrial supervision where a risk of injury to person or damage or destruction of property will not be involved

8. Other supervisory services

NOTE: Items 2 and 3 may have equal priority; items 5 and 6 may have equal priority; and items 7 and 8 may have equal priority.

OPERATIONAL REQUIREMENTS

Operation/Testing

1. **Readers** are tested by reading a sample card and observing the results on the Monitoring Station application. If the reader and card formats are properly set, an "*access granted*" or "*access denied*" message appears on the screen. A "*card misread*" message indicates that the reader is not properly installed or the card format does not match the settings in the C•CURE 9000 Administration application.

2. **Inputs** are tested by opening/closing (activating/deactivating) the device. Input devices must have the proper supervision resistors installed to function with C•CURE 9000. When inputs are working properly, you see the messages "input xxx activated" and "input xxx deactivated. Shorting or opening the cable is indicated as "input xxx shorted" or "input xxx open loop" on the Monitoring Station application.

3. **Outputs** are tested by performing a manual action in the Monitoring Station application. You can momentary open a door or activate any other relay. You can then use a resistance meter to determine if the relay contacts close and open properly.

Maintenance

- **For electronic modules exposed to high dust environments:** Check the assemblies for excess dust build-up every 6 months and remove the dust and dirt from the assemblies with forced air.

- **For readers exposed to external weather conditions:** Check the enclosure sealing for leaks at 6-month intervals. If the seal is not intact, replace the gasket

Recommended PC Configuration for C•CURE 9000

Server and Client PCs must be UL Listed (NWGQ), (Series L-N) Intel Pentium Core or greater (Series P-S) Quad Core Intel Xeon or greater with the following specifications:

	CPU	RAM	Disk	O/S	SQL
MAS	Xeon Quad Core E5 – 2450 or greater ≥ 2.1 GHz	16 GB	Dual 600 GB ≥15K RPM	Win Server 2008 R2 SP1 (Standard/Ent) 64-bit Win Server 2012 R2 (Standard) 64-bit	SQL Server 2008 R2 SP2 (Standard/Ent) 64-bit SQL Server 2012 SP2 (Standard/Ent) 64-bit SQL Server 2014 (Standard/Ent) 64-bit
SAS (P-S)	Xeon Quad Core E3 – 1240 or greater ≥ 3.3 GHz	16 GB	Dual 300 GB ≥ 15K RPM	Win Server 2008 R2 SP1 (Standard/Ent) 64-bit Win Server 2012 R2 (Standard) 64-bit Win7 SP1 Pro/Ent 64-bit Win 8.1 SP1 (Pro/Ent) 64-bit	SQL Server 2008 R2 SP2 (Standard/Ent) 64-bit SQL Server 2012 SP2 (Standard/Ent/Express) 64-bit SQL Server 2014 (Standard/Ent/Express) 64-bit

SAS (L-N)	Intel 3rd Generation Core i7-3770 or greater ≥ 8MB	8 GB	Dual 80 GB ≥ 7200 RPM	Win Server 2008 R2 SP1 (Standard/Ent) 64-bit Win Server 2012 R2 (Standard) 64-bit Win 7 SP1 Pro/Ent 64-bit Win 8.1 SP1 (Pro/Ent) 64-bit	SQL Server 2008 R2 SP2 (Standard/Ent) 64-bit SQL Server 2012 SP2 (Standard/Ent/Express) 64-bit SQL Server 2014 (Standard/Ent/Express) 64-bit
Client	Intel Core i5 – 3470 or greater ≥ 3.2 GHz ≥ 6MB	4 GB on 32-bit 8 GB on 64-bit	500 GB ≥ 7200 RPM	Win 7 SP1 (Pro/Ent) (32 or 64-bit) Win Server 2008 R2 SP1 (Standard/Ent) 64-bit Win 8.1 SP1 (Pro/Ent) (32 or 64-bit) Win Server 2012 R2 (Standard) (64-bit)	N/A
victor Unified SiteServer	Intel i5-4570 3.2 GHz Quad-Core	16 GB	240 GB 4 or 6 TB (Storage)	Windows 7 Embedded, (Standard) 64-bit	SQL Server 2012 SP2 Standard/Ent/Express (32 or 64-bit)

NOTE: All computers used in the C•CURE 9000 System must be UL Listed.

Installation Locations

The system must be installed within the protected premise and wired in accordance with the National Electrical Code (NFPA 70), and the local authorities having jurisdiction.

NOTE: The hardware comprising this system is not for outdoor use except the RM1, RM2, and RM2 readers. In an outdoor application or when the temperature is expected to drop below 40°F, these readers must be configured with gasket and an optional heater kit
(P/N 130-915) for use in a 115 VAC installation only.

C•CURE 9000 FEATURES

Table 2 shows the features and whether or not they were evaluated by UL.

Table 2. Features Evaluated by UL

Feature	UL Evaluated
Enterprise Architecture option	Yes
Database Synchronization	Yes
Global Objects	Yes
Central Reporting	Yes
Dynamic Views/Queries/Reports	Yes
Application Server Editor	Yes
Central Monitoring	Yes
Synchronization of Journal and Audit	Yes
Global System Variables	Yes
Editing objects on remote servers	Yes
Global Personnel-related or Operator-related objects	Yes
Report on personnel with access to a door	Yes
Elevator Swipe and Show	Yes
Card Admit and Reject Activity Viewer Options	Yes
Remove Clearances menu selection	Yes
Event/Alarm Monitoring	Yes
Door Control	Yes
Elevator Control	No
Schedules	Yes
Time Zone Management	Yes
Operator Privileges	Yes
Card Record Definitions	Yes
Card Format Definitions	Yes
Database Partitioning	Yes
Automated Personnel Data Import	Yes
Clearances	Yes

Feature	UL Tested
Reports	Yes
Audit Trail	Yes
Activity Monitoring	Yes
iSTAR Panel Support	No
Paging and E-mail	No
Closed Circuit Television Integration (CCTV)	No
Cardholder Access Events	Yes
Redundancy Qualification (everRun MX, everRun Enterprise)	Yes
iSTAR Configurable Activity Buffer Size Enhancement	Yes
Encryption Box Qualification	Yes
Audit Trail of Security Objects	Yes
Event Triggered Database Backup (on iSTAR)	Yes
Enhanced Partitioning	Yes
Multiple Cards per cardholder	Yes
256-bit card numbers	No
128 total card formats	No
NetVue Presets and Patterns Enhancement	Yes
iSTAR Reader LED and beep patterns	Yes
Additional user-named fields	Yes
PIN-only access	Yes
Holidays	Yes
LDAP Import of Personnel Records	No
Role Based Clearances	Yes
Role Based Clearances	Yes
Double Swipe	Yes
NetVue Alarm Management	Yes
NetVue Popup Window	Yes
Integration with Video Edge NVR System	No
Preset Log Messages	Yes
Long Term Comm. Loss Functionality	Yes

Feature	UL Tested
iSTAR eX 8 Readers	Yes
Role Support with Import of Personnel	Yes
Automated Import of Personnel Records	No
Support of apC Panels	Yes
C•CURE Mobile	No
Wireless Access System	No
Double Swipe with Triggers	Yes
iSTAR Clusters	Yes
Refresh of Live Displays after communication loss and restore	Yes
Specialized Security Limited Functionality (SSLF)	No
Import/Export Enhancements	No
Vista Support for Client Applications	Yes
Intellex 5.0	No
VideoEdge 4.7.1	No
Hardware Drivers as Window Services	No
Export Selection to CSV from Dynamic Views and Query Results	Yes
iSTAR Cluster based Antipassback and Time Antipassback	Yes
C•CURE ID 3.1	Yes
Smartcard Programming and Enrollment	Yes
iSTAR Intrusion Zones	Yes
Keypad Commands	Yes
Report Performance Improvements	Yes
Client/Server Encryption	Yes
C•CURE Encryption Engine 1.0	Yes
iSTAR Edge Support	Yes
C•CURE 800 Field Compatibility	Yes
Web Client	No
Personnel View	Yes
User Defined Fields	Yes
Area Phase 2	Yes

Feature	UL Tested
Occupancy restriction	Yes
N-Man rule	Yes
Manual Action Challenge	Yes
RM LCD Messages	Yes
Clearance Filters	Yes
Holiday Schedule Enhancement	Yes
iSTAR FAI support	Yes
iSTAR Edge 4-reader model	Yes
iSTAR Edge Dual Range – added SWH Dual 1K NO/NC selection to list of supported EOL circuit types on the controller's General tab.	Yes
FlexNet Licensing	Yes
Global Antipassback	Yes
Area Lockout	Yes
Area Demuster	Yes
Escorted Access	Yes
DMP XR500E Panels	Yes
DMP XR500N Panels	Yes
DMP XR100N Panels	Yes
apC Time Zones	Yes
iSTAR Ultra	Yes
Inactivity Card Deactivation	Yes
Individual Card Access Events	Yes
First/ Last Card Read Report	Yes
Custom Clearances	Yes
Latch/Unlatch/Toggle/Pulse Event	Yes
Web Client Portraits and Acknowledgement	Yes
Journal Triggers	Yes
Encryption Enhancements • iSTAR Pro AES Encryption • FIPS 140-2 Algorithm Updates	No

Feature	UL Tested
Guard Tour	Yes
Advanced Door Monitoring	Yes
Dual Phase Acknowledgement	Yes
Assigning Privilege Groups to Operators	Yes
Schlage Wireless Lock support on iSTAR Controllers	Yes
Dynamic Area Management and Conditional Access	Yes
Visitor Management Portal	Yes
Personnel Pin Exempt (ADA)	Yes
Multi-version Enterprise Sync	Yes
Support of IP-ACM controller module	No
Support of RM2-4000-PI26 and RM2L-4000-PI26 Readers	Yes
iSTAR Ultra SE (Pro Mode)	Yes
iSTAR Ultra SE (Ultra Mode)	Yes
Dial-up controller support	No

UL Components

The following system components meet UL requirements.

UL Evaluated Panels		
Panel	**Firmware**	**Comments**
apC/8X	8.7Zx	None
iSTAR- Pro	5.2.x	None
iSTAR- eX	6.x	None
iSTAR-Edge	6.x	None
iSTAR Ultra	6.x	None
iSTAR Ultra SE (Pro Mode and Ultra Mode)	6.x	None
DMP XR500E	2.x	512 Zones and Encryption
DMP XR500N	2.x	512 Zones

DMP XR100N	2.x	142 Zones

- Power Supply Backup Systems
  - apS
- RM Series Readers:
  - RM2L-4000-PI26, RM2-4000-PI26, RM1-4000, RM2-4000, RM2L-4000, RM1-IC, RM2-IC, RM2L-IC, RM1-MP, RM2-MP, RM3-MP, RM2L-MP, RM1-PH, RM2-PH, RM2L-PH, RM3-PH, RM1-PI, RM2-P1, RM2L-PI, RM1-W
- SWH Series Readers:
  - SWH-4000, SWH-4100, SWH-4130, SWH-2100, SWH-5100, SWH-5200, SWH-4200, SWH-3100
- Accessories
  - RM-4, RM-DCM2, RM-4E, RM-4T, RM-4TE
  - I/8, R/8, I8-CSI
- The following system components have not been tested to UL requirements.
  - Optional communication converter: AS002
  - Optional dual communication converter: AS003
  - Smart Card Readers: SCR series of readers.
  - Auxiliary relay module: ARM-1
    - All other readers not manufactured by Software House. (However, these readers may be UL Listed. Contact the manufacturer for details.

NOTES:

- Only readers included in the UL Components section can be employed in a UL-compliant system.
- All interconnecting devices are to be UL Listed and, if applicable, powered only by UL Listed access control or burglar alarm power-limited power supplies capable of 24 hours of standby power.
- See individual panel installation instructions for panel-specific compatible readers, accessories, and power supplies.
- An RM2L-4000 reader must be in each area/partition for signal acknowledgement.

Installation Manuals

Table 4 Installation Guide Reference Chart

Access Control Panel	
apC/8X	UM-247
iSTAR Pro	UM-293
iSTAR eX	UM-248
iSTAR Edge Quick Start (2 & 4-Rdr)	UM-298
iSTAR Edge 1-Rdr Quick Start	UM-274
iSTAR Ultra	UM-266
iSTAR Ultra SE	UM-311
Auxillary Boards	
RM-4	UM-064
RM-DCM2	UM-215
RM-4T	UM-302
I/8	UM-204
I/8-CSI	UM-218
R/8	UM-205
Readers	
RM1	UM-207
RM2	UM-207
RM3	UM-207
RM-IC	UM-208
RM2L-4000	UM-209
RM2L-NH	UM-235
RM2-4000-PI26 & RM2L-4000-PI26	8200-1179-01

Stratus Fault Tolerant Solution for C•CURE

Stratus Technologies' everRun® fault tolerant redundancy solutions deliver a fault tolerant solution that requires limited or zero downtime. Stratus Technologies' everRun Enterprise and Express, and SplitSite provide a high availability, fault tolerant solution for C•CURE 9000 systems. Stratus' everRun fault tolerant redundancy platforms offer additional reliability to C•CURE access control systems. While some redundancy platforms run on a recovery-based model in the event of failures, everRun platforms utilize a new preventative-based model which allows ability to continue to compute through failures. everRun Snapshots provide information rollback of the C•CURE database at a single point in time to assist with the recovery of data loss or system corruption.

everRun Enterprise and Express

everRun Enterprise and Express combining the physical resources of two standard Windows servers into a single, unified operating environment. This provides complete redundancy of all underlying data and hardware. By keeping the operating environment in the single, unified system you are able to keep applications up and running in the event of a system or component failure. everRun Enterprise provides a full, level-3 fault tolerant system with no restarts for continuous operation. everRun Express provides a component, level-2 fault tolerant system with failover restart in seconds to minutes for minimal downtime. everRun is a fault tolerant solution that supports symmetric multiprocessing and multi-core environments, allowing businesses to have an affordable, continuous security solution during component system failures.

Servers that employ the everRun Enterprise and Express solution are required to be in the same room of each other ideally less than 6 Feet.

everRun SplitSite

everRun SplitSite delivers fault tolerance between systems located in a campus type of environment. Utilizing a LAN, everRun SplitSite links geographically separated systems with the same core capabilities of everRun software. If a system is down in one location, C•CURE will remain available and fully operational at the other location.

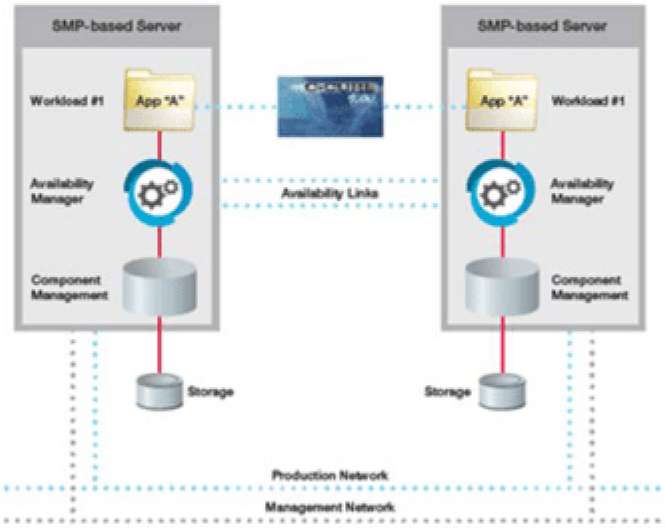
Servers that employ the everRun SplitSite solution are required to be within 3 Miles of each other.

Minimum System Requirements

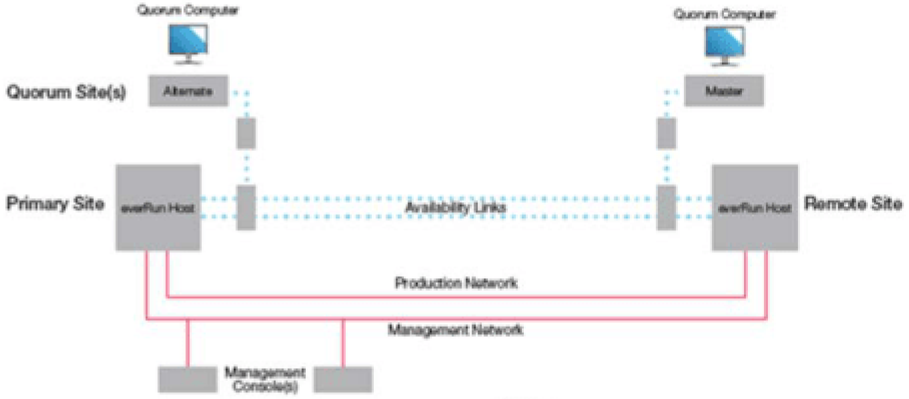
DELL-RACKSVR3 (for C•CURE 9000 Series, L, M, N, P):

- Intel Xeon E5-2440v2 processor, 1.9Ghz, 8 cores
- 24GB 1600MHz RDIMM
- PERC H710 RAID Controller
- Two 600GB SAS Hotplug Disk Drives, 15K RPM, RAID 1
- Gigabit ET Quad Port NIC
- USB Keyboard, Mouse, DVD-ROM SATA
- Windows 2012 Server R2, SE, 64-bit, 5 CALs

everRun Diagram



everRun SplitSite Diagram



Notes:

- Only one Management Console needed
- Quorum computer required to be in third location (not primary or remote site)
- Multiple Production networks are supported

Stratus Technologies' everRun S/W running on Servers will protect and keep mission critical data and applications available by mirroring information from one server to another over a local area network (LAN). Data is updated in real time. Should a server fail, the peer server will assume control of the system with an exact copy of the data and application.

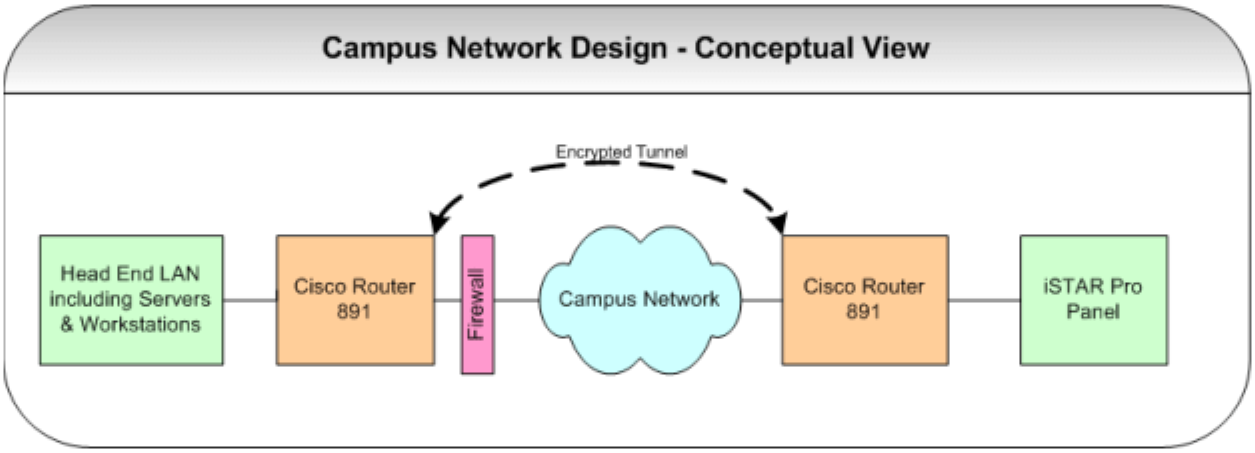
UL Listed Encrypted Line Security Configuration .

Conceptual View of Network

A conceptual view of the UL Listed Encrypted Line Security Configuration is shown in the following diagram "**Conceptual View of Campus Network.**"

The head end LAN is isolated from the campus network by a firewall and an encrypting router (Cisco Router 891). Communication from the C•CURE 9000 server to the iSTAR Pro panel is through an encrypted VPN tunnel between the two encrypting routers (both Cisco Router 891).

The Cisco 891 routers have been validated as correctly implementing the **Advanced Encryption Standard (AES 256-bit)** algorithm, specified in the Federal Information Processing Standard Publication 197 (FIPS 197), *Advanced Encryption Standard*.



Conceptual View of Campus Network

Encryption Methods

C•CURE 9000 controllers use the following encryption methods:

- **iSTAR Ultra SE in Pro Mode** – AES 256-bit encryption, FIPS 197, when used with approved Software House routers.
- **iSTAR Ultra SE in Ultra Mode** – AES 256-bit encryption, FIPS 197-listed, with custom key management and digital certificates.
- **iSTAR Ultra –** AES 256-bit encryption, FIPS 197-listed, with custom key management and digital certificates.
- **iSTAR Pro –** AES 256-bit encryption, FIPS 197, when used with approved Software House routers.
- **iSTAR eX –** AES 256-bit encryption, FIPS 197-listed with custom key management and digital certificates.
- **iSTAR Edge –** AES 256-bit encryption, FIPS 197-listed, with custom key management and digital certificates.
- **DMP XR500E -** AES 128-bit encryption, with custom key management and digital certificates.

UL 1076 Line Security

Standard line security will detect a compromise in the communication channel between the central receiving station and the protected area. Standard line security is default enabled and is verified by disconnecting the protected area from the receiving station and receiving notification of disconnection. Reconnect the communication line and verify communication has been restored,

Encrypted line security is detailed on page 18. In default encryption mode, the digital certificates are generated internally. Please refer to the appropriate hardware manual for any hardware configuration.

UL Switching Protection Mode Requirements

There are two Arming Mode methods. The first method is no intrusion zone arming if connection to the host is lost. The second method is indication of acknowledgement from the central supervising station of arming of intrusion zone.

The First Method:

A control unit shall provide a visual and/or audible signal to indicate to the attendant at the protected area that the closing signal has been received by the central supervising station.

The protection zone shall contain at least one RM2L-4000 reader, which will utilize keypad commands.

The keypad command will activate a host based event which arms/disarms the protection zone.

Create a keypad command that will activate a controller based event. The controller event will then activate a host based event. The host based event will arm the protected area.

With the RM2L, the acknowledgement on the LCD will indicate “area secured”. If the monitoring station has not received the signal, no message will be displayed.

The Second Method:

Conversely, the control unit shall provide a visual and/or audible signal to indicate to the attendant at the protected area that the closing signal has been received by the central supervising station.

When arming an intrusion zone, create a host based event that will activate an output that will notify the arming personnel that the host received the arming notification.

The output shall be an LED that is powered from a UL603 listed supply with appropriate battery capability. The LED sourced shall be flush mounted securely located within a meter of the arming zone.

A representative LED would be part number 1091M5-12V by CML (Chicago Miniature Lighting). It is 12V, 2W (0.1667A) rated. It has 390ohms internal. The LED can be connected to the output of the RM2L-4000, or the output of the iSTAR and UL listed supply capable of power, or if wet outputs on the iSTAR.

For specifics on creating host based events, refer to the CCURE 9000 guides.

Cisco 891 Router

Secure Network Connectivity

Cisco 890 Series Routers deliver high performance with integrated security and threat defense. Network security has become a fundamental building block of any network, and Cisco routers play an important role in embedding security at the customer's access edge. Cisco recognizes this requirement, so Cisco 890 Series Routers are equipped with security hardware acceleration and Cisco IOS Software (by default, a universal image with Advanced IP Services feature license).

This Cisco IOS Software feature set facilitates hardware-based IPsec encryption on the motherboard and provides a robust array of security capabilities such as Cisco IOS Firewall, content filtering, IPS support, IPsec VPNs (DES, 3DES, and AES), SSL VPN, tunnel-less Group Encrypted Transport VPN, DMVPN, Easy VPN server and client support, Secure Shell (SSH) Protocol Version 2.0, and Simple Network Management Protocol (SNMP) in one solution set.

Cisco 891 Router

Network Configuration

The "UL Listed Encrypted Line Security Configuration" drawing shows a sample wiring diagram for the Cisco Router UL Test Configuration.

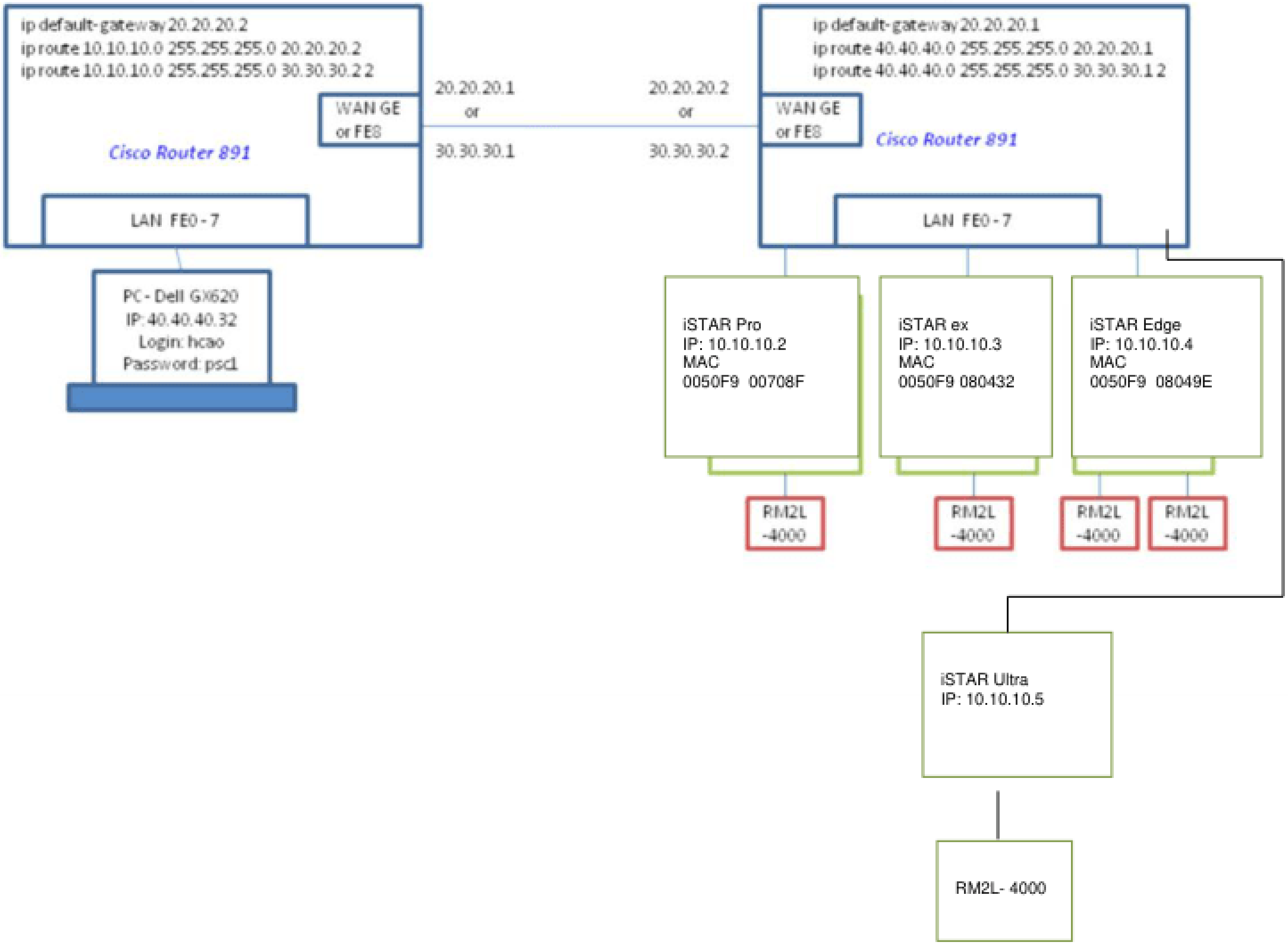
- The Cisco encryption device and iSTAR control panels must be installed in the same room.
- The Cisco 891 router must be powered by Cisco power supply [P/N 341-0231-02] in all installations.
- The power supply must be connected to an uninterruptible power supply (UPS) LISTED to UL 1076.

NOTE: UL has not evaluated the wireless or POE capabilities of this router.

Cisco Router 891 UL Test Configuration and Setup

- Cisco 891: S/N: FTX1405YBE6
- FELAN 0 – 7 All Devices on 40.40.40.x/24
- Subnet mask: 255.255.255.0
- Gateway: 40.40.40.1
- WAN FE8 All Devices on 20.20.20.x/24
- Subnet mask: 255.255.255.0
- Gateway: 20.20.20.1
- WAN GE0 All Devices on 30.30.30.x/24
- Subnet mask: 255.255.255.0
- Gateway: 30.30.30.1
- Username: manager
- Password: manager

- Cisco 891: S/N: FTX1405YE32
- FELAN 0 – 7 All Devices on 10.10.10.x/24
- Subnet mask: 255.255.255.0
- Gateway: 10.10.10.1
- WAN FE8 All Devices on 20.20.20.x/24
- Subnet mask: 255.255.255.0
- Gateway: 20.20.20.2
- WAN GE0 All Devices on 30.30.30.x/24
- Subnet mask: 255.255.255.0
- Gateway: 30.30.30.2
- Username: manager
- Password: manager



```
ip default-gateway 20.20.20.2
ip route 10.10.10.0 255.255.255.0 20.20.20.2
ip route 10.10.10.0 255.255.255.0 30.30.30.2 2
```

```
ip default-gateway 20.20.20.1
ip route 40.40.40.0 255.255.255.0 20.20.20.1
ip route 40.40.40.0 255.255.255.0 30.30.30.1 2
```

UL Notes

- FIPS 140-2 not evaluated by UL.
- PCMCIA not evaluated by UL.
- DHCP not evaluated by UL.
- Tamper, power failure, low battery enabled for UL installations.
- Communication failure must be enabled for UL installations.
- Elevator output assignment not evaluated by UL.
- Elevator controls not evaluated by UL.
- apC, apC/L not evaluated by UL.
- Unsupervised inputs not evaluated by UL.
- Mini star reader not evaluated by UL.
- ISC controllers not evaluated by UL.
- Secondary communication ports not evaluated by UL.
- UL requires a maximum of 200 seconds supervision on the communication line between the ported premise and central station.
- Cluster tab not evaluated by UL.
- Send state changed to the monitoring station must be selected.
- Range 1-99, 10 is default, 99 must be selected for UL installations.
- Video support not evaluated by UL.
- Bi-directional interface for CCTV not evaluated by UL.
- Net view not evaluated by UL.
- Controller based Key management not evaluated by UL.
- Host based key management not evaluated by UL.
- Custom encryption not evaluated by UL.
- Digital Certificates not evaluated by UL.
- OSDP (Open Supervised Device Protocol) not evaluated by UL.