iSTAR Ultra G2 SE

Cyber-hardened Access Controller for up to 32 Readers

Key features

- Powerful cyber-hardened network door controller for up to 32 readers
- Trusted Execution Environment (TEE) provides advanced hardware-based cybersecurity protection
- Hardened Linux embedded OS for improved security and scalability
- Power over Ethernet (PoE) module features PoE++ to power the GCM
- Up to 1M cardholders in local memory
- Dual GigE network ports with IPv6, DHCP and 802.1X support
- Onboard 256-bit AES network encryption
- Supports OSDP Secure Channel for encrypted reader communications
- Supports Embedded High Assurance FICAM operation without third-party hardware

iSTAR Ultra G2 SE is a powerful, cyber-hardened and network door controller that supports up to 32 readers. Built using a Trusted Execution Environment (TEE) with advanced network security features, iSTAR Ultra G2 SE answers the most demanding access control requirements of enterprise and government applications. Rack mount and wall-mount options provide installation flexibility, while iSTAR Ultra G2 SE features a hardened Linux kernel for its operating system, improving the security and scalability of the system.

Supports up to 32 Readers

iSTAR Ultra G2 SE uniquely combines support for traditional hard-wired access control doors with support for wireless lock sets, all in the same controller. Up to 32 readers are supported by the iSTAR Ultra G2 SE, which can be comprised of readers from Access Control Modules (ACMs), IP-ACM Ethernet door modules, and/or wireless locksets. iSTAR Ultra G2 SE is ideal for areas that require many readers near the panel. For more distributed installations, iSTAR Ultra G2 SE includes up to 32 RS-485 ports, allowing the installer to run longer distances to each door.

iSTAR Ultra G2 SE uses a General Controller Module (GCM) which includes standard 2GB RAM and 16GB memory and has two onboard gigabit network ports for reliable network communications. The GCM controls up to four ACMs, with each ACM supporting up to eight

Wiegand, RM or OSDP readers, 16 supervised inputs, and 8 outputs dry-configured.

iSTAR Ultra G2 SE also includes an alphanumeric LCD to provide status and troubleshooting information. Database backups and all buffered transactions are stored to non-volatile memory. A rechargeable clock battery keeps the clock powered during a power failure.

iSTAR Pro Hardware Upgrade and Conversion Tool

The iSTAR Ultra G2 SE ACM size, footprint, and connectors are identical to the iSTAR Pro ACM, allowing for an easy hardware upgrade to the iSTAR Ultra G2 SE. (Note: the Ultra G2 SE ACM does not support the legacy "Pro Mode"). With the seamless database conversion tool available in C•CURE 9000 v2.7 and up, the upgrade is easy from "Pro" to "Ultra".

Advanced Cybersecurity using TEE

iSTAR Ultra G2 SE utilizes a hardware-based Trusted Execution Environment (TEE), a secure, isolated environment within its CPU that runs in parallel to the main Linux operating system. TEE guarantees confidentiality and integrity of code and data loaded by using hardware and software as protection mechanisms. TEE provides reliable storage of keys and other cryptographic materials and manages a secure boot process to guarantee authenticated sources for hardware and software.

Advanced Network Security

iSTAR Ultra G2 SE features dual GigE Ethernet LAN ports, providing primary and secondary communications to C•CURE 9000. iSTAR Ultra G2 SE supports static and dynamic IP addresses and IPv4 and IPv6 protocols, supporting DHCP, DNS, SNMP, and 802-1X port authentication protocol, for added security and to simplify network installation. Potential network threats are further reduced with embedded denial-of service protection, 256-bit FIPS 197 AES network encryption, and unique controller-based TLS 1.3 certificates for network authentication.

In addition, an embedded web page features unique password management and TLS 1.3 authentication reducing startup time by allowing you to view online controllers, change configuration parameters, and download new firmware from a single interface. The web page feature is managed centrally by C•CURE 9000 and can be disabled if desired.

Features

Ensure Reliable Communication with Clusters

iSTAR Ultra G2 SE supports peer-to-peer communications across clusters, meaning that the controllers communicate with one another with limited host intervention. Clusters are user-defined groups of up to 16 controllers and can be created to enhance scalability for C•CURE 9000 and security by separating a widely dispersed facility into different controlled areas. For example, events linking inputs on one controller to outputs on another controller will still be active without the host, as will any anti- passback rules that are set up within the cluster.

Local and Global Anti-Passback Provides Effective System-Wide Security

Anti-passback prevents cardholders from passing their credentials back to others in order to gain access to secured areas. Global anti-passback is critical for ensuring uncompromised security on a large scale. Building upon cluster-based anti-passback, as described above, the controllers can send an anti-passback violation notice to the C•CURE server. Tailgating, or following another cardholder into a secured area without presenting a separate badge, can easily be flagged within the C•CURE monitoring station.

Rack-Mount Flexibility

iSTAR Ultra G2 SE is available in a modular rack-mount configuration, reducing the space requirements and costs associated with installing a panel on the wall. Separate GCM and ACM modules can be arranged in the rack to optimize your server room installation. For example, the GCM can be mounted in the front of a four-post rack, while the ACM and field wiring can be located in the rear of the rack. Field wiring on the ACM is easily routed through the top and/or bottom of the enclosure,

with the ACM board mounted front and center for convenient servicing.

Keypad Commands Provide the Ultimate in Control

iSTAR Ultra G2 SE supports custom keypad commands which provide a powerful way to easily activate events in C•CURE 9000. These commands include anything from triggering a duress call and sounding an alarm, to locking and unlocking doors directly from a keypad reader or dedicated touchscreen keypad. Commands can be configured to require a card presentation and/or a card and PIN to validate the command. Keypad commands can also be used to arm and disarm intrusion zones.

Extended Card Formats Enhance Security

iSTAR Ultra G2 SE supports extended card formats of up to 256 bits, providing the utmost in flexibility when configuring custom card formats. iSTAR Ultra G2 SE supports the full 200-bit FASC-N format for compliance with the U.S. Government's FIPS 201 initiative, as well as the 128-bit GUID format for PIV-I credentials. These extended cardholder formats are stored locally in iSTAR allowing the controller to make the access decision even when it is offline from the host. Each format supports multiple data fields such as card number, facility code, agency code, system code, plus up to four custom card integer fields. Longer card numbers and formats offer greater protection against card duplication and are especially valuable to customers who require card numbers that exceed 10 digits.

Cardholder Flexibility

Used with C•CURE 9000, iSTAR Ultra G2 SE allows administrators to assign up to five active cards per cardholder record rather than having to create a separate record for each card. This simplifies the management and maintenance of personnel records. For additional flexibility, iSTAR Ultra G2 SE can support up to 128 card formats system-wide and ten card formats per reader, including smart cards. This expanded ability to use multiple card types (such as 26-bit, 37-bit, or Corporate 1000) at a single reader frees customers from having to consolidate or re-issue new cards.

Built-in Diagnostics to Easily Test and Troubleshoot

iSTAR Ultra G2 SE includes both built-in web diagnostics pages and a local LCD to test and troubleshoot inputs, outputs, reader ports, and last card read. In addition, via the network, you can retrieve real-time status and diagnostics of:

- controller diagnostics
- controller time/boot time
- total/available memory
- connection status
- firmware and OS versions
- hardware (MAC) and IP addresses
- downloaded clearances and cardholders

Fully Integrated and Managed Wireless Lock Solution

Utilizing iSTAR Ultra G2 SE, wireless locks from ASSA ABLOY or Schlage communicate with C•CURE 9000, provides a fully integrated and managed lock solution. Up to 32 ASSA ABLOY Aperio or Schlage AD300, AD400, NDE and LE locksets can be managed by a single iSTAR Ultra G2 SE. In addition to traditional locksets, the ASSA ABLOY Aperio line also includes cabinet and data center locks, allowing you to extend the breadth of your access control system to non-traditional openings. Each lockset communicates using AES 128-bit encrypted wireless technology to the wireless hub, which is then connected to the iSTAR Ultra G2 SE with a simple RS-485 communications bus. Each hub can accommodate up to eight Aperio wireless locks. The PIM supports up to 16 Schlage wireless locks. All activity and alarms from each wireless device are sent to the iSTAR Ultra G2 SE and then up to the C•CURE 9000 in real time, guaranteeing a high level of control and visibility of door actions. Besides standard card access transactions, each device also communicates low battery, tamper, and communications status to the system.

Embedded Support for FICAM High Assurance

Used with the Innometriks suite of High Assurance ID Management software, iSTAR Ultra G2 SE supports PKI-based authentication at the door, including CAK and PAK, card plus PIN, and biometric match in panel. Unique cardholder PKI information and biometric templates are stored and authenticated directly in the iSTAR Ultra G2, on the secure side of the door, for reliable stand-alone operation. High Assurance PKI-based authentication is required to comply with the U.S. Government's FICAM standards and is ideal for commercial and non-government customers as well.

Specifications

C•CURE 9000 Software Compatibility	
C•CURE 9000 v2.90 SP2 CU02 and above (full feature set)	
C•CURE 9000 v2.50 and above (reduced feature set)	
Physical	
Dimensions (H x W x D)	
Wall-Mount (supports a GCM G2 and up to two ACM SEs)	61.6 x 42.0 x 10.3 cm (24.25 x 16.65 x 4.07in)
Rack Mount GCM	8.5 x 44.6 x 27.0 cm (3.34 x 17.56 x 10.62in)
Rack-Mount ACM SE	17.5 x 44.4 x 12.3 cm (6.90 x 17.47 x 4.86in)
GCM G2 Board	155 x 266 x 27 mm (6.1 x 10.5 x 1.06 in)
ACM SE Board	121 x 311 x 38 mm (4.75 x 12.25 x 1.5 in)
Weight	
Wall-Mount	10.6 kg (23.4 LB)
Rack Mount GCM G2	4.3 kg (9.4 LB)
Rack-Mount ACM SE	4.1 kg (9 LB)
Enclosure Material	Wall Mount: 18-gauge galvanized steel, with tamper switch Rack Mounts: GCM: 16-gauge galvanized steel, with tamper switch ACM SE: 18-gauge galvanized steel, with tamper switch
Environmental	
Operating Temperature	0-50°C (32-122°F)
Operating Relative Humidity	5-95% RH non-condensing
Storage Temperature	-20-60°C (-4-140°F)
Electrical	
Power Requirements, GCM G2	12/24 VDC +/- 20%, 0.5 A plus up to 1.5 A per RS-485 port
Power Requirements, Each ACM SE	12V +/- 20%, 12A max or 24V +/- 20%, 3.5A
Heat Dissipation	GCM: 61 BTU/hr, each ACM: 20.5 BTU/hr

Electrical (Continued)	
Memory and RTC Backup	Rechargeable lithium battery provides RTC backup; database and buffered transactions stored in non-volatile memory
Electrical - Optional PoE+ and PoE++ Modules	
Standards Supported	PoE (802.3af), 12.95 W max. PoE+ (802.3at), 25.5 W max. PoE++ (802.3bt), 62 W max.
Power Available for Attached Devices	PoE: 24V @ 540mA PoE+: 24V @ 1.06A PoE++: 24V @ 2.58A
Network Port for PoE	Port 1
System and Network	
CPU	NXP i.MX7 1.2 GHz dual core ARM Cortex-A7 +, Cortex-M4
Operating System	Hardened Linux kernel, Yocto project
System Memory	2 GB RAM
Non-volatile Storage	16 GB multi-mode eMMC
Network	Dual GigE LAN ports
Network Encryption	AES 256-bit
Network Authentication	TLS 1.3 using AES256 symmetric encryption, unique certificates
Port Authentication	802.1X port authentication protocol
Indicators and Switches	LCD for diagnostics, LEDs for power, LAN activity, serial port activity, output status, encryption-enable switch
Memory Capacity[3]	
Five clearances, one card/person, 20-digit card	1,000,000 cardholders
Inputs/Outputs, GCM	
Dedicated Inputs	Cabinet tamper, AC fail, low battery
Distance, GCM to ACM	Up to 1.83 m (6 ft)
Number of ACMs supported per GCM	4 (C•CURE 9000 v2.90 SP2 and higher)

[2] Memory allocation is dynamic and shared between cardholders, event storage, and configuration information.

Specifications per ACM Board[4]

Readers	
Number of Readers Supported, per ACM Board	8
Types of Readers Supported	OSDP v2 encrypted (RS-485), Wiegand and RM (RS-485), TST-100 in Smart Mode
Reader Technologies Supported	Multi-Technology, Proximity, Smart Card (incl. PIV II & TWIC), Wiegand, and Magnetic Stripe (RM only)
Maximum Distance to Door	RM and OSDP: 1,219 m (4,000 ft) Wiegand: 150 m (500 ft)
Reader Power Available (dependent on power supply)	12 VDC, 1.5 A max per reader (including RM port power)
Reader Power Status Indication	On/off indication per port, through C•CURE 9000
OSDP and RM Bus Communications	Eight RS-485 ports, four full duplex and four half duplex 2x FD, 6x HD
OSDP Support	Secure Channel encryption, AES128
Maximum Readers per RS-485 Port	8, either OSDP or RM. (You cannot mix OSDP and RM on the same port.)
Maximum Readers per RS-485 Port, in High Assurance Mode	8
Inputs	
Number of General Purpose Inputs per ACM	16, configurable supervision per input
Additional Dedicated Inputs	Cabinet tamper
Input Expansion	Up to 128 additional inputs using I8 modules on RM bus

Outputs	
Number of Relay Outputs per ACM	8
Relay Rating, Dry Contact	30 VAC/DC, 5 A max
Output Expansion	Up to 128 additional relay outputs using R8 modules on RM bus
Regulatory	
Access Control	UL 294
Burglar Alarm	UL 1076, ULC/ORD - C1076
Security Alarm	UL 2610
CE	Low Voltage Directive (LVD) 2014/35/EU EMC Directive 214/30/EU
Safety	IEC/UL/EN 60950-1, IEC/UL/EN 62368-1
EMC/EMI	FCC Part 15 Class A, ICES-003 (Canada), VCCI Class A ITE (Japan), AS/NZS CISPR 32 (Australia/New Zealand) EN 50130-4, IEC 62599-2, IEC/EN 61000-4-4, IEC/EN 61000-4-5, IEC/EN 61000-4-8
Seismic Certification	OSHPD Certification File # OSP-0425-10
Network Symmetric Encryption	AES256
FIPS 140-2	Cryptographic Module Certificate #3389

[4] iSTAR Ultra G2 SE supports up to 4 ACMs and up to 32 readers. Reader total is the combined count from ACMs, IP-ACMs and wireless locksets.

Wireless Lockset Support[5]

Wireless Lockset	
Technologies Supported	ASSA ABLOY Aperio, Schlage AD300 and AD400, WA Series, Schlage NDE/LE[6]
GCM RS485 Ports Available to Connect Wireless Hubs	2
Max # of Locksets per RS485 Port	16 Aperio or Schlage
Max # of Locksets per Wireless Hub / PIM	8 (Aperio), 16 (Schlage)
Max # of Wireless Hubs / PIMs per RS485 Port	15 (Aperio), 16 (Schlage)

[5] iSTAR Ultra G2 SE supports 32 readers (ACM and/or wireless); ASS ABLOY Aperio and Schlage locksets cannot be mixed on the same iSTAR Ultra G2 SE controller.
[6] Up to four ACM boards per iSTAR Ultra G2 SE. Note that ACMs are not required if only using wireless locks and/or IP-ACMs

Ordering information

Model number	Description
GSTAR-ACM-SE	iSTAR G2 ULTRA SE ACM BOARD
GSTAR-ACM-SE-4U	iSTAR G2 ULTRA SE ACM,4U ENCL
GSTAR008-SE	iSTAR G2 ULTRA SE,8 RDR,ENC,PSU
GSTAR016-SE	iSTAR G2 ULTRA SE,16 RDR,ENC,PSU
GSTAR008-SE-NPS	iSTAR G2 ULTRA SE,8 RDR,ENC,NPS
GSTAR016-SE-NPS	iSTAR G2 ULTRA SE,16 RDR,ENC,NPS
GSTAR-PRO-SE08	KIT,PRO-GSTAR SE,GCM, 1 ACM
GSTAR-PRO-SE16	KIT,PRO-GSTAR SE,GCM, 2 ACM

About Johnson Controls

Johnson Controls is a global diversified technology and multi-industrial leader serving a wide range of customers in more than 150 countries. Our 120,000 employees create intelligent buildings, efficient energy solutions, integrated infrastructure and next generation transportation systems that work seamlessly together to deliver on the promise of smart cities and communities. Our commitment to sustainability dates back to our roots in 1885, with the invention of the first electric room thermostat.

For additional information, please visit www.swhouse.com or follow Software House on LinkedIn, Twitter, and Facebook.

SH1359-DS-202205-R01-HS-EN

Software House

Johnson Controls