# Table of Contents

## Preface

- Conventions .......................... x
- Finding More Information .................. xi
- Software House Customer Support Center .................. xii

## Chapter 1 Overview and Introduction

- Overview ........................................ 1-2
  - General Control Module ....................... 1-2
  - Access Control Module ....................... 1-2
  - IP-ACM Ethernet Door Module ................. 1-3
- Types of Mounting ............................... 1-4
  - Wall Mount Enclosure ....................... 1-4
  - Rack Mount Enclosures ..................... 1-5
  - iSTAR Ultra .................................. 1-6
- Main Features .................................. 1-7
  - Processor .................................. 1-7
  - Storage .................................. 1-7
  - Power .................................. 1-7
  - RM / Wiegand Signaling Readers (per ACM) 1-7
  - Aperio Hubs and Readers (per GCM RS-485 Comm Port) 1-8
  - I/O (per ACM) .............................. 1-8
  - I/O (per GCM) .............................. 1-9
  - Communications ......................... 1-9
  - FAI .................................. 1-9
  - Onboard Controls ......................... 1-9
  - Housing .................................. 1-10
- Part Numbers .................................. 1-10

## Chapter 2 Site Requirements and Installation

- Pre-Installation Planning and Requirements ....... 2-2
  - Equipment Check ............................ 2-2
  - Types of Mounting ......................... 2-2
  - Environmental Requirements ............... 2-2
  - Site Requirements ........................... 2-2
  - Grounding Requirements .................... 2-3
  - Wiring Requirements ....................... 2-3
  - Heat Dissipation ......................... 2-5
  - iSTAR Ultra Wall Mount Dimensions ........ 2-5
Table of Contents

Wall Mount Hardware .................................. 2-5
Power Requirements .................................. 2-7
    Electrical ........................................ 2-7
    Maximum Power .................................. 2-8
    Additional Power Requirements ................. 2-9
    Battery .......................................... 2-10
    Heat Dissipation ................................ 2-10
Other Interactions with the Power System .......... 2-12
    AC / Main Fail Input ............................... 2-12
    Low Battery Input ................................ 2-12
Reader Power Requirements ......................... 2-13
    Software House Readers ......................... 2-13
    Third Party Readers .............................. 2-14
Installation .......................................... 2-15
    Wall Mount Installation ......................... 2-15
        Requirements ................................ 2-15
    Rack Mount Installation ......................... 2-17
        Rack Mount Considerations .................. 2-17
    IP-ACM Installation .............................. 2-18
        Plastic Enclosure ............................. 2-18
        Requirements ................................ 2-18
        Metal Enclosure ............................... 2-19

Chapter 3  iSTAR Ultra Network Topology

iSTAR Ultra Network Topology ....................... 3-2
    LAN and WAN Configurations .................... 3-2
    Gateways and Firewalls .......................... 3-2
        Local Address Management ................... 3-3
    IP Management Tools ............................. 3-4
        Fully Qualified Domain Names ............... 3-4
Cluster Configuration ............................... 3-5
    Master and Member Configuration ............... 3-5
Master Configurations .............................. 3-7
    Single Master Configurations .................. 3-7
Communication Paths ................................ 3-8
    Primary Communications Path .................. 3-8
    Secondary Communications Path ................ 3-9
Maintaining Cluster Communication ................ 3-10
    Single Master Configurations .................. 3-10
Adding Controllers to the Cluster ................ 3-11
Configuring Communication Paths .................. 3-12
    Planning Primary Communications .............. 3-12
        Primary Communication Guidelines ........ 3-12
        Planning Secondary Communications ....... 3-12
Chapter 4  General Control Module (GCM)

General Control Module .......................................................... 4-2
   Network Connections ......................................................... 4-3
Switches ................................................................. 4-3
   SW7 - Soft Reset (Reboot) ................................................ 4-3
   SW2 - Hard Processor Reset ............................................ 4-3
   SW3 Rotary Switch .......................................................... 4-4
   S1-1 (Encryption) ............................................................ 4-4
   S1-2 - CPNI ................................................................. 4-5
   S1-3 ................................................................. 4-5
   S1-4 ................................................................. 4-5
   RS - 485 Terminators - SW5 and SW6 ............................ 4-5
   LCD Contrast Potentiometer - RV1 .................................... 4-5
   AC Fail - Low Battery - J2 .............................................. 4-5
   AC Fail Input .............................................................. 4-6
   Low Battery Input .......................................................... 4-6
   Tamper - J1 ................................................................. 4-6
   GCM Power - J4 ............................................................ 4-7
   J14 SD Card ................................................................. 4-7
Ports ................................................................. 4-8
   RS-485 1 and 2 (J12 and J13) .......................................... 4-8
   USB Type A - J8 and J9 .................................................... 4-8
   USB Micro A-B - J7 ........................................................ 4-8
   RS-232 Diagnostic Port (P4) .............................................. 4-8
   COMM Board Connector - J15 ........................................... 4-8
Visual Indicators ............................................................. 4-8
   Power - DS1 and DS2 ...................................................... 4-8
   LCD ................................................................. 4-8
   LEDs ................................................................. 4-9

Chapter 5  Access Control Module (ACM)

Access Control Module .......................................................... 5-2
Switches and Jumpers .......................................................... 5-5
   SW10 - ACM MCU Reset ............................................... 5-5
   J1 USB Type B 2.0 Port .................................................. 5-5
   SW32 ACM Address Switch ............................................. 5-5
   RS - 485 Terminators ..................................................... 5-6
   Wet/ Dry Jumpers .......................................................... 5-6
   Output Relay Wet or Dry Jumpers .................................... 5-6
   Jumper Settings ........................................................... 5-6
   Activate on FAI ............................................................ 5-7
   FAI on this ACM - SW31 ................................................ 5-7
   Enable FAI Latch - SW30 ............................................... 5-7
Ports and Connectors .......................................................... 5-7
   J1 USB connection to GCM .............................................. 5-7
   Tamper - J22 ............................................................... 5-7
### Table of Contents

- Reader Power - J4 .................................................. 5-7
- LOCK 1 Power - J2 .................................................. 5-8
- LOCK 2 Power - J3 .................................................. 5-8
- FAI and Key - J84 .................................................. 5-8

**Wiegand Connections** ........................................... 5-9
- Wiegand Port Rating ............................................... 5-10
- RS-485 .................................................................. 5-10
- AUX Outputs ......................................................... 5-12
- INPUTS .................................................................. 5-12
- Supervision Wiring ................................................ 5-12
- Relay Outputs ......................................................... 5-13
- Dry Relay Wiring ..................................................... 5-14
- Wet Relay Wiring ..................................................... 5-14
- Wet Wiring for a Magnetic Lock ............................... 5-15

**Inputs** .................................................................. 5-18
- NO/NC Dual EOL 1K .................................................. 5-21
- NO/NC Dual EOL 5K, 10K ........................................... 5-21
- Double EOL 1K, 5K, 10K ............................................ 5-22
- Single EOL 5K, 10K .................................................. 5-23
- Non-Supervised ....................................................... 5-23

**FAI Connections** .................................................... 5-24
- FAI Scenarios ......................................................... 5-24
- FAI Modes ............................................................. 5-24
  - FAI without Latch ................................................. 5-24
  - FAI with Latch followed by Key Unlatch .................. 5-25
  - F and K input Supervision ...................................... 5-25
  - State of F, K, and Relay Drive ............................... 5-27
- iSTAR Controller Status Tab ................................. 5-28

- Reader - Voltage Requirements and Distance ........... 5-29

**Inputs and Accessory Boards** .................................. 5-31

---

**Chapter 6**  
**IP-ACM Ethernet Door Module v2**

Overview ................................................................. 6-2

**Chapter 7**  
**iSTAR Ultra Controller Configuration**

iSTAR Ultra Network Configuration ............................. 7-2
  - Board Configuration ............................................. 7-2
  - iSTAR Ultra DHCP IP Address Configuration ........... 7-2
  - STAR Ultra Static IP Address Configuration ............ 7-2

iSTAR Configuration .................................................. 7-4
  - ICU ................................................................. 7-4
    - Using the ICU in LAN Configurations ................. 7-4
    - Using the ICU in WAN Configurations ............... 7-5
  - iSTAR Ultra Web Utility ...................................... 7-5
  - C•CURE 9000 .................................................... 7-7

STAR Ultra Local Database Backups ............................ 7-7
Proper Shutdown Sequence ........................................ 7-8

Chapter 8  Maintenance

LCD Message Display ........................................... 8-2
  Displaying Status Messages .................................. 8-3
  Setting LCD Status Message Display ......................... 8-3
Diagnostic Tests .................................................... 8-4
  Hardware Test ...................................................... 8-4
  Card Reader Diagnostics ......................................... 8-5
  Output Diagnostics ............................................... 8-5
    Output Change Display (Slow Mode) ......................... 8-5
  Input Change Display Mode ..................................... 8-5
  Ethernet Port Test ............................................... 8-6
GCM Battery Replacement ......................................... 8-7
Preface

This guide is designed for new and experienced security system users. The guide describes procedures for installing, configuring, using, and maintaining the iSTAR Ultra controller.

The guide assumes that you are a certified C•CURE 9000 Technician and C•CURE 9000 is installed.

In this Preface
◆ Conventions ................................................................. x
◆ Finding More Information .................................................. xi
◆ Software House Customer Support Center ................................ xii
Conventions

This manual uses the following text formats and symbols.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>This font indicates screen elements, and also indicates when you should take a direct action in a procedure. Bold font describes one of the following items:</td>
</tr>
<tr>
<td></td>
<td>▪ A command or character to type, or</td>
</tr>
<tr>
<td></td>
<td>▪ A button or option on the screen to press, or</td>
</tr>
<tr>
<td></td>
<td>▪ A key on the keyboard to press</td>
</tr>
<tr>
<td></td>
<td>▪ A screen element or name</td>
</tr>
<tr>
<td><strong>Regular italic font</strong></td>
<td>Indicates a new term, or a book title.</td>
</tr>
<tr>
<td><strong>&lt;text&gt;</strong></td>
<td>Indicates a variable.</td>
</tr>
</tbody>
</table>

The following items are used to indicate important information.

- **NOTE** Indicates a note. Notes call attention to any item of information that may be of special importance.
- **TIP** Indicates an alternate method of performing a task.
- ! Indicates a caution. A caution contains information essential to avoid damage to the system. A caution can pertain to hardware or software.
- Indicates a warning. A warning contains information that advises users that failure to avoid a specific action could result in physical harm to the user or to the hardware.
- Indicates a danger. A danger contains information that users must know to avoid death or serious injury.
Finding More Information

You can access the C•CURE manuals and online Help for more information about C•CURE.

Manuals

C•CURE 9000 software manuals are available in Adobe PDF format on the C•CURE 9000 installation media. You can access the manuals if you copy the appropriate PDF files from the C•CURE 9000 installation media Manuals\CCURE folder.

The available C•CURE 9000 and Software House manuals are listed in the C•CURE 9000 Installation and Upgrade Guide.

These manuals are also available from the Software House Member Center website (http://www.swhouse.com/TechnicalLibrary/TechLibSW.aspx).

Online Help

You can access C•CURE Help by pressing F1 or clicking Help from the menu bar in the Administration and Monitoring Station applications.
Software House Customer Support Center

Technical Support Portal

The Technical Support Portal provides knowledge-based articles, technical documents, and tips to install and use Software House products.


The email address you use to register for access to the portal must be the same one you used for the certification course.

If the request is approved, log in credentials are emailed twenty-four to forty-eight hours after received.

Telephone Technical Support

During the period of the Agreement, the following guidelines apply:

- Software House accepts service calls only from employees of the Systems Integrator of Record for the installation associated with the support inquiry.

Before Calling

Ensure that you:

- Are the Dealer of record for this account.
- Are certified by Software House for this product.
- Have a valid license and current Software Support Agreement (SSA) for the system.
- Have the system serial number available.
- Have your certification number available.

<table>
<thead>
<tr>
<th>Hours</th>
<th>Normal Support Hours</th>
<th>Monday through Friday, 8:00 a.m. to 8:00 p.m., EST. Except holidays.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Emergency Support Hours</td>
<td>24 hours/day, seven days a week, 365 days/year.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Requires Enhanced SSA “7 x 24” Standby Telephone Support (emergency)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>provided to Certified Technicians.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For all other customers, billable on time and materials basis.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Minimum charges apply – See MSRP.</td>
</tr>
<tr>
<td>Phone</td>
<td>For telephone support contact numbers for all regions, see <a href="http://www.swhouse.com/support/contact_technical_support.aspx">www.swhouse.com/support/contact_technical_support.aspx</a>.</td>
<td></td>
</tr>
</tbody>
</table>

EMEA

Hours: 8:00 a.m. to 6:00 p.m. CET

- Toll Free: +800 CALLTYCO or +800-2255 8926
Direct: +31 475 352 722

Local Direct Dial Numbers:
- UK: +44 330 777 1300
- Israel: +972-772 201 350
- Spain: 900 99 31 61
- Denmark: +45-4494 9001
- France: 0800 90 79 72
- Germany: 0800 1806 757
- Italy: +39-0230 510 112
- Belgium: 0800 76 452
- Ireland: 1800943570
- Nordic: 04494 9001
- Greece: 00800-312 294 53
- South Africa: +27-211 003 882
- Russia: 81080020521031
- Turkey: 00800-31923007
- UAE: 800-03107123
- Bahrain: 800-04127

Asia Pacific

Hours: 9:00 a.m. to 5:00 p.m. CST
- Toll Free: +800 CALLTYCO or (+800-2255 8926)
- Direct: +86 21 61916510
- China only Hotline: 4006711528
- India only Hotline: 1-800-1082-008
- Australia: 02-9684-3980

Latin America

- Colombia: + 57 1 344-1422 +57 2 8912476 +57 4 2040519
- Costa Rica: + 506 4000-1655
- República Dominicana: +1 8292353047
- El Salvador: + 503 21368703
- Guatemala: + 502 22681206
- Panamá: + 507 836-6265
- Mexico: + 52 5585261801
- Perú: + 511 6429707
- Venezuela: + 58 212-720-2340
- Buenos Aires: + 54 11 5199 3104
- Santiago de Chile: + 56 2 3210 9662
- Sao Paulo: + 55 11 3181 7377
Overview and Introduction

The iSTAR Ultra is an enhanced, intelligent controller for networked security systems. iSTAR Ultra hardware and firmware includes a general purpose board General Controller Module (GCM) and one or more special purpose Access Control Modules (ACM) or IP-ACM v2 modules.

This guide assumes you are a certified dealer who has attended iSTAR Ultra training, that you are familiar with networking concepts and hardware installation, and you are using firmware v6.5.2 or higher.

In This Chapter:

- Overview ........................................................................................................................................................... 1-2
  - General Control Module................................................................................................................................... 1-2
  - Access Control Module................................................................................................................................. 1-2
  - IP-ACM Ethernet Door Module .................................................................................................................. 1-3
- Types of Mounting ........................................................................................................................................ 1-4
  - Wall Mount Enclosure .................................................................................................................................. 1-4
  - Rack Mount Enclosures ............................................................................................................................... 1-5
- Main Features ................................................................................................................................................... 1-7
  - iSTAR Ultra .................................................................................................................................................. 1-6
  - Processor ....................................................................................................................................................... 1-7
  - Storage ........................................................................................................................................................... 1-7
  - Power ............................................................................................................................................................ 1-7
  - RM / Wiegand Signaling Readers (per ACM) ............................................................................................ 1-7
  - Aperio Hubs and Readers (per GCM RS-485 Comm Port) ........................................................................ 1-8
  - I/O (per ACM) ............................................................................................................................................. 1-8
  - I/O (per GCM) ............................................................................................................................................. 1-9
  - Communications ........................................................................................................................................... 1-9
  - FAI ................................................................................................................................................................. 1-9
  - Onboard Controls ........................................................................................................................................ 1-9
  - Housing ....................................................................................................................................................... 1-10
- Part Numbers .................................................................................................................................................. 1-10
Overview

The iSTAR Ultra can support up to 16 traditional hard-wired readers and clustering of up to sixteen controllers. The Ultra supports wireless lock sets up to 32 total (this includes traditional and wireless) locksets. The iSTAR Ultra controller consists of the following hardware components:

- General Controller Module (GCM)
- Access Control Module (ACM) - a maximum of two can be connected
- IP-ACM - a maximum of 32 can be connected

General Control Module

The GCM is a General Purpose Module running the Linux® operating system. The GCM provides the following features:

- Two network Gigabit Ethernet ports.
- Two RS-485 Ports for Aperio™ hubs and wireless locks, or Schlage® PIMs and wireless locks.
  - Up to 30 eight-port Aperio hubs (15 per RS485 port) up to 32 Aperio locks.
  - Or, up to 32 16-port Schlage PIMs (16 per RS485 port) up to 32 Schlage locks.
- An LCD panel that displays the current status, and provides built-in diagnostics.
- Four USB ports to communicate with the Access Control Modules (ACM) and import encryption keys.
- One Micro A-B port. (For future use).

Access Control Module

The ACM is a special purpose Access Control Module that interfaces with the GCM and provides inputs, outputs, reader interfaces, and AUX outputs. An iSTAR Ultra can contain up to two ACMs that interface directly with Wiegand signaling devices and RM reader buses. The RM reader busses can interface with Wiegand signaling devices and ABA (magnetic) signaling devices. External lock power can be used to “wet” the relay contacts, or to run them “dry” using an external power supply. FAI (Fire Alarm Interface) is also supported along with the ability to selectively latch the relays until released by a Key switch.

The ACM contains the following ports:

- Supervised Inputs (24 ports) - supervision type is individually selected on each input.
- Socket mounted Primary Relays 5A Dry or 0.75A Wet.(8 ports)
- Permanently soldered Secondary Relays 1A Dry or Wet (8 ports)
- Reader Power In (12 Vdc)
- Lock 1 Power In (0 to 30 Vdc)
- Lock 2 Power In (0 to 30 Vdc)
- FAI (Fire Alarm Interface) and FAI Key signals
- AUX Output (8 ports) (12 Vdc)*
The ACM supports a total of 8 readers in any combination of the following:

- RS-485 RM Reader (8 readers across 8 ports)
- Wiegand Reader (8 readers)

There are eight basic sections, on each ACM, that support the total of eight Readers. Each section has:

- One Reader port (either)
  - One RM / RS-485 Reader port*
  - One Wiegand signaling port*
- Three supervised Inputs
- Two relay Outputs
- One AUX output (12 Vdc)*

* The AUX power and whichever reader power is used, are limited to a total of 1.5 Amp.

See Chapter 5, "Access Control Module (ACM)" for more information.

**IP-ACM Ethernet Door Module**

The IP-ACM Ethernet Door Module v2 provides connection and management of access control for two readers. The GCM supports a maximum of 32 IP-ACM modules with 1 reader per IP-ACM or a maximum 16 IP-ACMs with 2 readers per IP-ACM. The limiting factor is a maximum of 32 readers.

For the iSTAR Ultra to operate with the IP-ACM v2 modules, the GCM must be running firmware version 6.5.4 or higher and C•CURE 9000 must be version 2.61 or higher.

See Chapter 6, "IP-ACM Ethernet Door Module v2" for an overview of the IP-ACM module.

For more information regarding the features and installation of the IP-ACM, refer to the IP-ACM Ethernet Door Module v2 Quick Start Guide.
Types of Mounting

The iSTAR Ultra and its components can be installed in a wall mount enclosure or in separate rack mount enclosures.

Wall Mount Enclosure

Figure 1-1 on page 1-4 shows a photograph of the iSTAR Ultra and two ACMs in a wall mount enclosure.
Rack Mount Enclosures

Figure 1-2 on page 1-5 shows the GCM in a rack mount enclosure.

Figure 1-2: GCM Rack Mount Enclosure

Figure 1-3 on page 1-5 shows the rear of the GCM rack mount enclosure.

Figure 1-3: GCM Rear Rack Mount Enclosure
Figure 1-4 shows the iSTAR Ultra enclosure. The bright power LED will shine through the Power decal when the door is closed. The bright LED will extinguish when the door is opened.
Main Features

Processor
- Freescale i.MX6 ARM processor, 1GHz

Storage
- 2GB DDR3 RAM
- 16GB SD Card

Power
- Powered by 12 Vdc, from UL Listed apS power source or other UL 603 Listed, power-limited power supply with appropriate ratings and a minimum 4 hours of standby power.
- Provides up to 1.5A @ 12Vdc unswitched to external devices:
  - Wiegand signaling readers
  - RS-485 ports
- Provides power to relays:
  - Relays configurable to be wet or dry by jumper.
  - Wet Relays provide current at main input voltage (12 or 24V with external DC supply).
  - Each wet relay is limited to 0.75A (at 12 or 24V).
  - Each Primary dry relay is limited to 5.0A (at 12 or 24V).
  - Each Secondary dry relay is limited to 1.0A (at 12 or 24V).
- Full operating backup power is not provided by the board itself.
  - Achieved with apS or external UPS,
  - Upon loss of external power, data is written to onboard flash.

RM / Wiegand Signaling Readers (per ACM)
The ACM supports a total of 8 readers in any combination of the following:
- RS-485 RM Reader (8 readers across 8 ports)
- Wiegand Reader (8 readers)

There are eight basic sections, on each ACM, that support the total of eight Readers. Each section has:
- One Reader port (either)
  - One RM / RS-485 Reader port*
  - One Wiegand signaling port*
- Three supervised Inputs
Main Features

- Two relay Outputs
- One AUX output (12 Vdc)*

* The AUX power and whichever reader power is used, are limited to a total of 1.5 Amp.

Aperio Hubs and Readers (per GCM RS-485 Comm Port)

An iSTAR Ultra GCM RS-485 Port supports a total of up to:
- 15 Aperio Hubs
  - Hubs can be 1 Port or 8 Ports
- 16 Aperio Wireless Readers reporting to the Hubs

In other words, there can be up to 30 Hubs and/or 32 Wireless Readers per iSTAR Ultra.

There can be any combination of Hubs and Wireless Readers that do not exceed these limits.

The configured RM / Wiegand Readers can only exist to the extent that the configured Aperio Readers are less than 32.

NOTE
- The maximum number of enabled readers, wired or wireless, per iSTAR Ultra is 32.
- The maximum number of readers hard wired to ACMs is 16.

I/O (per ACM)

- 24 general purpose inputs.
- 16 general purpose relays:
  - Dry or wet contact settable per relay by jumpers.
  - 4-pin connectors to support NO/NC and Dry/Wet configurations.
- Special purpose inputs:
  - Tamper (from enclosure door).
  - Main AC fail (from apS).
  - Low external battery (from apS.)

NOTE
- The following 4 inputs to the host are determined by the firmware. There is no actual wiring to the iSTAR Ultra board.
  - FAI Alarm State (J40 F input).
  - FAI Relay Control State.
  - FAI Interlock Key State (J40 K input).
- Onboard battery low.
- Large standard two-piece terminal blocks and spacing minimize the potential of mis-wiring.
Main Features

- 1 USB 2.0 Port for communication to the GCM.

I/O (per GCM)

- RS-485 Comm Ports
  - 2 four-pin Ports for Aperio Hubs
- USB 2.0 Ports
  - 4 USB host port.
  - The only use of USB in the first version is to connect to the ACMs and to import encryption keys.
  - 1 USB Micro B port. (not currently used).

Communications

- Two 1 Gbps full duplex, Auto Sense Ethernet Ports.
- FIPS-197 and AES 256-bit encryption.
- Can cluster with other iSTAR Ultras either encrypted or non-encrypted.
- Can cluster with iSTAR Edge, iSTAR eX, iSTAR Pro, iSTAR Ultra SE (Ultra Mode) and other iSTAR Ultras, when encrypted.

FAI

Fire Alarm Interlock. When the F (Fire) input is true, FAI activates relays that are enabled for FAI by individual enable switches. The Primary relays (large, mounted in sockets) can be configured to activate when the FAI signal goes true.

Onboard Controls

- LCD with back light for Status and Diagnostics.
- Rotary switch for diagnostics.
- LEDs for serial, Ethernet, power and relay states.
  - Two power LEDs: one super bright LED that is on when the enclosure door is closed, and one green LED that is always on when main power is present.
  - Relay activation LEDs are not affected by enclosure door.
  - All other LEDs only turn on when enclosure door is open.
- Soft Reboot button. (Also backs up the DB).
- Hard Reset (Stops Linux. Can be used to restore Factory defaults) See Table 4-1 on page 4-4.
- Switches for serial termination of RM ports.
- Switches for selection of relays for control by FAI.
- Switches for LED/beep control for Wiegand Ports.
Part Numbers

- Switch for ACM address, unit 0 or unit 1.
- Switch for FAI Enable.
- Switch for FAI Latch Enable.
- Switch for AES Encryption.
- Jumpers for relay wet/dry control.
- Switch for Backup/Restore.

Housing

- Rack mount Enclosures
- Wall mount Enclosure

Part Numbers

Table 1-1: Part Numbers

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USTAR008</td>
<td>Contains one GCM (0312-7101-01), one ACM (0312-5015-01), and one enclosure (0505-0411-01)</td>
</tr>
<tr>
<td>USTAR016</td>
<td>Contains one GCM (0312-7101-01), two ACM (0312-5015-01), and one enclosure (0505-0411-01)</td>
</tr>
</tbody>
</table>

Subassemblies

- USTAR-GCM General Controller Module
- USTAR-ACM Access Controller Module
- USTAR-CAN Enclosure
- USTAR-GCM-2U GCM Rack Mount enclosure with GCM (0312-7101-02)
- USTAR-ACM-4U ACM Rack Mount enclosure with ACM

Subassemblies - IP-ACM v2 Ethernet Door Module

- IP-ACM2A-MB IP-ACM V2, 2 Reader, board only
- IP-ACM2A-EM IP-ACM V2, 2 Reader in metal enclosure
- IP-ACM2A-EP IP-ACM V2, 2 Reader in plastic enclosure
Site Requirements and Installation

This chapter provides information about site requirements and installation for the iSTAR Ultra hardware.

In This Chapter:

- **Pre-Installation Planning and Requirements** ................................................................. 2-2
  - Equipment Check ........................................................................................................ 2-2
  - Types of Mounting ..................................................................................................... 2-2
  - Environmental Requirements .................................................................................... 2-2
  - Site Requirements ..................................................................................................... 2-2
  - Grounding Requirements .......................................................................................... 2-3
  - Wiring Requirements ................................................................................................. 2-3
  - Heat Dissipation ....................................................................................................... 2-5
  - iSTAR Ultra Wall Mount Dimensions ....................................................................... 2-5
  - Wall Mount Hardware ................................................................................................ 2-5
- **Power Requirements** ................................................................................................. 2-7
  - Electrical .................................................................................................................... 2-7
  - Additional Power Requirements ................................................................................ 2-9
  - Battery ....................................................................................................................... 2-10
  - Software House Readers .......................................................................................... 2-13
  - Third Party Readers .................................................................................................. 2-14
- **Installation** ................................................................................................................ 2-15
  - Wall Mount Installation ............................................................................................ 2-15
  - Rack Mount Installation ............................................................................................ 2-17
  - IP-ACM Installation .................................................................................................... 2-18
Pre-Installation Planning and Requirements

Pre-installation involves the following:

1. Checking equipment (hardware, software, power supply, and wiring).
2. Checking power, wiring, equipment clearances, and code compliance at the site.
3. Ensuring the proper tools are available.

Equipment Check

Verify that the contents of the shipped boxes match the packing lists. Contact Software House if any items are missing or damaged.

The iSTAR Ultra hardware does not include mounting hardware for an installation. Mounting hardware depends upon the site and must be approved by a structural engineer or other certified professional.

Software House recommends anchoring systems capable of sustaining a 75 lb. load (without cables).

Types of Mounting

The iSTAR Ultra and its components can be installed in a wall mount enclosure or in a separate rack mount enclosure.

Environmental Requirements

Table 2-1 on page 2-2 lists the iSTAR Ultra environmental requirements.

<table>
<thead>
<tr>
<th>Status</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>32° F (0° C) to 122° F (50° C)</td>
</tr>
<tr>
<td>Storage</td>
<td>4° F (-20° C) to 158° F (70° C)</td>
</tr>
</tbody>
</table>

Site Requirements

Ensure that the site is ready:

- The iSTAR Ultra installation must be performed by a certified installer.
- The iSTAR Ultra must be installed and wired according to local and national regulations.
- The iSTAR Ultra must be installed in a restricted access, protected area.
- Non-limited power supply lines must maintain (1/2 inch (1.3 cm)) spacing from limited power supply lines and other signaling lines. Secure lines must be installed in accordance to local and national electric codes.
- The site must be approved and all wiring must comply with UL requirements and other codes, in accordance with the National Electric Code, ANSI/NFPA70-1993.
Pre-Installation Planning and Requirements

- All preliminary site work is complete.
- System power needs to be 12 Vdc. Appropriate circuit breakers must be accessible. Power supplies must be listed to UL-603 or UL-294.
- The site is clean and free of dust or other contaminants.
- Ensure that the mounting site is ready to accommodate the iSTAR dimensions.

Grounding Requirements

Grounding requirements are as follows:
- Ensure that the iSTAR Ultra controller is properly connected to an earth ground at any of the ground studs.
- Ensure that the shield wires are grounded at one end of the cable to the nearest earth/ground connection. Ground shields of both the GCM and ACMs.
- When disconnecting wiring, disconnect ground wires last (to provide maximum protection to the equipment and personnel).

NOTE

- Ethernet cabling must be CAT-5E or better.
- Use shielded Ethernet cabling in rack mount configurations.
- The input terminals on the iSTAR Ultra accept conductor size up to 2mm² (12 AWG).

Wiring Requirements

The iSTAR Ultra Ethernet connections are:
- GCM Onboard Ethernet ports - support 1 Gbps each.

Table 2-2 on page 2-3 lists the general wiring requirements for the iSTAR Ultra and its components.

<table>
<thead>
<tr>
<th>Signal</th>
<th>From</th>
<th>To</th>
<th>Belden # or equiv.</th>
<th>AWG</th>
<th># Prs</th>
<th>Shield</th>
<th>Max Length</th>
<th>Max. Wire Resistance</th>
</tr>
</thead>
<tbody>
<tr>
<td>RS-485 Comm, Data Half-duplex 2 wire</td>
<td>iSTAR Ultra</td>
<td>RM &amp; I/O Modules</td>
<td>9841</td>
<td>24</td>
<td>1</td>
<td>Yes</td>
<td>4000 ft. (1212 m)</td>
<td>103Ω</td>
</tr>
<tr>
<td>RS-485 Comm, Power</td>
<td>iSTAR Ultra</td>
<td>RM &amp; I/O Modules</td>
<td>8442/8461</td>
<td>22/18</td>
<td>1</td>
<td>Yes</td>
<td>Range of 600 ft. to 1500 ft. depends on AWG</td>
<td>See Note b</td>
</tr>
</tbody>
</table>
Table 2-2: Equipment Wiring Specifications, continued

<table>
<thead>
<tr>
<th>Signal</th>
<th>From</th>
<th>To</th>
<th>Belden # or equiv.</th>
<th>AWG</th>
<th># Prs</th>
<th>Shield</th>
<th>Max Length</th>
<th>Max. Wire Resistance</th>
</tr>
</thead>
<tbody>
<tr>
<td>RJ45-Ethernet</td>
<td>iSTAR Ultra</td>
<td>Hub, Host</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
<td>328 ft. (100 m)</td>
<td>8.4 Ω</td>
</tr>
<tr>
<td>Supervised Input</td>
<td>iSTAR Ultra or I8</td>
<td>Input</td>
<td>8442/8461</td>
<td>22/18</td>
<td>1</td>
<td>No</td>
<td>2000 ft. (606 m)</td>
<td>32 Ω</td>
</tr>
<tr>
<td>Request-to-exit (REX or RTE)</td>
<td>iSTAR Ultra or RM-4/4E module</td>
<td>Switch</td>
<td>8442/8461</td>
<td>22/18</td>
<td>1</td>
<td>No</td>
<td>2000 ft. (606 m)</td>
<td>32 Ω</td>
</tr>
<tr>
<td>Door State Monitor (DSM)</td>
<td>iSTAR Ultra or RM-4/4E module</td>
<td>Contact</td>
<td>8442/8461</td>
<td>22/18</td>
<td>1</td>
<td>No</td>
<td>2000 ft. (606 m)</td>
<td>32 Ω</td>
</tr>
<tr>
<td>Supervised Input (UL) Note a</td>
<td>iSTAR Ultra or I8</td>
<td>Input</td>
<td>9462</td>
<td>22</td>
<td>1</td>
<td>Yes</td>
<td>2000 ft. (606 m)</td>
<td>32 Ω</td>
</tr>
<tr>
<td>Relay Control</td>
<td>RM-4 module</td>
<td>ARM-1</td>
<td>9462</td>
<td>22</td>
<td>1</td>
<td>Yes</td>
<td>25 ft. (7.6 m)</td>
<td>.04Ω</td>
</tr>
<tr>
<td>Reader Data</td>
<td>iSTAR Ultra or RM-4/4E module</td>
<td>Proximity/ Wiegand signaling read head</td>
<td>9942 9260 Alpha wire 5386C</td>
<td>22 20 18</td>
<td>3</td>
<td>Yes</td>
<td>200 ft. (60.96 m)</td>
<td>3.2 Ω (22)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>300 ft. (91.4 m)</td>
<td>3.2 Ω (20)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>500 ft. (152.4 m)</td>
<td>3.2 Ω (18)</td>
</tr>
</tbody>
</table>

a. To comply with UL requirements, use shielded, minimum 22 AWG stranded, twisted pair cable for monitor points, supervised inputs, DSMs, and REXs. Use Belden 9462 or equivalent.

b. Check wire lengths to verify that voltage drops are acceptable.

Calculations are based on a single RM-4 reader with keypad and LCD (250 mA):
- Using 22 AWG, distance = 600 ft. (.0165 Ω/ft.)
- Using 18 AWG, distance = 1500 ft. (.0065 Ω/ft.)

NOTE

- The Tamper, Low Battery, and AC power fail inputs must be enabled and connected to the iSTAR Ultra to report for compliance with UL requirements.
- For UL listed products, burglar alarm inputs must be supervised.
- UL Listed panic hardware shall be used to allow emergency exit from a protected area.
- The USTAR-GCM AC Fail/Lo Batt and COMM, USTAR-GCM and USTAR-ACM Tamper, USTAR-GCM power, USTAR-ACM power (Reader), USTAR-ACM lock 1 and lock 2 connections are not to leave the room of installation or 25’ beyond control unit. Therefore, these connections were not tested for output transients.
Heat Dissipation

Table 2-3 on page 2-5 lists the heat dissipation for the rack and wall mount configurations.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Power Dissipated in Enclosure</th>
<th>BTU/hour</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rack GCM</td>
<td>17.88 Watts</td>
<td>61.0</td>
</tr>
<tr>
<td>Rack ACM</td>
<td>6 Watts</td>
<td>20.5</td>
</tr>
<tr>
<td>Wall GCM and (1) ACM</td>
<td>23.88 Watts</td>
<td>81.5</td>
</tr>
<tr>
<td>Wall GCM and (2) ACMs</td>
<td>29.88 Watts</td>
<td>102.0</td>
</tr>
</tbody>
</table>

iSTAR Ultra Wall Mount Dimensions

Table 2-4 on page 2-5 lists the iSTAR Ultra Cabinet Wall Mount Dimensions.

<table>
<thead>
<tr>
<th>Item</th>
<th>Dimension/Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weight</td>
<td>26.5 lb (12.02 kg)</td>
</tr>
<tr>
<td>Height</td>
<td>21.5 in. (54.61 cm)</td>
</tr>
<tr>
<td>Width</td>
<td>25 in. (63.5 cm)</td>
</tr>
<tr>
<td>Depth</td>
<td>5 in. (12.7 cm)</td>
</tr>
<tr>
<td>Upper Mounting Holes</td>
<td>10 in. (22.86 cm) center to center. The outer two mount holes are keyhole type.</td>
</tr>
<tr>
<td>Bottom three Mounting Holes</td>
<td>Directly below the upper mount holes.</td>
</tr>
</tbody>
</table>

Wall Mount Hardware

Table 2-5 on page 2-6 lists the hardware recommended for wall mounting the iSTAR Ultra. The hardware listed in Table 2-5 is not included with the iSTAR Ultra.

You must consult a Structural Engineer when mounting to meet local Seismic requirements.

Consult a structural expert for mounting configurations not listed in Table 2-4.
### Table 2-5: Wall Mount Hardware Recommendations

<table>
<thead>
<tr>
<th>Anchor Type</th>
<th>Screw Type (Pan Head)</th>
<th>Wood Studs, Plywood Wall</th>
<th>Drywall Plaster Board</th>
<th>Concrete, Brick, or Block Wall</th>
<th>Minimum Number of Screws</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Anchor</td>
<td>Wood Screws</td>
<td>#10 x 1-1/4 inch</td>
<td></td>
<td></td>
<td>6</td>
</tr>
<tr>
<td>No Anchor</td>
<td>Concrete Screws</td>
<td></td>
<td></td>
<td>#10 x 1-1/4 inch</td>
<td>4</td>
</tr>
<tr>
<td>Super Hold Plastic Anchors</td>
<td>Wood, sheet metal</td>
<td>#10 x 1-1/4 inch</td>
<td>#10 x 1-1/4 inch</td>
<td></td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Plastic Anchors</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Toggle Bolts</td>
<td>(bolt included)</td>
<td>(only for keyholes)</td>
<td>10-24 x 1-1/4 inch</td>
<td>10-24 x 1-1/4 inch</td>
<td>2</td>
</tr>
<tr>
<td>Hollow Wall Anchor</td>
<td>(screw included)</td>
<td>10-24 x 1-1/4 inch</td>
<td>10-24 x 1-1/4 inch</td>
<td></td>
<td>6</td>
</tr>
<tr>
<td>Sleeve Anchor</td>
<td>(screw and nut</td>
<td>1/4-20 x 1-3/8 inch</td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>included)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wedge Anchor</td>
<td>(screw and nut</td>
<td>1/4-20 x 1-3/8 inch</td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>included)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Machine Screw Anchor</td>
<td>Machine screw</td>
<td>10-24 x 1 inch</td>
<td></td>
<td></td>
<td>6 X# 10, 4 x 1/4</td>
</tr>
<tr>
<td>Lag Shield Anchor</td>
<td>Lag screws</td>
<td>1/4 x 1 inch</td>
<td></td>
<td></td>
<td>6</td>
</tr>
</tbody>
</table>
Power Requirements

Electrical

This section provides the power requirements for the iSTAR Ultra and its components. Electrical ratings are dependent upon the configuration.

GCM

- Power Input (12 Vdc ± 20%)
  12 Vdc, 1.5A minimum, 4.5A maximum (if fully loaded)
- Power Output
  RS485: 12 Vdc (11.14 Vdc as measured), 1.5A maximum per port

ACM

- Power Input (12 Vdc ± 20%)
  - Vreader: 12 Vdc, 12.5A maximum.
  - Vlock1: 0 - 30 Vdc, 12A maximum.
  - Vlock2: 0 - 30 Vdc, 12A maximum.
- Power Output
  - RS485 AUX: 12 Vdc (11.64 Vdc as measured), 1.5A maximum each
  - Wiegand/AUX: 12 Vdc, 800MA maximum each
  - Primary Wet Relay Out: 0 - 30 Vdc, 0.75A maximum each
  - Secondary Wet Relay Out: 0 - 30 Vdc, 0.75A maximum each
  - Secondary Dry Relay Out: 0 - 30 Vdc, 1A maximum each

NOTE

The Wiegand, RS-485, and Aux ports are power limited on the ACM.

IP-ACM

- Power Input
  - 12 or 24 Vdc 32W maximum
  - IEEE 802.3af (PoE) and 802at (PoE Plus), 25.5W max. LLDP supported for PoE Plus
- Power Output
  - RS485/Wiegand: 12 Vdc; The aggregate load of each pair of RS-485 and Wiegand connections together must not exceed 750mA. Each set of RS-485 and Wiegand can support 750mA. Maximum combined output limit for readers and locks is 20W.
  - Wet Relay: 12 or 24 Vdc (jumper selectable), 0.5A (per lock)
  - Dry Relay: 0 to 30 Vdc, 5A max. NO, 3A max. NC
## Maximum Power

The iSTAR Ultra system power ratings are listed in Table 2-6 through Table 2-8.

### Table 2-6: iSTAR Ultra GCM Rack System Ratings

<table>
<thead>
<tr>
<th>Voltage (Vdc)</th>
<th>Current (A)</th>
<th>Local External Circuit Breaker Rating (A)</th>
<th>System Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>4.49</td>
<td>-</td>
<td>(1) GCM with (2) RS-485 Loads</td>
</tr>
</tbody>
</table>

### Table 2-7: iSTAR Ultra ACM Rack Ratings

<table>
<thead>
<tr>
<th>Voltage (Vdc)</th>
<th>Current (A)</th>
<th>Local External Circuit Breaker Rating (A)</th>
<th>System Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>5</td>
<td>-</td>
<td>(1) ACM with (3) Wiegand/RS485/Aux load</td>
</tr>
<tr>
<td>12</td>
<td>8</td>
<td>10</td>
<td>(1) ACM with (5) Wiegand/RS485/Aux load</td>
</tr>
<tr>
<td>12</td>
<td>9.5</td>
<td>12</td>
<td>(1) ACM with (6) Wiegand/RS485/Aux load</td>
</tr>
<tr>
<td>12</td>
<td>11</td>
<td>15</td>
<td>(1) ACM with (7) Wiegand/RS485/Aux load</td>
</tr>
<tr>
<td>12</td>
<td>12.5</td>
<td>29</td>
<td>(1) ACM with (8) Wiegand/RS485/Aux load</td>
</tr>
</tbody>
</table>

### Lock 1 and 2 Power Ratings:

<table>
<thead>
<tr>
<th>Voltage (Vdc)</th>
<th>Current (A)</th>
<th>Local External Circuit Breaker Rating (A)</th>
<th>System Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - 30</td>
<td>4.5</td>
<td>-</td>
<td>(6) Locks</td>
</tr>
<tr>
<td>0 - 30</td>
<td>6</td>
<td>7.5</td>
<td>(8) Locks</td>
</tr>
<tr>
<td>0 - 30</td>
<td>7.5</td>
<td>10</td>
<td>(10) Locks</td>
</tr>
<tr>
<td>0 - 30</td>
<td>9</td>
<td>12</td>
<td>(12) Locks</td>
</tr>
<tr>
<td>0 - 30</td>
<td>12</td>
<td>15</td>
<td>(16) Locks</td>
</tr>
</tbody>
</table>

### Table 2-8: iSTAR Ultra Wall Mount Ratings

<table>
<thead>
<tr>
<th>Voltage (Vdc)</th>
<th>Current (A)</th>
<th>Local External Circuit Breaker Rating (A)</th>
<th>System Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>3.99</td>
<td>-</td>
<td>(1) GCM with (1) RS-485 Loads &amp; (2) ACM with no loads</td>
</tr>
<tr>
<td>12</td>
<td>4.99</td>
<td>-</td>
<td>(1) GCM with (2) RS-485 Loads &amp; (1) ACM with no loads</td>
</tr>
<tr>
<td>12</td>
<td>7.99</td>
<td>10</td>
<td>(1) GCM with (2) RS-485 Loads &amp; (1) ACM with (2) Wiegand/RS485/Aux load</td>
</tr>
<tr>
<td>12</td>
<td>9.49</td>
<td>12</td>
<td>(1) GCM with (2) RS-485 Loads &amp; (1) ACM with (3) Wiegand/RS485/Aux load</td>
</tr>
</tbody>
</table>
Additional Power Requirements

- An external over-current protection device (i.e. circuit breaker) must be installed in a secure location readily accessible to a service person.
- Circuit Breakers need to be sized so that its normal sourced current does not exceed 80% of the circuit breaker rating.
Power Requirements

FOR BURGLAR ALARM INSTALLATIONS:

- The iSTAR Ultra is not provided with backup power. An external power supply must be provided with the following characteristics:
  - UL 603 or UL 294 Listed
  - Minimum four hours of standby power

Tyco / Software House Advanced Power Supply (apS) meets these requirements. Several apS units, wired in parallel, will provide 12Vdc output at [units x 3.75A] in excess of four hours when using the supplied 17AH batteries.

- All Burglar Alarm and Intrusion Zone inputs must be supervised and have Triggers configured to Alarm upon Tamper.
- At least one RM2L-4000 reader must be in each area/partition for signal acknowledgement.

There are multiple power inputs to the unit. To completely de-energise the unit, disconnect ALL power sources.

NOTE

For UL Listed products, a UL 603 or UL 294 listed power supply must be used.

- This device must be suitably rated for the installation; see electrical ratings guidance.
- The conductor size for the inputs must be selected based on the rating of their corresponding over-current device and in accordance with local and national regulations.

Battery

The GCM contains a 3V CR2032 lithium coin cell battery that is used to retain the real-time clock.

The battery should be replaced no longer than every 5 years, and the replacement battery must be UL approved. See Chapter 8, “GCM Battery Replacement” for more information.

Heat Dissipation

Table 2-9 on page 2-10 lists the heat dissipation for the Rack and Wall mount configurations.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Power Dissipated in Enclosure</th>
<th>BTU/hour</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rack GCM</td>
<td>17.88 Watts</td>
<td>61.0</td>
</tr>
<tr>
<td>Rack ACM</td>
<td>6 Watts</td>
<td>20.5</td>
</tr>
</tbody>
</table>
Table 2-9: Maximum Heat Dissipation, continued

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Power Dissipated in Enclosure</th>
<th>BTU/hour</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wall GCM and (1) ACM</td>
<td>23.88 Watts</td>
<td>81.5</td>
</tr>
<tr>
<td>Wall GCM and (2) ACMs</td>
<td>29.88 Watts</td>
<td>102.0</td>
</tr>
</tbody>
</table>

**ELECTROSTATIC SENSITIVE DEVICES:** Observe precautions for handling.

- Before handling any internal components, discharge static electricity by touching and holding a grounded surface for three seconds.
- Wear a grounding wrist strap and stand on a grounded static mat.
- Reduce movement during installation to reduce static buildup.
- Make sure work area is safeguarded.
- Transport components in static-shielded containers.
  
  Note: The outside of the ESD bags are not ESD protective.
- Verify that all components, materials, and the installer are referenced to a common ground.
Other Interactions with the Power System

All of iSTAR Ultras other interactions with the power system are essentially informational in nature and do not directly affect iSTAR Ultra behavior with regard to power loss, power saving and backup. Most of the other interactions appear in the host as configurable inputs. This allows user to both monitor them and allow them to trigger other actions.

For example, the user could configure the AC / Main Fail and Low Battery inputs to both trigger a configuration backup. It does not affect how iSTAR Ultra treats power loss. iSTAR Ultra still watches for input voltage to move outside of the normal operating voltage range, and at that time will perform a full state and configuration backup.

AC / Main Fail Input

- Indicates whether the external power source has reported loss of its main power.
- Shares connector and Ground pin with Low Battery.
- Normally closed dry relay contacts are required. This signal is normally wired to the energized NO output on the apS.
- Configurable on host as an unsupervised input.

Low Battery Input

- Indicates whether external power source, has reported its battery is low.
- Wired in from external power source.
- Shares connector and Ground pin with AC / Main Fail.
- Normally closed dry relay contacts are required.
- Configurable on host as unsupervised input.
Reader Power Requirements

This section lists the power requirements for the readers.

Software House Readers

Table 2-10 on page 2-13 shows power requirements for Software House readers.

<table>
<thead>
<tr>
<th>Reader</th>
<th>Model Numbers</th>
<th>Current Draw at 12 VDC</th>
</tr>
</thead>
<tbody>
<tr>
<td>RM with Multi-Technology Reader</td>
<td>RM1-4000, RM2-4000, RM1-SE, RM2-SE</td>
<td>300 mA max</td>
</tr>
<tr>
<td>RM with Multi-Technology Reader and LCD</td>
<td>RM2L-4000, RM2L-SE</td>
<td>300 mA max</td>
</tr>
<tr>
<td>RM with mag stripe</td>
<td>RM1-MP, RM2-MP</td>
<td>80 mA max</td>
</tr>
<tr>
<td>RM with mag stripe and LCD</td>
<td>RM2L-MP</td>
<td>180 mA max</td>
</tr>
<tr>
<td>RM with mag stripe nullion</td>
<td>RM3-MP</td>
<td>80 mA max</td>
</tr>
<tr>
<td>RM with Indala proximity</td>
<td>RM1-P, RM2-PI</td>
<td>80 mA max</td>
</tr>
<tr>
<td>RM with Indala proximity and LCD</td>
<td>RM2L-PI</td>
<td>180 mA max</td>
</tr>
<tr>
<td>RM with HID proximity</td>
<td>RM1-PH, RM2-PH</td>
<td>250 mA max</td>
</tr>
<tr>
<td>RM with HID proximity and LCD</td>
<td>RM2L-PH</td>
<td>250 mA max</td>
</tr>
<tr>
<td>RM with HID proximity nullion</td>
<td>RM3-PH</td>
<td>250 mA max</td>
</tr>
<tr>
<td>RM with Wiegand</td>
<td>RM1-W</td>
<td>80 mA max</td>
</tr>
<tr>
<td>Multi-Technology Contactless Reader</td>
<td>SWH-4000&lt;sup&gt;a&lt;/sup&gt;, SWH-4100&lt;sup&gt;a&lt;/sup&gt;, SWH-4200&lt;sup&gt;a&lt;/sup&gt;, SWH-3000&lt;sup&gt;a&lt;/sup&gt;, SWH-3100&lt;sup&gt;a&lt;/sup&gt;</td>
<td>125 mA</td>
</tr>
<tr>
<td>Multi-Format Proximity Reader</td>
<td>SWH-5000&lt;sup&gt;a&lt;/sup&gt;, SWH-5100&lt;sup&gt;a&lt;/sup&gt;</td>
<td>125 mA</td>
</tr>
<tr>
<td>Auxiliary Relay Module</td>
<td>ARM-1&lt;sup&gt;a&lt;/sup&gt;</td>
<td>20 mA (relay active)</td>
</tr>
<tr>
<td>RM with HID iClass</td>
<td>RM1-IC, RM2-IC</td>
<td>100 to 200 mA max</td>
</tr>
<tr>
<td>RM with HID iClass and LCD</td>
<td>RM2L-IC</td>
<td>100 to 200 mA max</td>
</tr>
<tr>
<td>TST-100 Touchscreen Terminal Reader</td>
<td>SWH-TST-100, SWH-TST-100-V</td>
<td>300 mA max</td>
</tr>
<tr>
<td>Cheetah SE</td>
<td>INN-SECHTA-RF, INN-SECHTA-CT, INN-SECHTA-RFO, INN-SECHTA-CFO</td>
<td>600 mA max</td>
</tr>
<tr>
<td>Cheetah</td>
<td>INN-CHTA-RF, INN-CHTA-RF-OD, INN-CHTA-CT, INN-CHTA-CT-OD, INN-CHTA-BIO, INN-CHTA-BIO-CT</td>
<td>1000 mA max</td>
</tr>
</tbody>
</table>
Third Party Readers

Table 2-11 shows power requirements for third party readers.

<table>
<thead>
<tr>
<th>Reader</th>
<th>Current Draw at 12VDC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indala Flex Pass Series</td>
<td>65 mA</td>
</tr>
<tr>
<td>Sensor Eng WR1, WR2</td>
<td>30 mA</td>
</tr>
<tr>
<td>HID MiniProx</td>
<td>60 mA</td>
</tr>
<tr>
<td>HID ProxPro</td>
<td>100 mA</td>
</tr>
<tr>
<td>HID MaxiProx</td>
<td>200 mA</td>
</tr>
<tr>
<td>HID iCLASS</td>
<td>100 mA to 200 mA</td>
</tr>
</tbody>
</table>

**NOTE**
The readers in Table 2-11 have not been evaluated by UL for use with the iSTAR Ultra.
Installation

This section assumes that the site meets the requirements.

The iSTAR Ultra does not include mounting hardware. The mounting hardware depends on the site, and must be approved by a structural engineer or other certified professional. See Table 2-5 on page 2-6 for more detail.

### ELECTROSTATIC SENSITIVE DEVICES

**Observe precautions for handling:**

- Before handling any internal components, discharge static electricity by touching and holding a grounded surface for three seconds.
- Wear a grounding wrist strap and stand on a grounded static mat.
- Reduce movement during installation to reduce static buildup.
- Make sure work area is safeguarded.
- Transport components in static-shielded containers.

Note: The outside of the ESB bags are not ESD protective.

- Verify that all components, materials, and the installer are referenced to a common ground.

### Wall Mount Installation

The most common installation is the wall mount. In this installation, the enclosure is mounted directly to a wall or uni-strut using suitable user-supplied hardware. See Table 2-5 on page 2-6 for more detail.

### Requirements

- The anchoring system must be capable of sustaining 75 lb (34 kg). This weight does not include the cables.
- The cables are protected by use of conduit, which is metal, plastic, or flexible.
- An external power supply provides 12 Vdc to run the logic of the iSTAR and the read heads. There is an option for two external power supplies to supply the locks using wet relays. The lock power supplies are rated at 0 - 30 Vdc, but are usually 12 Vdc or 24 Vdc. In some installations, the locks can be two 12 Vdc or two 24 Vdc, or either combination of both voltages.
- The enclosure has knock-outs for installing and removing wires into and out of the wall mount enclosure.
- The enclosure door supports up to four accessory boards.
- Refer to “Wall Mount Hardware” on page 2-5 for the recommended hardware to use on the different types of surfaces.

### To Wall Mount the Controller:

1. Carefully unpack the components. Software House recommends removing the GCM and the ACM(s) from the enclosure before mounting. Use ESD procedures while handling the boards.
2. Open the enclosure door and disconnect the grounding wire on the door.

3. Carefully lift the door off the hinges, and place it on a padded surface.

4. Verify that the upper mounting screws (or equivalent) are in place on the mounting site for the keyhole locations.

**NOTE** See Figure 2-1 on page 2-16 for the location of the keyhole slots, screws, and knockouts.

Figure 2-1: iSTAR Ultra Controller with Door Removed (Two ACMs Mounted)

5. Align the mounting keyhole slots at the upper back of the enclosure with the two upper mounting screws, and lower the enclosure into position.

6. Install the three lower mounting screws and the remaining top mounting screw in between the two keyhole mounts.

7. Attach the conduit couplings to the knockout openings as needed to comply with local code requirements.

8. Reattach the grounding wire between the door and the enclosure.
9. Secure the power inputs with zip-ties to maintain minimum safe distance for electrical safety. Install in accordance with local and national regulations. Non-limited power supply lines must maintain a minimum of 1/2” spacing from limited power supply lines and other signaling lines.

10. When routing signal cables from the ACM to accessory boards on the door, ensure that the cables are not pinched by the door and cables are routed in accordance with NEC Codes or the applicable Local codes.

Rack Mount Installation

The GCM and ACMs are mounted separately in standard 19-inch racks. The cables will be inside the cable management system of the rack. The components must remain secure, be clearly labeled, and be easily accessible when using the correct tools.

NOTE Use a service loop when connecting the cables.

Rack Mount Considerations

Be aware of the following considerations when mounting the iSTAR Ultra as a Rack Mount.

- Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Verify that 0°C to 50°C is maintained.

- Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised. Verify that 0°C to 50°C is maintained.

- Reliable Grounding - Reliable earth ground of rack-mounted equipment should be maintained.

NOTE The iSTAR Ultra must be installed in a UL-listed rack mount.

To Perform a Rack Mount Installation:

1. Pick a location for the rack, while observing the Rack Mount Considerations on page 2-17.
2. Disconnect the grounding wire on the controller.
3. Mount the unit with either 10/32 or 12/24 hardware.
4. Connect Ethernet, as required, to the Ethernet port(s).
5. Reconnect the grounding wire to the controller.
6. Secure the power inputs with zip-ties to maintain minimum safe distance for electrical safety. Install in accordance with local and national regulations.
IP-ACM Installation

The IP-ACM is mounted separately from the Ultra GCM in a plastic or metal enclosure. The following sections describe the enclosures and their installation with the IP-ACM board.

**NOTE** See the *IP-ACM Ethernet Door Module Quick Start Guide* for power and cabling requirements.

Plastic Enclosure

**Figure 2-2:** Plastic Enclosure for the IP-ACM

![Plastic Enclosure Diagram]

**Table 2-12:** IP-ACM and Reader Plastic Enclosure Dimensions

<table>
<thead>
<tr>
<th>Item</th>
<th>Dimension</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weight</td>
<td>2.2lb (1kg)</td>
</tr>
<tr>
<td>Height</td>
<td>12.1in (307mm)</td>
</tr>
<tr>
<td>Width</td>
<td>7.2in (183mm)</td>
</tr>
<tr>
<td>Depth</td>
<td>2.46in (62.4mm)</td>
</tr>
</tbody>
</table>

**Requirements**

- The anchoring system must be capable of sustaining 25lb (11.4kg). This weight does not include the cables.
- The cables are protected by use of conduit, which is metal, plastic, or flexible cable grip strain relief.
- 12VDC or 24VDC local power or Power over Ethernet (PoE or PoE+).
For a UL installation the power must be approved to UL-294 and/or UL-603.

**To Install the IP-ACM and Plastic Enclosure:**

1. Remove the screws using the Software House security screwdriver and lift the enclosure cover off of the plastic IP-ACM enclosure.

2. Secure the IP-ACM enclosure to the selected wall or support surface using the holes provided in the enclosure’s molded base. Refer to Figure 2-2 on page 2-18 for dimensions and hole pitch for mounting.

   **NOTE**

   It is essential to use all five securing screws when mounting the plastic enclosure. Ensure that the mounting hole at 5.16 inches across and 1.03 inches up is used, see Figure 2-2 on page 2-18, as this is required for the “whole unit off the wall” anti-tamper feature to be operational.

3. Secure the IP-ACM Ethernet door module to the right of the enclosure.

4. Fit and connect all customer cables.

5. Secure the cover with two tamper-proof screws using the Software House security screwdriver (Part Number: 132-183).

**Metal Enclosure**

![Metal IP-ACM Enclosure Diagram]
To Install the IP-ACM and Metal Enclosure:

1. Open the door of the IP-ACM metal enclosure.
2. Secure the enclosure to selected wall or support surface using holes provided in the enclosure’s base. Refer to Table 2-3 for dimensions and hole pitch for mounting.
3. Fit and connect all customer cables. See the *IP-ACM Ethernet Door Module Quick Start Guide* regarding power and wiring requirements.
4. Close and secure the metal enclosure cover.

### Table 2-13: IP-ACM Metal Enclosure Dimensions

<table>
<thead>
<tr>
<th>Item</th>
<th>Dimension</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weight</td>
<td>~2.6lb (~1.2kg)</td>
</tr>
<tr>
<td>Height</td>
<td>8.25in (209.6mm)</td>
</tr>
<tr>
<td>Width</td>
<td>7.34in (186.5mm)</td>
</tr>
<tr>
<td>Depth</td>
<td>3.46in (87.8mm)</td>
</tr>
</tbody>
</table>
iSTAR Ultra Network Topology

This chapter provides an overview of iSTAR Ultra topology and configuration options.

iSTAR Ultra configurations vary according to site requirements. You must understand iSTAR Ultra topology and customer requirements to ensure the correct layout, connections, and configuration of iSTAR Ultra components.

In This Chapter:

- iSTAR Ultra Network Topology ................................................................. 3-2
- LAN and WAN Configurations ................................................................. 3-2
- Gateways and Firewalls ........................................................................... 3-2
- IP Management Tools ............................................................................... 3-4
- Fully Qualified Domain Names ................................................................. 3-4
- Cluster Configuration ................................................................................ 3-5
- Master Configurations ............................................................................... 3-7
- Communication Paths ............................................................................... 3-8
- Maintaining Cluster Communication ......................................................... 3-10
- Adding Controllers to the Cluster ............................................................ 3-11
- Configuring Communication Paths ............................................................ 3-12
iSTAR Ultra Network Topology

iSTAR Ultra supports communications over 10/100/1000 Mbps Ethernet networks using TCP/IP.

LAN and WAN Configurations

The TCP/IP protocol transfers data across a number of networks. Because iSTAR Ultra controllers use the TCP/IP protocol for network communications, they can communicate with each other within a LAN or across a WAN, as shown in Figure 3-1.

![Figure 3-1: Sample iSTAR Ultra Network](image)

Gateways and Firewalls

iSTAR Ultra configurations provide access to remote C•CURE systems across firewalls and Network Address Translators. This is because the master controller automatically accepts a translated IP address if one is assigned from a remote host, or from an attached Network Address Translator.

Generally, the TCP/IP ports, listed in Table 3-1, must be open through a firewall.


<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>Protocol</th>
<th>Destination System</th>
</tr>
</thead>
<tbody>
<tr>
<td>68</td>
<td>DHCP client. A function of Linux and networking.</td>
<td>UDP</td>
<td>Network</td>
</tr>
<tr>
<td>80</td>
<td>Redirect to HTTPS (port 443)</td>
<td>TCP</td>
<td>Web</td>
</tr>
<tr>
<td>443</td>
<td>Secure web connection used for diagnostic website. Port is closed in FIPS mode. Only necessary for diagnostics.</td>
<td>TCP</td>
<td>Web</td>
</tr>
<tr>
<td>1999</td>
<td>iSTAR master port for incoming non-encrypted member connections, plus incoming ICU requests.</td>
<td>TCP</td>
<td>Master</td>
</tr>
</tbody>
</table>

Table 3-1: TCP Ports
Local Address Management

Although it is not required, System Managers who want to maintain local address management can configure iSTAR Ultra with locked IP addresses. Locked IP addresses retain the iSTAR Ultra address that is specified locally or by a local Dynamic Host Configuration Protocol (DHCP) server. When IP addresses are locked, iSTAR Ultra communicates across gateways using only the IP address that you configure: translated addresses are not accepted.

Before you lock an IP address, ensure that it is reliable (not subject to translation) and can be reached from the local network.

Example:

The example displayed in Figure 3-2 on page 3-4 shows a locked iSTAR Ultra configuration. To configure this cluster, the System Manager is in the branch office:

- Use PING to check communication to the exposed (translated) address from the Corporate Office.
- Use the ICU to configure the master controller and lock the exposed C•CURE address.
- Use the ICU to configure the member controllers and lock the local subnet addresses.

### Table 3-1: TCP Ports, continued

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>Protocol</th>
<th>Destination System</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008</td>
<td>iWATCH connection port. Not open by default, but can be enabled via web page diagnostic settings.</td>
<td>TCP</td>
<td>iWATCH</td>
</tr>
<tr>
<td>28004</td>
<td>Used to accept signed certification for encryption.</td>
<td>TCP</td>
<td>Encryption</td>
</tr>
<tr>
<td>28009</td>
<td>iSTAR Ultra incoming encrypted member connection port.</td>
<td>TCP</td>
<td>iSTAR Member</td>
</tr>
<tr>
<td>255</td>
<td>ICMP broadcast.</td>
<td>raw</td>
<td>Host</td>
</tr>
<tr>
<td>2900</td>
<td>Communication to the IP-ACM</td>
<td>TCP</td>
<td>Communication</td>
</tr>
<tr>
<td>30000-60000</td>
<td>This port number is generated during bootup and is the stunnel communication for C•CURE [port 28010 (stunnel)].</td>
<td>TCP</td>
<td>Server</td>
</tr>
<tr>
<td>2001</td>
<td>iSTAR port for ICU broadcasts.</td>
<td>UDP</td>
<td>ICU</td>
</tr>
</tbody>
</table>
IP Management Tools

iSTAR Ultra controllers can be configured to accept IP addresses and device names from one of the following:

- Local DHCP
- Windows Internet Naming Service (WINS)
- Domain Name System (DNS) servers

DHCP servers simplify IP management by automatically distributing an IP address to clients when they broadcast to the DHCP server. DHCP servers typically manage a range of IP addresses. WINS and DNS servers complement DHCP address assignment by providing name-to-IP address mapping.

Fully Qualified Domain Names

Configurations where IP addresses are subject to change (leased DHCP addresses, for example) can connect to the C•CURE system using the fully qualified domain name (FQDN). The configuration must contain a WINS or DNS server, for name/address resolution.

If you are not using DHCP, use the ICU to configure FQDNs. If you specify the FQDN name for a C•CURE host, you must also use the ICU to supply the IP addresses of the DNS or WINS server.
Cluster Configuration

iSTAR Ultra controllers are organized for network communications into user-defined, logical groups called clusters.

iSTAR controllers must belong to a user-defined group called a cluster. It is possible to have from one to sixteen controllers in a cluster. One of the controllers is designated as the Master and the Master acts as a relay agent to the Host for all of the controllers in the cluster.

There are two different types of clusters based on whether or not the data transfers are encrypted or not. Encrypted clusters employ the Advanced Encryption Standard (AES) utilizing 256 bits FIPS-197.

Encrypted clusters can contain the following controllers:
- iSTAR Ultra (If running default Encrypted mode set by S1-1=true)
- iSTAR Ultra SE (If Ultra mode (S1-4 = False) and Encrypted mode (S1-1=True)
- iSTAR Ultra LT (Encryption mode S1-1 = ON)
- iSTAR Edge (1, 2, or 4 reader models)
- iSTAR eX (4 or 8 reader models)

Non-Encrypted clusters can contain the following controllers:
- iSTAR Ultra (If not running Encrypted mode set by S1-1=false)
- iSTAR Ultra SE (Pro Mode) (If not running Encrypted mode set by S1-1 = False)
- iSTAR Ultra SE (Ultra Mode) (If not running Encrypted mode set by S1-1 = False)
- iSTAR Ultra LT (Encryption mode S1-1 = OFF)
- iSTAR Classic
- iSTAR Pro

Master and Member Configuration

Each cluster has one controller that serves as the master; any other controller in the cluster is a cluster member. The master manages all communications between the cluster and a C•CURE host computer.

Cluster members can communicate with each other via the master, over an Ethernet network. Cluster members cannot communicate with each other directly. In Figure 3-3 on page 3-6, the diagram on the left shows how cluster member A communicates with the host via the master. The diagram on the right shows how cluster member A communicates with cluster member B via the master.
Figure 3-3: Cluster Member Communications

Cluster Member A to Host

Cluster Member A to Member B
Master Configurations

To ensure continuous connection, the iSTAR Ultra cluster can communicate with C•CURE using a primary and optional communication secondary path, configured on a single master controller.

Figure 3-4 shows primary and secondary communications using a single master.

![Single Master Configuration Diagram]

Single Master Configurations

Table 3-2 on page 3-7 shows the configuration options for clusters that provide communication using a single master controller.

<table>
<thead>
<tr>
<th>Primary</th>
<th>Secondary</th>
</tr>
</thead>
<tbody>
<tr>
<td>C•CURE 9000</td>
<td>None</td>
</tr>
<tr>
<td>Network</td>
<td>Network</td>
</tr>
</tbody>
</table>
Communication Paths

The master controller connects to the host over a primary communication path. An optional secondary path can be configured to ensure continuous host communication.

Primary Communications Path

The primary path is the first communication path that clusters use to establish communications with the host. The master is the only controller in a cluster that passes messages between the host and cluster members. Cluster members do not communicate with the host directly; they communicate with the host through the master. Connections are established in the following bottom-to-top order:

- Cluster members are responsible for establishing connections with the master.
- The master is responsible for establishing a connection with the host.

The Connection type is how the master connects to the host. Allowable types are network. Cluster members are connected to the master only via a network connection.

Figure 3-5 shows the primary path for cluster member A. In this case, the master/host connection type is network.
Secondary Communications Path

A secondary path is the host communications path that is used by a cluster if a communications failure occurs on the primary path.

Figure 3-6 on page 3-9 shows an example of a secondary path on a single master configuration using two network connections.

Figure 3-6: The Secondary Path
Maintaining Cluster Communication

Maintaining cluster communications involves establishing and maintaining connections via the primary communication path or (optional) secondary communication path. If the primary connection is lost, the secondary communication path is used to re-establish cluster communications.

Single Master Configurations

If a configuration with a single master loses its connection with the host, as shown in Figure 3-7 on page 3-10:

- Cluster members continue to communicate with the master.
- The master continues to pass cluster members’ messages to the host.
- The master uses the secondary path to communicate with the host.

Example:

If the secondary path is an alternate network connection between the master and host, the master uses the alternate network to communicate with the host.

Figure 3-7: Communication Failure with Single Master Configuration
Adding Controllers to the Cluster

Follow these guidelines when adding controllers to a cluster.

- A controller must be assigned to a cluster before the controller can communicate with the host, master, or other controllers.
  
  Use the Cluster window in the C•CURE System Administration Application to add controllers to a cluster. When added to a cluster, the controller becomes a cluster member.

- One controller can comprise a cluster. You can configure a controller as its own cluster by configuring a cluster that includes only the controller and specifying that controller as the master.

- A cluster member communicates with other cluster members through the master.

- A cluster communicates with the C•CURE host via the cluster’s primary or secondary path.

- A cluster communicates with other clusters and with apC panels via the C•CURE host.

- A cluster can communicate with the C•CURE server across a WAN. You can configure clusters that are spread across WAN topologies.
Configuring Communication Paths

This section includes guidelines and procedures for configuring primary and secondary communication paths.

Planning Primary Communications

Configuring a primary communication path involves:

- Specifying a master for the cluster
- Specifying a communication methods between the master and the C•CURE host.
- Specifying connection parameters for establishing and maintaining the primary path.

Primary Communication Guidelines

Follow these guidelines when configuring a primary path:

- Every cluster must have a master.
- Only one master is allowed per cluster.
- If a cluster contains only one controller, that controller is the master.
- Any controller in a cluster can be designated as the master.

Planning Secondary Communications

Configuring a secondary communications path involves:

- Specifying the same controller responsible for secondary communications with the C•CURE host via another NIC when a communications failure occurs on the primary path.
- Specifying the connection type.
General Control Module (GCM)

This chapter describes the GCM switches, buttons, jumpers, LEDs, and the LCD.

In This Chapter:

- General Control Module ................................................................. 4-2
- Switches ................................................................................................. 4-3
  - SW7 - Soft Reset (Reboot) ................................................................. 4-3
  - SW2 - Hard Processor Reset ............................................................. 4-3
  - SW3 Rotary Switch ........................................................................... 4-4
  - S1-1 (Encryption) ................................................................................ 4-4
  - S1-2 - CPNI .......................................................................................... 4-5
  - S1-3 ..................................................................................................... 4-5
  - S1-4 ..................................................................................................... 4-5
  - RS - 485 Terminators - SW5 and SW6 .............................................. 4-5
- Ports .................................................................................................... 4-8
  - RS-485 1 and 2 (J12 and J13) ............................................................ 4-8
  - USB Micro A-B - J7 ............................................................................ 4-8
  - RS-232 Diagnostic Port (P4) .............................................................. 4-8
  - COMM Board Connector - J15 .......................................................... 4-8
- Visual Indicators ................................................................................. 4-8
  - Power - DS1 and DS2 ........................................................................ 4-8
  - LCD .................................................................................................. 4-8
  - LEDs ................................................................................................ 4-9
Network Connections

Connect a shielded CAT-5E, or better, RJ45 cable to either J5 or J6 (or both for redundancy).
- J5 Ethernet up to 1 Gbps (10, 100, 1000)
- J6 Ethernet up to 1 Gbps (10, 100, 1000)

There are built in LEDs in the connectors that indicate the Ethernet Link and Receive Data signals.

Switches

SW7 - Soft Reset (Reboot)

The SW7 push button saves all data in non-volatile memory and then reboots the unit. It may take several minutes for the formatting and saving of the data. The iSTAR Ultra is fully capable of operating without contact with the Host after the reboot.

SW7 should be used to **Reset to Factory Default** by changing the Rotary Switch (SW3) to ‘D’ and pressing SW7. See Table 4-1 on page 4-4 for Rotary Switch descriptions.

---

To Clear Memory and Reboot the Unit

1. Set rotary SW3 to D.
2. Press and release switch SW7.
   - Instructions appear on the LCD in approximately ten seconds.
3. Follow the instructions.
4. Set rotary SW3 back to 0 or F.
5. Press and release SW7. The controller restarts and the LCD is blank
6. Use the ICU to configure the controller.

SW2 - Hard Processor Reset

SW2 Hard Processor Reset should only be used by a Certified Integrator.

- Press and release SW2.
  - The panel reboots immediately with no database backup.
  - During reboot, the panel restores database from the SD card. This occurs only if there has already been a previous backup.
SW3 Rotary Switch

SW3 is an onboard 16-position rotary switch. Most of the positions are used to control LCD diagnostics. Table 4-1 on page 4-4 provides descriptions of the iSTAR Ultra rotary switch functions.

<table>
<thead>
<tr>
<th>Position</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>ICU Block Off (Read/Write/Update) Display General Messages</td>
</tr>
<tr>
<td>1</td>
<td>Display card data from last card read, 7 second LCD display (slow mode)</td>
</tr>
<tr>
<td>2</td>
<td>Display card data from last card read, 2 second LCD display (fast mode)</td>
</tr>
<tr>
<td>3</td>
<td>Display supervised input changes, 2 second LCD display (slow mode)</td>
</tr>
<tr>
<td>4</td>
<td>Display supervised input changes, 1 second LCD display (fast mode)</td>
</tr>
<tr>
<td>5</td>
<td>Display manual output changes (include readers and R/8 boards), 2 second LCD display (slow mode)</td>
</tr>
<tr>
<td>6</td>
<td>Display manual output changes (include readers and R/8 boards), 1 second LCD display (fast mode)</td>
</tr>
<tr>
<td>7</td>
<td>Not used</td>
</tr>
<tr>
<td>8</td>
<td>Hardware Test (Onboard Ethernet 1 and 2, USB ports)</td>
</tr>
<tr>
<td></td>
<td>NOTES:</td>
</tr>
<tr>
<td></td>
<td>• Ethernet tests require a good IP (Static or DHCP, and a good network link) and at least one ICU running on the same subnet.</td>
</tr>
<tr>
<td></td>
<td>• USB port tests require the thumb drive to be formatted to a FAT32 file format.</td>
</tr>
<tr>
<td>9</td>
<td>Not used</td>
</tr>
<tr>
<td>A</td>
<td>Not used</td>
</tr>
<tr>
<td>B</td>
<td>MFG-ATE (Automated Test Equipment) (Software House only)</td>
</tr>
<tr>
<td>C</td>
<td>Disable watchdog (Software House only)</td>
</tr>
<tr>
<td>D</td>
<td>Restore Factory Default. Erase data backups and communication parameters from flash. (Press GCM reset, wait for LCD instructions, set rotary switch back to 0 or F, press reset again.)</td>
</tr>
<tr>
<td>E</td>
<td>Boot to previous image (Software House only)</td>
</tr>
<tr>
<td>F</td>
<td>ICU Block On (Read only) - Display General Messages</td>
</tr>
</tbody>
</table>

S1-1 (Encryption)

The Encryption switch enables FIPS 197 AES 256-bit encryption. The switch setting must match the software configuration of the cluster and the controller.

If encrypted, the iSTAR Ultra controller can cluster with:

- iSTAR Ultra LT with encryption set to ON
- Other iSTAR Ultras and iSTAR Ultra SEs (Ultra Mode) with the Encryption Switch set to ON
- iSTAR Edge
- iSTAR eX
If non-encrypted, the iSTAR Ultra controller can cluster with:

- iSTAR Ultra LT with the Encryption Switch set to OFF
- Other iSTAR Ultras and Ultra SE (Ultra Mode) with the Encryption Switch set to OFF
- iSTAR Pros

**NOTE**

iSTAR Encryption Mode is required to implement FIPS 140-2 (future feature). FIPS 140-2 is not evaluated by UL.

**S1-2 - CPNI**

When this switch is set to ON, the iSTAR Ultra runs in CPNI (Centre for the Protection of National Infrastructure) mode and all database and transactions are stored in RAM. The database and transactions are not backed up on the SD.

The default setting is OFF.

**S1-3**

For future use.

**S1-4**

Not used in the iSTAR Ultra Controller.

**RS - 485 Terminators - SW5 and SW6**

These switches provide termination at the end of the two RS-485 ports.

**LCD Contrast Potentiometer - RV1**

Used to adjust the contrast of the LCD. Requires a 2 mm screwdriver.

**AC Fail - Low Battery - J2**

Figure 4-1 on page 4-6 shows AC Fail and Low Battery wiring. They are NC (Normally Closed) connections, and share a common ground pin.
Switches

**AC Fail Input**
- Indicates whether the external power source has reported loss of its main power.
- Shares the connector and Ground pin with Low Battery.
- Normally closed dry relay contacts are required. This signal is normally wired to the energized NO (Normally Open) output on the apS.
- Configurable on the host as an unsupervised input.

**Low Battery Input**
- Indicates whether the external power source has reported its battery as low.
- Wired in from external power source.
- Shares the connector and Ground pin with AC Fail.
- Normally closed dry relay contacts are required.
- Configured on the host as unsupervised input.

**Tamper - J1**

Figure 4-2 on page 4-7 shows Tamper - J1 NC (Normally Closed). It is connected to the Tamper switch on the enclosure. If there is no standard enclosure, be sure that there is a jumper across the two pins.

In a standard wall enclosure, the GCM and ACMs have a Tamper Input. The Tamper switch can be only be connected to the GCM. Remove the two configurations in C•CURE 9000 for the ACMs. Alternatively, short the two pins on the unused ACM Tamper Inputs, since it is an NC connection.
The tamper switch controls many LEDs, to preserve power and also turns off the super bright LED when the door is open. When the door is opened the small power LEDs are on. The LCD is also off when the door is closed.

**NOTE**
- The Tamper, Low Battery, and AC power fail inputs must be enabled and connected to report for compliance with UL requirements.
- Shielded cable must be used for AC Fail and Low Battery Input connections.

**GCM Power - J4**
12 Vdc @ 4.5 Amps max (Note: pin 1 on the left is +12 Vdc, pin 2 is GND.)

Once the Ultra GCM is powered on, you must follow the shutdown procedures described in “Proper Shutdown Sequence” on page 7-8 to shutdown the Ultra GCM.

**J14 SD Card**
Located on the back of the GCM to the left of the SOM, near the Hard Reset switch. This non-volatile memory is where backups are stored.
Ports

RS-485 1 and 2 (J12 and J13)
Used for Aperio Hubs and Schlage PIMs.
Each Port can support up to fifteen Hubs. Each Hub can support either one Reader or eight Readers.

USB Type A - J8 and J9
Four type A ports used to communicate with ACMs and to import encryption keys from a Certificate Authority using a thumb flash drive.

USB Micro A-B - J7
Not currently used. Future option.

RS-232 Diagnostic Port (P4)
Software House Tech Support and Engineering use for troubleshooting.

COMM Board Connector - J15
Not supported. Future option.

Visual Indicators

Power - DS1 and DS2
Indicate that power is supplied to the unit.

LCD
The LCD displays status and diagnostics messages.
- Diagnostics are controlled by the rotary switch, SW3. See “SW3 Rotary Switch” on page 4-4.
- Contrast controlled by potentiometer, RV1.
- The back light is on when door is open, off when door is closed.

Common LCD displays are:
- Firmware version and Date/Time loaded.
- Indication of whether a CFG Restore occurred.
- FIPS self test.
- Master Connected or Host Connected
**Visual Indicators**

- IP address of Host or Master
- Name of the iSTAR Ultra and MAC address of the NIC
- IP address of iSTAR Ultra
- Voltage
- Member or Master with Date and Time
- Configured Power and Measured Power
- Cluster Connected or Fragmented
- Indication of whether a database has been restored
- Indication of whether the iSTAR is encrypted
- Results of diagnostics

**LEDs**

The super-bright white Power LED is illuminated when the enclosure door is closed. For example, when the tamper switch closes. The power LED extinguishes at ~8V.

The relay activation LEDs remain active regardless of the state of the enclosure door.

The remainder of the indicators are illuminated when the enclosure door is opened. The LCD back light and all LEDs other than the power LED and the relay LEDs are under firmware control and are extinguished when the unit detects input power failure and enters sleep mode to minimize power consumption.

Users have the ability, via the host, to configure LCD back light and LEDs other than Power LED, the Bright White external view Power LED, and the relay activation LEDs to be always off, regardless of tamper state.

Table 4-2 on page 4-9 provides descriptions of the GCM LEDs.

<table>
<thead>
<tr>
<th>LED</th>
<th>Function</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS2</td>
<td>Main Power - Internal View</td>
<td>Always on if Voltage in &gt; 8V</td>
</tr>
<tr>
<td>DS1</td>
<td>Main Power - External View</td>
<td>Super bright White LED, visible from outside of the enclosure when the door is closed. Off when the door is open.</td>
</tr>
<tr>
<td>DS6</td>
<td>RS-485 Port 1 Enabled</td>
<td>Used for Aperio Hubs and Schlage PIMs.</td>
</tr>
<tr>
<td>DS3</td>
<td>RS-485 Port 2 Enabled</td>
<td>Used for Aperio Hubs and Schlage PIMs.</td>
</tr>
<tr>
<td>DS9</td>
<td>COMM board Enabled</td>
<td>Not currently supported.</td>
</tr>
<tr>
<td>N/A</td>
<td>Ethernet Carrier</td>
<td>LEDs built in to J5 and J6</td>
</tr>
<tr>
<td>N/A</td>
<td>Ethernet Activity</td>
<td>LEDs built in to J5 and J6</td>
</tr>
<tr>
<td>DS4</td>
<td>RS-485-1 Tx</td>
<td>Port 1 Transmit Data</td>
</tr>
<tr>
<td>DS5</td>
<td>RS-485-1 Rx</td>
<td>Port 1 Receive Data</td>
</tr>
<tr>
<td>DS7</td>
<td>RS-485-2 Tx</td>
<td>Port 2 Transmit Data</td>
</tr>
<tr>
<td>DS8</td>
<td>RS-485-2 Rx</td>
<td>Port 2 Receive Data</td>
</tr>
</tbody>
</table>
Access Control Module (ACM)

This chapter explains the ACM switches, buttons, jumpers, LEDs, and the LCD. The wiring of various external connections are also shown.

In This Chapter:
- **Access Control Module** ................................................................................................................................... 5-2
- **Switches and Jumpers** .................................................................................................................................... 5-5
- **SW10 - ACM MCU Reset** ............................................................................................................................ 5-5
- **RS - 485 Terminators** ................................................................................................................................... 5-6
- **Wet/ Dry Jumpers** ....................................................................................................................................... 5-6
- **Activate on FAI** ............................................................................................................................................ 5-7
- **FAI on this ACM - SW31** ............................................................................................................................ 5-7
- **Ports and Connectors** .................................................................................................................................. 5-7
- **Tamper - J22** ................................................................................................................................................. 5-7
- **Reader Power - J4** ........................................................................................................................................ 5-7
- **LOCK 1 Power - J2** ....................................................................................................................................... 5-8
- **LOCK 2 Power - J3** ....................................................................................................................................... 5-8
- **Wiegand Connections** ................................................................................................................................... 5-9
- **Inputs** ............................................................................................................................................................... 5-18
- **FAI Connections** ........................................................................................................................................ 5-24
  - **FAI Scenarios** ........................................................................................................................................... 5-24
  - **FAI Modes** .................................................................................................................................................. 5-24
- **Reader - Voltage Requirements and Distance** ........................................................................................... 5-29
- **Readers and Accessory Boards** .................................................................................................................... 5-31
Access Control Module

The ACM provides Readers, Inputs and Outputs used in access control. An iSTAR Ultra contains either one or two ACMs.

Figure 5-1 on page 5-3, Figure 5-2 on page 5-4, and Figure 5-3 on page 5-5 show ACM components, switches, and LEDs.

The ACM has eight different sections that contain all of the components needed for a Door as indicated below:

- RS-485 Port for an RM Bus or other generic RS-485 Reader.
  - Termination switch for the RS-485 Port
- Direct Connect Wiegand Port with LED and Beep drives. This is for ‘Wiegand signaling’ devices that communicate using Data 1 and Data 0.
- AUX Port to power devices such as a PIR or Motion Sensor
- FAI Activate Switch (Only for Primary Relay)
- Two Relays - One Primary and one Secondary
  - Primary Relays (Field replaceable - mounted in a socket)
    - Physically larger than the secondary relays
    - 8 per ACM
    - Can be Wet or Dry (Wet powered by either LOCK 1 or 2)
    - Can be used for FAI
    - Dry Rating 5 Amps @ 30 Vdc or 30 Vac
    - Wet Rating 0.75 Amps @ 12 Vdc
    - Form C
  - Secondary Relay (permanently soldered)
    - 8 per ACM
    - Can be Wet or Dry (Wet powered by either VLOCK 1 or 2)
    - Cannot be used by FAI
    - Dry Rating 1 Amp @ 30 Vdc or 30 Vac
    - Wet Rating 0.75 Amps @ 30 Vdc
    - Form C
- Jumper for each relay to select Wet / Dry and Wet power source

It is convenient to configure a Door with all the components together in one of these sections, but it is not a requirement. However, all door components must come from the same controller.

Figure 5-1 on page 5-3 indicates the eight basic sections of the ACM.
Figure 5-2 on page 5-4 indicates all of the components of sections 1 and 8. This pair is typical of the other 3 pairs. It also shows the Power IN ports and the FAI inputs and controls.
The various user visible controls, connectors and displays are shown. Sections 1 and 8 are indicated on most of the components. The jumper technique for wet or dry relays is shown on the left.

The power connector labeled Reader is used for the reader and the logic.

The next 2 sets are not shown, but are identical to Figure 5-3.

Figure 5-3 on page 5-5 shows the other end of the ACM and locates the USB connector, ACM Reset, and some of the LED locations. Sections 4 and 5 are shown.
**Switches and Jumpers**

**SW10 - ACM MCU Reset**

SW10 reboots both MCUs. It should only be used when it seems the ACM is not responding.

**J1 USB Type B 2.0 Port**

Communication link to the GCM.

**SW32 ACM Address Switch**

The address switch is used to identify the ACM boards connected to the GCM. Each ACM address switch must be set differently before you configure the board.
- SW32-1 = OFF ACM is unit 0 (zero)
- SW32-1 = ON ACM is unit 1
Examples:

- One ACM:
  - S2 OFF
  - S1 OFF
- Two ACMs:
  - ACM 1 - S2 OFF, S1 OFF
  - ACM 2 - S2 OFF, S1 ON

RS - 485 Terminators

SW29, SW28, SW14, SW12, SW15, SW25, SW24, SW27

These switches are set to ON by default, and are not usually changed. Setting the switch to OFF places the RS-485 port in the middle of the RS-485 chain, which allows the technician to connect two sections of a reader bus to this point. In this case, termination must be provided at the end of each of the connections, but not at the RS-485 port connector. Termination is 121 ohms across D+ and D-.

Wet/Dry Jumpers

J10, J11, J20, J23, J24, J26, J32, J36, J55, J56, J58, J85, J89, J90, J91, J92

Output Relay Wet or Dry Jumpers

The sixteen output relays can be Dry or Wet, based on the position of these jumpers.

- When Dry, the integrator must supply the external power that the relay switches. When set to Dry, use the C, NO, and NC connections.
- When Wet, the iSTAR Ultra sources the power from LOCK Power 1 or lock Power 2. When set to Wet, use the GND, NO, and NC connections.

Jumper Settings

- Wet sourced from LOCK Power 1 - Jumper 1 to 2
- Wet sourced from LOCK Power 2 - Jumper 3 to 4
- Dry use External Power - Park Jumper on 2 to 3

![Figure 5-4: Wet/Dry Relay Jumper](imageurl)
Activate on FAI

SW2, SW4, SW22, SW19, SW18, SW6, SW26, SW23

The Primary relays (large, mounted in sockets) can be configured to Activate when the FAI signal goes true.

FAI on this ACM - SW31

There are identical FAI controls on all ACMs. Set this switch to ON on the ACM that is sensing the FAI and KEY signals.

Using the FAI Pull-Up Resistor

- There must be a pull-up resistor in the circuit for the FAI to operate (regardless of whether or not the FAI switch is supervised). If you are using one ACM with an individual FAI switch, the pull-up resistor switch must be in the ON (enabled) position.
- If the FAI switch is to be wired to multiple ACM boards, it should be wired in parallel to FAI connectors on each board. If the FAI switch is supervised, or unsupervised, the pull-up resistor should be enabled (ON) on only one ACM board, and disabled (OFF) on the other ACM boards.

Enable FAI Latch - SW30

If FAI Latch is true, all relays that have Activate on FAI true, will latch and remain latched until the KEY signal resets them.

Ports and Connectors

J1 USB connection to GCM

USB cable connection to the GCM.

Tamper - J22

The NC Tamper is connected to the GCM. Do not connect it here. Place a jumper across the two pins and be sure the ACM Tamper is not configured in the C•CURE software.

NOTE

Shielded cable must be used for AC fail and Low Battery Input connections.

Reader Power - J4

This is the primary power input to the ACM. (12 Vdc @ 0.5 to 12.5 Amps maximum)

The input power is also the voltage supplied on the reader power lines.

When connecting power to J2, J3, or J4, observe polarity as indicated in Figure 5-5 on page 5-8. The plus (+) sign is located on the bottom pin.
LOCK 1 Power - J2
This is one of the power inputs to the relay outputs that are jumpered as Wet LOCK 1. It can be either 12 Vdc or 24 Vdc. It will also supplement the J4 Reader Power.

LOCK 2 Power - J3
This is one of the power inputs to the relay outputs that are jumpered as Wet LOCK 2. It can be either 12 Vdc or 24 Vdc. It will also supplement the J4 Reader Power.

FAI and Key - J84
The FAI signal is NC and the Key signal is NO. Wire the supervised resistors as shown in Figure 5-6 on page 5-8.
Wiegand Connections

J16, J25, J31, J78, J79, J80, J22, J28

Direct Wiegand signaling read head connections are shown in Figure 5-7 on page 5-9.

Figure 5-7: Wiegand Readers

The data line maximum lengths are:
- 18 AWG - 500 feet
- 20 AWG - 300 feet
- 22 or 24 AWG - 200 feet

Table 5-1 on page 5-9 describes the pinouts.

Table 5-1: Wiegand Port Pinouts

<table>
<thead>
<tr>
<th>Wiegand Port Pin Number</th>
<th>Signal/Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Power +12 Vdc</td>
</tr>
<tr>
<td>2</td>
<td>GND - PWR Return</td>
</tr>
<tr>
<td>3</td>
<td>Data 0 - Wiegand Input</td>
</tr>
<tr>
<td>4</td>
<td>Data 1 - Wiegand Input</td>
</tr>
<tr>
<td>5</td>
<td>Red LED - active low</td>
</tr>
<tr>
<td>6</td>
<td>Yellow LED - active low</td>
</tr>
<tr>
<td>7</td>
<td>Green LED - active low</td>
</tr>
<tr>
<td>8</td>
<td>Beeper - active low</td>
</tr>
</tbody>
</table>
Wiegand Port Rating

The ACM Wiegand ports and their ratings are listed in Table 5-2 on page 5-10.

<table>
<thead>
<tr>
<th>Port</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reader Output Control (Red, Green, Yellow, Beeper)</td>
<td>4.0v - 5.25v, 20mA max</td>
</tr>
<tr>
<td>Reader Input Lines (D0, D1)</td>
<td>Low level &lt; .8v</td>
</tr>
<tr>
<td>Reader Output Voltage</td>
<td>+12 Vdc</td>
</tr>
<tr>
<td>Reader Current</td>
<td>1.5 A per port</td>
</tr>
</tbody>
</table>

RS-485

The RS485 ports can be configured for either the Software House “RM” protocol or the OSDP (Open Supervised Device Protocol) v2.1.6 using secure channel (AES 128 encryption). Both protocols use half duplex RS485 communications.

It is important that the ports are wired as shown in Table 5-3 on page 5-10.

<table>
<thead>
<tr>
<th>STARx Pin</th>
<th>Signal</th>
<th>Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>+12 Vdc</td>
<td>Red</td>
</tr>
<tr>
<td>2</td>
<td>Tx+ / Rx+</td>
<td>White</td>
</tr>
<tr>
<td>3</td>
<td>Tx- / Rx-</td>
<td>Green</td>
</tr>
<tr>
<td>4</td>
<td>GND</td>
<td>Black</td>
</tr>
</tbody>
</table>

The RS-485 connectors are not keyed so it is possible to reverse the signals. If the ground connector (pin 4) is connected to +12 Vdc (pin 1), damage to the power supply or the RM could result.

RM Readers

RM Readers - I/8s - R/8s

Normal RM bus wiring is used for RM readers, I/8 boards, and R/8 boards.

Either Wiegand signaling or Magnetic signaling read heads are connected to RM-4s or RM-4Es. The RM-4 or RM-4E readers are interfaced using RS-485 1 through RS-485-8.

The reader number is determined by a hexadecimal switch on the RM, not by the Port into which the reader is plugged.

OSDP Readers

OSDP is supported in C•CURE 9000 v2.50 and higher. Support in v2.50 includes point-to-point configuration only (daisy chain is not allowed).
Figure 5-8: HID and aptiQ Reader Wiring

HID Readers

<table>
<thead>
<tr>
<th>+12VDC</th>
<th>P1-4</th>
<th>Red</th>
<th>+D+</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDX-A</td>
<td>P2-7</td>
<td>Red/Green</td>
<td>D+</td>
</tr>
<tr>
<td>HDX-B</td>
<td>P2-6</td>
<td>Tan</td>
<td>D-</td>
</tr>
<tr>
<td>Ground</td>
<td>P1-3</td>
<td>Black</td>
<td>Gnd</td>
</tr>
</tbody>
</table>

Terminal Block

aptiQ Readers

<table>
<thead>
<tr>
<th>+12VDC</th>
<th>+</th>
<th>iSTAR Ultra ACM RS485 Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>RS485-A/Y</td>
<td>D+</td>
<td></td>
</tr>
<tr>
<td>RS485-B/Z</td>
<td>D-</td>
<td></td>
</tr>
<tr>
<td>Ground</td>
<td>Gnd</td>
<td></td>
</tr>
</tbody>
</table>
**AUX Outputs**

The AUX outputs can supply 1.5A for motion sensor or PIR type devices.

The voltage is 12 Vdc.

See Figure 5-9 on page 5-12 for AUX wiring.

Wire the switch contacts of the PIR to one of the iSTAR Ultra inputs, using the proper resistor supervision.

**INPUTS**

J13, J40, J42, J17, J44, J72, J68, J69

There are 24 onboard inputs, in sets of three, available on the ACM. The Input supervision method is individually selected in the host.

Pins 2, 4, and 6 of the Input connectors are common Ground.

**Supervision Wiring**

The wiring of supervised inputs is shown in Figure 5-11 on page 5-13. Note that the resistor network is different for Normally Opened (NO) and Normally Closed (NC) switches.
This method reports:

- Short
- Alert (500 ohms)
- Normal (1K)
- Alert (2K)
- Open (>30K)
- Line Fault (Any unexpected value) Usually due to wrong value resistors or faulty resistors.

Each input can be individually configured to use any of the 22 supervision methods supported by the I8 - CSI Board.

**Relay Outputs**

The relays are Form C and can be WET or DRY. There is a jumper for each relay to set the mode.

Two Types of Relays - One Primary and one Secondary for each section

- **Primary Relay** (mounted in a socket)
  - Physically larger than the secondary relays
  - 8 per ACM
  - Can be Wet or Dry (Wet powered by either LOCK 1 or 2)
  - Can be used for FAI
  - Dry Rating 5 Amps @ 30 Vdc or 30 Vac
  - Wet Rating 0.75 Amps @ 30 Vdc
  - Form C

- **Secondary Relay** (permanently soldered)
  - Can be Wet or Dry (Wet powered by either LOCK 1 or 2)
  - Cannot be used by FAI
  - Dry Rating 1 Amp @ 30 Vdc or 30 Vac
  - Wet Rating 0.75 Amps @ 30 Vdc
• Form C

Jumper for each relay to select Wet/Dry and Wet power source

It is convenient to configure a Door with all the components together in one of these sections, but it is not a requirement. However, all door components must come from the same controller.

Use the C•CURE Administration Workstation to configure the output as Normally Energized for the Fail Safe case.

Dry Relay Wiring

Figure 5-12 on page 5-14 shows DRY relay wiring. Use NO or NC as appropriate. Notice that jumper is in the Dry position.

Wet Relay Wiring

Figure 5-13 on page 5-15 shows Wet wiring for a normal NO Latch. The iSTAR Ultra will supply 0 to 30 Vdc, depending on the input supply. Current is limited to 0.75 A. Notice that the GND is used for common, not the C pin. Notice that the jumper is in the Wet position.
Figure 5-13: Wet NO Latch

Wet Relay Wiring – NO Latch

Wet Wiring for a Magnetic Lock

Magnetic Locks are normally energized so the GND and NC pins are used in this case. Notice that jumper is in the Wet position, as shown in Figure 5-14 on page 5-15.

Figure 5-14: WET Magnetic Lock

Table 5-4 on page 5-15 summarizes the function and designation of the ACM LEDs.

<table>
<thead>
<tr>
<th>LED</th>
<th>Function</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS21</td>
<td>Main Power - Reader Power - J4</td>
<td>12 Vdc</td>
</tr>
<tr>
<td>DS52</td>
<td>Main Power - LOCK 1 - J2</td>
<td>12 or 24 Vdc</td>
</tr>
<tr>
<td>DS54</td>
<td>Main Power - LOCK 2 - J3</td>
<td>12 or 24 Vdc</td>
</tr>
</tbody>
</table>
Table 5-5: Wiegand Port LEDs (Upper Set)

<table>
<thead>
<tr>
<th>Function</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx</td>
<td>DS50</td>
</tr>
<tr>
<td></td>
<td>DS20</td>
</tr>
<tr>
<td></td>
<td>DS25</td>
</tr>
<tr>
<td></td>
<td>DS27</td>
</tr>
<tr>
<td>Tx</td>
<td>DS51</td>
</tr>
<tr>
<td></td>
<td>DS22</td>
</tr>
<tr>
<td></td>
<td>DS23</td>
</tr>
<tr>
<td></td>
<td>DS28</td>
</tr>
<tr>
<td>Power</td>
<td>DS19</td>
</tr>
<tr>
<td></td>
<td>DS17</td>
</tr>
<tr>
<td></td>
<td>DS53</td>
</tr>
<tr>
<td></td>
<td>DS12</td>
</tr>
</tbody>
</table>

Table 5-5 on page 5-16 and Table 5-6 on page 5-17 summarizes the upper and lower sets of the Wiegand port LEDs for power, Rx, and Tx.
Table 5-6: Wiegand Port LEDs (Lower Set)

<table>
<thead>
<tr>
<th>Power</th>
<th>DS49</th>
<th>DS48</th>
<th>DS47</th>
<th>DS55</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tx</td>
<td>DS44</td>
<td>DS41</td>
<td>DS26</td>
<td>DS46</td>
</tr>
<tr>
<td>Rx</td>
<td>DS43</td>
<td>DS42</td>
<td>DS24</td>
<td>DS45</td>
</tr>
</tbody>
</table>

Table 5-7: ACM RS-485 LED Functions

<table>
<thead>
<tr>
<th>RS-485</th>
<th>Connector</th>
<th>LED - Tx</th>
<th>LED - Rx</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>J96</td>
<td>DS28</td>
<td>DS27</td>
</tr>
<tr>
<td>2</td>
<td>J83</td>
<td>DS23</td>
<td>DS25</td>
</tr>
<tr>
<td>3</td>
<td>J82</td>
<td>DS22</td>
<td>DS20</td>
</tr>
<tr>
<td>4</td>
<td>J101</td>
<td>DS51</td>
<td>DS50</td>
</tr>
<tr>
<td>5</td>
<td>J97</td>
<td>DS44</td>
<td>DS43</td>
</tr>
<tr>
<td>6</td>
<td>J98</td>
<td>DS41</td>
<td>DS42</td>
</tr>
<tr>
<td>7</td>
<td>J99</td>
<td>DS26</td>
<td>DS24</td>
</tr>
<tr>
<td>8</td>
<td>J100</td>
<td>DS46</td>
<td>DS45</td>
</tr>
</tbody>
</table>

Table 5-7 on page 5-17 summarizes the RS-485 LEDs for Power, Tx, and Rx.
There are 24 onboard inputs, in sets of three, available on the ACM.
Pins 2, 4, and 6 of the Input connectors are common Ground.

The type of supervision is configured in the host. Supervision Modes are listed in Table 5-8 on page 5-18.

Values for resistor configurations are described in terms of NC (Normally Closed) or NO (Normally Open), resistor placement, and supervising resistor value.

Resistor placement refers to how many resistors are used, and where they are placed in relation to the switch. Settings are “Non-supervised”, “Single”, “Dual”, or “Double”.

- Unsupervised - the user wires no external resistors.
- Single - the user wires a single resistor.
- Dual - the traditional Software House method of supervision. Both NO and NC are handled by one input.
- Double - the user wires two resistors, one in parallel and one in series with the switch.

Resistor values are labeled as 1k/5k/10k (in Ohms). In the Double cases, both resistors have the same value.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1K Dual NO/NC</td>
<td>Wire with Parallel/Serial for NO and Serial/Parallel for NC.</td>
</tr>
<tr>
<td></td>
<td>- Normal = 1K</td>
</tr>
<tr>
<td></td>
<td>- NO Alert = 0.5K</td>
</tr>
<tr>
<td></td>
<td>- NC Alert = 2K</td>
</tr>
<tr>
<td></td>
<td>NOTE: This is the default setting for the C•CURE 9000.</td>
</tr>
<tr>
<td>1K Single Series NC</td>
<td>Series Resister</td>
</tr>
<tr>
<td></td>
<td>- Normal = 1K</td>
</tr>
<tr>
<td></td>
<td>- Alert = open (Ω)</td>
</tr>
</tbody>
</table>
### Table 5-8: Supervision Modes, continued

<table>
<thead>
<tr>
<th>Mode</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1K Single Parallel NO</td>
<td>Parallel Resistor</td>
</tr>
<tr>
<td></td>
<td>■ Normal = 1K</td>
</tr>
<tr>
<td></td>
<td>■ Alert = short (0 Ω)</td>
</tr>
<tr>
<td>5K Dual NO/NC</td>
<td>Wire with Parallel/Serial for NO and Serial/Parallel for NC.</td>
</tr>
<tr>
<td></td>
<td>■ Normal = 5K</td>
</tr>
<tr>
<td></td>
<td>■ NO Alert = 2.5K</td>
</tr>
<tr>
<td></td>
<td>■ NC Alert = 10K</td>
</tr>
<tr>
<td>5K Single Series NC</td>
<td>Series Resistor</td>
</tr>
<tr>
<td></td>
<td>■ Normal = 5K</td>
</tr>
<tr>
<td></td>
<td>■ Alert = open (= Ω)</td>
</tr>
<tr>
<td>5K Single Parallel NO</td>
<td>Parallel Resistor</td>
</tr>
<tr>
<td></td>
<td>■ Normal = 5K</td>
</tr>
<tr>
<td></td>
<td>■ Alert = short (0 Ω)</td>
</tr>
<tr>
<td>10K Dual NO/NC</td>
<td>Wire with Parallel/Serial for NO and Serial/Parallel for NC.</td>
</tr>
<tr>
<td></td>
<td>■ Normal = 10K</td>
</tr>
<tr>
<td></td>
<td>■ NO Alert = 5K</td>
</tr>
<tr>
<td></td>
<td>■ NC Alert = 20K</td>
</tr>
<tr>
<td>10K Single Series NC</td>
<td>Series Resistor</td>
</tr>
<tr>
<td></td>
<td>■ Normal = 10K</td>
</tr>
<tr>
<td></td>
<td>■ Alert = open (= Ω)</td>
</tr>
<tr>
<td>10K Single Parallel NO</td>
<td>Parallel Resistor</td>
</tr>
<tr>
<td></td>
<td>■ Normal = 10K</td>
</tr>
<tr>
<td></td>
<td>■ Alert = short (0 Ω)</td>
</tr>
<tr>
<td>Unsupervised NC</td>
<td>No Resistors</td>
</tr>
<tr>
<td></td>
<td>■ Normal = short (0 Ω)</td>
</tr>
<tr>
<td></td>
<td>■ Alert = open (= Ω)</td>
</tr>
<tr>
<td>Unsupervised NO</td>
<td>No Resistors</td>
</tr>
<tr>
<td></td>
<td>■ Normal = open (= Ω)</td>
</tr>
<tr>
<td></td>
<td>■ Alert = short (0 Ω)</td>
</tr>
<tr>
<td>1K/2K Double NC (MDI)</td>
<td>Serial and Parallel Resistors</td>
</tr>
<tr>
<td></td>
<td>■ Normal = 1K</td>
</tr>
<tr>
<td></td>
<td>■ Alert = 3K</td>
</tr>
<tr>
<td>6.8K/18K Double NC (Infographics)</td>
<td>Serial and Parallel Resistors</td>
</tr>
<tr>
<td></td>
<td>■ Normal = 6.8K</td>
</tr>
<tr>
<td></td>
<td>■ Alert = 24.8K</td>
</tr>
<tr>
<td>6.8K/18K Double NO (Infographics)</td>
<td>Parallel and Serial Resistors</td>
</tr>
<tr>
<td></td>
<td>■ Normal = 24.8K</td>
</tr>
<tr>
<td></td>
<td>■ Alert = 6.8K</td>
</tr>
<tr>
<td>200/10K Double NC (Infographics)</td>
<td>Serial and Parallel Resistors</td>
</tr>
<tr>
<td></td>
<td>■ Normal = 196</td>
</tr>
<tr>
<td></td>
<td>■ Alert = 10K</td>
</tr>
</tbody>
</table>
### Table 5-8: Supervision Modes, continued

<table>
<thead>
<tr>
<th>Mode</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>200/10K Double NO (Infographics)</td>
<td>Parallel and Serial Resistors</td>
</tr>
<tr>
<td></td>
<td>◦ Normal = 10K</td>
</tr>
<tr>
<td></td>
<td>◦ Alert = 196</td>
</tr>
<tr>
<td>1K Double NC (Casi-Rusco)</td>
<td>Serial and Parallel Resistors</td>
</tr>
<tr>
<td></td>
<td>◦ Normal = 1K</td>
</tr>
<tr>
<td></td>
<td>◦ Alert = 2K</td>
</tr>
<tr>
<td>1K Double NO (Casi-Rusco)</td>
<td>Parallel and Serial Resistors</td>
</tr>
<tr>
<td></td>
<td>◦ Normal = 2K</td>
</tr>
<tr>
<td></td>
<td>◦ Alert = 1K</td>
</tr>
<tr>
<td>5K Double NC (Simplex)</td>
<td>Serial and Parallel Resistors</td>
</tr>
<tr>
<td></td>
<td>◦ Normal = 5K</td>
</tr>
<tr>
<td></td>
<td>◦ Alert = 10K</td>
</tr>
<tr>
<td>5K Double NO (Simplex)</td>
<td>Parallel and Serial Resistors</td>
</tr>
<tr>
<td></td>
<td>◦ Normal = 10K</td>
</tr>
<tr>
<td></td>
<td>◦ Alert = 5K</td>
</tr>
<tr>
<td>10K Double NC (Andover)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>◦ Normal = 5K</td>
</tr>
<tr>
<td></td>
<td>◦ Alert = 10K</td>
</tr>
<tr>
<td>10K Double NO (Andover)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>◦ Normal = 10K</td>
</tr>
<tr>
<td></td>
<td>◦ Alert = 5K</td>
</tr>
<tr>
<td>4.02K/8.04K Triple NC (Atlantek)</td>
<td>Normal = 4.02K, Tamper = 10.06K</td>
</tr>
<tr>
<td></td>
<td>Alert = 8.04K, Tamper + Alarm = 14.08K</td>
</tr>
</tbody>
</table>
NO/NC Dual EOL 1K

Figure 5-16 on page 5-21 shows the traditional Software House method of supervision where 1K Ω is considered Secure and 500 Ω or 2K Ω are considered Alert. Notice that the wiring is different for NO and NC.

![Figure 5-16: NO / NC Dual EOL 1K](image)

This method will report:
- Short
- Alert (500 ohms)
- Normal (1K)
- Alert (2K)
- Open (>30K)
- Line Fault (Any unexpected value) Usually due to wrong value resistors or faulty resistors.

NO/NC Dual EOL 5K, 10K

Figure 5-17 on page 5-22 shows a method similar to the traditional Software House method of supervision.

- For 5K resistors - 5K = Normal. NO Alert = 2500 ohms, NC Alert = 10K
- For 10K resistors - 10K = Normal. NO Alert = 5K, NC Alert = 20K

Notice that the wiring is different for NO and NC.
For the remainder of the choices you have to choose either NO or NC.

**Double EOL 1K, 5K, 10K**

For UL Listed products, burglar alarms must be supervised.
**Single EOL 5K, 10K**

*Figure 5-19: Single EOL 5K, 10K*

For UL Listed products, burglar alarms must be supervised.

**Non-Supervised**

*Figure 5-20: Non-Supervised*

For UL Listed products, burglar alarms must be supervised.
FAI Connections

FAI Scenarios

FAI (Fire Alarm Interlock) is a hardware feature that will activate all enabled relays when the F input of J84 opens. It is NC (Normally Closed).

The concept of activating relays when a fire is signaled can be used in two basic scenarios:
- Unlock all doors when fire is present.
- Remove power from various devices when fire is present.

The implementation could be a combination of both scenarios by selecting the correct NO or NC contact of the relay.

Magnetic Door Locks have power applied most of the time with a break in the power to open the door. You have to be aware of NO or NC in those cases also.

Set SW31 to True on the ACM that has the FAI/Key signals connected.

SW2, SW4, SW22, SW19, SW18, SW6, SW26, SW23 are the switches that allow the large relays to be activated when FAI is True.

FAI Modes

There are two basic modes:
- FAI without Latch - This method requires the F input (NC) of J84 plus the individual enable switches for each relay (SW2, SW4, SW22, SW19, SW18, SW6, SW26, SW23). See Figure 5-21 on page 5-25.
- FAI with Latch and subsequent Unlatch - This method requires the F input of J84 plus the individual enable switches for each relay, plus SW30 to enable the Latch and J84 K input (NO) to reset the Latch. See Figure 5-22 on page 5-26.

FAI without Latch

This mode is fairly basic.
- The normally closed F input goes true by opening.
- The Relay Drive goes true and activates all relays that have their FAI enable switches on (SW2, SW4, SW22, SW19, SW18, SW6, SW26, SW23).
- The normally closed F input goes false by closing.
- The Relay Drive goes false and deactivates all relays that have their FAI enable switches on (SW2, SW4, SW22, SW19, SW18, SW6, SW26, SW23).
FAI with Latch followed by Key Unlatch

If the Latch Enable switch (SW30) is on and the F input goes true the selected relays will activate and stay that way until an Unlatch is given.

1. J84 is in its normal state with F (NC) closed and K (NO) open.
2. F opens signaling a Fire Alarm and all enabled relays are activated by the Relay Drive, as in FAI without Latch.
3. F input closes indicating the Fire Alarm has been reset, BUT the relays stay activated (Latched).
4. Sometime later, probably after investigation, K closes and deactivates the relays. This input is named K because this input is usually a Key operated switch.
5. When K opens again, everything is back to normal.
F and K input Supervision

Although the F and K inputs will work when they are unsupervised, as shown in Figure 5-21 on page 5-25 and Figure 5-22 on page 5-26, Software House recommends that you use the standard Software House method of supervising the inputs. Use parallel/serial for the normally open K input and use serial/parallel for the normally open F signal.

The wiring is shown in Figure 5-23 on page 5-26. Be sure that the resistors are as close as possible to the F and K switches for the most security.
State of F, K, and Relay Drive

In addition to the added security gained by using supervision, the state of F, K, and Relay Drive signals will be available in the C•CURE system.

All three of the inputs, shown in Figure 5-24 on page 5-27, support event triggers based on their active or inactive states. These event triggers can activate alarms, send emails, run a Roll Call Report, etc.

If F or K have a supervision error (short, open, or line fault), that will be reported in the normal way.

Figure 5-24: FAI Inputs (C•CURE 9000)
iSTAR Controller Status Tab

The iSTAR Controller dialog box Status tab in the C•CURE 9000, shown in Figure 5-25 on page 5-28, indicates encryption status plus other read-only information about the Ultra.

Figure 5-25: Controller Dialog Box - Status Tab
Reader - Voltage Requirements and Distance

To operate properly, each reader requires the following minimum voltage:

- A standard RM Series Reader or RM-4 board requires at least 7.5 volts.
- An RM-4E board requires at least 11 volts.

The iSTAR Ultra supplies 12 volts at its reader connectors; however, the amount of voltage that reaches the reader is affected by the following:

- Number of devices on the bus
- Current draw of each device
- Wiring length between the devices and iSTAR Ultra
- Wire gauge that connects the devices
- State of the battery (if running on apS)
- Tolerance if sourced by an external power supply.

To determine the maximum distance of a reader from an iSTAR Ultra, calculate the voltage that reaches each reader. If the voltage is insufficient, you can shorten the wire length, use a heavier wire, or add UL294 power-limited power supply.

- Wire resistance is as follows:
  - 24 AWG = 26.0 Ω per 1000 ft.
  - 22 AWG = 16.5 Ω per 1000 ft.
  - 20 AWG = 10.2 Ω per 1000 ft.
  - 18 AWG = 6.5 Ω per 1000 ft.

**NOTE**

You must consider the wire length both to and from the reader, in the calculation.

**Example:**

- The RM-4 is 500 feet away. (1000' round trip)
- The RM-4 draws 250 mA. and is connected with 20 AWG wire.

The equation to calculate voltage drop is:

\[ E = I \times R \]

\[ I = 0.25 \text{ A (250 mA)} \]
\[ R = 10.2 \text{ ohms (from the table)} \]
\[ E = 0.25 \times 10.2 \]
\[ E = 2.55 \text{ (voltage drop)} \]

12 Vdc - 2.55 Vdc = 9.45 Vdc

The connection meets the requirement.

Table 5-9 on page 5-30 lists the general wiring requirements for an iSTAR Ultra and its components.
Table 5-9: Equipment Wiring Specifications

<table>
<thead>
<tr>
<th>Signal</th>
<th>From</th>
<th>To</th>
<th>Belden # or equiv.</th>
<th>AWG</th>
<th># Prs</th>
<th>Shield</th>
<th>Max Length</th>
<th>Max. Wire Resistance</th>
</tr>
</thead>
<tbody>
<tr>
<td>RS-485 Comm, Data Half-duplex 2 wire</td>
<td>iSTAR Ultra</td>
<td>RM &amp; I/O Modules</td>
<td>9841</td>
<td>24</td>
<td>1</td>
<td>Yes</td>
<td>4000 ft. (1212 m)</td>
<td>103Ω</td>
</tr>
<tr>
<td>RS-485 Comm, Power</td>
<td>iSTAR Ultra</td>
<td>RM &amp; I/O Modules</td>
<td>8442/8461</td>
<td>22/18</td>
<td>1</td>
<td>Yes</td>
<td>Range of 600 ft. to 1500 ft. depends on AWG</td>
<td>See Note²</td>
</tr>
<tr>
<td>RJ45-Ethernet</td>
<td>iSTAR Ultra</td>
<td>Hub, Host</td>
<td>N/A</td>
<td>2</td>
<td>No</td>
<td>Yes</td>
<td>328 ft. (100 m)</td>
<td>8.4 Ω</td>
</tr>
<tr>
<td>Supervised Input</td>
<td>iSTAR Ultra or I8</td>
<td>Input</td>
<td>8442/8461</td>
<td>22/18</td>
<td>1</td>
<td>No</td>
<td>2000 ft. (606 m)</td>
<td>32 Ω</td>
</tr>
<tr>
<td>Request-to-exit (REX or RTE)</td>
<td>iSTAR Ultra or RM-4/4E module</td>
<td>Switch</td>
<td>8442/8461</td>
<td>22/18</td>
<td>1</td>
<td>No</td>
<td>2000 ft. (606 m)</td>
<td>32 Ω</td>
</tr>
<tr>
<td>Door State Monitor (DSM)</td>
<td>iSTAR Ultra or RM-4/4E module</td>
<td>Contact</td>
<td>8442/8461</td>
<td>22/18</td>
<td>1</td>
<td>No</td>
<td>2000 ft. (606 m)</td>
<td>32 Ω</td>
</tr>
<tr>
<td>Supervised Input (UL) Note¹</td>
<td>iSTAR Ultra or I8</td>
<td>Input</td>
<td>9462</td>
<td>22</td>
<td>1</td>
<td>Yes</td>
<td>2000 ft. (606 m)</td>
<td>32 Ω</td>
</tr>
<tr>
<td>Relay Control</td>
<td>RM-4 module</td>
<td>ARM-1</td>
<td>9462</td>
<td>22</td>
<td>1</td>
<td>Yes</td>
<td>25 ft. (7.6 m)</td>
<td>.04Ω</td>
</tr>
<tr>
<td>Reader Data (Direct Wiegand Connection)</td>
<td>iSTAR Ultra or RM-4/4E module</td>
<td>Proximity/ Wiegand signaling read head</td>
<td>9942</td>
<td>22</td>
<td>3</td>
<td>Yes</td>
<td>200 ft. (60.96 m)</td>
<td>3.2 Ω (22)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>9260</td>
<td>20</td>
<td></td>
<td></td>
<td>300 ft. (91.4 m)</td>
<td>3.2 Ω (20)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Alpha wire 5386C</td>
<td>18</td>
<td></td>
<td></td>
<td>500 ft. (152.4 m)</td>
<td>3.2 Ω (18)</td>
</tr>
</tbody>
</table>

¹ To comply with UL requirements, use shielded, minimum 22 AWG stranded, twisted pair cable for monitor points, supervised inputs, DSMs, and REXs. Use Belden9462 or equivalent.

² Check wire lengths to verify that voltage drops are acceptable.

Calculations are based on a single RM-4 reader with keypad and LCD (250 mA):
Using 22 AWG, distance = 600 ft. (.0165 W ft.)
Using 18 AWG, distance = 1500 ft. (.0065 W ft.)

**NOTE**

- Cables that need to be shielded are described in Table 5-9 on page 5-30.
- The Tamper, Low Battery, and AC power fail inputs must be enabled and connected to the iSTAR Ultra to report for compliance with UL requirements.
- For UL listed products, burglar alarm inputs must be supervised.
- UL Listed panic hardware shall be used to allow emergency exit from a protected area.
Readers and Accessory Boards

The following readers and accessory boards are supported:

- Wiegand Signaling Readers:
  - SWH-4000
  - SWH-4200
  - SWH-4100
  - SWH-5100
  - P345KPMTR
  - HID 5365 series
  - HID RP40 multiCLASS
  - HID RPK40 multiCLASS
  - HID RP15 multiCLASS

- RS-485 RM Bus:
  - RM2L-P1 (SWH)
  - RM1 series (SWH)
  - RM2 series (SWH)
  - RM3 series (SWH)
  - RM2L series (SWH)
  - RM2L-4000 (SWH)
  - RM2L-NH (SWH)

- Accessory boards:
  - I/8
  - R/8
  - I/8-CSI
  - RM-4
  - RM-4E
  - RM-DCM-2
Readers and Accessory Boards
IP-ACM Ethernet Door Module v2

This chapter provides an overview of the IP-ACM Ethernet Door Module v2.

For more information regarding the specifications, features, and installation of the IP-ACM, refer to the IP-ACM Ethernet Door Module v2 Quick Start Guide.

In This Chapter:

◆ Overview ........................................................................................................................................................... 6-2
Overview

The IP-ACM Ethernet Door Module v2, Figure 6-1 on page 6-3, provides connection and management of access control for two readers. The maximum number of IP-ACM Ethernet door modules supported per iSTAR Ultra is 32. Each IP-ACM can support two doors, or one door with in and out readers.

The IP-ACM Ethernet Door Module v2 supports the following features:

- 12VDC or 24VDC local power or Power over Ethernet (PoE or PoE+)
- Two RJ45 ports:
  - Port 1: Ethernet port, internally bound to MAC with the MAC address and used as the network connection port for the board (10/100/1000)
  - Port 2: Switch port, not a secondary port, used for iSTAR Ultra LT connection (10/100, no PoE)
- Four supervised Inputs and two Outputs
- Communication to readers through Wiegand or RS-485 ports
- SSL network encryption from the unit to the GCM
- IPv4 and IPv6 network protocols
- 802.1X port-base authentication
- HTTPS Web-based configuration
- Offline mode for two readers that allows the last 1,000 previous card admits and/or a specific personnel group of no more than 1000

See the IP-ACM v2 Ethernet Door Module Quick Start Guide for requirements, specification, installation, and configuration information.

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-ACM2A-MB</td>
<td>IP-ACM V2, 2 Reader, board only</td>
</tr>
<tr>
<td>IP-ACM2A-EM</td>
<td>IP-ACM V2, 2 Reader in metal enclosure</td>
</tr>
<tr>
<td>IP-ACM2A-EP</td>
<td>IP-ACM V2, 2 Reader in plastic enclosure</td>
</tr>
<tr>
<td>IP-ACM2-CAN</td>
<td>IP-ACM metal enclosure without board</td>
</tr>
<tr>
<td>IP-ACM2-CAN-P</td>
<td>IP-ACM plastic enclosure without board</td>
</tr>
<tr>
<td>IP-ACM2A-MB-5PK</td>
<td>IP-ACM V2, 2 Reader, board only five pack box</td>
</tr>
</tbody>
</table>
Figure 6-1: IP-ACM Ethernet Door Module v2

Overview

iSTAR Ultra Installation and Configuration Guide

6–3
This chapter describes the iSTAR Ultra controller configuration and diagnostics.

In This Chapter:

- **iSTAR Ultra Network Configuration** ................................................................. 7-2
- **Board Configuration** ...................................................................................... 7-2
- **iSTAR Ultra DHCP IP Address Configuration** ............................................... 7-2
- **STAR Ultra Static IP Address Configuration** .................................................. 7-2
- **iSTAR Configuration** ...................................................................................... 7-4
- **ICU** .................................................................................................................. 7-4
- **iSTAR Ultra Web Utility** .................................................................................. 7-5
- **C•CURE 9000** .................................................................................................. 7-7
- **STAR Ultra Local Database Backups** ............................................................... 7-7
- **Proper Shutdown Sequence** ............................................................................ 7-8
iSTAR Ultra Network Configuration

The Ultra GCM board has two Ethernet ports, either of which can be set to DHCP or static IP addresses. By default, **Ethernet port 1** is set to DHCP and **Ethernet port 2** is set to a static IP of 192.168.1.253. Once the controller is connected through the ICU application, any combination of DHCP and static IP address can be used on the ports. Use the following sections to make an initial connection to the controller and facilitate any desired changes.

Software House recommends that you use a Static IP address when configuring iSTAR controllers.

The following limitation applies to iSTAR controllers with member connected controllers and iSTAR controllers with connected IP-ACMs that use DHCP IP address assignments:

If DHCP is used, the lease may expire and assign a new IP address to the iSTAR controller. If this happens, all members and IP-ACMs will not be able to connect to the iSTAR controller with the new IP address. The IP address will need to be reassigned as follows:

1. The Master’s IP address of a member controller can be updated using the ICU.
2. The iSTAR controller’s IP address of an IP-ACM can be configured in IP-ACM Configuration/Status web page.

**Board Configuration**

1. Ensure the following switches, shown in General Control Module on page 4-2, are in the default positions:
   a. S1-1 ON, S1-2 OFF, S1-3 OFF, S1-4 OFF, SW3 is in position 0.
   b. If they are not, change them to the positions in step a.

**iSTAR Ultra DHCP IP Address Configuration**

To configure the controller to use a DHCP IP address:

1. Connect to the network using the Ethernet port 1 of the iSTAR Ultra.
2. Perform a factory default reset as directed in this document. After the reset, the iSTAR Ultra boots with the DHCP IP address.
3. Use the ICU, or the iSTAR Ultra Web Utility, to configure the iSTAR Ultra. See iSTAR Configuration on page 7-4.

**STAR Ultra Static IP Address Configuration**

This section describes the procedure for a Factory Reset / first time connection to Ethernet port 2.

To configure the controller to use a Static IP address:

1. Remove all network cables from the controller.
2. Turn rotary switch (SW3) to position ‘D’ and press the reset button (SW7) or cycle power.
3. Wait until the LCD says to reset the board.

4. Plug in an Ethernet cable from a **standalone** (no network connection including WIFI) laptop/PC to the secondary adapter.

5. Turn rotary switch (SW3) back to position '0'.

6. Reset or power cycle the board using SW7.

7. Wait for the firmware message to appear on LCD.

8. Ping to 192.168.1.253 from the host machine (which should be configured on the same subnet).

9. The 'Secondary address' message on LCD may or may not be shown with the configuration. (See note 1).

10. Use the ICU, or the iSTAR Ultra Web Utility, to change the configuration of the iSTAR Ultra. After configuration, the unit reboots. See iSTAR Configuration on page 7-4.

**NOTE**

- Due to high priority messages appearing on the LCD for the primary adapter, the secondary adapter's IP message frequently gets lost and does not display.

- When there is no active network link (for example, unplugged cable or powered down switch) the LCD displays 0.0.0.0 for the network adapter.

- If there _is_ link _and_ configuration (DHCP or static), the LCD displays the address.

- After factory reset, once a connection is made to the host, the factory default static configuration for the second adapter gets overwritten by the configuration on the host, regardless if it is connected to the network or not. Repeat the factory reset process to perform configuration through the secondary adapter again.

- If leaving Ethernet 2 at the default IP address, do not connect Ethernet 2 to the production network. This exposes the same default 192.168.1.253 address and causes duplicate IP addresses if you perform a simultaneous factory reset on multiple iSTAR Ultra panels.

- Never connect more than one factory default iSTAR Ultra to a network via ETH2. Otherwise, multiple Ultra panels will expose the same default IP 192.168.1.253 address and cause duplicate IP issues.

- The ETH2 and ETH1 NICs use an autosense function for speed and MDIX crossover. You do not have to use a crossover cable for the direct connection.
iSTAR Configuration

The iSTAR configuration is accomplished using the C•CURE Administration Station and the iSTAR Configuration Utility (ICU).

See the following:
- ICU on page 7-4
- iSTAR Ultra Web Utility on page 7-5
- C•CURE 9000 on page 7-7
- STAR Ultra Local Database Backups on page 7-7

ICU

The ICU provides iSTAR configuration, diagnostic, and troubleshooting options.

Use the ICU to designate the master controller, define master IP addresses, and define the IP address for the C•CURE host. Other configuration information should be defined and downloaded from the C•CURE host. However, sites that use locked IP addresses to provide local management can use the ICU utility for local cluster configuration.

To ensure correct configuration, the information that you enter in the ICU must match the information that you enter in the C•CURE Administration application.

**NOTE**

Software House recommends that you use the ICU only for initial setup of master controller address information and for occasional troubleshooting. This is because configuration information in C•CURE is downloaded to the iSTAR and overwrites the values that you specify in the ICU.

The ICU provides a set of troubleshooting tools that help you to monitor the iSTAR network. Use the troubleshooting tools to:
- PING IP addresses.
- Send messages to other ICU users.
- Open a Real Time Monitor Controller Diagnostics window within the ICU and display reports and diagnostic messages.

Refer to the *iSTAR Configuration Utility User Guide* for configuration information. The guide is available from the Software House Web site.

Using the ICU in LAN Configurations

Requirements for LAN configurations vary from site to site. The following procedure describes most configurations.

**Perform the following steps:**

1. Connect and power on all iSTAR controllers.
2. Use the ICU to configure the following:
• Define the master.
• Specify the IP address of the master.
• Obtain the Domain Name Server addresses automatically.
• Define the host IP address or FQDN (Fully Qualified Domain Name) with which the master will communicate.

3. Use the C•CURE Administration application to configure:
   • Master and member names.

4. Master and member IP and MAC addresses.

Using the ICU in WAN Configurations

NOTE

- The ICU only sees iSTARs in the local subnet, by default, because ICU uses a broadcast to awaken iSTARs.
- The ICU can connect to an iSTAR across a WAN provided you know the IP address of the remote iSTAR.

Perform the following steps for the ICU to detect an iSTAR address beyond the local subnet:

1. Connect and power on all iSTAR controllers.
2. Install the ICU.
3. Connect the PC or laptop with the ICU to the subnet on which the target iSTAR resides.
4. Open the ICU.
5. Enter the default password “manager”.
6. Use the ICU to do the following:
   • Identify MAC addresses for members.
   • If not using DHCP, configure the IP address for the master
7. If applicable, configure gateway addresses for members and masters.

iSTAR Ultra Web Utility

The iSTAR Ultra Web uses a Web page interface that is included in the iSTAR firmware. iSTAR Ultra Web provides access to the iSTAR Ultra SE controller configuration, status, and diagnostic information.
Use the iSTAR Ultra Web Utility to designate the master controller, define master IP addresses, and define the IP address for the C•CURE host. To ensure correct configuration, the information that you enter must match the information that you enter in the C•CURE Administration application.

**NOTE**
- The iSTAR Ultra Web is supported on Microsoft® Internet Explorer 10, Internet Explorer 11 and Chrome. It is not supported on Microsoft Edge.
- The iSTAR Ultra Web has not been evaluated by UL.

**To access iSTAR Ultra Web Utility:**

1. In a browser window, enter the IP Address of the iSTAR Ultra controller (for example, https://10.10.10.10) in the browser **Address** window and press **Enter** or click **Go**.
   
   You can also access the iSTAR Ultra Web from the ICU by right-clicking the controller and clicking **Controller Status**, or click **Tools** and select **Controller Status**.

   **NOTE**
   - If using Internet Explorer and you receive a Certificate Error indicating "There is a problem with this website's security certificate", click **Continue to this website (not recommended)**.
   - If using Google Chrome and you receive an error indicating “Your connection is not private”, click **ADVANCED** and then click **Proceed to x.x.x.x (unsafe)**.

   The iSTAR Ultra log in screen opens in the default browser.

2. Enter the username and password and click **LOG IN**.

   **NOTE**
   - The default case-sensitive username and password is "iSTAR".

3. The iSTAR Ultra Welcome page opens in the default browser.
For LAN configurations, Software House recommends that you configure information for member controllers in the C•CURE Administration application. The C•CURE Administration Station downloads member configuration information to the master at start-up, and the master uses the information to configure the member controllers.

See the C•CURE 9000 Hardware Configuration Guide and the C•CURE 9000 help for more information.

STAR Ultra Local Database Backups

NOTE

If CPNI mode is enabled on the iSTAR Ultra, then all database and transactions are stored in RAM. The database and transactions are not backed up on the SD card.

The iSTAR Ultra configuration data (doors, personnel, etc.) is held in volatile RAM during normal operation (IP settings are stored in the controller’s onboard flash memory). This data is backed up to non-volatile SD Card memory on a periodic basis during normal operation. Data is automatically backed up after a fast download to the panel, and, upon a soft reset on the GCM board.

To ensure that the backup is current, Software House recommends to trigger an additional database backup whenever the Low Battery or AC Fail input is activated on the GCM board. This is accomplished by creating an event with an action of “Backup iSTAR Database” and
then triggering the event from the **Low Battery** and **AC Fail** inputs. If your power supply does not have this feature, then you can trigger the database backup event using a schedule. For example, set the backup to run at 2AM every Monday.

When power is restored after an outage, the Ultra first attempts to connect to its host server. If successful, the host will download the current time to the Ultra, and download the current database. However, if the host is not present, then the Ultra will use its local backed-up time, and it will use the last saved database from the SD card.

When the host is offline, transaction buffers of card activity and other activity are automatically written to non-volatile memory, and do not require database backup configuration.

- See the **C•CURE 9000 Software Configuration Guide** for information about configuring events and scheduling backups.
- See the **C•CURE 9000 Hardware Configuration Guide** for information about configuring inputs.

## Proper Shutdown Sequence

You must properly shut down the iSTAR Ultra unit. If you do not properly shut down the iSTAR Ultra GCM using the following procedure, the SD card can become corrupted.

Perform the following procedure when shutting down the iSTAR Ultra at all times, regardless of removing or replacing the SD card.

1. On the iSTAR Ultra GCM board, locate the **SW3** rotary switch and the restart button **SW7**.
2. Set the rotary switch SW3 to position **0**.
3. Press and release the restart button **SW7**.
5. The LCD display goes black for about five seconds. In this time, remove the power cable from the Ultra GCM board.
   - If you miss the opportunity to remove the power cable from the iSTAR Ultra GCM and it begins the boot-up sequence again, you must wait for a full boot-up cycle to complete and repeat the steps above before you remove the SD card.

- **The iSTAR Ultra GCM must be completely powered off before you remove the SD card.**
- **Do not remove power when the Ultra GCM is going through its boot-up process. It is possible to corrupt the on-board SD card during that time.**
The iSTAR Ultra includes an LCD message display. For normal operations, configure the LCD
to display status messages. For troubleshooting operations, configure the LCD to display
diagnostic messages about readers, card data, inputs, outputs, network ports and devices.

In This Chapter:

- LCD Message Display ................................................................. 8-2
- Displaying Status Messages............................................................ 8-3
- Setting LCD Status Message Display .............................................. 8-3
- Card Reader Diagnostics ............................................................... 8-5
- Hardware Test ............................................................................. 8-4
- Card Reader Diagnostics ............................................................... 8-5
- Output Diagnostics ..................................................................... 8-5
- Input Change Display Mode ......................................................... 8-5
- Ethernet Port Test ..................................................................... 8-6
- GCM Battery Replacement ......................................................... 8-7
The iSTAR Ultra includes an LCD display for status and diagnostic messages. SW3 is an onboard 16-position rotary switch. Most of the positions are used to control LCD diagnostics.

Figure 8-1 shows the location of the rotary switch SW3. See Table 8-1 on page 8-2 for a summary of SW3 settings.
Displaying Status Messages

Under normal conditions, set the LCD to display status messages, including:

- iSTAR boot information
- Date and time
- Firmware version
- Controller status information.

Messages typically display for approximately four seconds, separated by an interval of about one second. In some instances, however, a message can display until it is cancelled or terminated.

Setting LCD Status Message Display

You can display LCD general status messages for a controller by setting the SW3 rotary switch to positions 0 (zero) or F. Setting the SW3 switch to 0 or F also controls the ICU Block feature, preventing or allowing users from modifying the ICU configuration, as shown in Table 8-2.

- **When ICU Block is On** (set SW3 to F) – the LCD displays general status messages; however, fields in the ICU dialog box are unavailable and cannot be edited.

- **With ICU Block Off** (set SW3 to 0) – the LCD displays general status messages, and users can read, write, and update the ICU configuration.

---

Table 8-1: iSTAR Ultra Rotary Switch Functions, continued

<table>
<thead>
<tr>
<th>Position</th>
<th>Description</th>
</tr>
</thead>
</table>
| 8        | Hardware Test (Onboard Ethernet 1 and 2, USB ports).  
**NOTES:**  
- Ethernet tests require a good IP (Static or DHCP, and a good network link) and at least one ICU running on the same subnet.  
- USB port tests require the thumb drive to be formatted to a FAT32 file format.  
| 9        | Not used.   |
| A        | Erase DB files from flash. (Press SW2 GCM Hard reset, wait for LCD instructions, set rotary switch back to 0 or F, press reset again.) This is similar to position D, but leaves the basic Comm setup of IP, etc.  
| B        | MFG - ATE (Automated Test Equipment) (Software House only).  
| C        | Disable watchdog (Software House only).  
| D        | Restore Factory Default. Erase data base files and communication parameters from flash. (Press SW7 Hard GCM reset, wait for LCD instructions, set rotary switch back to 0 or F, press reset again.)  
| E        | Boot to backup image (Activate on Software House instruction only).  
| F        | ICU Block On (Read only) - Display General Messages.  

---

NOTES:

- Ethernet tests require a good IP (Static or DHCP, and a good network link) and at least one ICU running on the same subnet.

- USB port tests require the thumb drive to be formatted to a FAT32 file format.

---

9 Not used.

A Erase DB files from flash. (Press SW2 GCM Hard reset, wait for LCD instructions, set rotary switch back to 0 or F, press reset again.) This is similar to position D, but leaves the basic Comm setup of IP, etc.

B MFG - ATE (Automated Test Equipment) (Software House only).

C Disable watchdog (Software House only).

D Restore Factory Default. Erase data base files and communication parameters from flash. (Press SW7 Hard GCM reset, wait for LCD instructions, set rotary switch back to 0 or F, press reset again.)

E Boot to backup image (Activate on Software House instruction only).

F ICU Block On (Read only) - Display General Messages.
**Diagnostic Tests**

iSTAR Ultra firmware provides diagnostic information for:

- Readers
- Cards
- Outputs
- Inputs
- Ethernet port

Use rotary switch **SW3** on the GCM to activate diagnostic tests. Diagnostic information displays on the iSTAR Ultra LCD.

![Use caution when activating outputs in a live system. For example, if the output opens the shipping door, the shipping door will open when you test it.]

**NOTE**

- Diagnostic tests add overhead to iSTAR Ultra processing, and may degrade system performance. When the diagnostic tests are complete, deactivate the test by resetting SW3 to display status information.
- Either 0 to display with full control, or F to display as read only.

**Hardware Test**

The onboard Ethernet tests display diagnostic information about both on-board Ethernet connections, the USB ports, and the SD drive.

**To Test the Ethernet port**

1. Set switch **SW3** to the position shown in Table 8-3.

**Table 8-3: Ethernet Test Switch Settings**

<table>
<thead>
<tr>
<th>Switch Position</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW3 set to 8</td>
<td>Hardware Test (Onboard Ethernet 1 and 2, USB ports, SD drive)</td>
</tr>
</tbody>
</table>

2. Observe the LCD display for test results.
3. When the test is complete, set SW3 back to 0 or F to display status messages.

The LCD displays only success messages. If no message displays, the circuit is defective or the port is not communicating.

Card Reader Diagnostics

You can display the most recent card data processed by any reader on iSTAR Ultra in either fast mode or slow mode.

- **Fast mode** – In this mode, the most recent card swipe data displays on the LED for approximately one second.
- **Slow mode** – In this mode, the most recent card swipe data displays for seven seconds.

### To Set the Mode for Card Reader Diagnostics

- Set the SW3 rotary switch to the positions shown in Table 8-4.

<table>
<thead>
<tr>
<th>Rotary Switch</th>
<th>Slow Mode Reader Diagnostics Position</th>
<th>Fast Mode Reader Diagnostics Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set SW3 to:</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

You can also use the iSTAR Web Page Diagnostic Utility to view reader diagnostic information. For information about this utility, see “Web Page Diagnostics” on page 9-2.

Output Diagnostics

Output Change Display (Slow Mode)

The manual output test is an end-to-end test that displays information about outputs activated manually by a technician. The outputs you are testing can be attached to iSTAR Ultra through readers and R/8 boards. Information displays on the LED for two seconds.

### To Activate the Output Change Display Test

- Set rotary switch SW3 to the position shown in Table 8-5 on page 8-5.

<table>
<thead>
<tr>
<th>Switch Position</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW3 set to 5</td>
<td>Activate output change display for two seconds (slow mode)</td>
</tr>
</tbody>
</table>

Input Change Display Mode

The input change display mode tests and displays information about inputs that are activated manually. Inputs tested can be attached to iSTAR Ultra through the main board, RMs, and I/8 boards.
Diagnostic Tests

Information displays on the LED for either one second (Position 4, On) or two seconds (Position 3, On).

To Activate Input Change Display Tests

Set the SW3 rotary switch to the positions shown in Table 8-6.

Table 8-6: Input Test Switch Settings

<table>
<thead>
<tr>
<th>Switch Position</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW3 set to 3</td>
<td>Two-second LED input change display is on (slow mode)</td>
</tr>
<tr>
<td>SW3 set to 4</td>
<td>One-second LED input change display is on (fast mode)</td>
</tr>
</tbody>
</table>

Ethernet Port Test

The onboard Ethernet tests display diagnostic information about Ethernet connections.

To Test the Ethernet Port

1. Set switch SW3 to the position shown in Table 8-7 on page 8-6.

Table 8-7: Ethernet Test Switch Settings

<table>
<thead>
<tr>
<th>Switch Position</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW3 set to 8</td>
<td>Tests the Ethernet Port</td>
</tr>
</tbody>
</table>

2. Observe the LCD display for test results.
GCM Battery Replacement

The GCM coin cell battery should be tested annually and replaced as necessary.
- The battery is a CR2032 Lithium 230 mA/h coin cell.
- The battery retains power for the Real Time Clock for at least 3 weeks. After three weeks of accumulated power outage, the battery should be replaced.
- The battery should last 5 years if there’s no power outages.

To Remove and Replace the Battery

1. With a small screwdriver, gently pry the battery up at point A.
2. At the same time, use your thumb to push the black tab back B.
3. Gently slide the battery to the left and out.
4. To replace, slide the battery in from the left, under the black tab and under the metal spring C.

Caution - Do not bend or break the metal spring C. The spring is important to the operation of the battery.

Figure 8-2: GCM Lithium Battery Replacement