C•CURE and Software House are registered trademarks of Tyco International Ltd. and its respective companies.

The trademarks, logos, and service marks displayed on this document are registered in the United States [or other countries]. Any misuse of the trademarks is strictly prohibited and Tyco International Ltd. will aggressively enforce its intellectual property rights to the fullest extent of the law, including pursuit of criminal prosecution wherever necessary. All trademarks not owned by Tyco International Ltd. are the property of their respective owners, and are used with permission or allowed under applicable laws.

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

C•CURE 800/8000 version 10.3 and later with iSTAR firmware version 5.2.0 and later.
C•CURE 9000 version 2.02 and later with iSTAR firmware version 5.1.7 and later.

Document Number: UM-236
Revision Number: E0
Release Date: May 2012

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

Copyright © 2012 by Tyco International Ltd. and its Respective Companies.

All rights reserved.
# Table of Contents

## Preface

- How to Use this Manual ................................................................. xii
- Finding More Information ............................................................ xiii
- Conventions .................................................................................. xiv
- Important Safety Information ......................................................... xv

## Chapter 1  Overview and Introduction

- Overview and Introduction ............................................................ 1-2
  - iSTAR Edge Photograph .............................................................. 1-2
  - iSTAR Edge Layout ................................................................. 1-4
- Main Features .................................................................................. 1-5
  - Processor ...................................................................................... 1-5
  - Storage ......................................................................................... 1-5
  - Power .......................................................................................... 1-5
  - Readers ......................................................................................... 1-6
  - I/O ............................................................................................... 1-6
  - Communications .......................................................................... 1-8
  - FAI ............................................................................................... 1-8
  - Onboard Controls .......................................................................... 1-8
  - Housing ......................................................................................... 1-9
  - Compliance .................................................................................... 1-9
  - 2-Reader Models ............................................................................ 1-9
  - 4-Reader Models ............................................................................ 1-9
  - Accessories ................................................................................... 1-9
- Product Comparison ......................................................................... 1-10
Chapter 2  
Site Requirements

Pre-Installation Planning ................................................. 2-2
  Equipment Check .................................................. 2-2
  Site Check ......................................................... 2-2
    iSTAR Edge Mounting Requirements ......................... 2-3
  Voltage Requirements and Distance ............................. 2-4
  Installation Tools .................................................. 2-4

Installation Requirements ............................................ 2-5
  Host System Requirements ........................................ 2-5
  iSTAR Edge Cabinet Requirements ............................... 2-5
  Environmental Requirements ..................................... 2-5
  Power Requirements ............................................... 2-6
    iSTAR Edge Components and Boards .......................... 2-6
    iSTAR Edge Input Power Rating ............................... 2-7
  Individual/Total Loads ........................................... 2-7
    iSTAR Edge Wiegand Reader Ports ............................ 2-8
    Software House Readers ....................................... 2-9
    Third Party Readers ........................................... 2-10
  Ethernet Requirements ........................................... 2-11
  Wiring Requirements ............................................... 2-11
  Grounding Requirements ......................................... 2-13

Chapter 3  
iSTAR Edge/eX Topology

iSTAR Edge 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
    Using NetBIOS and Fully Qualified Domain Names ........... 3-5

Cluster Configuration .................................................. 3-6
  Master and Member Configuration ............................... 3-6

Single Master and Alternate Master Configurations ............... 3-7
  Primary Communications Path .................................... 3-8
  Secondary Communications Path .................................. 3-9
Maintaining Cluster Communication ........................................ 3-10
  Single Master Configurations ........................................... 3-10
  Alternate Master Configuration ......................................... 3-11
  Communication Between Members and Master ......................... 3-12
Adding Controllers to the Cluster ....................................... 3-13
Configuring Communication Paths ....................................... 3-14
  Planning Primary Communications ..................................... 3-14
    Primary Communication Guidelines ................................. 3-14
  Planning Secondary Communications ................................. 3-15

Chapter 4  iSTAR Edge Power and Backup

Power - Batteries - Backup ................................................ 4-2
  Power General ............................................................. 4-3
  Power in ................................................................. 4-7
    12 / 24 V DC ......................................................... 4-7
  Onboard backup batteries ............................................. 4-8
  Backup ................................................................. 4-8
  Power Out .............................................................. 4-11

Chapter 5  iSTAR Edge Controls and Displays

Controls and Displays ...................................................... 5-2
  Switches-Jumpers-LEDs ................................................ 5-2
  Visual Indicators ....................................................... 5-3
    LCD ................................................................. 5-3
    LEDs ............................................................... 5-3
  Onboard controls ....................................................... 5-6
    Reset button ....................................................... 5-6
    Switches and Jumpers .............................................. 5-6
  Rotary switch .......................................................... 5-7
  RM Port Termination Switches ......................................... 5-8
  Output Relay Wet or Dry Jumpers ..................................... 5-8
  PoE Jumpers ............................................................ 5-8
  PoE or PoE Plus Jumper ............................................... 5-8
### Chapter 6 iSTAR Edge Connections

#### Connections - 2 Reader Model

- Reader - I8 - R8 Combinations ................................................. 6-2
- Two Wiegand Readers ............................................................. 6-2
- Two RM Readers .................................................................... 6-3
- One Wiegand and One RM Reader ........................................... 6-4
- RM Port Terminators .............................................................. 6-5

#### Connections - 4 Reader Model

- Reader - I8 - R8 Combinations ................................................. 6-7
- Four Wiegand Readers ............................................................. 6-7
- Four RM Readers .................................................................... 6-8
- Two Wiegand and Two RM Readers ........................................ 6-9
- RM Port Terminators .............................................................. 6-10

#### Inputs

- NO/NC Double EOL 1K ............................................................ 6-12
- NO/NC Double EOL 5K, 10K ................................................. 6-15
- Double EOL 1K, 5K, 10K ......................................................... 6-16
- Single EOL 5K, 10K ................................................................. 6-17
- Non-Supervised .................................................................... 6-17

#### AUX Outputs

- ................................................................. 6-18

#### Relay Outputs

- Dry Relay Wiring ................................................................. 6-19
- Wet Relay Wiring ................................................................. 6-20
- WET Wiring for a MagLock .................................................... 6-21

#### Wiegand Readers

- ................................................................. 6-22

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

- ................................................................. 6-23

#### AC Fail / Low Battery

- ................................................................. 6-24

#### Tamper

- ................................................................. 6-25

#### FAI Connections

- FAI Scenarios ................................................................. 6-26
- FAI Modes ................................................................. 6-27
- F and K input Supervision ................................................... 6-28
- FAI without Latch ............................................................. 6-29
- FAI with Latch followed by Key Unlatch ............................ 6-30
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>State of F, K, and Relay Drive</td>
<td>6-31</td>
</tr>
<tr>
<td>Special Purpose Inputs</td>
<td>6-32</td>
</tr>
<tr>
<td>C•CURE 9000 Status Tab</td>
<td>6-34</td>
</tr>
</tbody>
</table>

## Chapter 7  
**Using the iSTAR Configuration Utility (ICU)**

- Overview                                                               | 7-2  |
- Configuring a Master Controller                                       | 7-3  |
- Troubleshooting Tools                                                 | 7-3  |
- General Configuration Procedure                                        | 7-4  |
- LAN Configurations                                                    | 7-4  |
- WAN Configurations                                                    | 7-5  |
- Copying the ICU onto a PC or Laptop                                   | 7-7  |
- Understanding the ICU                                                 | 7-8  |
  - Displaying and Updating Cluster Information                          | 7-8  |
- ICU Block Feature                                                     | 7-9  |
- Starting the ICU                                                       | 7-10 |
- Refreshing Controller Information                                      | 7-12 |
- Setting ICU Options                                                   | 7-12 |
  - Setting a Refresh Interval                                           | 7-13 |
  - Changing the ICU Password                                           | 7-14 |
  - Setting the Public IP Address for Firmware Downloads                 | 7-14 |
  - Setting the TCP/IP Port for Firmware Downloads                      | 7-14 |
- Using the ICU Window                                                  | 7-15 |
  - The Toolbar                                                          | 7-15 |
  - Icons                                                                | 7-16 |
  - Display Area                                                         | 7-18 |
  - Menu Bar                                                             | 7-21 |
  - Status Bar                                                          | 7-21 |
- Configuring a Controller                                              | 7-22 |
  - Prerequisite Information                                             | 7-22 |
- Configuring SNMP                                                      | 7-28 |
- Digital Certificate Signing and Restore Options                        | 7-32 |
Chapter 8  Web Page Diagnostics

Starting the Diagnostic Utility ..................................................8-2
Navigating the Diagnostic Utility ..............................................8-3
Viewing the Status Screen .........................................................8-4
Viewing the Cluster Information Screen ....................................8-7
Viewing the Object Store Database Screen .................................8-8
Diagnostic Screens .................................................................8-10
  Network Diagnostics ..............................................................8-10
  Reader and I/O Diagnostics ......................................................8-11
  SID Diagnostic Levels ............................................................8-12
    Displaying Diagnostic Information ......................................8-13
    To use the ICU to display diagnostic messages ......................8-13
iWatch2 Network Diagnostic Tool .............................................8-14
  Installation ........................................................................8-14
  Starting iWatch2 .................................................................8-14
    iWatch2 Opens ................................................................8-15
    iWatch2 Screen ...............................................................8-16
    iWatch2 Connects to iSTAR to Capture Data .........................8-17
    iWatch2 Fields .................................................................8-18
    Output File Commands .....................................................8-19
  iSTAR Diagnostic System .....................................................8-20

Chapter 9  Maintenance

Setting the LCD Message Display .............................................9-2
Displaying Status Messages .....................................................9-4
  Setting LCD Status Message Display ..................................9-4
iSTAR Edge Diagnostic Tests ..................................................9-5
  Card Reader Diagnostics .....................................................9-5
Table of Contents

Output Diagnostics ................................................................. 9-6
  Output Change Display (Slow Mode) .................................... 9-6
  Output Change Display (Fast Mode) ..................................... 9-7
  Output Test Mode .............................................................. 9-7
Input Change Display Mode ................................................... 9-7
Ethernet Port Test ................................................................. 9-8

Glossary

Index
This manual is designed for new and experienced security system users. The manual describes procedures for installing, configuring, and using the iSTAR Edge controller.

The manual assumes that you have already installed C•CURE and have familiarized yourself with the basic C•CURE information provided in the C•CURE Getting Started Guide.

In this preface
◆ How to Use this Manual .................................................. xii
◆ Finding More Information .................................................. xiii
◆ Conventions ................................................................. xiv
◆ Important Safety Information .......................................... xv
**How to Use this Manual**

This manual contains the following information:

<table>
<thead>
<tr>
<th>Chapter/Appendix</th>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1</td>
<td>Introducing iSTAR Edge</td>
<td>Provides basic information about iSTAR Edge, and includes an overview of iSTAR Edge hardware and features.</td>
</tr>
<tr>
<td>Chapter 2</td>
<td>Site Requirements</td>
<td>Provides physical requirements for iSTAR Edge configuration.</td>
</tr>
<tr>
<td>Chapter 3</td>
<td>iSTAR Edge Topology</td>
<td>Provides the information that you need to set up iSTAR Edge controllers for network communications.</td>
</tr>
<tr>
<td>Chapter 4</td>
<td>Power and Backup</td>
<td>Provides details of iSTAR Edge Power and Backup.</td>
</tr>
<tr>
<td>Chapter 5</td>
<td>iSTAR Edge Controls and Indicators</td>
<td>Describes the LEDs and indicators on iSTAR Edge.</td>
</tr>
<tr>
<td>Chapter 6</td>
<td>Connections</td>
<td>Provides wiring details for readers, I/O modules, Aux ports, wet and dry relay outputs, inputs, alarm inputs, and FAI (Fire Alarm Interface).</td>
</tr>
<tr>
<td>Chapter 7</td>
<td>Using the iSTAR Configuration Utility (ICU)</td>
<td>Provides instructions for configuring iSTAR Edge controllers using the iSTAR Configuration Utility (ICU).</td>
</tr>
<tr>
<td>Chapter 8</td>
<td>iSTAR Edge Web Page Diagnostic Utility</td>
<td>Describes how to monitor controllers and observe controller diagnostics.</td>
</tr>
<tr>
<td>Chapter 9</td>
<td>Maintenance and Diagnostics (LCD diagnostics and tests)</td>
<td>Describes how to monitor controllers and run controller diagnostics.</td>
</tr>
</tbody>
</table>
Finding More Information

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

Manuals

C•CURE software manuals and Software House hardware manuals are available in PDF format on the C•CURE DVD.

You can access the manuals from the Administration and Monitoring Station applications if you copy them from the DVD to the appropriate directory. See the C•CURE Installation Guide for more information.

The manuals are also available from the Software House Member Center.

To access the Software House Member Center, go to: http://www.swhouse.com/TechnicalLibrary/TechLibSW.aspx.

Online Help

You can access C•CURE help by pressing F1.
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.</td>
</tr>
<tr>
<td></td>
<td>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 your keyboard to press</td>
</tr>
<tr>
<td></td>
<td>- A screen element or name</td>
</tr>
<tr>
<td><em>Regular italic font</em></td>
<td>Indicates a new term, or a book title.</td>
</tr>
<tr>
<td><em>&lt;text&gt;</em></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.
Important Safety Information

Operating problems are often caused by failure to ground system components properly. Be sure to follow all instructions for grounding described in this document.

Changes to the iSTAR Edge not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

The following precautions apply to all procedures described in this manual.

1. To meet life safety requirements, a fail-safe mechanism override must be installed at each card reader exit to allow people to leave the secure area in case of electromechanical device failure.

2. The iSTAR Edge device described in this manual could cause electrical shock. Installation and maintenance should be performed only by qualified personnel. Make sure power is removed before the system is installed.

3. The iSTAR Edge and printed circuit boards in the reader devices are susceptible to damage by static electricity. When handling these devices:
   - Make sure your work area is safeguarded
   - Transport all components in static-shielded containers
The iSTAR Edge is a smaller, cost effective, 2 or 4 reader iSTAR that can be powered over its Ethernet connection using PoE, and is suitable for placement above or near the door. iSTAR Edge can be clustered with other iSTAR Edges and iSTAR eXs.

In This Chapter

- Overview and Introduction........................................................................................................... 1-2
- Main Features ............................................................................................................................ 1-5
- Product Comparison................................................................................................................... 1-10
Overview and Introduction

iSTAR Edge has:

- 8 onboard inputs plus 32 or 64* optional I8 inputs
- 4 onboard relay outputs plus 32 or 64* optional R8 outputs
- 2 onboard direct connect Wiegand reader connectors
- 3 serial ports for RMs, I8s, I8-CSIs, and R8s.
- 2 AUX power outputs for PIRs, etc.

* 4 Reader model supports 8 I/8s and 8 R/8s.

**NOTE** You cannot upgrade the iSTAR Edge 2 reader model to a 4 reader model.

iSTAR Edge Photograph

Figure 1-1 shows a photograph of the iSTAR Edge enclosure. The bright power LED will shine through the Power decal when the door is closed.

**Figure 1-1:** STAR Edge Photo
Figure 1-2 shows a photograph of the iSTAR Edge with an optional PoE board and with an I8 and R8 mounted on the door.

The 4 reader model can be ordered with 2 RM-4s mounted on the door.
Overview and Introduction

iSTAR Edge Layout

Figure 1-3: iSTAR EDGE Layout

- 4 Inputs
- AUX Output
- Wiegand Connector 1
- RM Port 1
- Relay 1
- Relay 2
- Power Fail
- Low Batt
- Power In
- Tamper
- E-net
- FAI Input
- Key Latch input
- USB Device Port (Not used)
- USB Host Ports
- AUX Output
- Wiegand Connector 2
- RM Port 2
- Relay 3
- Relay 4
Main Features

This section describes the iSTAR Edge main features.

Processor

- Atmel 9260 ARM processor, @ 180 MHz
- Compare iSTAR Pro @ 60 MHz, iSTAR eX @ 400 MHz

Storage

- > 250k cards.
- 64 MB of RAM.
- 128 MB of onboard flash.

Power

- Powered by
  - Ethernet connection: PoE or PoE Plus using optional add-on board (edgePower). A UL Listed surge protector must be used with the PoE module. The PoE board can supply either 12VDC or 24VDC to the relay outputs (selectable via a jumper on the PoE board).
  - or -
  - 12/24V DC, 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 @ 12V unswitched to external devices:
  - Wiegand readers
  - RS-485 ports
  - Two 2-pin Aux power connectors for PIRs and motion sensors.
- Provides power to relays:
  - Relays configurable to be wet or dry by jumper.
  - Wet Relays provide current at main input voltage (12 or 24V on PoE, 12 or 24V with external DC supply).
Main Features

- Each wet relay is limited to 0.75A (at 12 or 24V).
- Each dry relay is limited to 3.0A (at 12 or 24V).
- Full operating backup power is not provided by the board itself.
  - Achieved with apS, external UPS, or by backing up the Power Sourcing Equipment (PSE) in a PoE system.
- Upon loss of external power, data is written to onboard flash.
  - Four onboard non-rechargeable alkaline AA batteries provide power for the backup process and maintaining the clock afterwards.
  - Backup is valid for the period the onboard batteries can maintain the clock. The period has been tested for >3 days.

**NOTE**

On board battery backup retention was tested for 3 days but will last for weeks in actual practice.

AA battery backup time (3 days) has not been evaluated by UL.

- Health of onboard batteries is reported to user. Because batteries are non-rechargeable alkaline, their health can be monitored with reasonable accuracy.

Readers

- 2 or 4 readers total.
  - 2 Wiegand connectors are available.
  - 2 RMs are available to be configured for the 4 reader model to provide 4 Wiegand connectors.
  - 3 RS-485 serial ports are available.
  - Readers can be any combination of 2 from Wiegand ports and/or RMs on any of 3 serial ports.

I/O

- 8 general purpose inputs.
- 4 general purpose relays:
Main Features

- Dry or wet contact settable per relay by jumpers.
- 4-pin connectors to support NO/NC and dry/wet configurations.
- 2 reader model, 4- I8 and 4- R8 allowed to be configured on any of the three RS-485 ports.
- 4 reader model, 8- I8 and 8- R8 allowed to be configured on any of the three RS-485 ports or the optional 2 RM-4s.

Special purpose inputs:
- Tamper (from enclosure door)
- Main AC fail (from apS)
- Low external battery (from apS)
- FAI Supervision State (J40 F input)
- FAI Key Supervision State (J40 K input)

NOTE: The following 2 inputs to the host are determined by the firmware. There is no actual wiring to the iSTAR Edge board.

- FAI Relay Control
- Onboard battery low

- Large standard two-piece terminal blocks and spacing minimize the potential of mis-wiring.
- Connectors placed to allow (but not force) user to place all devices associated with one door on one side of the board, for 2 reader model.

- 3 RS 485 serial ports.

- USB Ports
  - 2 USB host ports. (These are the wide and flat USB connectors used by memory sticks, used when the iSTAR Edge is the host of the attached devices.)
  - 1 USB device port. (This is the square connector used when the iSTAR Edge itself is the client device.) (not currently used)
  - The only use of USB in the first version is to import encryption keys, in the same way as iSTAR eX.

- No serial debug port. Data is available using ICU iWatch2.
Main Features

Communications

- One 10/100 Ethernet port.
- No secondary communication path.
- Full 256 bit AES encryption, as with iSTAR eX
- Can cluster with other iSTAR Edges
- Can cluster with iSTAR eXs

FAI

- FAI (Fire Alarm Interface) - When the F (Fire) input is true, FAI activates relays that are enabled for FAI by individual enable switches.
- Latch option is available by switch control. If the selected relays are latched, they will be cleared to normal by the K (Key) input.

Onboard Controls

- LCD with backlight for diagnostics.
- Rotary switch for diagnostics, as with iSTAR eX.
- LEDs for serial, Ethernet, power and relay state.
  - 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.
- Reset button.
- Switches for serial termination of RM ports.
- Switches for selection of relays for control by FAI.
- Switch for FAI Latch.
- Jumpers for relay wet/dry control.
Main Features

Housing

- Enclosure is similar to RM 4e enclosure.
- Mountable in existing apC/L enclosure.

Compliance

- FCC, CE, EN50133, UL60950 by CB Scheme (International Safety) & RoHS.

2-Reader Models

Table 1-1: 2 Reader Models

<table>
<thead>
<tr>
<th>Model No.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESTAR002</td>
<td>2-reader iSTAR Edge in small enclosure</td>
</tr>
<tr>
<td>ESTAR002-PoE1</td>
<td>2-reader iSTAR Edge in small enclosure, with PoE/PoE+</td>
</tr>
<tr>
<td>ESTAR002-MB</td>
<td>2-reader iSTAR Edge, board only</td>
</tr>
</tbody>
</table>

4-Reader Models

Table 1-2: 4 Reader Models

<table>
<thead>
<tr>
<th>Model No.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESTAR004</td>
<td>4-reader iSTAR Edge in small enclosure</td>
</tr>
<tr>
<td>ESTAR004-RM</td>
<td>4-reader iSTAR Edge in small enclosure with 2 RM-4s on the enclosure door</td>
</tr>
<tr>
<td>ESTAR004-MB</td>
<td>4-reader iSTAR Edge, board only</td>
</tr>
</tbody>
</table>

Accessories

Table 1-3: Edge Accessories

<table>
<thead>
<tr>
<th>Model No.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESTAR-CAN</td>
<td>iSTAR Edge small enclosure, 12” x 12” with tamper switch</td>
</tr>
<tr>
<td>ESTAR-PoE1</td>
<td>iSTAR Edge PoE Plus Module 12/24 VDC</td>
</tr>
</tbody>
</table>
Table 1-4 compares the iSTAR Edge with other iSTAR controllers.

### Table 1-4: Product Comparison Table (i2, i3, i4 are firmware suffixes)

<table>
<thead>
<tr>
<th>Feature</th>
<th>iSTAR Edge i4</th>
<th>iSTAR eX i3</th>
<th>iSTAR Pro i2</th>
<th>iSTAR Classic i2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>ARM Atmel 9260</td>
<td>ARM Marvell PXA255</td>
<td>PowerPC Motorola MPC860</td>
<td>PowerPC Motorola MPC860</td>
</tr>
<tr>
<td>Speed, MHz</td>
<td>180</td>
<td>400</td>
<td>60</td>
<td>50</td>
</tr>
<tr>
<td>Win CE Version</td>
<td>5</td>
<td>5</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>RAM</td>
<td>64 mb</td>
<td>64 mb</td>
<td>64 mb</td>
<td>16 mb</td>
</tr>
<tr>
<td>Flash</td>
<td>128 mb</td>
<td>32 mb plus 256 mb on included CF Card</td>
<td>16 mb</td>
<td>8 mb</td>
</tr>
<tr>
<td>Cards - average card record</td>
<td>&gt;250k</td>
<td>&gt;250k</td>
<td>&gt;250k</td>
<td>27k</td>
</tr>
<tr>
<td>Cards - very large card record</td>
<td>&gt; 100k</td>
<td>&gt; 100k</td>
<td>&gt; 100k</td>
<td>10k</td>
</tr>
<tr>
<td>Cards - very small card record</td>
<td>&gt; 400k</td>
<td>&gt; 400k</td>
<td>&gt; 400k</td>
<td>45k</td>
</tr>
<tr>
<td>Full operating backup power provided</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>External backup power supported</td>
<td>apS, other external UPS or backup of Power Sourcing Equipment</td>
<td>Other external UPS, if wired correctly and our other hardware still used.</td>
<td>apS, other external UPS</td>
<td>apS, other external UPS</td>
</tr>
<tr>
<td>Power fail data backup</td>
<td>To onboard flash</td>
<td>To CF card</td>
<td>Sleep with memory retained by onboard batteries.</td>
<td>To flash simm</td>
</tr>
<tr>
<td>Event triggered data backup</td>
<td>To onboard flash</td>
<td>To CF card</td>
<td>To PC card</td>
<td>To flash simm</td>
</tr>
<tr>
<td>Onboard ethernet</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Secondary ethernet</td>
<td>Not supported</td>
<td>Onboard</td>
<td>Optional PC card</td>
<td>Optional PC card</td>
</tr>
<tr>
<td>Expansion connectors</td>
<td>USB, 2 host, 1 client</td>
<td>USB, 1 host</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
### Table 1-4: Product Comparison Table (i2, i3, i4 are firmware suffixes), continued

<table>
<thead>
<tr>
<th>Feature</th>
<th>iSTAR Edge i4</th>
<th>iSTAR eX i3</th>
<th>iSTAR Pro i2</th>
<th>iSTAR Classic i2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expansion functions</td>
<td>Encryption key transfer</td>
<td>Encryption key transfer, 8-reader expansion</td>
<td>2nd ethernet, dialup, event triggered backup.</td>
<td>2nd ethernet, dialup, event triggered backup.</td>
</tr>
<tr>
<td>supported</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dialup</td>
<td>no</td>
<td>no</td>
<td>yes, PC card, RAS</td>
<td>yes, PC card, RAS</td>
</tr>
<tr>
<td>Serial host comm</td>
<td>no</td>
<td>no</td>
<td>yes, RAS</td>
<td>yes, RAS</td>
</tr>
<tr>
<td>Total readers allowed</td>
<td>2 Reader - 2</td>
<td>4, 8 with USB key</td>
<td>8, 16 with second ACM</td>
<td>8, 16 with second ACM</td>
</tr>
<tr>
<td></td>
<td>4 Reader - 4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wiegand readers</td>
<td>2 Reader - 2</td>
<td>4</td>
<td>8, 16 with second ACM</td>
<td>8, 16 with second ACM</td>
</tr>
<tr>
<td></td>
<td>Wiegand</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4 Reader - 4</td>
<td>4</td>
<td>8, 16 with second ACM</td>
<td>8, 16 with second ACM</td>
</tr>
<tr>
<td></td>
<td>Wiegand</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RMs allowed</td>
<td>2 Reader - 2</td>
<td>4, 8 with USB key</td>
<td>8, 16 with second ACM</td>
<td>8, 16 with second ACM</td>
</tr>
<tr>
<td></td>
<td>RM rdrs.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4 Reader - 4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RM rdrs.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I8s allowed</td>
<td>2 Reader - 4</td>
<td>8</td>
<td>8, 16 with second ACM</td>
<td>8, 16 with second ACM</td>
</tr>
<tr>
<td></td>
<td>I/8s</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4 Reader - 8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I/8s</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R8s allowed</td>
<td>2 Reader - 4</td>
<td>8</td>
<td>8, 16 with second ACM</td>
<td>8, 16 with second ACM</td>
</tr>
<tr>
<td></td>
<td>R/8s</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4 Reader - 8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>R/8s</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wyreless (Readers/</td>
<td>-</td>
<td>16 (800 only)</td>
<td>16 (800 only)</td>
<td>16 (800 only)</td>
</tr>
<tr>
<td>PIMs)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>General purpose</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>serial ports</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>V. Strong, FIPS-197, AES 256, OpenSSL</td>
<td>V. Strong, FIPS-197, FIPS-140-2, AES 256, OpenSSL</td>
<td>RSA RC4 128 bit</td>
<td>RSA RC4 128 bit</td>
</tr>
<tr>
<td>General purpose</td>
<td>8</td>
<td>16</td>
<td>16, 32 with second ACM</td>
<td>16, 32 with second ACM</td>
</tr>
<tr>
<td>Inputs onboard</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Input resistor</td>
<td>15 choices per board, including dual range SWH 1K</td>
<td>15 choices per board, including dual range SWH 1K</td>
<td>SWH 1K dual range</td>
<td>SWH 1K dual range</td>
</tr>
<tr>
<td>configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Relays onboard</td>
<td>4</td>
<td>4</td>
<td>8, 16 with second ACM</td>
<td>8, 16 with second ACM</td>
</tr>
<tr>
<td>Open collector</td>
<td>-</td>
<td>4</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>outputs onboard</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Table 1-4: Product Comparison Table (i2, i3, i4 are firmware suffixes), continued

<table>
<thead>
<tr>
<th>Feature</th>
<th>iSTAR Edge i4</th>
<th>iSTAR eX i3</th>
<th>iSTAR Pro i2</th>
<th>iSTAR Classic i2</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAI</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>PoE</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Hosts</td>
<td>9000, 800</td>
<td>9000, 800</td>
<td>9000, 800</td>
<td>9000, 800</td>
</tr>
<tr>
<td>Clustering</td>
<td>16 iSTAR Edges/ iSTAR eXs</td>
<td>16 iSTAR Edges/ iSTAR eXs</td>
<td>16 Pros or Classics</td>
<td>16 Pros or Classics</td>
</tr>
<tr>
<td>Diagnostic LCD</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Site Requirements

This chapter provides information on site planning for iSTAR Edge hardware.

In This Chapter:

- Pre-Installation Planning ................................................................. 2-2
- Equipment Check ............................................................................. 2-2
- Site Check ........................................................................................ 2-2
- Voltage Requirements and Distance .............................................. 2-4
- Installation Requirements ............................................................... 2-5
- Environmental Requirements ........................................................ 2-5
- Individual/Total Loads .................................................................... 2-7
- Ethernet Requirements ................................................................. 2-11
- Wiring Requirements ..................................................................... 2-11
- Grounding Requirements ............................................................. 2-13
Pre-Installation Planning

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 Edge 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 20 lb. load.

Site Check

Ensure that the mounting site is ready:

- Mounting dimensions
  - The can is 12” by 12” (30.48 x 30.48 cm)
  - Upper mounting holes are 9” (22.86 cm) center to center.
  - Bottom mounting holes are 10.5” (26.67 cm) below the upper mount holes.
- The site has been approved and all wiring complies with UL requirements and other codes, as appropriate.
- All preliminary site work is complete.
- An appropriate power supply is accessible.
- The site is clean and free of dust or other contaminants.
iSTAR Edge Mounting Requirements

The mounting dimensions and board overlay are shown in Figure 2-1.

Figure 2-1: Mounting Requirements
Voltage Requirements and Distance

To operate properly, each reader must conform to voltage requirements.

- 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 Edge supplies 12 volts at its reader connectors; however, the amount of voltage that reaches the reader is impacted by the following:

- Number of devices on the bus
- Current draw of each device
- Wiring length between the devices and iSTAR Edge
- 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 Edge, 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.

Installation Tools

- Antistatic floor mat, tabletop mat, and wrist strap.
- Standard tool kit
- 3/32" (2.4 mm) screwdriver (supplied with iSTAR Edge)
- Security screwdriver (contact Software House)
- Small needlenose pliers; small Phillips screwdriver; wire strippers
- 5/16" (#10) nut driver (for securing shield wires to a ground stud)
Installation Requirements

This section describes iSTAR Edge hardware, software, environmental, and configuration requirements.

Host System Requirements

iSTAR Edge requires a host computer configured as a C•CURE system server/host that meets all the hardware and software requirements for servers described in the C•CURE Installation Guide.

iSTAR Edge Cabinet Requirements

The iSTAR Edge cabinet must conform to the specifications shown in Table 2-1.

<table>
<thead>
<tr>
<th>Item</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weight</td>
<td>&lt;10 lbs (&lt;4.6 kg)</td>
</tr>
<tr>
<td>Height</td>
<td>12&quot; (30.48 cm)</td>
</tr>
<tr>
<td>Width</td>
<td>12&quot; (30.48 cm)</td>
</tr>
<tr>
<td>Depth</td>
<td>4.5&quot; (11.4 cm)</td>
</tr>
</tbody>
</table>

Environmental Requirements

Table 2-2 shows the iSTAR Edge environmental requirements.

<table>
<thead>
<tr>
<th>Status</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>32° F (0° C) to 120° F (48.9° C)</td>
</tr>
<tr>
<td>Storage</td>
<td>4° F (-20° C) to 158° F (70° C)</td>
</tr>
</tbody>
</table>
**Installation Requirements**

## Power Requirements

The standard iSTAR Edge uses a UL Listed 603 External Power Supply, such as the Software House apS or uses a Power Over Ethernet (PoE) injector with UL listed surge protector.

To ensure adequate power, calculate the total power requirements of iSTAR Edge and its related hardware, as follows.

- Add the total current power for components in the system (modules, relays, optional modules, readers, and wire resistance).
- Use the information in Table 2-3 through Table 2-8 to compute the current draw of components attached to iSTAR Edge.

### NOTE

See Chapter 4, “iSTAR Edge Power and Backup” for more details about iSTAR Power.

### iSTAR Edge Components and Boards

Table 2-3 shows the power requirements of iSTAR Edge components and attached boards.

<table>
<thead>
<tr>
<th>Component/Board</th>
<th>Current Draw at 12VDC</th>
</tr>
</thead>
<tbody>
<tr>
<td>iSTAR Edge</td>
<td>400 mA with LCD - no load</td>
</tr>
</tbody>
</table>
| RM-4 board\(^a\) | 80 mA without LCD - no load  
|                 | 180 mA with LCD - no load |
| RM-4E board\(^b\) | 125 mA - no load |
| I/8 board       | 125 mA - no load |
| R/8 board       | 150 mA - no active relays.  
|                 | Add 20 mA for each active relay |

\(^a\) RM-4 board has only been evaluated by UL with RM Series readers (RM 1,2,3)

\(^b\) RM-4E boards have only been evaluated by UL for use with RM-DCM-2 enclosure.
iSTAR Edge Input Power Rating

The iSTAR Edge has the following input ratings when using an external power supply:

- 12 VDC, 3.8 A
- 24 VDC, 3.1 A

Individual/Total Loads

- RS-485 Reader Power Outputs: 10.6-12.5 VDC, 1.5 A max each.
- Wiegand Reader Power Outputs: 10.6-12.5 VDC, 350 mA max each.
- Total of all Reader and AUX outputs combined (RS-485 & Wiegand) not to exceed 1.5 A
- Four (4) activated relay coils = 100 mA, 25 mA/relay
- One I/8 module - 12 VDC, total= 125 mA
- One R/8 module - 12 VDC, total= 325 mA (125 ma + 25 mA for each active relay (max 4))
- R/8 relay contact ratings – 30 VDC at 3A (resistive)
iSTAR Edge Wiegand Reader Ports

Table 2-4 shows the maximum ratings for iSTAR Edge Wiegand direct reader ports.

<table>
<thead>
<tr>
<th>Port</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reader output control</td>
<td>Low = 0 v to 0.8 v</td>
</tr>
<tr>
<td>(red, green, yellow, beeper)</td>
<td>High = 4.0 v to 5.25 v</td>
</tr>
<tr>
<td></td>
<td>20 mA maximum</td>
</tr>
<tr>
<td>Reader input data lines</td>
<td>Low = 0 v to 0.8 v</td>
</tr>
<tr>
<td>(D0, D1)</td>
<td>High = 4.0 v to 5.25 v</td>
</tr>
<tr>
<td>Reader output voltage</td>
<td>+12 VDC</td>
</tr>
<tr>
<td>Reader current</td>
<td>350 mA max per reader, not to exceed 1.5 A for Readers and AUXs</td>
</tr>
</tbody>
</table>

Table 2-5 shows maximum rating for RM Reader ports.

<table>
<thead>
<tr>
<th>Port</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reader output voltage</td>
<td>+12 VDC</td>
</tr>
<tr>
<td>Reader current</td>
<td>1.5 A max per port, not to exceed 1.5 A for Readers and AUXs</td>
</tr>
</tbody>
</table>
Software House Readers

Table 2-6 shows power requirements for Software House readers.

**Table 2-6:** Software House Reader Power Requirements

<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</td>
<td>300 mA max</td>
</tr>
<tr>
<td>RM with Multi-Technology Reader and LCD</td>
<td>RM2L-4000</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 mullion</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 mullion</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>Contactless Smart Card Reader</td>
<td>SWH-2100&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>300 mA max</td>
</tr>
<tr>
<td>RM with HID iClass and LCD</td>
<td>RM2L-IC</td>
<td>300 mA max</td>
</tr>
</tbody>
</table>

<sup>a</sup> In Table 2-6, <sup>a</sup> indicates readers that have not been evaluated for use with the iSTAR Edge. All other readers in Table 2-6 are UL Listed compatible readers that can be used with the iSTAR Edge.
Third Party Readers

Table 2-7 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</td>
</tr>
</tbody>
</table>

NOTE: The readers in Table 2-7 have not been evaluated by UL for use with the iSTAR Edge.
### Ethernet Requirements

The iSTAR Edge Ethernet connection is:

- **Onboard 1 Ethernet port** – supports 10/100Base-T Ethernet connections.

### Wiring Requirements

Table 2-8 shows general wiring requirements for an iSTAR Edge and its components.

**Table 2-8: 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, two wire</td>
<td>iSTAR Edge</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>Power</td>
<td>iSTAR Edge</td>
<td>RM &amp; I/O Modules</td>
<td>8442/8461</td>
<td>22/18</td>
<td>1</td>
<td>No</td>
<td>Range of 600 ft. to 1500 ft. depends on AWG</td>
<td>See Note b</td>
</tr>
<tr>
<td>RJ45-Ethernet</td>
<td>iSTAR Edge</td>
<td>Hub, Host</td>
<td>N/A</td>
<td>Cat 5 or more 24</td>
<td>2</td>
<td>N/A</td>
<td>328 ft. (100 m)</td>
<td>8.4 Ω</td>
</tr>
<tr>
<td>Supervised Input</td>
<td>iSTAR Edge 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>32Ω</td>
</tr>
<tr>
<td>Request-to-exit (REX or RTE)</td>
<td>iSTAR Edge 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>32Ω</td>
</tr>
<tr>
<td>Door contact (DSM)</td>
<td>iSTAR Edge 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>32Ω</td>
</tr>
<tr>
<td>Supervised Input (UL) Note a</td>
<td>iSTAR Edge 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>32Ω</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>
</tbody>
</table>
## Installation Requirements

**Table 2-8: 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>Reader Data</td>
<td>iSTAR Edge 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>

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

b. 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**
UL Listed Panic hardware shall be used to allow emergency exit from a protected area.

**NOTE**
For UL Listed products, burglar alarm inputs must be supervised.

**NOTE**
For UL Listed applications, USB connections must be no more than 25 ft. from iSTAR Edge controllers.
Grounding Requirements

Grounding requirements are as follows:

- Ensure that the iSTAR Edge controller is properly connected to an earth ground at the ground stud in the cabinet. Identified by symbol.) Use 16 AWG or larger wire.

- Ensure that the shield wires for the readers, inputs, outputs, and AUX cables are grounded to the nearest earth/ground connection at one end only of the cable.

- Disconnect the ground wire last to provide maximum protection to the equipment and personnel.

NOTE

All cabling must be shielded.
This chapter provides an overview of iSTAR Edge/eX topology and configuration options.

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

In This Chapter

- iSTAR Edge Network Topology ................................................................. 3-2
- Cluster Configuration .................................................................................. 3-6
- Single Master and Alternate Master Configurations ................................. 3-7
- Maintaining Cluster Communication ......................................................... 3-10
- Adding Controllers to the Cluster ............................................................ 3-13
- Configuring Communication Paths .......................................................... 3-14
iSTAR Edge Network Topology

iSTAR Edge supports communications over 100Base-T and/or 10Base-T Ethernet networks using TCP/IP.

Lan and Wan Configurations

The TCP/IP protocol transfers data across a number of networks. Because iSTAR Edge controllers use the TCP/IP protocol for network communications, they can communicate with each other even when controllers are located on different networks separated by other network platforms, as shown in Figure 3-1.

Figure 3-1: Sample iSTAR Edge/eX Network

Gateways and Firewalls

iSTAR Edge/eX 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.
iSTAR Edge/eX configurations that accept translated network addresses are usually managed at the remote site.

During firewall configuration the following TCP/IP ports must be open:

- 1999
- 2001
- 2800-2802
- 28000-28010

Local Address Management

Although it is not required, System Managers who want to maintain local address management can configure iSTAR Edge/eX with locked IP addresses. Locked IP addresses retain the iSTAR Edge/eX address that is specified locally or by a local Dynamic Host Configuration Protocol (DHCP) server. When IP addresses are locked, iSTAR Edge/eX 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 Edge/eX 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.
IP Management Tools

iSTAR Edge/eX 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.
Using NetBIOS and 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 NetBIOS or 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 NetBIOS and FQDNs. If you specify a NetBIOS or 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 Edge/eX controllers are organized for network communications into user-defined, logical groups called clusters. Clusters contain one or more iSTAR Edge/eX controllers. A host can be connected to several clusters. This section describes the key elements of an iSTAR Edge/eX cluster.

**NOTE** For UL Listed products, all controllers and networking equipment in a cluster must be UL Listed.

**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, 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**

[Diagram showing cluster member communications]
Single Master and Alternate Master Configurations

To ensure continuous connection, the iSTAR Edge/eX cluster can communicate with C•CURE via:

- A primary and optional secondary path configured on a single master controller (iSTAR eX only.)
- A primary path on a master controller and an optional secondary path on an alternate controller. (iSTAR eX or Edge.)

Figure 3-4 shows primary and secondary communications using a single master (on the left side of the diagram) and alternate master (on the right side of the diagram).

Figure 3-4: Single and Alternate Master Configurations

Single Master Configuration

Alternate Master Configuration

NOTE

The iSTAR Edge only has one ethernet connection. If an iSTAR Edge is the Master, there is no secondary communications connection.

NOTE

For UL Listed products, UL has only evaluated the Primary communications path.
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.

Cluster members are connected to the master only via a 10/100Base-T network connection.

*Figure 3-5* shows the primary path for cluster member A.

*Figure 3-5: The Primary Path*
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, or if the master controller fails. Figure 3-5 on page 3-8 shows the configuration options for primary and secondary communications.

Figure 3-6 shows two examples of secondary communications:

- A secondary path on a single master configuration using two network connections (on the left side of the diagram).
- A secondary path on the alternate master (on the right side of the diagram). Configurations that use an alternate master must connect to the host over 10/100Base-T Ethernet on both primary and secondary paths.

**NOTE**

The iSTAR Edge only has one ethernet connection. If an iSTAR Edge is the Master, there is no secondary communications connection.
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:

- 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
Alternate Master Configuration

If the master loses its network connection with the host, or if the master hardware fails, a secondary path can connect an alternate master and the host (Figure 3-8).

The following describes the sequence of events:

- The alternate master establishes a connection with the host via the secondary path.
- Cluster members establish connections with the alternate master via the network.
- The alternate master sends the cluster members’ messages to the host, and also sends messages from member to member.

*Figure 3-8: Communication Failure with Alternate Master Configuration*
### Communication Between Members and Master

If a cluster member loses its connection with the master and the secondary path is a connection between the host and an alternate master (Figure 3-9):

- The cluster member connects directly to the alternate master.
- The alternate master passes the cluster members’ messages to the host.

**Figure 3-9:** Re-establishing Connections During Communication Failure

[Diagram showing communication flow between host, hub, master, and alternate master with numbered arrows indicating the path of messages.]
Adding Controllers to the Cluster

Follow these guidelines when adding iSTAR Edge/eX 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. There cannot be a secondary path to an iSTAR Edge Master, but the secondary path can be used to connect to an Alternate Master that is an iSTAR Edge.

- 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 method between the master and the C•CURE host:
  - Onboard 1 Ethernet (default)
  - Onboard 2 Ethernet (iSTAR eX only.)
- 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 (although an alternate master may be designated for secondary communications).
- 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 a controller responsible for secondary communications with the C•CURE host when a communications failure occurs on the primary path.
- Specifying the connection type.
This chapter describes the detail of iSTAR Edge Power, backup batteries, and system backups.

In This Chapter

- Power General ................................................................. 4-3
- Power in ............................................................................. 4-7
- Onboard backup batteries .................................................. 4-8
- Backup ............................................................................ 4-8
- Power Out ........................................................................ 4-11
Power - Batteries - Backup

As indicated on the door map shown in Figure 4-1, the following are power specifications for the iSTAR Edge:

- **Entire Unit**
  - Local Power 12 VDC, 3.8 Amp Max.
  - Local Power 24 VDC, 3.1 Amp Max.

- **Reader and I/O Module Supply (Total of AUX, RM, and Wiegand Ports)**
  - 12 VDC, 1.5 Amp
    - AUX Ports 12 VDC 350 mA each
    - RM Ports 12 VDC, 1.5 Amp each (but the max. is also 1.5 Amp for all)
    - Wiegand Ports, 12 VDC, 350 mA each

- **Relays**
  - 30 VAC/DC 3.0 Amp Max. (Dry) each
  - 12 or 24 VDC 0.75 Amp Max. (Wet) each

*Figure 4-1: Specifications*
Power General

The iSTAR Edge can be powered by PoE, PoE Plus, or traditional 12V or 24V DC power supplies. PoE and PoE Plus provide a method to significantly reduce installation costs using 100 meters of ethernet cable for both power and data to the controller.

- PoE (IEEE 802.3af) installation is limited to 12.95W of power consumption including the controller. This translates to about 1.1 Amps.
- PoE Plus (IEEE 802.3at) installation is limited to 25.5W of power consumption including the controller. This translates to about 2.125 Amps.

A UL Listed surge protector must be used with the PoE module.

Careful selection of components allows a 1-door system to operate from PoE and a 2-door system to operate from PoE Plus. There is no standard 4 reader model that includes PoE, but it is possible to order the PoE module separately.

Traditional power supplies include:

- An apS
Any external UPS (12/24 VDC)

**NOTE**

For UL Listed products, a UL 603 Listed, power-limited power supply must be used.

**Alternate Power**

For those systems that exceed these limits, alternate DC supplies can be deployed including external PoE splitters.

Alternate DC supplies are installed by the customer per the requirements of the particular installation. When alternate DC supplies are deployed for devices on the relay circuits, the relays circuits are configured as *dry*. The devices/loads do not source power from the iSTAR Edge and are removed from the power budget calculation.

Devices commonly referred to as *PoE splitters* are installed directly to CAT5/6 cabling and reduce installation costs. If spare PoE/Poe Plus ports are not available in the system, *PoE injectors* can be used at the source of the CAT5/6 cable.

**Power Logic**

The PoE module has a jumper that determines whether the module provides 12VDC or 24VDC.

In general, the iSTAR Edge automatically determines whether it is running off of 12V or 24V DC. Once the iSTAR Edge is running off of 24V, however, it does not automatically switch back to 12V without user intervention.

The iSTAR Edge, along with the PoE board, treat all sources of external power, including all flavors of PoE and external DC supplies basically the same way: iSTAR Edge monitors the input voltage.

When that voltage moves outside of the normal operating voltage range (10.2 V - 14.4 V for 12 V nominal systems or below 20.4 V for 24 V nominal systems), iSTAR Edge firmware stops its internal processes and writes all data to onboard flash, and then will *cycle*, continuously monitoring the input power voltage until either of these two conditions occurs:

- If the input power voltage goes below a *Wake-up threshold* of 7 V, the iSTAR Edge will go to sleep;
If the voltage returns to the normal operating range, the iSTAR Edge will reboot and restart.

If the iSTAR Edge goes to sleep, it will automatically *wake-up* when the input power voltage rises above the *Wake-up threshold*, and the firmware will reboot and load the backed up data into RAM.

Additionally, when iSTAR Edge is *asleep*, it will wake up periodically (once every 5 minutes) to see if main power has returned to the normal operating range, and if it has, the iSTAR Edge will reboot, or if the voltage is still below the *Wake-up threshold*, the iSTAR Edge will go back into its *sleep* state.

**Batteries**

When onboard batteries are installed they must be *fresh* (they must produce more than 5V), otherwise a *too low* battery-cut circuit will disconnect them. The LCD will display information about the state of the batteries.

**Other Interactions**

All of iSTAR Edge's other interactions with the power system are essentially *informational* in nature and do not directly affect iSTAR Edge's 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. From the iSTAR Edge's point of view, however, this is incidental. It does not affect how iSTAR Edge treats power loss. iSTAR Edge 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.

**Other interactions with the power system include:**

**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, as with iSTAR eX, iSTAR Pro.

**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.
- Configured on host as unsupervised input, as with iSTAR eX, iSTAR Pro.

**Onboard Battery Low input**

- Internal measurement (no connections necessary) of onboard AA alkaline batteries.
- Active if their voltage is below 4.6 volts or they are not present or one or more of them is not making full connection.
- This informs user that they should replace the onboard backup batteries for this controller as soon as possible.
- No need to power down the controller to remove/replace the batteries
- Onboard batteries are alkaline and non-rechargeable, so this is a reasonably accurate measure of when the batteries need to be changed.
- Configured on host as an unsupervised input. This is a new input not present in iSTAR eX or iSTAR Pro.

**PoE Board Installed**

- Internal sensing of whether PoE module is attached.
- Is visible to user in the Status Tab of the iSTAR Edge Controller editor in the C•CURE Application program. The PoE module should only be installed or removed when board is entirely powered off.
Power in 12 / 24 V DC

iSTAR Edge can run off either 12VDC or 24 VDC power applied to the PWR connector. Normal operating ranges include:

- 12V operation: 10.2 V to 14.4 V (-15/+20%)
- 24V operation: 20.4 to 30.0 V (-15/+25%)

Configuration for either 12V or 24V operation is stored in flash. As shipped from the factory, or after performing a Clear Memory operation, iSTAR Edge is configured for 12V. During boot up, the iSTAR Edge detects an input power voltage as either 12 or 24V VDC and automatically sets the operation accordingly.

The iSTAR Edge will not automatically re-adjust back from 24V to 12V. This is because a measurement of 12V input power could indicate a 12V supply or a 24V supply with a very low battery.

To set the board back to 12V from 24V, manual intervention is required:

1. Remove external power from the iSTAR Edge.
2. Select position 9 on the rotary switch.
3. Connect a power supply of the desired voltage (12V or 24V) to the iSTAR Edge.
4. Watch the LCD for the message to reset the board.
5. Select position 0 (or other desired position other than 9).
6. Press RESET button.

NOTE
The Tamper, Low Battery, and AC power fail inputs must be enabled and connected to report for compliance with UL requirements.

NOTE
Shielded cable must be used for AC Fail & Low Battery Input connections.
The board will also be set back to 12 VDC if the memory is cleared using position D on the rotary switch.

The iSTAR Edge Wiegand reader power, RS-485 serial port power and AUX power are always configured at 12 VDC.

The Relay Wetted power is either 12 VDC or 24 VDC, depending on the input power source.

### Onboard backup batteries

iSTAR Edge uses four onboard AA batteries to power backup to flash on loss of main input power. These batteries must be non-rechargeable Alkaline batteries, specifically:

- AA
- Alkaline
- 2.5 Amp hour
- Button top

In order to prevent voltages that partially run the processor, the iSTAR Edge has a battery-cut circuit. When the batteries fall below 4V, they are disconnected from the rest of the board.

The user has an onboard battery low input configured in the host that will indicate when the onboard batteries need to be changed. This input will be active when batteries are not present, not making contact, or too low to guarantee a backup and three days of power for the clock. The user should replace the batteries immediately when this input is active.

### Backup

iSTAR Edge handles backup in essentially the same way as iSTAR Classic and iSTAR Ex. When power (input voltage) drops too low to support full operation, power usage is reduced as much as possible, processes are stopped and data is written into flash. Processes remain stopped until the input voltage returns to a normal operating range. At that point, iSTAR Edge reboots and reloads data from flash to RAM and starts processing again.

The only input that controls the initiation of iSTAR Edge’s power-fail backup process is iSTAR Edge’s own onboard measurement of incoming power voltage. iSTAR Edge measures external power voltage every 1/10 of a second. When external power voltage moves outside of normal operating
Voltage (10.2 V to 14.4 V for nominal 12 V operation, or below 20.4 V for nominal 24 V operation), iSTAR Edge will initiate the backup process.

When the backup process starts iSTAR Edge will:

- Cut power to as many non-critical devices as possible, including:
  - LEDs
  - LCD backlight
  - Wiegand readers
  - AUX power ports
  - WET relays
  - Relay coils are de-energized, i.e. relays revert to normal state - NO contacts open and NC contacts close.

- Set the following devices to low power or shutdown mode
  - Ethernet circuit
  - Serial transceivers

- Stop all processes
- Write data in RAM to flash.
- iSTAR Edge issues an activity report indicating a backup is beginning.
- As with iSTAR Classic and iSTAR eX, the backup process will finish even if power returns during the backup process.

When the backup completes, iSTAR Edge will check whether power voltage has returned to normal operating range.

If the voltage is within the normal range, iSTAR Edge will reboot.

If the voltage is below the hardware Wake-up Threshold (7 V) the iSTAR Edge will go into a sleep state: an alarm will be programmed for 5 minutes, and then the processor will cut its power to its own core.

The Real Time Clock inside the processor will remain powered from the iSTAR Edge onboard batteries.

When the clock reaches the alarm time, it will restore power to the processor core, causing it to start the reboot process. Early in the boot process, iSTAR
Edge will measure the input power voltage. If the voltage is (still) below the hardware Wake-up Threshold the iSTAR Edge will go back to sleep.

This cycle will continue until the input power voltage is at least above the hardware Wake-up threshold. In addition to the alarm, the iSTAR Edge has a circuit to detect that the input power voltage has risen above the Wake-up Threshold, in which case the circuit will trigger the iSTAR Edge processor to begin the reboot process immediately.

If the bootloader determines the input power voltage is above the hardware Wake-up Threshold it will load the firmware image from FLASH into RAM and execute it. During the image startup process, the input power voltage is measured again. If the voltage has returned to the normal operating range, the image startup process will continue. If the input power voltage is below the hardware Wake-up Threshold, the iSTAR Edge will put itself back into the sleep and power down the processor. The iSTAR Edge startup process will not continue until either of these conditions is met.

Near the end of the boot process, iSTAR Edge, like iSTAR Classic, iSTAR Pro and iSTAR eX, looks for a valid backup in flash. If it finds one, it restores the data in that backup to RAM, and then runs the processes that depend on that data.

If the onboard battery voltage was above the 4.6 V Onboard Battery Low threshold (as reported to user with Onboard battery low input) before the backup started, the iSTAR Edge onboard batteries will be able to power the clock for at least 3 days (more when the batteries are fresh).

As with iSTAR Classic, iSTAR Pro and iSTAR eX, data can only be restored if the clock is valid when the iSTAR boots. Otherwise, the firmware would not be able to make valid access control decisions. As with iSTAR Pro, iSTAR Classic and iSTAR eX, if the clock is not valid on reboot the iSTAR will not restore any data, and will in fact invalidate all data, including activity history.

If the onboard batteries were reported as low at time of backup, no guarantees are made about how long the clock, and therefore the backup, can be maintained. For iSTAR Classic, iSTAR Pro, and iSTAR eX, the check for available main power starts every time the board boots, not just when it reboots out of sleep following power loss.
Power Out

iSTAR Edge has various ways to provide power to external devices:

- The following power outputs combined can provide a total of 1.5A at 12V.
  - each of three serial ports
  - each of two Wiegand ports
  - each of two aux ports, suitable, for example, for motion sensor power.
- The relays can be configured by jumper to provide wet power.
  - Each relay is limited to 0.75A by an individual resettable fuse.
  - If one load is shorted the individual fuse limits the shutdown to the shorted load
  - Power fed to wetted relay contacts is either 12V or 24VDC depending on the input voltage from PoE or an external power supply.
- USB provides 500mA at 5V for each device port. Each port has a resettable fuse, this meets the USB standard and should not be exceeded by a well functioning device.

If powered by an external DC supply the amount of power available will depend on that supply, subject to the above limits.

The user may want to modify the power budget by inserting the limits of the external DC supply to determine the appropriate equipment that can be attached to the iSTAR Edge.

PoE and PoE Plus have the following power limits

- PoE provides 12.95W with 100 meters of cable between PSE (Power Sourcing Equipment) and iSTAR Edge
- PoE Plus provides 25.5W with 100 meters of cable between PSE and iSTAR Edge
- Cable length is part of the power budget, i.e. a shorter cable increases available power, e.g. PoE Plus provides about 10% more power with 50 meters of cable between PSE and iSTAR Edge

**NOTE**

USB interface was not evaluated by UL.
iSTAR Edge Controls and Displays

This chapter explains the switches, buttons, jumpers, LEDs, and the LCD.

In This Chapter

◆ LCD ................................................................. 5-3
◆ LEDs ....................................................................... 5-3
◆ Onboard controls ................................................. 5-6
◆ Reset button .......................................................... 5-6
◆ Switches and Jumpers ........................................... 5-6
◆ RM Port Termination Switches .......................... 5-8
◆ Output Relay Wet or Dry Jumpers ...................... 5-8
◆ PoE Jumpers .......................................................... 5-8
Controls and Displays

Switches-Jumpers-LEDs

Figure 5-1 shows the location of the Switches, Jumpers, and LEDs.

Figure 5-1: Switches, Jumpers, LEDs
Visual Indicators

LCD

LCD will display diagnostic messages in a similar way to the iSTAR eX. As with the iSTAR eX and iSTAR Pro, LCD is for diagnostics, not access control.

- Diagnostics are controlled by the rotary switch, SW1. See “Rotary switch” on page 5-7.
- Contrast controlled by potentiometer, RV1.
- Backlight is on when door is open, off when door is closed, and during power-fail backups.

Common displays are:

- Master Connected or Host Connected
- IP address of Host or Master
- Name of iSTAR Edge and MAC address
- IP address of iSTAR Edge
- Battery Voltage
- Member or Master with Date and Time
- Configured Power and Measured Power
- Cluster Connected or Split
- Indication of whether a DB has been restored.
- Results of diagnostics

LEDs

The super-bright white Power LED is illuminated when the enclosure door is closed, i.e. when the tamper switch closes. The power LED has varying brightness from 12V to 24V and 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 backlight and all LEDs other than the power LED and the
Controls and Displays

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 backlight and LEDs other than Power LED, the Bright White external view Power LED, and the relay activation LEDs to be always be off, regardless of tamper state.

Table 5-1 below summarizes the operation of the LEDs.

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Input power good, door closed</th>
<th>Input power good, door open</th>
<th>Input power lost, backing up/sleeping</th>
<th>Input power &lt; 8V</th>
<th>Controlled by</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power LED</td>
<td>On</td>
<td>On</td>
<td>n/a</td>
<td>Off</td>
<td>Hardware</td>
</tr>
<tr>
<td>Bright White LED</td>
<td>On</td>
<td>Off</td>
<td>Off</td>
<td>n/a</td>
<td>Firmware</td>
</tr>
<tr>
<td>Relay Activation LEDs</td>
<td>On</td>
<td>On</td>
<td>Off</td>
<td>Off</td>
<td>Firmware</td>
</tr>
<tr>
<td>All other indicators, and LCD backlight</td>
<td>Off</td>
<td>On</td>
<td>Off</td>
<td>n/a</td>
<td>Firmware</td>
</tr>
<tr>
<td>All other indicators, and LCD backlight if configured OFF in host</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>n/a</td>
<td>Firmware</td>
</tr>
</tbody>
</table>

**NOTE** The iSTAR Edge LCD display and associated diagnostic tests have not been evaluated by UL.
Table 5-2 summarizes the function and designation of each LED.

**Table 5-2: Functions of LEDs**

<table>
<thead>
<tr>
<th>LED</th>
<th>Function</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS21</td>
<td><strong>Main Power - Internal View</strong></td>
<td>Always on if Voltage in &gt; 8V</td>
</tr>
<tr>
<td>DS20</td>
<td><strong>Main Power - External View</strong></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></td>
<td><strong>Relay Outputs</strong></td>
<td></td>
</tr>
<tr>
<td>DS15</td>
<td>Output 1 NO Closed</td>
<td>Always on if Voltage in &gt; 8V</td>
</tr>
<tr>
<td>DS14</td>
<td>Output 2 NO Closed</td>
<td>Always on if Voltage in &gt; 8V</td>
</tr>
<tr>
<td>DS13</td>
<td>Output 3 NO Closed</td>
<td>Always on if Voltage in &gt; 8V</td>
</tr>
<tr>
<td>DS8</td>
<td>Output 4 NO Closed</td>
<td>Always on if Voltage in &gt; 8V</td>
</tr>
<tr>
<td></td>
<td><strong>Ethernet</strong></td>
<td></td>
</tr>
<tr>
<td>DS4</td>
<td>Ethernet Activity</td>
<td>Off when door is closed</td>
</tr>
<tr>
<td>DS2</td>
<td>Ethernet Full Duplex</td>
<td>Off when door is closed</td>
</tr>
<tr>
<td>DS3</td>
<td>Ethernet 100 Mbps</td>
<td>Off when door is closed</td>
</tr>
<tr>
<td></td>
<td><strong>Serial</strong></td>
<td></td>
</tr>
<tr>
<td>DS17</td>
<td>RS-485-1 Tx</td>
<td>Off when door is closed</td>
</tr>
<tr>
<td>DS19</td>
<td>RS-485-1 Rx</td>
<td>Off when door is closed</td>
</tr>
<tr>
<td>DS12</td>
<td>RS-485-2 Tx</td>
<td>Off when door is closed</td>
</tr>
<tr>
<td>DS11</td>
<td>RS-485-2 Rx</td>
<td>Off when door is closed</td>
</tr>
<tr>
<td>DS10</td>
<td>RS-485-3 Tx</td>
<td>Off when door is closed</td>
</tr>
<tr>
<td>DS9</td>
<td>RS-485-3 Rx</td>
<td>Off when door is closed</td>
</tr>
</tbody>
</table>
Onboard controls

Reset button

Does a hard reset of processor and as many peripherals as possible. Causes all RAM to be erased. Flash, including backups and ICU configuration information, is not erased. As with iSTAR eX, use Rotary switch position D to clear flash and restore factory defaults.

Switches and Jumpers

Table 5-3 provides a list of switches and jumpers.

<table>
<thead>
<tr>
<th>Ref</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW1</td>
<td>Rotary</td>
<td>Diagnostics, restore factory default and other options.</td>
</tr>
<tr>
<td>SW2</td>
<td>DIP Slide</td>
<td>Allow FAI to activate Relay1</td>
</tr>
<tr>
<td>SW3</td>
<td>DIP Slide</td>
<td>Allow FAI to activate Relay2</td>
</tr>
<tr>
<td>SW4</td>
<td>DIP Slide</td>
<td>Allow FAI to activate Relay3</td>
</tr>
<tr>
<td>SW5</td>
<td>DIP Slide</td>
<td>Allow FAI to activate Relay4</td>
</tr>
<tr>
<td>SW6</td>
<td>DIP Slide</td>
<td>FAI Latch Enable</td>
</tr>
<tr>
<td>SW7</td>
<td>Dual DIP Slide</td>
<td>RS485-3 Termination</td>
</tr>
<tr>
<td>SW8</td>
<td>Dual DIP Slide</td>
<td>RS485-2 Termination</td>
</tr>
<tr>
<td>SW9</td>
<td>Dual DIP Slide</td>
<td>RS485-1 Termination</td>
</tr>
<tr>
<td>SW10</td>
<td>Push button</td>
<td>Reset</td>
</tr>
<tr>
<td>J10</td>
<td>Jumper</td>
<td>Relay Output 1 Source/Dry</td>
</tr>
<tr>
<td>J5</td>
<td>Jumper</td>
<td>Relay Output 2 Source/Dry</td>
</tr>
<tr>
<td>J11</td>
<td>Jumper</td>
<td>Relay Output 3 Source/Dry</td>
</tr>
<tr>
<td>J23</td>
<td>jumper</td>
<td>Relay Output 4 Source/Dry</td>
</tr>
<tr>
<td>PoE Board - J2</td>
<td>Jumper</td>
<td>Select PoE or PoE+</td>
</tr>
<tr>
<td>PoE Board - J3</td>
<td>Jumper</td>
<td>Select 12VDC or 24VDC input to Edge</td>
</tr>
</tbody>
</table>
Rotary switch

There is an onboard 16 position rotary switch, SW1. Most of the positions are used to control LCD diagnostics, and is similar to iSTAR eX.

Table 5-4 is a reference table for iSTAR Edge 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 output changes (does not include readers and R/8 boards), 1 second LCD display (fast mode)</td>
</tr>
<tr>
<td>7</td>
<td>Activate output test mode (include readers and R/8 boards)</td>
</tr>
<tr>
<td>8</td>
<td>Test Onboard Ethernet</td>
</tr>
<tr>
<td>9</td>
<td>Used to reset 24 V mode to 12 V mode (See Power chapter.)</td>
</tr>
<tr>
<td>A</td>
<td>Not used</td>
</tr>
<tr>
<td>B</td>
<td>Not used</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.) Will also reset 24V mode back to 12V mode.</td>
</tr>
<tr>
<td>E</td>
<td>Boot to backup image (Software House only)</td>
</tr>
<tr>
<td>F</td>
<td>ICU Block On (Read only) - Display General Messages</td>
</tr>
</tbody>
</table>
RM Port Termination Switches

Each of the RM ports have a switch that controls whether there are two 110 ohm RS-485 termination resistors on the iSTAR Edge end of the RM Bus. In most cases, leave this switch in its default (ON) position. When retrofitting an iSTAR Edge to reuse readers that were previously on an iSTAR Classic it may be desirable to turn off the termination. Another possibility would be the need for a four way STAR arrangement of RM busses. See the Connections chapter for details.

Output Relay Wet or Dry Jumpers

The four output relays can be either 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 Edge sources the power. When set to Wet, use the GND, NO, and NC connections. Be sure to stay within the power budget when using the Wet setting and powering by PoE.

See Chapter 6, “Relay Outputs” on page 6-19, for information

PoE Jumpers

PoE or PoE Plus Jumper

The PoE board has a set of 4 jumper locations, as shown in Figure 5-2 on page 5-9. The right most jumper location indicates PoE+ and the one left of it indicates PoE. Put the one jumper on the appropriate location. See Chapter 4, “iSTAR Edge Power and Backup” for more detail.

There is also a jumper to select whether the PoE board supplies 12VDC or 24 VDC to the iSTAR Edge. Whichever is selected will carry through to the Wet Relay voltage frequently used for Door locks.
Figure 5-2: PoE Board Jumpers
Controls and Displays
This chapter explains the wiring of various external connections.

In This Chapter

◆ Reader - I8 - R8 Combinations .......................................................... 6-2
◆ Inputs ...................................................................................................... 6-12
◆ AUX Outputs .......................................................................................... 6-18
◆ Relay Outputs ........................................................................................ 6-19
◆ Wiegand Readers .................................................................................. 6-23
◆ RM Readers - I/8s - R/8s ..................................................................... 6-24
◆ AC Fail / Low Battery ........................................................................ 6-25
◆ Tamper .................................................................................................... 6-26
◆ FAI Connections .................................................................................. 6-27
Connections - 2 Reader Model

Reader - I8 - R8 Combinations

The iSTAR Edge 2 reader model supports up to two readers, four I8 boards, and four R8 boards. The readers can be any combination of RM readers and direct connect Wiegand signaling devices. There are two Wiegand connectors and three RM ports. The RM readers can use any combination of Ports 1-3, including both readers on one port. Figure 6-1 illustrates some typical connection scenarios.

Two Wiegand Readers

Figure 6-1 shows two Wiegand signaling devices with multiple I/O Modules.

Figure 6-1: Two Wiegand Readers with I/O Modules
Two RM Readers

Figure 6-2 shows two RM readers connected to RM1 and RM2.

Figure 6-2: Two RM Readers with I/O Modules
One Wiegand and One RM Reader

Figure 6-3 shows one Wiegand reader and one RM reader.

Figure 6-3: One of Each Reader
RM Port Terminators

The three RM ports, shown in Figure 6-4, have an RS-485 Terminator switch that is normally on. You will usually leave these switches in the default position. The RM reader bus is a half duplex RS-485 connection that must have terminators at each end of the bus. When the switch is on the iSTAR Edge provides the 110 ohm terminators. The other end of the bus is terminated by a switch in the RM4, RM4E, I8, I8-CSI, or R8.

Figure 6-4: RM Termination Switches
In a special case, such as needing a Star configuration in four directions, it is possible to turn off the Edge terminator and use a Y type of connection from the RM port. Figure 6-5 shows an example of how that special case could be wired.

The 4000 foot maximum is measured from terminator to terminator.

**NOTE**

Figure 6-5 shows a fully loaded 2 Reader iSTAR Edge - 2 Readers, 4 - I8s, and 4 - R8s.
Connections - 4 Reader Model

Reader - I8 - R8 Combinations

The iSTAR Edge 4 reader model supports up to four readers, eight I8 boards, and eight R8 boards. The readers can be any combination of RM readers and direct connect Wiegand signaling devices. There are two Wiegand connectors and three RM ports. The RM readers can use any combination of Ports 1-3, including all readers on one port. The following figures illustrate some typical connection scenarios.

Four Wiegand Readers

Figure 6-6 shows four Wiegand signaling devices with multiple I/O Modules.

Figure 6-6: Four Wiegand Readers with I/O Modules
Four RM Readers

Figure 6-7 shows four RM readers connected to RM1, RM2, and RM3.

Figure 6-7: Four RM Readers with I/O Modules
Two Wiegand and Two RM Readers

Figure 6-8 shows two Wiegand readers and two RM readers.

Figure 6-8: Two of Each Reader Type
RM Port Terminators

The three RM ports, shown in Figure 6-9, have an RS-485 Terminator switch that is normally on. You will usually leave these switches in the default position. The RM reader bus is a half duplex RS-485 connection that must have terminators at each end of the bus. When the switch is on the iSTAR Edge provides the 110 ohm terminators. The other end of the bus is terminated by a switch in the RM4, RM4E, I8, I8-CSI, or R8.

Figure 6-9: RM Termination Switches
In a special case, such as needing a Star configuration in four directions, it is possible to turn off the Edge terminator and use a Y type of connection from the RM port. Figure 6-5 on page 6-6 shows an example of how that special case could be wired.

The 4000 foot maximum is measured from terminator to terminator.

Figure 6-10 shows an iSTAR Edge - 4 RM Readers, 3 - I8s, and 3 - R8s. The symbols indicate RS-485 Termination.
Inputs

There are eight onboard inputs, shown in Figure 6-11, available on the iSTAR Edge.

Pin 2 of the Input connectors is Ground.

Figure 6-11: iSTAR Edge Inputs

The type of supervision is configured in the host. Supervision Modes are listed in Table 6-1 on page 6-13.

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 EOL (End Of Line) resistors are used and where they are placed in relation to the switch. Settings are “Non-supervised”, “Single EOL”, or “Double EOL”.

- Non-supervised - the user wires no external resistors.
- Single EOL - the user wires a single EOL resistor.
- Double EOL - the user wires two EOL resistors, one in parallel and one in series with the switch.

Resistor values are labeled as 1k/5k/10k (in Ohms). In the Double EOL cases, both resistors have the same value.
Table 6-1: Supervision Modes

<table>
<thead>
<tr>
<th>Mode</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO/NC Double EOL 1K</td>
<td>Wire with Parallel/Serial for NO and Serial/Parallel for NC. [ Normal = 1K ] [ NO Alert = 0.5K ] [ NC Alert = 2K ] NOTE: This is the default value, and the traditional Software House method of supervision.</td>
</tr>
<tr>
<td>NO/NC Double EOL 5K</td>
<td>Wire with Parallel/Serial for NO and Serial/Parallel for NC. [ Normal = 5K ] [ NO Alert = 2.5K ] [ NC Alert = 10K ]</td>
</tr>
<tr>
<td>NC Single EOL 5K</td>
<td>Series Resistor [ Normal = 5K ] [ Alert = open (∞ Ω) ]</td>
</tr>
<tr>
<td>NO Single EOL 5K</td>
<td>Parallel Resistor [ Normal = 5K ] [ Alert = short (0 Ω) ]</td>
</tr>
<tr>
<td>NO/NC Double EOL 10K</td>
<td>Wire with Parallel/Serial for NO and Serial/Parallel for NC. [ Normal = 10K ] [ NO Alert = 5K ] [ NC Alert = 20K ]</td>
</tr>
<tr>
<td>NC Single EOL 10K</td>
<td>Series Resistor [ Normal = 10K ] [ Alert = open (∞ Ω) ]</td>
</tr>
<tr>
<td>NO Single EOL 10K</td>
<td>Parallel Resistor [ Normal = 10K ] [ Alert = short (0 Ω) ]</td>
</tr>
<tr>
<td>NC Non-Supervised</td>
<td>No Resistors [ Normal = short (0 Ω) ] [ Alert = open (∞ Ω) ]</td>
</tr>
</tbody>
</table>
### Table 6-1: Supervision Modes, continued

<table>
<thead>
<tr>
<th>Mode</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO Non-Supervised</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>NC Double EOL 1K</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>NO Double EOL 1K</td>
<td>Parallel and Serial Resistors</td>
</tr>
<tr>
<td></td>
<td>• Normal = 1K</td>
</tr>
<tr>
<td></td>
<td>• Alert = 0.5K</td>
</tr>
<tr>
<td>NC Double EOL 5K</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>NO Double EOL 5K</td>
<td>Parallel and Serial Resistors</td>
</tr>
<tr>
<td></td>
<td>• Normal = 5K</td>
</tr>
<tr>
<td></td>
<td>• Alert = 2.5K</td>
</tr>
<tr>
<td>NC Double EOL 10K</td>
<td>Serial and Parallel Resistors</td>
</tr>
<tr>
<td></td>
<td>• Normal = 10K</td>
</tr>
<tr>
<td></td>
<td>• Alert = 20K</td>
</tr>
<tr>
<td>NO Double EOL 10K</td>
<td>Parallel and Serial Resistors</td>
</tr>
<tr>
<td></td>
<td>• Normal = 10K</td>
</tr>
<tr>
<td></td>
<td>• Alert = 5K</td>
</tr>
</tbody>
</table>
NO/NC Double EOL 1K

Figure 6-12 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.

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 Double EOL 5K, 10K

Figure 6-13 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

For UL Listed products, burglar alarms must be supervised.
Notice that the wiring is different for NO and NC.

**Figure 6-13:** NO / NC Double EOL 5K, 10K

For the remainder of the choices you have to choose either NO or NC.

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

**Figure 6-14:** Double EOL 1K, 5K, 10K

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

*Figure 6-15: Single EOL 5K, 10K*

For UL Listed products, burglar alarms must be supervised.

**Non-Supervised**

*Figure 6-16: Non-Supervised*

For UL Listed products, burglar alarms must be supervised.
AUX Outputs

The AUX outputs can supply 350 mA for motion sensor or PIR type devices. The voltage is 12 VDC.

**Figure 6-17: AUX Wiring**

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

The relays can be used as DRY or WET. There is a jumper for each relay to set the mode.

Figure 6-18: Relay Outputs Dry/Wet Jumpers
Dry Relay Wiring

*Figure 6-19* shows DRY relay wiring. Max current is 3A at 30 VAC/VDC. Use NO or NC as appropriate. Notice that jumper is in the Dry position.

**Figure 6-19:** DRY Relay Wiring

---

Note: Use NC or NO in combination with normally energized to implement Fail Safe or Fail Secure.
Wet Relay Wiring

Figure 6-20 shows WET wiring for a normal NO Latch. The iSTAR Edge will supply either 12 VDC or 24 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.

![Wet Relay Wiring – NO Latch](image)
WET Wiring for a MagLock

Mag 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 6-21.

Figure 6-21: WET Mag
Wiegand Readers

Direct Wiegand signaling read head connections are shown in Figure 6-22.

**Figure 6-22**: Wiegand Readers

LED connections vary.
The following cases are typical:
- Green, Yellow, Red connected (Three Wire)
- Green and Red only (Two Wire)
- Green or Yellow or Red individually (One Wire (A,B,C))
Normal RM bus wiring is used for RM readers, I/8 boards, and R/8 boards. In Figure 6-23, notice that the connectors are oriented so that a connector taken off of RM1 can be used on RM2 or RM3 without moving the wires.

**Figure 6-23:** RM Wiring
AC Fail / Low Battery

Figure 6-24 shows AC Fail and Low Battery wiring. They are NC connections, and share a common ground pin.

NOTE

The Low Battery and AC power fail inputs must be enabled and connected to report for compliance with UL requirements.

NOTE

Shielded cable must be used for AC Fail & Low Battery Input connections.
Tamper

Tamper is NC. It is usually 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.

**Figure 6-25:** Tamper

The tamper switch controls many LEDs, to preserve power and also not blind users with the super bright LED when the door is open. When the door is closed the two power LEDs are the only ones on. The LCD is also off when the door is closed.

**NOTE**

The tamper input must be enabled and connected to report for compliance with UL requirements.
FAI Connections

NOTE

The FAI features are only supported on the following iSTAR Edge models:

- 0312-5010-02
- 0312-5010-04

FAI Scenarios

FAI (Fire Alarm Interface) is a hardware feature that will activate all enabled relays when the F (Fire) input of J40 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 (Normally Opened) 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.

FAI Modes

There are two basic modes:

- **FAI without Latch** - This method requires the F input (NC) of J40, plus the individual enable switches for each relay (SW2 through SW5).

- **FAI with Latch and subsequent Unlatch** - This method requires the F input of J40 plus the individual enable switches for each relay (SW2 through SW5), plus SW6 to enable the Latch and J40 K input (NO) to reset the Latch.

The Key input is usually a key switch that momentarily closes when the key is inserted and rotated.
F and K input Supervision

The F and K 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 closed F signal.

The wiring is shown in Figure 6-26. Be sure that the resistors are as close as possible to the F (Fire) and K (Key) switches for the most security.

![Figure 6-26: K and F Supervision](image)

Supervision Values are listed in Table 6-2.

Table 6-2: Supervision Values for F and K

<table>
<thead>
<tr>
<th>Input</th>
<th>Method</th>
<th>Signal State = True</th>
<th>Signal State = False</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fire (F)</td>
<td>NC</td>
<td>Switch Open 2K Ω</td>
<td>Switch Closed 1K Ω</td>
</tr>
<tr>
<td>Key (K)</td>
<td>NO</td>
<td>Switch Closed 500 Ω</td>
<td>Switch Open 1K Ω</td>
</tr>
</tbody>
</table>

NOTE

The following diagrams, Figure 6-27 on page 6-29 and Figure 6-28 on page 6-30, are shown without Supervision resistors for clarity. In actual practice, they must be supervised as in Figure 6-26.

Any resister values other than 500, 1K, or 2K ohms are treated as alarms that are indicative of tampering with the input.
**FAI without Latch**

This mode is fairly basic (see Figure 6-27):

1. The normally closed F (Fire) input goes true by opening.

2. The Relay Drive goes true and activates all relays that have their FAI enable switches on (SW2 through SW5).

3. The normally closed F (Fire) input goes false by closing.

4. The Relay Drive goes false and deactivates all relays that have their FAI enable switches on (SW2 through SW5).

*Figure 6-27: FAI without Latch*

**NOTE**  
Use supervision resisters in the actual wiring.
FAI with Latch followed by Key Unlatch

If the Latch Enable switch (SW6) is on and the F (Fire) input goes true the selected relays will activate and stay that way until an Unlatch K (Key) is given. See Figure 6-28.

1. J40 is in its normal state with F (NC) closed and K (NO) open.

2. F (Fire) opens signaling a Fire Alarm and all enabled relays are activated by the Relay Drive, as in “FAI without Latch” on page 6-29.

3. F (Fire) input closes indicating the Fire Alarm has been reset, BUT the relays stay activated (Latched).

4. Sometime later, probably after investigation, someone momentarily activates K (Key) and deactivates the relays. This input is named K because this input is usually a Key operated switch.

5. When K (Key) opens again, everything is back to normal.

Figure 6-28: FAI with Latch

NOTE

Use supervision resisters in the actual wiring.
State of F, K, and Relay Drive

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

All three of the inputs 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 (Fire) or K (Key) have a supervision error (short, open, or line fault), that will be reported in the normal way.

Figure 6-29 shows the FAI inputs in the C•CURE 9000 Controller dialog box. Figure 6-30 on page 6-32 shows the FAI inputs in the C•CURE 800/8000 Controller dialog box.

![Figure 6-29: FAI Inputs in C•CURE 9000](image)
Special Purpose Inputs

Special purpose inputs are described in Table 6-3.

Table 6-3: Special Purpose Inputs

<table>
<thead>
<tr>
<th>C•CURE 9000</th>
<th>C•CURE 800/8000</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tamper</td>
<td>Tamper</td>
<td>Activates when the iSTAR Edge cabinet is opened.</td>
</tr>
<tr>
<td>Power Failure</td>
<td>AC power fail input</td>
<td>Indicates that the UPS (Un-interruptible Power Supply) or apS, had an AC power failure and is now supplying battery power to the iSTAR Edge.</td>
</tr>
</tbody>
</table>
**Battery Low**

The UPS or apS battery has reached a yellow warning level. Most UPS units have about 10 to 20 minutes of run time left when this condition occurs. Software House recommends that you shut down the unit being powered by the low battery. Do not confuse this input with the Onboard Battery Low input.

**FAI Supervision State**

This is the F (Fire) Input State. Indicates the state of the F (Fire) input coming into J40 of the iSTAR Edge. In other words, this is the fire alarm.

**FAI Relay Control**

This pseudo input indicates the state of the Relay Drive signal that activates or latches the selected relays when the F (Fire) input is true.

**FAI Key Supervision State**

This is the K (Key) input state. Indicates the state of the K (Key) switch at J40 of the iSTAR Edge.

**Onboard Battery Low**

Indicates loss of external or PoE power to the iSTAR Edge. Upon external or PoE power loss, data is written to onboard flash. Four onboard batteries non-rechargeable alkaline AA batteries provide power for the backup process and maintaining the clock afterwards.

Onboard Battery Low also occurs when the voltage of all four batteries in series reaches 4.6 volts, or if a battery is missing.

Backup is valid for the period that the onboard batteries can maintain the clock. This period was tested for >3 days, but should reasonably last for two weeks.

It is very important that the alkaline batteries be replaced when they reach the low battery state.

---

### Table 6-3: Special Purpose Inputs, continued

<table>
<thead>
<tr>
<th>C•CURE 9000</th>
<th>C•CURE 800/8000</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Battery Low</td>
<td>Low battery input</td>
<td>The UPS or apS battery has reached a yellow warning level. Most UPS units have about 10 to 20 minutes of run time left when this condition occurs. Software House recommends that you shut down the unit being powered by the low battery. Do not confuse this input with the Onboard Battery Low input.</td>
</tr>
<tr>
<td>FAI Supervision State</td>
<td>FAI State</td>
<td>This is the F (Fire) Input State. Indicates the state of the F (Fire) input coming into J40 of the iSTAR Edge. In other words, this is the fire alarm.</td>
</tr>
<tr>
<td>FAI Relay Control</td>
<td>FAI Relay Control</td>
<td>This pseudo input indicates the state of the Relay Drive signal that activates or latches the selected relays when the F (Fire) input is true,</td>
</tr>
<tr>
<td>FAI Key Supervision State</td>
<td>FAI Key State</td>
<td>This is the K (Key) input state. Indicates the state of the K (Key) switch at J40 of the iSTAR Edge.</td>
</tr>
<tr>
<td>Onboard Battery Low</td>
<td>Onboard Battery Low</td>
<td>Indicates loss of external or PoE power to the iSTAR Edge. Upon external or PoE power loss, data is written to onboard flash. Four onboard batteries non-rechargeable alkaline AA batteries provide power for the backup process and maintaining the clock afterwards. Onboard Battery Low also occurs when the voltage of all four batteries in series reaches 4.6 volts, or if a battery is missing. Backup is valid for the period that the onboard batteries can maintain the clock. This period was tested for &gt;3 days, but should reasonably last for two weeks. It is very important that the alkaline batteries be replaced when they reach the low battery state.</td>
</tr>
</tbody>
</table>
The C•CURE 9000 Controller Status tab indicates the iSTAR Edge Model, whether a PoE board is installed, and other information about the state of the iSTAR Edge.

**Figure 6-31: iSTAR Edge Controller Status Tab**

The State Images tab has icons defined for the various states of the panel and the inputs. The icons can be modified as required.
This chapter describes how to use the iSTAR Configuration Utility (ICU) to configure iSTAR Edge/eX controllers.

In This Chapter
◆ Overview .......................................................................................................................... 7-2
◆ General Configuration Procedure ................................................................................ 7-4
◆ Copying the ICU onto a PC or Laptop ......................................................................... 7-7
◆ Understanding the ICU ................................................................................................. 7-8
◆ ICU Block Feature ......................................................................................................... 7-9
◆ Starting the ICU ............................................................................................................. 7-10
◆ Refreshing Controller Information ............................................................................. 7-12
◆ Setting ICU Options ...................................................................................................... 7-12
◆ Using the ICU Window ................................................................................................. 7-15
◆ Configuring a Controller .............................................................................................. 7-22
◆ Configuring SNMP ........................................................................................................ 7-28
◆ Digital Certificate Signing and Restore Options ...................................................... 7-32
◆ Connecting to the iSTAR Web Page Diagnostic Utility ........................................... 7-34
◆ Sending Messages to Other ICU Users ...................................................................... 7-38
◆ Downloading Firmware Updates ............................................................................... 7-39
The ICU provides iSTAR Edge/eX 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 the C•CURE is downloaded to iSTAR Edge/eX and overwrites the values that you specify in the ICU.

**NOTE** UL has not evaluated or approved the ICU utility.
Configuring a Master Controller

Use the ICU to define the controller type (master), the controller IP address, the primary connection type, and the C•CURE address.

For LAN configurations, Software House recommends that you configure information for member controllers in the C•CURE Administration application. The C•CURE downloads member configuration information to the master at start-up, and the master uses the information to configure the member controllers.

Troubleshooting Tools

The ICU provides a set of troubleshooting tools that help you to monitor the iSTAR Edge/eX network. Use troubleshooting tools to:

- PING IP addresses.
- Send messages to other ICU users.
- Open a Real Time Monitor Controller Diagnostic window within the ICU and display reports and diagnostic messages.
General Configuration Procedure

iSTAR Edge/eX configuration is accomplished using the C•CURE Administration application and the ICU.

LAN Configurations

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

To configure an iSTAR Edge/eX cluster

1. Connect and power on all iSTAR components.
2. Use the ICU to configure the following:
   - IP address of the master
   - IP address of the host with which the master communicates
   - IP address of the member iSTARs (when not using DHCP)
3. Use the C•CURE Administration application (Hardware Pane in the C•CURE 9000 or the Hardware Menu in the C•CURE 800/8000) to configure:
   - Master and member names
   - Master and member IP and MAC addresses
4. Use the C•CURE Administration Application (Hardware Pane in the C•CURE 9000 or the Hardware Menu in the C•CURE 800/8000) to configure the cluster and download cluster information. During download, the following occurs:
   - Master establishes a connection with C•CURE host.
   - C•CURE host downloads member address information.
   - Members beacon a “request for service” message across the subnet.

NOTE: You can also use the NetBIOS name or the FQDN.
General Configuration Procedure

- Master matches the “request for service” message with the member address information and downloads its’ own IP address.
- Members establish connections with the master.

WAN Configurations

NOTE
The ICU can connect to an iSTAR Edge/eX across a WAN provided you know the IP address of the remote iSTAR Edge/eX.

Because the ICU cannot detect an iSTAR Edge/eX address beyond the local subnet, you must do the following:

1. Connect and power on all iSTAR components.
2. Copy the ICU to a PC or laptop.
3. Connect the PC or laptop with the ICU to the subnet on which the target iSTAR Edge/eX resides.
4. Use the ICU to do the following:
   - Identify MAC addresses for members, as shown in Figure 7-4 on page 7-11.
   - If not using DHCP, configure the IP address for the master on the Ethernet Adaptor tab, as shown in Figure 7-1 on page 7-6.)
   - Configure gateway addresses for members and masters on the Ethernet Adaptor tab.
5. Use the C•CURE Administration Application to configure:
   - Master and member names
   - Master and member IP and MAC addresses (Hardware Pane in the C•CURE 9000 or the Hardware Menu in the C•CURE 800/8000) to configure cluster and download cluster information across network.

During download, the following occurs:
   - Master establishes a connection with C•CURE host.
   - C•CURE host downloads member address information.
   - Members beacon a “request for service” message across the network.
   - Master matches the “request for service” message with the member address information, and downloads its own IP address.
   - Members establish connections with the master.
Copying the ICU onto a PC or Laptop

When you install C•CURE 9000 on a server or client workstation, the ICU is included in the following locations:

- For the C•CURE 9000: Program Files \SWSystem \Server Components\iSTAR \ICU.
- For C•CURE 800/8000: CCURE800\ICU.

To use the ICU to configure iSTAR Edge/eX that is not in the subnet, you must know the IP address.

Copy the following ICU files from the \ICU directory on the C•CURE DVD to a C•CURE server or client:

- ICU.exe – The executable that runs the ICU.
- iWatch.exe – An executable that provides real-time monitoring of iSTAR Edge/eX controllers.

Copy iWatch.exe and iWatch2.exe files to the same folder as ICU.exe.

- iWatch2.exe – An executable that provides real-time monitoring of iSTAR Edge/eX controllers.
- iSTARDiagConnection.dll - Dynamic link library to establish connections.
- icu.chm – The help file for the ICU.
- ICU_5.x.x.txt – Information about this release of the ICU.

Be sure to record the location of these files on the PC or laptop so you can find them later.
Understanding the ICU

The ICU window allows access to all ICU functionality, including cluster configuration. The ICU also displays a list of controllers connected to the subnet and the configuration information as it is stored on each controller.

Displaying and Updating Cluster Information

At startup, the ICU broadcasts a query across the subnet to controllers, requesting their configuration information. Controllers that are powered on respond to the query by sending their information to the ICU, which then displays the information in the ICU window.

The ICU window is updated whenever a controller connection status changes. Refresh the window for the latest connection information. See “Refreshing Controller Information” on page 7-12 for additional information.
ICU Block Feature

You can prevent users from using the ICU to change the configuration of an iSTAR Edge/eX controller by setting the ICU Block feature on the controller.

To block the ICU configure option for a given iSTAR Edge/eX controller, set switch SW1 to F.

With ICU Block On, you cannot edit the ICU configuration.

- ICU dialog boxes are unavailable.
- LCD displays read-only status messages.

To turn off ICU blocking and allow users to modify the configuration, set switch SW1 to the 0 position.

### Table 7-1: ICU Block and Unblock Settings - with LCD Status Display Messages

<table>
<thead>
<tr>
<th>Switch Position</th>
<th>ICU Block On (Read only) - Display General Messages</th>
<th>ICU Block Off (Read/Write/Update) - Display General Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW1</td>
<td>F</td>
<td>0</td>
</tr>
</tbody>
</table>

**NOTE**

To achieve maximum security when iSTAR Edge/eX controllers are not running in FIPS 140-2 mode, Software House strongly recommends that you block the ICU configure feature on the controllers.

Running in FIPS 140-2 mode also blocks the ICU.
Starting the ICU

To start the ICU

1. In Windows, click **Start** > **Run**. The **Run** dialog box opens, as shown in Figure 7-2.

   **Figure 7-2:** Run Dialog Box

   ![Run Dialog Box](image)

   2. In the **Open** field, enter the path and filename for ICU.exe.

   3. Click **OK**. The **iSTAR Configuration Utility** dialog box opens, as shown in Figure 7-3.

   **Figure 7-3:** Password Dialog Box

   ![Password Dialog Box](image)

   4. Enter the default password and click **OK**. The default password is **manager**. Software House recommends that you change the default password for the ICU. For information about setting up passwords, see “Changing the ICU Password” on page 7-14.

   The ICU starts and the main window opens, as shown in Figure 7-4 on page 7-11, displaying controller information. See “Using the ICU Window” on page 7-15.
Figure 7-4: ICU Main Window
Refreshing Controller Information

To refresh controller information in the ICU window, use any of the following methods:

- Click the **Refresh** icon ( ) on the ICU toolbar. This method refreshes information for all controllers in the utility’s subnet.

- Choose **Refresh List** from the **View** menu. This method refreshes information for all controllers in the ICU’s subnet.

- Select a controller in the ICU window, right-click, and choose **Refresh** from the pop-up menu. This method refreshes information only for the selected controller.

- Set a refresh interval to automatically refresh the ICU window. See “Setting a Refresh Interval” on page 7-13.

**NOTE** Setting an automatic refresh interval increases network activity.

Setting ICU Options

To access the ICU **Options** dialog box, shown in Figure 7-5 on page 7-13, select **File> Options** from the ICU menu bar.

Use the ICU **Options** dialog box to:

- Enable and specify a refresh interval to automatically refresh the ICU window.

  **NOTE** Setting an automatic refresh interval increases network activity.

- Change the password for the ICU.

- Specify the public IP address of the PC being used to download firmware to iSTAR Edge/eX controllers.

- Set the download port on the PC being used to download firmware to iSTAR Edge/eX controllers.
Setting a Refresh Interval

You can set the ICU to refresh the controller list automatically, at the interval you specify.

To refresh the ICU window automatically

1. In the Auto-Refresh section of the Options dialog box, select the Enable option.
2. Enter the refresh interval (in minutes) or use the up/down arrows to the right of the Refresh Interval box to select the time.
3. Click OK.
Changing the ICU Password

You can change the password for the ICU using the Options dialog box.

**NOTE** Software House recommends that you change the default ICU password.

To change the ICU password

1. In the ICU User Password section of the Options dialog box, enter the new password in the Password field.
2. Confirm the password by entering it again in the Re-Enter Password field.
3. Click OK.

Setting the Public IP Address for Firmware Downloads

If the public IP address of the PC you are using to download iSTAR Edge/eX firmware is different from the IP address assigned to the PC’s NIC card, enter the public IP address of the PC in the Public IP Address field on the Options dialog box. This is required when the PC is on a WAN located behind a NAT server that exposes a public IP address for the PC that is different from the IP address assigned to the PC’s NIC card. After you enter the public IP address, click OK.

Setting the TCP/IP Port for Firmware Downloads

By default, the computer on which you are running the ICU uses port 2222 to download firmware to the iSTAR controllers on your network. In some situations, other applications may be using port 2222 on the PC; in that case you must specify another port to use for firmware downloads.

To specify another firmware download port, enter the port number in the Download TCP/IP Firmware field on the Options dialog box.

To determine if port 2222 is in use, and to determine which ports are in use on the PC, enter the following command in a DOS command prompt window:

```
netstat -n
```
Using the ICU Window

You can use the ICU window, shown in Figure 7-6, to configure master and member controllers.

Figure 7-6: Parts of the ICU Main Window

The toolbar contains icons of frequently used ICU commands.

To display the toolbar, select Toolbar from the View menu. To hide the toolbar, select the Toolbar command again.

Place the cursor over each toolbar button to display a tip on the button’s use. Table 7-2 describes toolbar buttons.
Using the ICU Window

Table 7-2: Toolbar Button Description

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Refresh" /></td>
<td>Refreshes the controller list. The ICU broadcasts a query across the subnet, and controllers respond with their configuration information, which is then updated in the window.</td>
</tr>
<tr>
<td><img src="image" alt="Select" /></td>
<td>Select a controller and click this button to open the Controller window for the selected controller. This window lets you configure the controller. See “Configuring a Controller” on page 7-22 for more information.</td>
</tr>
<tr>
<td><img src="image" alt="Diagnostic" /></td>
<td>Select a controller and click this button to open a Monitor Controller Diagnostic window for the selected controller. The window displays reports for categories selected using Diagnostic Level Control.</td>
</tr>
<tr>
<td><img src="image" alt="Ping" /></td>
<td>Select a controller and click this button to open a Ping window for the selected controller.</td>
</tr>
<tr>
<td><img src="image" alt="Download" /></td>
<td>Select a controller and click this button to download updated firmware to the controller. See “Downloading Firmware Updates” on page 7-39 for more information.</td>
</tr>
<tr>
<td><img src="image" alt="Help" /></td>
<td>Opens the online Help for the ICU.</td>
</tr>
</tbody>
</table>

Icons

Icons in the ICU Window indicate the status or type of controller.

Table 7-3: ICU Window Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Controller" /> <img src="image" alt="PCMCIA" /></td>
<td>The controller on the left is an iSTAR Classic. The controller on the right is an iSTAR Classic with a PCMCIA card.</td>
</tr>
<tr>
<td><img src="image" alt="Connected to Host or Master" /></td>
<td>• Connected to Host, or • Connected to Master</td>
</tr>
</tbody>
</table>
### Table 7-3: ICU Window Icons, continued

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
</table>
| ![Icon](image1) ![Icon](image2) | The controller on the left is an iSTAR Classic.  
The controller on the right is an iSTAR Classic with a PCMCIA card.  
- Not Connected, or  
- Attempting Host Connection, or  
- Attempting Master Connection |
| ![Icon](image3) ![Icon](image4) | The controller on the left is an iSTAR Pro.  
The controller on the right is an iSTAR Pro with a PCMCIA card.  
- Connected to Host, or  
- Connected to Master |
| ![Icon](image5) ![Icon](image6) | The controller on the left is an iSTAR Pro  
The controller on the right is an iSTAR Pro with a PCMCIA card.  
- Not Connected, or  
- Attempting Host Connection, or  
- Attempting Master Connection |
| ![Icon](image7) | The controller is an iSTAR, an iSTAR Pro, or an iSTAR Edge/eX.  
- Beaconing for Host  
- Beaconing for Master  
- Beaconing for Configuration. |
| ![Icon](image8) | The controller is currently rebooting. |
| ![Icon](image9) | The controller is an iSTAR eX.  
The Status column indicates that the controller is:  
- Connected to Host  
- Connected to Master  
- Not Connected  
- Attempting Host Connection  
- Attempting Master Connection |
Using the ICU Window

**Table 7-3: ICU Window Icons, continued**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
</table>
| ![](image) | The controller is an iSTAR Edge. The Status column indicates that the controller is:  
  • Connected to Host  
  • Connected to Master  
  • Not Connected  
  • Attempting Host Connection  
  • Attempting Master Connection |
| ![image] Comm Fail | The controller is in a Communication Failure state, and the ICU is unable to communicate with the controller.  
This can be a transient state when you refresh the ICU display, and is replaced by one of the other states when the ICU receives a response from the controller. |

**Display Area**

The **Display Area** lists controllers that respond to the ICU broadcast. The ICU displays the information shown in **Table 7-4** for each controller.

**Table 7-4: ICU Window Columns**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Icon</td>
<td>Indicates the status of the controller.</td>
</tr>
</tbody>
</table>
| MAC Add| Displays the last six nibbles of the controller’s MAC address.  
MAC addresses are unique hardware addresses for iSTAR Edge/eX. A MAC address cannot be changed. The iSTAR eX MAC address is indicated by a label on the iSTAR eX GCM board. The first six nibbles of the MAC address are fixed for all controllers (set at 00-50-F9). |
<p>| Name   | Displays the name of the controller as it was configured in the C•CURE Controller dialog box. |</p>
<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Displays the controller’s IP address. Use the ICU to assign IP addresses to masters. Use the C•CURE Administrative application to assign IP addresses to cluster members. If “0.0.0.0” is displayed in this field, the IP address is not configured.</td>
</tr>
<tr>
<td>Parent IP Address</td>
<td>If this controller is a cluster member, displays the IP address of the controller’s master. If this controller is a master, displays the IP address of the host. If “0.0.0.0” is displayed in this field, a master is not assigned to the controller or the master IP address is not configured.</td>
</tr>
<tr>
<td>FW Version</td>
<td>Displays the controller’s firmware version. ICU Version 3.3.0 and higher recognize any firmware version higher than Version 2.1. Earlier firmware versions are listed as “Unknown”.</td>
</tr>
<tr>
<td>Type</td>
<td>If the controller is a cluster member, displays <strong>Member</strong>. If the controller is a master, displays <strong>Master</strong>.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Indicates if the controller is online. (Administration application&gt;Hardware&gt;Controller&gt;Edit&gt; Online box is checked or not checked) <strong>YES</strong> = Online; <strong>No</strong> = Offline</td>
</tr>
</tbody>
</table>
### Status Displays

- **Attempting master connection** – a member controller is attempting to connect to and communicate with its master controller.

- **Attempting host connection** – a master controller is attempting to connect to and communicate with the C•CURE host computer.

- **Not Connected** – the controller is configured, but is not communicating with the master (if a member) or host (if a master).

- **Connected to Host** – the master is configured and communicating with the host.

- **Connected to Master** – the member controller is configured and communicating with its master controller.

- **Connected to alternate master** – the member controller is configured and communicating with its alternate master controller. This indicates that the primary master controller is not communicating with the member.

- **Beaconing for Host** – the master is configured, but is not in communication with the host.

- **Beaconing for Master** – the controller is broadcasting a query across the subnet for the master’s IP address. The master responds by sending the controller the IP address. If the master does not respond in a set amount of time, the ICU responds by sending the controller the master’s IP address as specified in the utility’s controller database.

- **Beaconing for IP Address** – the member is broadcasting a query across the subnet for its own IP address. Since the controller is a member, the master can respond with the IP address information.

- **Rebooting** – the controller is rebooting.

- **Comm Fail** – the controller did not receive the latest ICU refresh message, and may be in communication failure.

### Table 7-4: ICU Window Columns, continued

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Displays the status of the controller:</td>
</tr>
<tr>
<td></td>
<td><strong>Attempting master connection</strong> – a member controller is attempting to connect to and communicate with its master controller.</td>
</tr>
<tr>
<td></td>
<td><strong>Attempting host connection</strong> – a master controller is attempting to connect to and communicate with the C•CURE host computer.</td>
</tr>
<tr>
<td></td>
<td><strong>Not Connected</strong> – the controller is configured, but is not communicating with the master (if a member) or host (if a master).</td>
</tr>
<tr>
<td></td>
<td><strong>Connected to Host</strong> – the master is configured and communicating with the host.</td>
</tr>
<tr>
<td></td>
<td><strong>Connected to Master</strong> – the member controller is configured and communicating with its master controller.</td>
</tr>
<tr>
<td></td>
<td><strong>Connected to alternate master</strong> – the member controller is configured and communicating with its alternate master controller. This indicates that the primary master controller is not communicating with the member.</td>
</tr>
<tr>
<td></td>
<td><strong>Beaconing for Host</strong> – the master is configured, but is not in communication with the host.</td>
</tr>
<tr>
<td></td>
<td><strong>Beaconing for Master</strong> – the controller is broadcasting a query across the subnet for the master’s IP address. The master responds by sending the controller the master’s IP address as specified in</td>
</tr>
<tr>
<td></td>
<td>the utility’s controller database.</td>
</tr>
<tr>
<td></td>
<td><strong>Beaconing for IP Address</strong> – the member is broadcasting a query across the subnet for its own IP address. Since the controller is a member, the master can respond with the IP address information.</td>
</tr>
<tr>
<td></td>
<td><strong>Rebooting</strong> – the controller is rebooting.</td>
</tr>
<tr>
<td></td>
<td><strong>Comm Fail</strong> – the controller did not receive the latest ICU refresh message, and may be in communication failure.</td>
</tr>
</tbody>
</table>
Menu Bar

The **Menu bar** provides options that activate dialog boxes. See the ICU online help for specific information about ICU dialog boxes.

Status Bar

The **Status Bar** provides helpful information about the current operation the ICU is performing.

The **Status Bar** also displays the number of active ICUs and the number of controllers responding to the utility’s broadcast.
Configuring a Controller

The **Controller** dialog box contains options that configure and edit iSTAR Edge/eX controllers.

**Prerequisite Information**

**Table 7-5** provides the information to configure an iSTAR Edge/eX controller.

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller IP address</td>
<td>The ICU prompts you for a specific IP address.</td>
</tr>
<tr>
<td>Host connection type</td>
<td>Master controllers support onboard Ethernet connection to the C•CURE.</td>
</tr>
<tr>
<td></td>
<td>Member controllers support one network connection (10/100 BaseT Ethernet).</td>
</tr>
<tr>
<td>C•CURE or master address</td>
<td>For master controllers, this is the IP address of the C•CURE system.</td>
</tr>
<tr>
<td></td>
<td>For member controllers, this is the IP address of the master controller.</td>
</tr>
<tr>
<td>Primary host connection</td>
<td>Master controllers can establish a primary connection to the C•CURE host over network connections.</td>
</tr>
<tr>
<td>Secondary host connection</td>
<td>Master controllers can establish a secondary connection to the host over network connections.</td>
</tr>
</tbody>
</table>

To configure a controller using the ICU

1. Power up the controllers in the cluster.
2. Start the ICU.

**NOTE**

To use the ICU, connect a PC or laptop to the same subnet as the cluster.

The ICU window opens, as shown in Figure 7-7 on page 7-23, and displays controllers and their configuration information.
If a controller is not configured, the ICU displays:

- Last six nibbles of the controller’s MAC address
- “0.0.0.0” for the controller’s IP address
- “Disconnected” icon ( , , , or  or )
- “Broadcasting for...” for Status

Figure 7-7: ICU Main Window Messages

3. Use one of the following methods to open the Controller dialog box for a given controller:

- Double-click the controller.
- Highlight the controller, right-click, and choose Edit Controller Information from the drop down menu.
- From the Main Menu bar, select Edit and choose Controller.
- Click the Edit Controller icon.

Controllers are identified by their MAC addresses. The Controller dialog box opens for the selected controller, shown in Figure 7-8 on page 7-24, with the Controller Identity tab selected by default.
4. Provide the information described in Table 7-6 on page 7-25 through Table 7-9 on page 7-27.

5. When done, click OK.
**Table 7-6: Controller Identity Tab**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC address</td>
<td>Displays the last six nibbles of the controller’s MAC address. You cannot edit this field. MAC addresses are unique hardware addresses that identify controllers and other Ethernet devices. They are built into the iSTAR Edge/eX GCM at production time. A controller’s MAC address is printed on a label attached to the iSTAR Edge/eX GCM. The first six nibbles of the MAC address are fixed for all controllers (set at 00-50-F9).</td>
</tr>
<tr>
<td>NetBIOS name</td>
<td>Displays the NetBIOS name of the controller. You cannot edit this field.</td>
</tr>
<tr>
<td>Master controller</td>
<td>Select this option to indicate that the controller is a master. If you select this option, the Master tab changes to a Host tab. You can then use the Host tab to specify the host with which the controller communicates and the type of connection to the host (see Table 7-8). If you do not select this option, it indicates that the controller is a member controller communicating with a master controller. You can then use the Master tab to specify the master controller with which the controller communicates and the type of connection to the master controller.</td>
</tr>
</tbody>
</table>

**Table 7-7: Ethernet Adapter Tab**

<table>
<thead>
<tr>
<th>Field/Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptor</td>
<td>Defines the type of Ethernet connection. Options are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Onboard Ethernet Adaptor</strong> – connected via 10/100Base-T Ethernet.</td>
</tr>
<tr>
<td>Use this as the</td>
<td>If checked, uses the Ethernet adaptor specified on this tab as the primary Ethernet connection. Use the Host tab to configure secondary Ethernet connections (master controllers only).</td>
</tr>
<tr>
<td>Primary Ethernet Adaptor</td>
<td></td>
</tr>
</tbody>
</table>
Obtain an IP address from a DHCP Server

Select this option to tell the controller to use the IP addresses assigned by the DHCP server you specify.

Software House recommends that you select this option.

**Note:** If locked (using the lock icon), the controller only accepts addresses from the DHCP server; it does not accept a translated address downloaded from a Network Address Translator, C•CURE system, or other remote device.

Specify an IP address

Select this option if you want to use a specific IP address for the controller.

**Note:** If locked (using the lock icon), the controller only uses the IP address you specify, and does not accept translated addresses downloaded from a Network Address Translator, C•CURE system, or other remote device.

When you select this option, the following fields become active:

- **IP Address** – Enter the controller’s IP address. All controllers need an IP address to communicate on a TCP/IP network. The IP address must match the IP address you enter for the controller in the C•CURE System Administration application.
- **Subnet Mask** – Enter the subnet mask.
- **Default Gateway** – Enter the IP address of the default gateway for the controller. This field is required for an iSTAR Edge/eX that communicates across a WAN configuration.

Obtain Domain Name Server addresses automatically

Select this option to tell the controller to automatically obtain Domain Name Server addresses.

Software House recommends that you select this option.

Use the following Domain Name Server addresses

Select this option if you want to specify the Domain Name Server(s) that the controller should use. Then enter the IP addresses of the Primary and Secondary DNS Servers in the provided fields.

Optionally, you can also enter a DNS Query Suffix (for example, "yourcompany.com").

<table>
<thead>
<tr>
<th>Field/Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain an IP address from a DHCP Server</td>
<td>Select this option to tell the controller to use the IP addresses assigned by the DHCP server you specify.</td>
</tr>
<tr>
<td></td>
<td>Software House recommends that you select this option.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If locked (using the lock icon), the controller only accepts addresses from the DHCP server; it does not accept a translated address downloaded from a Network Address Translator, C•CURE system, or other remote device.</td>
</tr>
<tr>
<td>Specify an IP address</td>
<td>Select this option if you want to use a specific IP address for the controller.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If locked (using the lock icon), the controller only uses the IP address you specify, and does not accept translated addresses downloaded from a Network Address Translator, C•CURE system, or other remote device.</td>
</tr>
<tr>
<td></td>
<td>When you select this option, the following fields become active:</td>
</tr>
<tr>
<td></td>
<td><strong>IP Address</strong> – Enter the controller’s IP address. All controllers need an IP address to communicate on a TCP/IP network. The IP address must match the IP address you enter for the controller in the C•CURE System Administration application.</td>
</tr>
<tr>
<td></td>
<td><strong>Subnet Mask</strong> – Enter the subnet mask.</td>
</tr>
<tr>
<td></td>
<td><strong>Default Gateway</strong> – Enter the IP address of the default gateway for the controller. This field is required for an iSTAR Edge/eX that communicates across a WAN configuration.</td>
</tr>
<tr>
<td>Obtain Domain Name Server addresses</td>
<td>Select this option to tell the controller to automatically obtain Domain Name Server addresses.</td>
</tr>
<tr>
<td>automatically</td>
<td>Software House recommends that you select this option.</td>
</tr>
<tr>
<td>Use the following Domain Name Server</td>
<td>Select this option if you want to specify the Domain Name Server(s) that the controller should use. Then enter the IP addresses of the Primary and Secondary DNS Servers in the provided fields.</td>
</tr>
<tr>
<td>addresses</td>
<td>Optionally, you can also enter a DNS Query Suffix (for example, &quot;yourcompany.com&quot;).</td>
</tr>
</tbody>
</table>
### Table 7-8: Host/Master Tab

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary Host Connection</strong></td>
<td><strong>Connection Type</strong> – Defines the primary connection to the C•CURE host or the master controller. Selections include:</td>
</tr>
<tr>
<td>- or -</td>
<td>• Onboard Ethernet 1 – connects via 10/100Base-T Ethernet.</td>
</tr>
<tr>
<td><strong>IP Address or Name</strong></td>
<td>Specifies the IP address of the C•CURE host (if configuring a master) or master controller (if configuring a member).</td>
</tr>
<tr>
<td></td>
<td>When configuring a master controller, you can enter the NetBIOS or DNS name of the C•CURE host. When configuring a member controller, you can only enter the IP address of the master controller.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If the iSTAR Edge/eX is part of an AutoStart / Replistor redundant configuration, you must enter the NetBIOS or DNS name of the host or master controller.</td>
</tr>
<tr>
<td><strong>Secondary Host Connection</strong></td>
<td>Defines the type of secondary connection to the C•CURE host or master controller. Options include:</td>
</tr>
<tr>
<td>- or -</td>
<td>• Onboard Ethernet 2 – connects via 10/100Base-T Ethernet</td>
</tr>
<tr>
<td><strong>Secondary Master Connection</strong></td>
<td>Not Available on Edge.</td>
</tr>
</tbody>
</table>

### Table 7-9: Advanced Tab

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web Diagnostics</strong>&lt;sup&gt;a&lt;/sup&gt;</td>
<td>Select the <strong>Enabled</strong> option to allow viewing of Web Diagnostic pages for the selected controller. Clear the <strong>Enabled</strong> option to prevent viewing of Web Diagnostic pages for the selected controller. See Chapter 8 for more information on Web Diagnostics.</td>
</tr>
<tr>
<td><strong>SNMP</strong>&lt;sup&gt;a&lt;/sup&gt;</td>
<td>Select the <strong>Enabled</strong> option to enable SNMP. You can then define security levels for up to two community names, Clear the <strong>Enabled</strong> option to disable SNMP.</td>
</tr>
</tbody>
</table>

---

<sup>a</sup> This feature applies only to iSTAR controllers running firmware version 4.0.0 or greater.
On iSTAR controllers running firmware version 4.0.0 or greater, you can enable and configure Simple Network Management Protocol (SNMP) communication.

SNMP communication is enabled on all iSTAR controllers by default. You can use the ICU to do the following:

- Configure up to two SNMP community names.
- Select the security level for each community name.
- Specify an SNMP trap manager.
- Restrict SNMP communication to a particular SNMP host.
- Add the contact information for the person who administers SNMP at your site.

**To configure SNMP**

1. In the ICU controller list, select the iSTAR controller for which you want to enable SNMP.

2. Right-click and select *Edit Controller Information*.

3. Select the *Advanced* tab, shown in *Figure 7-9* on page 7-29.
4. Click the **Configure** button. The **SNMP** dialog box appears, as shown in **Figure 7-10** on page 7-30.

**NOTE**  
The **Configure** button is available only if the **Enabled** check box is selected.
5. See Table 7-10 for information about fields in the dialog box.

Table 7-10: SNMP Dialog Box Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community Name</td>
<td>Set the SNMP communities to which this Controller belongs. An SNMP device or agent can belong to more than one SNMP community. A device does not respond to requests from SNMP management stations that do not belong to one of its communities. Obtain this information from your Network Administrator.</td>
</tr>
<tr>
<td>Rights</td>
<td>Set the access right for the specified community. When an SNMP message is received by the Controller, it is evaluated based on these rights.</td>
</tr>
<tr>
<td></td>
<td><strong>No Access</strong> – The SNMP message from a management system in this community is discarded.</td>
</tr>
<tr>
<td></td>
<td><strong>Read Only</strong> – Only GET, GET-NEXT, and GET-BULK requests are processed. SET requests are not processed from this community.</td>
</tr>
<tr>
<td></td>
<td><strong>Read Create</strong> – SET, GET, GET-NEXT, and GET-BULK requests are processed.</td>
</tr>
</tbody>
</table>
6. Click **OK** to save your configuration and close the SNMP dialog.

### Table 7-10: SNMP Dialog Box Field Descriptions, continued

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SNMP Trap Manager IP Address or Host Name</strong></td>
<td>Enter the IP address or host name of the SNMP Trap Manager for this iSTAR Controller.</td>
</tr>
<tr>
<td><strong>SNMP Hosts</strong></td>
<td>Accept SNMP packets from any host – Select this option if you want the iSTAR controller to accept SNMP messages from any host. Only accept SNMP packets from this Host – Select this option if you want the iSTAR controller to accept SNMP messages from a specified host only. IPAddress or Host Name – Specify the IP address or host name of the SNMP Host for this iSTAR Controller.</td>
</tr>
<tr>
<td><strong>Contact</strong></td>
<td>Specify the snmp-contact, a 1- to 64-character string usually containing an emergency contact name and telephone or pager number.</td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td>Specify the snmp-location, a 1- to 64-character string usually containing location information about the Controller.</td>
</tr>
</tbody>
</table>
Digital Certificate Signing and Restore Options

The ICU can be used to request a digital certificate signing or to restore default certificates to selected iSTAR Edge/eX controllers, as shown in Figure 7-11.

Figure 7-11: ICU Digital Certificate Signing and Restore Options

The Digital Certificate menu items are available only if the selected controller is an iSTAR Edge/eX.

To request a digital certificate signing or to restore default certificates to the selected iSTAR Edge/eX controllers

1. In the ICU controller list, select the iSTAR Edge/eX controller.

2. Right-click and select Request Certificate Signing or Restore Default Certificates. The dialog box shown in Figure 7-12 on page 7-33 opens.
3. The system validates that the value in the **Host IP address or name** field is that of an existing Host. The **OK** button is not available if the **Host IP address or name** field is empty.

4. Clicking **OK** changes the **Mouse** icon to the **Wait** icon, as this operation may take up to 30 seconds to complete.

5. For detailed information about digital signature signing and restore options, see the *Hardware Configuration Guide*. 

---

**Figure 7-12:** Request for Certificate Signing
Connecting to the iSTAR Web Page Diagnostic Utility

The iSTAR Web Page Diagnostic Utility uses Internet Explorer to view status and diagnostics information. You can start the Diagnostic Utility from the ICU. You can also run the Diagnostic Utility by typing the IP address of the controller into the address bar of Internet Explorer.

Example:


NOTE

You must use Internet Explorer v5.0 or higher to run the Diagnostic Utility.

To start the iSTAR Web Page Diagnostic Utility from the ICU

1. In the ICU window, select a controller and right-click. A drop-down menu appears, as shown in Figure 7-13.

   **Figure 7-13: Web Page Diagnostic Utility**

2. Click Controller Status.
3. If you configured a Controller password in the **C•CURE Options & Tools/System Variables/iSTAR Driver** section, as shown in Figure 7-14, the **Connect To x.x.x.x** dialog box opens, as shown in Figure 7-15 on page 7-36. Continue to Step 4.

4. If a Controller password exists, as shown in Figure 7-14, enter the password in both the **User Name** and **Password** fields of the **Enter Network Password** Dialog box 📦.

   **Figure 7-14:** Configure Controller Network Password

   ![System Variables](image)

   **NOTE** If there is no Controller password, you can configure one on the **Options and Tools/System Variables/iSTAR Driver** section, by entering up to 16 characters.
5. If a Network Controller password was not configured for the utility, the Controller Status web page opens in the default web browser, as shown in Figure 7-16 on page 7-37. Internet Explorer displays the status of the selected controller in the main Diagnostic System window.

Use the Password from Options and Tools in both places.
Disabling Web Diagnostics

Web Diagnostics are enabled by default. You can, however, disable Web Diagnostics for selected iSTAR controllers running firmware version 4.0.0 and higher.

To disable Web Diagnostics

1. In the ICU Controller list, select an iSTAR controller that is running firmware version 4.0.0 or greater.

2. Right-click the controller and select Edit Controller Information.

3. Select the Advanced tab, shown on Figure 7-9 on page 7-29.

4. In the Web Diagnostics box, clear the Enabled check box and click OK.
Sending Messages to Other ICU Users

The Tools command on the main menu includes an option that lets you send messages to other users who are currently using the ICU.

**To send a message to other ICU users**

1. From the menu bar, choose Tools>Send ICU Message. The User Message dialog box opens, as shown in Figure 7-17.

2. Type your message and click Send. The ICU sends the message to all other ICU users in the subnet.

**NOTE**

Use the User Message dialog box to notify other users that you are configuring an iSTAR Classic, iSTAR Pro, or iSTAR Edge/eX within a specific cluster. This “good practice” procedure prevents other users from configuring the same iSTAR unit and maintains control over iSTAR addresses.
Downloading Firmware Updates

You can use the ICU to quickly download firmware updates to one or more controllers. Before starting the download process, copy the new firmware file to a local or network directory that you can access from the computer on which you are running the ICU.

Before starting the firmware download, note the following issues:

- If the public IP address for the PC on which you are running the ICU is different than the IP address assigned to the PC’s NIC card, you have to specify the public IP address of the PC on the ICU Options dialog box. See “Setting the Public IP Address for Firmware Downloads” on page 7-14 for more information.

- If the default port (2222) that is used for firmware downloads is in use by another application on the PC, you have to specify another port to use for firmware downloads. See “Setting the TCP/IP Port for Firmware Downloads” on page 7-14 for more information.

To download updated firmware to a controller

1. In the ICU window, select the controller(s) that you want to update. You can select multiple controllers by pressing the Ctrl key while you are selecting them.

2. After selecting the controller(s), right-click in the ICU window and select Download Firmware from the pop-up menu, as shown in Figure 7-13 on page 7-34.

   NOTE

You can also start the download process by clicking the icon on the toolbar.

3. The Download Firmware dialog box appears, listing all of the controllers you selected, shown in Figure 7-18 on page 7-40.
4. Click **Browse** and navigate to the directory in which you stored the firmware image file.

5. Select the firmware image file and click **Open**. The selected file is displayed in the **Firmware Image File to Download** box.

6. Click **Start Download** to initiate the download to all controllers in the **Download Firmware** list. The firmware is downloaded simultaneously to all controllers in the list. The **Progress** bar on each line indicates when the download is complete for each controller.
Use the iSTAR Controller editor in the C•CURE Administration Application to display the firmware and other data about specific iSTAR Edge/eX controllers, as shown in Figure 7-19.

**Figure 7-19:** Controllers Status Window

<table>
<thead>
<tr>
<th>Name: edge_080889</th>
<th>Description:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Dynamic Status**

- **Online Status:** Online
- **Firmware Version:** 5.1.0.19004.14
- **Boot Time:** 4/26/2010 8:02:41 AM
- **Free Program Memory:** 5980 KB
- **Total Program Memory:** 16384 KB
- **Free Storage Memory:** 36708 KB
- **Total Storage Memory:** 38900 KB
- **Free Physical Memory:** 44688 KB
- **Total Physical Memory:** 65536 KB
- **PoE Board Installed:** True
- **Edge Model Status:** 2-Door
Web Page Diagnostics

The iSTAR Web Page Diagnostic Utility uses a web page interface that is included in the iSTAR Edge firmware. Use the Diagnostic Utility to view diagnostic and status information for a controller or cluster in an Internet Explorer browser window.

In This Chapter

◆ Starting the Diagnostic Utility ................................................................. 8-2
◆ Navigating the Diagnostic Utility ........................................................... 8-3
◆ Viewing the Status Screen ......................................................................... 8-4
◆ Viewing the Cluster Information Screen .................................................... 8-7
◆ Viewing the Object Store Database Screen ................................................. 8-8
◆ Diagnostic Screens ..................................................................................... 8-10
◆ iWatch2 Network Diagnostic Tool ............................................................ 8-14
Starting the Diagnostic Utility

NOTE
The Web Page Diagnostic Utility has not been evaluated by UL.

Use the following procedure to start the Diagnostic Utility and connect to a controller.

To start the Diagnostic Utility

1. In an Internet Explorer browser window, enter the IP Address of the iSTAR Edge controller (for example, http://121.21.121.12) in the browser Address window and press Enter or click Go. The Enter Network Password dialog box, Figure 8-1, appears.

NOTE
You can also start the Diagnostic Utility from the ICU.

Figure 8-1: Enter Network Password Dialog Box

2. In both the User Name and Password fields, enter the password you configured in the C•CURE Administration Application.

After the login information has been verified, the Controller Status window appears, as shown in Figure 8-2 on page 8-3.

NOTE
The password that you enter for the Diagnostic Utility is different from the one used for the ICU.
Navigating the Diagnostic Utility

The Diagnostic Utility window is divided into two frames. Use the menu on the left-side frame, shown in Figure 8-2, to navigate to the other screens. The selected screen displays in the right-side frame.

**Figure 8-2:** Diagnostic Utility Frames

The menu in the left-side frame is the entry point to all the other screens. It remains fixed in the left-side frame while the right-side frame changes according to the menu selection.

Notice the drop-down list at the top of the menu. The MAC address of the selected controller appears in the rectangular box. Once connected to a controller, all of the cluster members associated with that controller are accessible. Connect to them by selecting them from the drop-down list box. Click the down arrow to expand the list. The numbers shown in the list correspond to the associated controllers’ MAC addresses.
Viewing the Status Screen

If the Controller Status screen is not displayed in the right-hand frame, click **Status** on the menu. A **Controller Status** screen appears. This screen displays status information for the selected controller.

**Figure 8-3** shows a portion of an iSTAR Edge master controller status screen. The information that is displayed for a member controller is slightly different.

**Figure 8-3: iSTAR Edge Controller Status Screen**

Status information varies and depends on the controller type and firmware version. **Table 8-1** on page 8-5 lists status information for the different iSTAR controller types: iSTAR Classic, iSTAR Pro, iSTAR eX, and iSTAR Edge.
### Table 8-1: Status Information Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller Type</td>
<td>Whether the selected controller is a cluster master or member.</td>
</tr>
<tr>
<td>Controller Name</td>
<td>The name assigned to the controller.</td>
</tr>
<tr>
<td>Online</td>
<td>The online status of the controller.</td>
</tr>
<tr>
<td>Main Image</td>
<td>The version of the firmware used by the controller.</td>
</tr>
<tr>
<td>Boot Image</td>
<td>The version of a secondary firmware image, used in the unusual event of corruption or download failure of the main image.</td>
</tr>
<tr>
<td>Bootloader</td>
<td>The version of the firmware that loads the Windows CE operating system onto the controller.</td>
</tr>
<tr>
<td>Processor</td>
<td>The version and type of iSTAR processor (for example MPC860 for a Motorola Power PC 860).</td>
</tr>
<tr>
<td>Board</td>
<td>The iSTAR board version.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The last six nibbles of the Media Access Control (MAC) address of the controller. The first six nibbles of the MAC address are the vendor portion, and are always 0050F9.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address assigned to the controller.</td>
</tr>
<tr>
<td>Master (or Host) IP address</td>
<td>The IP address or network name assigned to the cluster master controller or to the host.</td>
</tr>
<tr>
<td>Master MAC address</td>
<td>The MAC address assigned to the cluster master controller. This field is not displayed if the current controller is a master controller.</td>
</tr>
<tr>
<td>Local Date/Time</td>
<td>The local date, time, and time zone at the controller. This value is reported each time the controller is queried, and it is necessary to click the browser’s Refresh button to update it.</td>
</tr>
<tr>
<td>GMT Date / Time</td>
<td>The date and time expressed in Greenwich Mean Time or Universal Time. This value is reported each time the controller is queried, and it is necessary to click the browser’s Refresh button to update it.</td>
</tr>
</tbody>
</table>
Table 8-1: Status Information Description, continued

<table>
<thead>
<tr>
<th>Item</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>DST</td>
<td>YES or NO indicates whether or not the controller automatically adjusts the local time setting for Daylight Savings Time when it is in effect.</td>
</tr>
<tr>
<td>Boot Date / Time</td>
<td>The GMT date and time at which the controller was last booted.</td>
</tr>
<tr>
<td>Elapsed Time Since Boot</td>
<td>The amount of time that has passed since the system was booted.</td>
</tr>
<tr>
<td>Total Program Memory</td>
<td>The total amount of controller flash ROM memory, in bytes.</td>
</tr>
<tr>
<td>Free Program Memory</td>
<td>The number of bytes of controller flash ROM memory not in use.</td>
</tr>
<tr>
<td>Percent Free</td>
<td>The percentage of controller flash ROM memory not in use.</td>
</tr>
<tr>
<td>Total Storage Memory</td>
<td>The total amount of SDRAM available for C•CURE 800/8000 access control data.</td>
</tr>
<tr>
<td>Free Storage Memory</td>
<td>The amount of free SDRAM available for C•CURE 800/8000 access control data.</td>
</tr>
<tr>
<td>Total Physical Memory</td>
<td>The amount of SDRAM available on the controller.</td>
</tr>
<tr>
<td>Master (or Host) Connection Status</td>
<td>The status of the connection to the master controller (for members) or to the host (for masters).</td>
</tr>
<tr>
<td>Path to Host</td>
<td>Yes or No indicates whether or not the controller has a communications path to the C•CURE host.</td>
</tr>
<tr>
<td>Active Communication Type</td>
<td>The communication interface that is currently active.</td>
</tr>
<tr>
<td>Secondary Communication Type</td>
<td>Type of communication for secondary connection between the controller and host. This is shown only if a secondary connection was configured for the controller.</td>
</tr>
</tbody>
</table>
Viewing the Cluster Information Screen

Click **Cluster** on the left frame of the Diagnostic Utility window (shown in Figure 8-2 on page 8-3) to display the **Cluster Information** screen, shown in Figure 8-4. This screen displays the MAC address and IP address, plus the connection and enabled status for the master and all members of the cluster.

**Figure 8-4:** Cluster Information Screen

<table>
<thead>
<tr>
<th>Controller</th>
<th>IP Address</th>
<th>Connection Status</th>
<th>Enabled Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>51019 (Master)</td>
<td>10.30.1.46.9</td>
<td>Connected</td>
<td>Enabled</td>
</tr>
<tr>
<td>5101a</td>
<td>10.38.1.46.39</td>
<td>Connected</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
Click **Database** in the left frame of the Diagnostic Utility window (shown in Figure 8-2 on page 8-3) to display the **Object Store Databases** screen, shown in Figure 8-5. This screen displays the status of the database objects in the cluster. Information about memory displays in the top row.

The information on this screen indicates what is configured on a particular iSTAR Edge. This information can vary from unit to unit.

**Figure 8-5: Sample Object Store Databases Screen**

<table>
<thead>
<tr>
<th>Database Name</th>
<th>Number of Records</th>
<th>Total Bytes</th>
<th>Percent of Object Store</th>
<th>Time Last Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tracing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACM/ReadersDB</td>
<td>3</td>
<td>2772 Bytes</td>
<td>0.00%</td>
<td>Thu Dec 9 19:27:03 2004</td>
</tr>
<tr>
<td>ACM/DoorDB</td>
<td>1</td>
<td>2136 Bytes</td>
<td>0.01%</td>
<td>Thu Dec 9 19:27:03 2004</td>
</tr>
<tr>
<td>InputDB-SID-&gt;10</td>
<td>8</td>
<td>4384 Bytes</td>
<td>0.01%</td>
<td>Thu Dec 9 19:27:03 2004</td>
</tr>
<tr>
<td>OutputDB-SID-&gt;10</td>
<td>2</td>
<td>744 Bytes</td>
<td>0.00%</td>
<td>Thu Dec 9 19:27:04 2004</td>
</tr>
<tr>
<td>MaskDB-SID-&gt;1</td>
<td>2</td>
<td>56 Bytes</td>
<td>0.00%</td>
<td>Tue Jun 1 22:20:33 1999</td>
</tr>
<tr>
<td>MaskDB-SID-&gt;10</td>
<td>14</td>
<td>382 Bytes</td>
<td>0.00%</td>
<td>Thu Dec 8 16:57:40 2004</td>
</tr>
<tr>
<td>ACM/EntranceDB</td>
<td>1</td>
<td>140 Bytes</td>
<td>0.00%</td>
<td>Thu Dec 9 16:57:40 2004</td>
</tr>
<tr>
<td>ACM/FloorDB</td>
<td>3</td>
<td>216 Bytes</td>
<td>0.00%</td>
<td>Thu Dec 9 16:57:38 2004</td>
</tr>
<tr>
<td>ACM/CutOutlineDB</td>
<td>9</td>
<td>1336 Bytes</td>
<td>0.00%</td>
<td>Thu Dec 9 19:27:33 2004</td>
</tr>
<tr>
<td>ACM/ClearanceDB</td>
<td>2</td>
<td>212 Bytes</td>
<td>0.00%</td>
<td>Thu Dec 9 16:57:29 2004</td>
</tr>
<tr>
<td>ACM/LCIDB</td>
<td>47</td>
<td>3916 Bytes</td>
<td>0.01%</td>
<td>Thu Dec 9 16:57:40 2004</td>
</tr>
<tr>
<td>ACM/PeopleDB</td>
<td>0</td>
<td>0 Bytes</td>
<td>0.00%</td>
<td>Tue Jun 1 22:22:33 1999</td>
</tr>
<tr>
<td>SIS/UpgradeDB</td>
<td>1</td>
<td>144 Bytes</td>
<td>0.00%</td>
<td>Thu Dec 9 16:57:40 2004</td>
</tr>
<tr>
<td>GroupUP</td>
<td>11</td>
<td>1336 Bytes</td>
<td>0.00%</td>
<td>Thu Dec 9 16:57:41 2004</td>
</tr>
<tr>
<td>ActionListDB</td>
<td>8</td>
<td>736 Bytes</td>
<td>0.00%</td>
<td>Thu Dec 9 16:57:37 2004</td>
</tr>
<tr>
<td>EventLinkDB</td>
<td>3</td>
<td>532 Bytes</td>
<td>0.00%</td>
<td>Thu Dec 9 16:57:42 2004</td>
</tr>
<tr>
<td>TempSpecDB</td>
<td>18</td>
<td>2454 Bytes</td>
<td>0.00%</td>
<td>Thu Dec 9 16:57:40 2004</td>
</tr>
<tr>
<td>HolidayDB</td>
<td>4</td>
<td>480 Bytes</td>
<td>0.00%</td>
<td>Thu Dec 9 16:57:40 2004</td>
</tr>
<tr>
<td>CallBackPhoneNumber</td>
<td>0</td>
<td>0 Bytes</td>
<td>0.00%</td>
<td>Tue Jun 1 22:22:17 1999</td>
</tr>
<tr>
<td>PhoneNumber</td>
<td>0</td>
<td>0 Bytes</td>
<td>0.00%</td>
<td>Tue Jun 1 22:22:17 1999</td>
</tr>
<tr>
<td>ConnectionPath</td>
<td>2</td>
<td>256 Bytes</td>
<td>0.00%</td>
<td>Tue Jun 1 22:22:40 1999</td>
</tr>
<tr>
<td>AccessGroupDB</td>
<td>12</td>
<td>1536 Bytes</td>
<td>0.00%</td>
<td>Thu Dec 9 16:57:32 2004</td>
</tr>
<tr>
<td>DG_notify_events</td>
<td>0</td>
<td>0 Bytes</td>
<td>0.00%</td>
<td>Tue Jun 1 22:22:11 1999</td>
</tr>
<tr>
<td>DG_notify_group</td>
<td>0</td>
<td>0 Bytes</td>
<td>0.00%</td>
<td>Tue Jun 1 22:22:11 1999</td>
</tr>
</tbody>
</table>
Table 8-2 describes the controller SDRAM memory status that displays at the top of the window.

<table>
<thead>
<tr>
<th>Item</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Object Store</td>
<td>Indicates the total SDRAM memory that is available for the Object Store Database.</td>
</tr>
<tr>
<td></td>
<td>Total Object Store memory is based on the total system memory minus the 8 MB of memory that is used for the iSTAR driver processes.</td>
</tr>
<tr>
<td>Unused Object Store</td>
<td>Indicates the amount of available SDRAM.</td>
</tr>
<tr>
<td>Percent Free</td>
<td>The percentage of available SDRAM, which is the Unused Object Store divided by the Total Object Store.</td>
</tr>
</tbody>
</table>

In the database table, you can click the following database names to display more details about the selected database:

- **Personnel** – Displays personnel records.
- **Tracking** – Displays anti-passback information.
- **ACMClearanceDB** – Displays all clearances that have been configured.
- **EventLinkDB** – Displays the Link ID, State, Activation Time, Start Time, and Link time for event links.
- **TimeSpecDB** – Displays all time specifications that have been configured.
- **PhoneNumber** – The RAS telephone number.
- **ConnectionPath** – Displays all connection path information for the current controller.
Diagnostic Screens

Diagnostic screens display information about the following:
- iSTAR network
- Readers and I/O devices connected to iSTAR Edge
- SID (Subsystem ID) diagnostic level controls

Network Diagnostics

The **Network Diagnostics** section displays diagnostic information about iSTAR networks, addresses, data transmissions, protocols, and routing. Figure 8-6 shows a portion of the Network Diagnostics screen.

**Figure 8-6: Network Diagnostics Screen**

<table>
<thead>
<tr>
<th>Network Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ethernet Adaptors</strong></td>
</tr>
<tr>
<td>Onboard Ethernet#1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received Header Errors</td>
</tr>
<tr>
<td>Received Address Errors</td>
</tr>
<tr>
<td>Received Datagrams Discarded</td>
</tr>
<tr>
<td>Received Datagrams Delivered</td>
</tr>
<tr>
<td>Outgoing Datagram Requests</td>
</tr>
<tr>
<td>Outgoing Datagrams Discarded</td>
</tr>
<tr>
<td>Transmitted Datagrams Discarded</td>
</tr>
<tr>
<td>Datagrams With No Route</td>
</tr>
<tr>
<td>Datagrams For Which All Fragments Were Delivered</td>
</tr>
<tr>
<td>Datagrams Requiring Reassembly</td>
</tr>
<tr>
<td>Successful Reassemblies</td>
</tr>
<tr>
<td>Failed Reassemblies</td>
</tr>
<tr>
<td>Datagrams Fragmented</td>
</tr>
<tr>
<td>Successful Fragmentations</td>
</tr>
<tr>
<td>Failed Fragmentations</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connections Initiated</td>
</tr>
<tr>
<td>Connections Accepted</td>
</tr>
</tbody>
</table>

In addition to IP information, the Network Diagnostics screen also shows TCP, UDP, ICMP, ARP, and routing information.
Reader and I/O Diagnostics

The Reader & I/O Diagnostic selection displays information about devices, such as readers, that communicate with iSTAR Edge, shown in Figure 8-7. This screen also displays diagnostic output for iSTAR readers and cards. Refer to “iSTAR Edge Diagnostic Tests” on page 9-5 for information about iSTAR diagnostic tests.

**Figure 8-7:** Reader & I/O Screen

### Reader and I/O Diagnostics

<table>
<thead>
<tr>
<th>Last Input Change</th>
<th>State</th>
<th>Time (GMT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rd#3 CornStatus</td>
<td>Secure</td>
<td>Thu Nov 1 22:16:49 2004</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Last Output Change</th>
<th>State</th>
<th>Time (GMT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACM1 Output#1</td>
<td>Deactivated</td>
<td>Thu Nov 1 22:17:57 2004</td>
</tr>
</tbody>
</table>

### Last Card Swipe

<table>
<thead>
<tr>
<th>Reader Name</th>
<th>Time (GMT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rd#1-3</td>
<td>Thu Nov 1 22:17:52 2004</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Raw Card Data</th>
<th>Card Data Length</th>
<th>Config Flag</th>
<th>Data Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>841bd140</td>
<td>26 Bits</td>
<td>88H</td>
<td>0H</td>
</tr>
</tbody>
</table>

### Last Card Swipe for Each Reader

<table>
<thead>
<tr>
<th>Reader Name</th>
<th>Raw Card Data</th>
<th>Best Guess Card Information</th>
<th>Time (GMT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rd#1-3</td>
<td>841bd140</td>
<td>Reserved for future use</td>
<td>22:17:52</td>
</tr>
<tr>
<td>Rd#1-8</td>
<td>36bb0200</td>
<td>Reserved for future use</td>
<td>15:26:51</td>
</tr>
</tbody>
</table>
SID Diagnostic Levels

The SID Diagnostic Levels (Controller Diagnostics) selection displays the Diagnostic Level Control screen, shown in Figure 8-8. From this screen, you can choose the reports to display or log for the selected controller’s subsystem.

Figure 8-8: Diagnostic Level Control Screen

Each subsystem (General Controller I/O, Comm Server, etc.) has several report categories. To display or log any or all of these, click the appropriate check boxes.
Displaying Diagnostic Information

You can display diagnostic information from the iSTAR Diagnostic Control window using either:

- A terminal session, such as a Hyperterminal session.
- Or -
- A Real Time Monitor Controller Diagnostic window from the ICU.

To use the ICU to display diagnostic messages

1. In the ICU main window, highlight the controller you selected in the Web Page Diagnostic Utility, right-click, and select Real Time Monitor from the drop-down menu.
   The Set Diagnostic Levels window displays.

2. Click OK to display the message levels you selected in the Web Page Diagnostic Utility
   - Or -
   Select new levels by checking items on the Set Diagnostic Level dialog box.

3. Exit by selecting Edit and Clear levels on exit to stop diagnostic recording.

Because diagnostics can slow system performance, Software House recommends that you use them only as necessary.
iWatch2 Network Diagnostic Tool

**iWatch2** is a network diagnostic tool to help collect data for troubleshooting iSTAR Edge panels. iWatch2 uploads serial port data over the network using ICU without using a serial cable.

**Installation**

The **iWatch2** utility is installed with C•CURE (9000 Version 1.92 and later, and 800/8000 Version 10.0 and later) into the following folder:

\Software House\SWHSystem\ServerComponents\iSTAR\ICU

The **iWatch2** utility requires the following files:

- iWatch2.exe
- ICU.exe (Version 5.0.0 minimum)
- iWatch.exe
- iSTARDiagConnection.dll

**Starting iWatch2**

Perform these steps to start **iWatch2**:

1. Run ICU Version 5.x.x.
2. Select the iSTAR panel that you want to connect to.
3. Right-mouse click and select **Real-time Monitor**, as shown in Figure 8-9 on page 8-15.
iWatch2 Opens

4. When you select Real-time Monitor, iWatch2 opens, as shown in Figure 8-10 on page 8-16.

NOTE For iSTAR panels with firmware less than 5.0.0, the normal iWatch will open.
iWatch2 Screen

The iWatch2 screen contains the fields shown in Figure 8-10.

**Figure 8-10:** Watch2 Screen
iWatch2 Connects to iSTAR to Capture Data

5. The iWatch2 utility connects to the specified iSTAR to capture data, and places the data in an output file in the Output directory.

The captured data is also displayed in the Output area at the bottom of the screen, as shown in Figure 8-11.

Figure 8-11: iWatch2 Data
iWatch2 Fields

The following iWatch2 fields appear on the screen:

- **IP** - IP address of the iSTAR controller.
- **Port** - Read-only field that shows the port being used to connect.
- **Password** - Password of the iSTAR controller, if it is configured from C•CURE Administration application.
- **State** - Status of the iWatch utility (connected, disconnected).
- **Stream msgs** - Number of messages being streamed.
- **Bytes in** - Size of inbound messages in bytes.
- **Bytes out** - Size of outbound messages in bytes.
- **Last msg time** - Time when last message was received.
- **Reconnect in** - Number of seconds left until next automatic re-connection attempt.

**Connection type:**

- **Upload and stop** - Upload whatever data is on the panel, and then stop the capture.
- **Live** - Capture the live data.
- **Upload and stay live** - Upload whatever data is on the panel, and then continue to capture live data.

- **Attempt reconnect** - If this check box is checked, *iWatch2* will continue trying to reconnect to the iSTAR if the connection is unsuccessful.

- **Reconnect Wait** - Specify the time to wait before *iWatch2* tries to reconnect to the panel.

- **Output file** - By default, the output data file is stored in this folder:

  \Software House\SWHSystem\ServerComponents\iSTAR\ICU
Figure 8-12: Output File: \Software House\SWHSystem\ServerComponents\istar\ICU Directory

Output File Commands

- **Change Directory** - Click this button to browse a different destination for the output file.
- **Open file** - Click this button to open the current data file.
- **Delete file** - Click this button to delete the current data file.
- **Output directory** - A read-only field that shows the path of the output file.
- **Output file** - Name of the output file.

**Control**

- **Exit** - Click to exit iWatch2.
- **Connect** - Click to connect to the iSTAR panel.
- **Disconnect** - Click to disconnect from the iSTAR panel.
- **Output** - A read-only multi-line field that contains data.
iSTAR Diagnostic System

To run the iWatch2 utility and get data:

1. Select the “Net Diag” check box at the bottom of the iSTAR webpage
2. Click Submit, as shown in Figure 8-13.

Figure 8-13: STAR Diagnostic Level Control
The iSTAR Edge 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

- Setting the LCD Message Display ................................................................................ 9-2
- Displaying Status Messages .......................................................................................... 9-4
- iSTAR Edge Diagnostic Tests ........................................................................................ 9-5

**NOTE**
The iSTAR Edge LCD display and associated diagnostic tests have not been evaluated by UL.
Setting the LCD Message Display

The iSTAR Edge includes an LCD display for status and diagnostic messages. Set the LCD display for desired messages using rotary switch SW1.

Figure 9-1 shows the location of the rotary switch SW1. See Table 9-1 on page 9-3 for a summary of SW1 settings.
### Table 9-1: Rotary Switch SW1 Diagnostic Tests for iSTAR Edge

<table>
<thead>
<tr>
<th>Set SW1 to</th>
<th>Performs this Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>Displays general status messages. ICU fields are Read Only and cannot be changed.</td>
<td>ICU Block on</td>
</tr>
<tr>
<td>0</td>
<td>Displays general status messages. Users can Read, Write, and Update ICU configuration.</td>
<td>ICU Block off</td>
</tr>
<tr>
<td>1</td>
<td>Displays most recent card swipe for 1 second</td>
<td>Fast Mode on</td>
</tr>
<tr>
<td>2</td>
<td>Displays most recent card swipe for 7 seconds</td>
<td>Slow Mode on</td>
</tr>
<tr>
<td>3</td>
<td>Tests and displays information about manual <strong>inputs</strong> for 1 second</td>
<td>Slow Mode Input Test</td>
</tr>
<tr>
<td>4</td>
<td>Tests and displays information about manual <strong>inputs</strong> for 2 seconds</td>
<td>Fast Mode Input Test</td>
</tr>
<tr>
<td>5</td>
<td>Activates <strong>output</strong> change display tests for manually activated outputs and displays information for 2 seconds</td>
<td>Slow Mode Output Test</td>
</tr>
<tr>
<td>6</td>
<td>Activates and tests <strong>all outputs</strong> attached to an iSTAR Edge through readers and R/8 boards for 1 second</td>
<td>Fast Mode Output test. LCD does not display <strong>all info</strong></td>
</tr>
<tr>
<td>7</td>
<td>Activates and tests <strong>all outputs</strong> attached to an iSTAR Edge, one by one. Test results are indicated by the LED associated with each output.</td>
<td>Displays results on LED</td>
</tr>
<tr>
<td>8</td>
<td>Tests and displays diagnostic information about Ethernet #1 and Ethernet #2 ports.</td>
<td>Ethernet Port and CF Slot Test</td>
</tr>
</tbody>
</table>
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 SW1 rotary switch to positions 0 (zero) or F. Setting the SW1 switch to 0 or F also controls the ICU Block feature, preventing or allowing users from modifying the ICU configuration, as shown in Table 9-2.

- **When ICU Block is On** (set SW1 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 SW1 to 0) – the LCD displays general status messages, and users can read, write, and update the ICU configuration.

Table 9-2: LCD Status Display Messages

<table>
<thead>
<tr>
<th>Rotary Switch SW1</th>
<th>Display General Messages (Read only) ICU Block On</th>
<th>Display General Messages (Read/Write/Update) ICU Block Off</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set SW1 to:</td>
<td>F</td>
<td>0</td>
</tr>
</tbody>
</table>

iSTAR Edge Installation and Configuration Guide
iSTAR Edge Diagnostic Tests

iSTAR Edge firmware provides diagnostic information for:

- Readers
- Cards
- Outputs
- Inputs
- Ethernet port

Use rotary switch SW1 to activate diagnostic tests. Diagnostic information displays on the iSTAR Edge LCD.

**NOTE**
Diagnostic tests add overhead to iSTAR Edge processing, and may degrade system performance. When the diagnostic tests are complete, deactivate the test by resetting SW1 to display status information.

Card Reader Diagnostics

You can display the most recent card data processed by any reader on iSTAR Edge 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 SW1 rotary switch to the positions shown in Table 9-3.

<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 SW1 to:</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 9-3: Reader Diagnostic Switch Settings
You can also use the iSTAR Web Page Diagnostic Utility to view reader diagnostic information. For information about this utility, see “Diagnostic Screens” on page 8-10.

Output Diagnostics

CAUTION: Do not activate outputs on a live system!

The iSTAR Edge provides three types of output tests:

- **Output Change Display (slow)** – tests a specific output that is activated manually by the technician
- **Output Change Display (fast)** – activates and tests every output on the system
- **Output Test Mode** – activates and tests outputs one by one.

CAUTION: Do not activate outputs on a live system!

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 Edge through readers and R/8 boards. Information displays on the LED for two seconds.

To activate the output change display test, set rotary switch SW1 to the position shown in Table 9-4.

<table>
<thead>
<tr>
<th>Switch Position</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW1 set to 5</td>
<td>Activate output change display for two seconds (slow mode)</td>
</tr>
</tbody>
</table>
Output Change Display (Fast Mode)

The output change display test is an end-to-end test that automatically activates all outputs attached to iSTAR Edge. The outputs you are testing can be attached to iSTAR Edge through readers and R/8 boards. Output information displays on the LED for approximately one second. However, since outputs activate faster than the one-second LCD display, the LCD does not display all output information.

To activate the output change display test, set rotary switch SW1 to the position shown in Table 9-5.

### Table 9-5: Output Change Display Settings

<table>
<thead>
<tr>
<th>Switch Position</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW1 set to 6</td>
<td>Activate output change display test for one second (Fast mode)</td>
</tr>
</tbody>
</table>

Output Test Mode

The output test mode activates all outputs, one by one. Test results are indicated by the LED associated with each output.

To activate the output test, set switch SW1 to the position shown in Table 9-6.

### Table 9-6: Output Test Switch Settings

<table>
<thead>
<tr>
<th>Switch Position</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW1 set to 7</td>
<td>Output Test Mode activates and tests all outputs one by one</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 Edge through the main board, RM5, and I/8 boards.

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 SW1 rotary switch to the positions shown in Table 9-7.

### Table 9-7: Input Test Switch Settings

<table>
<thead>
<tr>
<th>Switch Position</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW1 set to 3</td>
<td>Two-second LED input change display is on (slow mode)</td>
</tr>
<tr>
<td>SW1 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, set switch SW1 to the position shown in Table 9-8.

### Table 9-8: Ethernet Test Switch Settings

<table>
<thead>
<tr>
<th>Switch Position</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW1 set to 8</td>
<td>Tests the Ethernet Port</td>
</tr>
</tbody>
</table>

Observe the LCD display for test results.

If the Ethernet card passes the diagnostic test, you will see the following message on the LCD:

```
Ethernet PC Card
* Passed *
```

1. When the test is complete, set SW1 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.
<table>
<thead>
<tr>
<th><strong>10BaseT</strong></th>
<th>A version of Ethernet in which stations are attached by twisted pair cable, the traditional cables used for telephone lines. 10BaseT uses a star topology, and has a bandwidth of 10 megabits per second.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>10BaseFL</strong></td>
<td>A version of Ethernet that uses fiber and has a bandwidth of 10 megabits per second.</td>
</tr>
<tr>
<td><strong>100BaseTX</strong></td>
<td>A version of Ethernet that uses copper and has a bandwidth of 100 megabits per second.</td>
</tr>
<tr>
<td><strong>100BaseFX</strong></td>
<td>A version of Ethernet that uses fiber and has a bandwidth of 100 megabits per second.</td>
</tr>
<tr>
<td><strong>1000BaseLX,SX</strong></td>
<td>A version of Ethernet that uses fiber and has a bandwidth of 1 gigabit per second.</td>
</tr>
<tr>
<td><strong>1000BaseT</strong></td>
<td>A version of Ethernet that uses copper and has a bandwidth of 1 gigabit per second.</td>
</tr>
<tr>
<td><strong>ABA 2</strong></td>
<td>American Banking Association track 2. The track that magnetic signaling cards are normally recorded on. The apC and iSTAR field controllers support both Wiegand signaling and Magnetic (ABA 2) signaling.</td>
</tr>
</tbody>
</table>
Glossary

access card
Token (typically a plastic card) by which a person is identified to the security system for access control, usually for admittance through a door or passageway.

activate
To cause a security object to become active, triggering the actions associated with the security object.

Active Directory
Active Directory provides a single point of management for Windows-based user accounts, clients, servers, and applications. It also helps organizations integrate systems not using Windows with Windows-based applications, and Windows-compatible devices, thus consolidating directories and easing management of the entire network operating system.

activity log
The portion of the journal database containing records of real-time system activity. See also historical journal.

ADA
See alternate shunt.

advanced processing Controller (apC)
See apC.

alarm circuit
The complete path of the electric current, including the apC input circuit, wiring, and alarm device.

alarm, alert
Sometimes used to refer to the active state of an alarm object.

alarm device
A sensor that is either on or off, connected to a C•CURE 800/8000 input. See also input.

alternate master
The alternate master assumes responsibility for communications with the host and cluster in the event of a communications failure on the primary communications path. If the secondary communications path uses a second connection on the master, there is no alternate master possibility.
<table>
<thead>
<tr>
<th>Glossary Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alternate shunt</td>
<td>The Alternate Shunt (ADA) flag on a cardholder’s record is set when a person has Americans with Disabilities (ADA) status. You configure the door output that activates to open the door when a user with the Alternate Shunt (ADA) flag set swipes his or her card on a door-by-door basis. The alternate shunt is sometimes used to control aircraft loading doors. The ADA output that is associated with the alternate shunt is a 100 milli-second pulse output that is used to control automatic doors.</td>
</tr>
<tr>
<td>Americans with Disabilities (ADA) Act</td>
<td>See alternate shunt.</td>
</tr>
<tr>
<td>antipassback</td>
<td>Antipassback prevents a person from going through any door if they are not at that door “legally.” It prevents “passing back” a card for another person to use as well as “tailgating.” See also GMT.</td>
</tr>
<tr>
<td>apC</td>
<td>The first generation of the field panel that performs access control functions. See also apC/8X and apC/L.</td>
</tr>
<tr>
<td>apC/8X</td>
<td>The field panel that performs access control functions, such as granting a cardholder access. The apC/8X is housed in a wall-mounted metal cabinet, and comprises a control board with 8 inputs, 8 outputs, and a reader port that supports 8 readers. The generic term for this processor is ‘panel.’ The current model of the panel has a higher storage capacity and uses newer technology than the earlier apC model.</td>
</tr>
<tr>
<td>apC/L</td>
<td>A smaller model of the panel that can be used for garages and small office buildings. The apC/L supports two readers, has two outputs, and no inputs. Inputs and outputs can be expanded using I/O bus modules.</td>
</tr>
<tr>
<td>apC Poll</td>
<td>The poll period that the host uses when communicating with an apC. It can be set as fast as every 100 milli-seconds. If the apC is connected through the network it is recommended to be set at every 1.5 - 3.0 seconds.</td>
</tr>
<tr>
<td>application programming interface</td>
<td>A set of routines used by an application program to direct the performance of procedures by the computer’s operating system. Acronym API. Also called application program interface.</td>
</tr>
</tbody>
</table>
Glossary

area A location monitored with one or more entrance readers and one or more exit readers for antipassback control and general monitoring of a cardholder’s location.

arm To enable a security object so it will report state changes and act on action requests. Disarmed supervised inputs will continue to report wiring tampering or supervision errors (short and open conditions). Inputs and events can be armed.

armed To “pay attention” to a security object. When a security object is armed, the system pays attention to any changes in its state and can then perform appropriate actions. An intrusion zone that is armed is considered to be in armed mode. See armed mode.

armed mode Intrusion zone mode during which the area is protected - all doors are locked and all inputs are armed. No one can enter an armed intrusion zone without activating these inputs and causing an intrusion zone violation.

ASCII Acronym for American Standard Code for Information Interchange. A coding scheme using seven or eight bits, assigning numeric values to up to 256 characters, including letters, numerals, punctuation marks, control characters, and other symbols. ASCII was developed in 1968 to standardize data transmission among disparate hardware and software systems and is built into most minicomputers and all PCs. ASCII is divided into two sets: 128 characters (standard ASCII) and an additional 128 (extended ASCII).

baud rate Rate of serial data transfer. Equivalent to bits per second. In most cases divide this number by 10 to get the number of bytes per second. This is because the typical character has 1 start bit, 8 data bits, and 1 stop bit for a total of 10.

bit A BInary digiT. The basic building block of card formats, computers and data transfer. A bit has 2 stable states, one and zero.

bits per second Rate of serial data transfer.

backup The technique of making copies of data that can be recovered in the event of a failure of the system.
| **badging** | The C•CURE ID option lets you layout, create and print badges. |
| **Bi-directional Interface** | A general purpose interface for third party devices. The interface is through an RS-232 communications port which can also be through a terminal server. The user can define actions to transmit and receive data to and from the device. Radionics alarm panels, the Stentofon intercom system, and the Simplex-Grinnel fire panel have been interfaced to C•CURE using this feature. |
| **Bi-Di Action** | An output message to a Bi-Di device. |
| **Bi-Di Action Protocol** | A set of Bi-Di actions. |
| **Bi-Di Device** | The device that the Bi-Di interface is communicating with. Supported devices are Radionics, Stentofon, Inovonics, BiDVideo, Simplex-Grinnel Fire, and General Purpose. |
| **Bi-Di Gateway** | An Inovonics Gateway that multiple Inovonics transmitters can interface to. |
| **Bi-Di Message Protocol** | The mechanism to capture an incoming message from a Bi-Di device. The Message Protocol can be used to activate events. |
| **Bi-Di Poll** | A form of a optional Bi-Di action that is used to poll the device. |
| **Biometrics** | The technique of using physical characteristics of a person such as finger prints, hand geometry, eye structure or voice pattern for access control. |
| **byte** | A group of 8 bits. Is sometimes broken into two 4 bit nibbles. |
| **camera iris** | The user can specify different iris settings for live video feeds and during flash snapshot capture. A delay can also be specified, allowing for manual synchronization between snapshot capture and the flash trigger. |
camera type
Indicates the camera type, either Dome or Video. Dome cameras cover an area on a 360 degree basis; video cameras are stationary, but may have zoom or move controls that allow a range of coverage manipulated by an operator.

card format
The way information is encoded on a security access card. A definition of which field is the card number, facility code, site code, etc.

card format offset
The offsetting or shifting of another card field such as Facility code into the personnel database card number. This technique is used to differentiate between duplicate card numbers.

card format complement
The ability of applying what is known as the “ones complement” to a card field. The ones complement means to reverse all of the bits. Example: the 1’s complement of 01100011 is 10011100. This technique is sometimes used to confuse would be hackers.

cardholder
An employee or visitor who has been given a functional security access card. The access the card provides is determined by values assigned in the C•CURE clearance database.

card number
Name of a credential field in the cardholder database that represents the card number. This field can also include parts of other fields that have been offset into it. Also, a field on an access card. It is the field that uniquely identifies that card. See also personnel and user.

card reader
See Reader.

cause list
The set of actions that affect the current state of an object. For example, all the active output change requests together affect the status for an output. The cause list always has at least one ‘cause,’ which is the default state of the value. The state is determined by the highest priority cause. If causes have equal priority, the most recent one takes precedence.

CCTV
Closed Circuit TeleVision. A C•CURE feature that lets you control video cameras and monitors that are attached to a CCTV switcher.

C•CURE ID
The imaging and badging system available as an option on C•CURE.
clearance  A security object containing a list of doors and/or elevators along with times during which the cardholder is allowed access.

client  A PC that uses the services provided by a Server PC, which contains centralized data. The C•CURE Client provides the administration interface, reporting capabilities, monitoring, maps and badging.

client time zone  The time zone for a client PC, set on the Windows 2003/XP Control Panel using the Date/Time icon.

Closed Circuit Television (CCTV)  See CCTV.

cluster  A cluster is a user-defined group of one or more iSTAR controllers that can communicate with each other, such that a designated Master is the centered iSTAR communicator with the host.

coaxial cable  A round, flexible, two-conductor cable consisting of (from the center outwards) a copper wire, a layer of protective insulation, a braided metal mesh sleeve, and an outer shield, or jacket of PVC or fire-resistant material. The shield prevents signals transmitted on the center wire from affecting nearby components and prevents external interference from affecting the signal carried on the center wire. Coaxial cable is used in networks and is similar to the type of wiring that is used for cable television.

communications  See primary communications path and secondary communications path.

company code  See site code and facility code.

connection path database  Contains the following information on all iSTAR controllers in the cluster: MAC address, IP address, type of device (master, member, host), and connection method (Ethernet, serial, dialup). See also media access control (MAC) address.

connection verification (keep alive or heartbeat)  A short message, sent by the Host or an iSTAR Controller during periods of message inactivity that lets the recipient know that the transmitter is connected and operating correctly. Users configure the message frequency.
### Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>controller ID</strong></td>
<td>The 32-bit IP Address of each General Controller Module that uniquely identifies each iSTAR.</td>
</tr>
<tr>
<td><strong>controller or cluster member (slave)</strong></td>
<td>An iSTAR Controller that is connected to a master controller within a cluster.</td>
</tr>
<tr>
<td><strong>DB-9</strong></td>
<td>A standard 9 pin connector that is typically used with COMM ports.</td>
</tr>
<tr>
<td><strong>DB-25</strong></td>
<td>A standard 25pin connector that is typically used with COMM ports and modems.</td>
</tr>
<tr>
<td><strong>DCE</strong></td>
<td>Data Communications Equipment. The port should have female pins and the required crossover connection inside the device. A modem is a typical DCE device. When you connect a DTE device to a DCE device there is no need to provide an external crossover (null modem).</td>
</tr>
<tr>
<td><strong>deactivate</strong></td>
<td>To cause a security object to become inactive.</td>
</tr>
<tr>
<td><strong>DES</strong></td>
<td>Data Encryption Standard - The name of the Federal Information Processing Standard (FIPS), which describes the data encryption algorithm (DEA). DES and DEA are interchangeable. The DEA has a 64-bit block size and uses a 56-bit key during execution (8 parity bits are stripped off from the full 64-bit key.</td>
</tr>
<tr>
<td><strong>DES 3</strong></td>
<td>Triple DES (3 DES) - The same as DES except that the input data is, in effect, encrypted three times using three keys. This mode of encryption is sometimes referred to as DES-EDE.</td>
</tr>
<tr>
<td><strong>DHCP</strong></td>
<td>Dynamic Host Configuration Protocol. A server that leases out and manages IP addresses on the network.</td>
</tr>
<tr>
<td><strong>digital</strong></td>
<td>Related to digits or the way they are represented. In computing, analogous to binary because the computers familiar to most people process information coded as combinations of binary digits (bits).</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>digital video cameras</td>
<td>NetVue provides independent camera configuration, which includes camera name (up to 32 characters), description, maximum pre-alarm time, and maximum post-alarm time. NetVue also provides independent camera controls, including pan and tilt zoom controls. NetVue recognizes the digital video server (DVS) and channel to which the camera is connected.</td>
</tr>
<tr>
<td>digital video servers (DVS)</td>
<td>NetVue is a scalable system, so different digital video systems may be used. It is necessary for users to obtain the appropriate license for each supported video server system in their configuration. Currently, Nice, Loronix, Integrel and Intellex Systems are supported.</td>
</tr>
<tr>
<td>direct cable connection</td>
<td>A link between the I/O ports of two computers using a single cable rather than a modem or other interface device.</td>
</tr>
<tr>
<td>direct connect</td>
<td>apCs, apC/8Xs, and apC/Ls that are in continuous communication with the C•CURE host. These panels may be directly wired to the host with copper or fiber optics, or connected long distance via lease line modems or line drivers. The host expects to be in communication with the panels at all times as contrasted to dialup panels where the contact is periodic.</td>
</tr>
<tr>
<td>disarm</td>
<td>Action taken on a security object to change its monitoring status to not monitored. The apC will ignore state changes of a disarmed security object but will still monitor the object for supervision errors.</td>
</tr>
<tr>
<td>disarmed</td>
<td>To ignore a security object’s state changes, but still monitor supervision errors. An intrusion zone that is disarmed is considered to be in disarmed mode. See disarmed mode.</td>
</tr>
<tr>
<td>disarmed mode</td>
<td>Intrusion zone mode that allows personnel to move freely throughout the intrusion zone without causing intrusion zone violations. When an intrusion zone is in disarmed mode, the inputs assigned to that intrusion zone are disarmed and do not generate intrusion zone violations when activated. When the intrusion zone is in disarmed mode, the user may configure the intrusion zone doors to be both unlocked, allowing free access, or locked to control access.</td>
</tr>
</tbody>
</table>
### Glossary

**DLL (dynamic link library)**
A collection of library routines, any of which can be called when needed by a larger program that is running in the computer. The small program that lets the larger program communicate with a specific device - for example, a printer or scanner - is often packaged as a DLL program (usually referred to as a DLL file). DLL files save space in RAM. When, and if, a DLL file is needed, it is loaded and run. For example, as long as a Microsoft Word user is editing a document, the printer DLL file does not need to be loaded into RAM. When the user decides to print the document, the Word application then causes the printer DLL file to be loaded and run.

**DNS**
Domain Name Service. A server or series of servers that translates IP addresses into Fully Qualified Domain Names (FQDN) or FQDN’s to IP addresses.

**Domain**
A group of computers and devices on a network that are administered as a unit with common rules and procedures. Within the Internet, domains are defined by the IP address. Domains also refer to the redundant servers and associated fail over group under EMC AutoStart.

**door**
The passageway through which the system controls access. A door can be configured with up to two access readers and a Door Latch Relay, or one reader and a Request to Exit (RTE).

**door latch relay**
An output in the system which controls the physical lock for the door.

**door switch monitor (DSM)**
An input that monitors whether a door is opened or closed. It can be set for automatic shunting so alarms do not occur during normal door access.

**DRAM**
Dynamic Random Access Memory for local database/event storage on the iSTARs.

**dry contact**
A relay contact that does not have a voltage source on it. Used to switch power to an output device.

**DSN (data source name)**
An ODBC data source configured on the ODBC Data Source Administrator dialog box accessed from the Windows 2003/XP Control Panel. See also *ODBC (open database connectivity)*.
**DTE**
Data Terminal Equipment. The port should have male pins. PC’s, apC’s, and dumb terminals are typical DCE devices. When you connect a DTE device to a DCE device there is no need to provide an external crossover (null modem). When you connect a DTE to a DTE there is a need for an external crossover or null modem.

**duress message**
A message sent to the C•CURE if a person is forced by an intruder to open a door. The card formats are set up so that a reverse swipe at a reader sends a duress message to the Monitoring Station. The duress condition can also be signaled by entering the PIN plus 1 if it is a proximity card.

**e-mail**
Electronic mail (messages) automatically passed from one computer user to another through a computer network and/or via modems over common-carrier lines.

**Entrance Delay Shunt**
Used to configure inputs on an iSTAR intrusion zone. If the Entrance Delay Shunt is selected, the input will not cause a violation during the entrance delay time. This is usually used to shunt a motion sensor inside the zone if you have to enter the zone in order to disarm the zone.

**Entrance Delay Trigger**
Used to configure inputs on an iSTAR intrusion zone. If the Entrance Delay Trigger is selected, the input will trigger an entrance delay when it is asserted. This might be used for a key operated door into an iSTAR intrusion zone. Inputs that are configured to trigger an entrance delay must also be shunted during the entrance delay.

**ethernet**
The most popular type of local area network, sending communications using signals carried by a coaxial cable, fiber-optic cable, or by twisted pair wiring. Ethernet uses a bus or star topology and relies on the form of access known as Carrier Sense Multiple Access with Collision Detection (CSMA/CD) to regulate communication line traffic.

Each computer checks to see if another computer is transmitting and waits its turn to transmit. If two computers accidentally transmit at the same time and their messages collide, they wait and send again in turn. Data is transmitted in variable length frames containing delivery and control information and up to 1,500 bytes of data.
The Ethernet standard provides for base band transmission at 10 megabits (10 million bits) per second and is available in various forms, including those known as Thin Ethernet, Thick Ethernet, 10Base2, 10Base5, 10Base-F, and 10Base-T. The IEEE standard dubbed 802.3z, or Gigabit Ethernet, operates at 10 times 100 Mbps speed. Software protocols used by Ethernet systems vary but include Novell Netware and TCP/IP. The General Controller Modules support communication by means of the Ethernet, using TCP/IP.

**even parity**

An error checking mechanism that requires that the total number of one bits, including the parity bit, is even. Used to verify the left side of wiegand cards and for the longitudinal check character of a magnetic card.

**event**

An event is a C•CURE security object that lets you link actions, annunciations, and timed activations into one component. Events are triggered by state changes, such as input activations, rejected accesses, or duress, or can be scheduled for specific times. Events can perform multiple functions depending on the actions you associate with them. For example, you can configure an event so that it sounds an alarm, or unlocks various doors.

**event beeping (event-audible alert)**

A system-wide option that causes the monitoring station to beep periodically when the highest-priority unacknowledged event activates.

**event breakthrough**

A feature which causes the monitoring station to become the active window (pop open, move to the top of the open applications, and enlarge) when an event requiring acknowledgment activates.

**event priority**

When events are configured they are given a priority level from 1 (low) to 200 (high). If two or more events are trying to perform conflicting actions the event with the highest priority will win. If the conflicting events have the same priority then the one that occurred last will win. Manual actions executed from the Monitor Station are subject to the same priority rules.

**event sound**

A feature that causes the monitoring station to play a sound instead of a beep, once or periodically, when the highest-priority unacknowledged event activates.
**external database**  
An ODBC-compliant database outside the C CURE System from which C CURE personnel data records are imported.

**facility code**  
Data field on an access card that contains information unique to the facility where the card is issued.

**field**  
Has two definitions:

In personnel views, a field is a dialog box element in the Layout area of the Configure Layout dialog box that is composed of one or two widgets. For example, PIN and its edit field are one field.

In the personnel record database, a field contains values that are stored in the cardholder record database.

**Fire wall**  
A form of router that is programmed to allow only certain IP addresses and TCP ports to pass through.

**fixed data field**  
Field on an access card that is the same for all access cards of a particular card format used in the system.

**flash ROM**  
A non-volatile memory chip that you can reprogram online while the chip is installed in the panel.

**follow input**  
An input whose activation triggers the arming of an intrusion zone and whose deactivation triggers the disarming of the same intrusion zone. An input, such as a key or switch which has definite on and off positions, is an example of a follow input. See also toggle input and input.

**force arm**  
Action taken on an intrusion zone to change its mode to armed. If an intrusion zone’s status is **Not Ready to Arm**, you must use the Force-Arm manual action to arm the zone. The status of an intrusion zone in disarmed mode is **Not Ready to Arm**, if:

- Any object assigned to the intrusion zone is not functioning normally.
- An intrusion zone input is active.
- An intrusion zone door is open.

See armed and armed mode.
<table>
<thead>
<tr>
<th><strong>Glossary</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FQDN</strong></td>
<td>Fully Qualified Domain Name. Example: HA1.accesssecurity.com</td>
</tr>
<tr>
<td><strong>gateway router</strong></td>
<td>A device that connects two computer networks that use different protocols. It translates between protocols so that devices in the connected networks can exchange data. For example, commercial online services often have gateways for sending email to Internet addresses. A MicroSoft Gateway is another word for Router.</td>
</tr>
<tr>
<td><strong>gateway IP address</strong></td>
<td>IP address for the gateway router.</td>
</tr>
<tr>
<td><strong>GCM</strong></td>
<td>General Controller Module - embedded microprocessor based controller card for iSTAR.</td>
</tr>
<tr>
<td><strong>General Purpose Interface</strong></td>
<td>See <em>Bi-directional Interface</em>.</td>
</tr>
<tr>
<td><strong>GMT</strong></td>
<td>Greenwich Mean Time, the local time at the 0 meridian passing through Greenwich, England. Greenwich mean time is the same everywhere. Also referred to as Universal Time (UT or UTC) or ZULU time.</td>
</tr>
<tr>
<td><strong>grace a card</strong></td>
<td>Used to forgive an antipassback. It allows the next access by this cardholder to work. There is also a Grace All function which allows all cardholders a free access.</td>
</tr>
<tr>
<td><strong>group</strong></td>
<td>A collection of security objects you can refer to using one name. Groups let you apply system conditions (such as a time specification) to more than one object at a time. Generally, anywhere in the system you can specify the name of a security object, you can also specify a group name. A group contains only objects of the same type.</td>
</tr>
<tr>
<td><strong>group box</strong></td>
<td>A widget in the layout area of the <em>Configure Layout</em> dialog box that consists of a box and label. See <em>group of fields</em> and <em>widget</em>.</td>
</tr>
<tr>
<td><strong>group of fields</strong></td>
<td>A group box and the fields and other group boxes that are located within the group box. See <em>group box</em>.</td>
</tr>
<tr>
<td>Glossary Item</td>
<td>Definition</td>
</tr>
<tr>
<td>---------------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>header character</strong></td>
<td>A value that defines the first character in a message from a Bi-Di device.</td>
</tr>
<tr>
<td><strong>Hexadecimal</strong></td>
<td>Using sixteen rather than ten as the base for representing numbers by digits. The hexadecimal system uses the digits 0 through 9 for the digits zero through nine and the letters A through F (uppercase or lowercase) for the digits ten through fifteen. One hexadecimal digit is equivalent to four bits, and one byte can be expressed by two hexadecimal digits. For example, binary 0101 0011 corresponds to hexadecimal 53. To prevent confusion with decimal numbers, hexadecimal numbers in programs or documentation are usually followed by H or preceded by &amp;, $, or 0x. Thus, 10H = decimal 16; 100H = decimal 256.</td>
</tr>
<tr>
<td><strong>historical journal</strong></td>
<td>The database that tracks two types of information: activity occurring in the system and monitored by the system, such as accesses, rejects, event activations, and input/output state changes (activity log); and changes made to the database through the Administration application, including additions, modifications, and deletions of security objects and personnel records (audit log). The historical journal may consist of several separate journal files.</td>
</tr>
<tr>
<td><strong>historical video journal</strong></td>
<td>Video actions are listed in the Journal, along with the associated event id. It is possible to replay the video segment from the Journal Replay function.</td>
</tr>
<tr>
<td><strong>Holiday</strong></td>
<td>An object that nullifies Time Specification based activities when the Holiday occurs. This is the object that ensures that the doors do not unlock on Thanksgiving but do unlock on other Thursdays. Holidays can be configured to be Once, Weekly, Monthly, and Yearly.</td>
</tr>
<tr>
<td><strong>Holiday list</strong></td>
<td>Groups of Holidays. There can be a maximum of 8 lists downloaded to apC’s and 24 downloaded to iSTAR’s. If there is a mixture of apC’s and iSTAR’s then use no more than 8.</td>
</tr>
<tr>
<td><strong>host</strong></td>
<td>The database and journal applications, residing on a host computer, interfaced to the iSTAR intelligent computer system. The host is used for initial cluster configuration, report activity generation, and management of peripheral hardware.</td>
</tr>
<tr>
<td><strong>I/8 input module</strong></td>
<td>A Reader Bus Module that monitors 8 supervised inputs and 1 tamper input. The I/8 Input Module connects to the reader bus on the iSTAR ACM or apC.</td>
</tr>
</tbody>
</table>
**ICU**  
iSTAR Configuration Utility. Used to setup the initial IP address and Master/Slave status.

**input**  
A security object that reports on the state of the security system. An input is connected to a switch which may be an alarm device. Examples of inputs are door switch monitors and motion detectors. Also known as a *monitor point*. See also *security object* and *alarm device*. 
### Glossary

**intrusion zone (iSTAR)**
User-defined group of doors and inputs that delineate a physical area monitored for alarms. The inputs assigned to an intrusion zone are usually used to monitor intrusion in the area. The doors assigned to an intrusion zone are used to define the entrance and exit points for the zone. In addition to doors and inputs, the user may assign four events to an intrusion zone. These events are used to indicate the current mode and status of the intrusion zone.

**intrusion zone doors**
One or more doors assigned to an intrusion zone that define the entrance and exit points for the intrusion zone.

**Intrusion zone events (iSTAR)**
Events that indicate the current mode and status of an iSTAR intrusion zone.

**intrusion zone inputs**
One or more inputs assigned to an intrusion zone that define the intrusion monitoring points for the area.

**intrusion zone readers**
All readers assigned to the intrusion zone doors.

**intrusion zone violation**
Situation that occurs when an intrusion zone input is activated in an armed intrusion zone. When an intrusion zone violation occurs, the apC notifies the C•CURE 800/8000 Server and activates the intrusion zone status output. In addition, the zone remains violated until the mode is changed to disarmed.

**IP Address**
Short for Internet Protocol address. A 32-bit (4-byte) binary number that uniquely identifies a host (computer) connected to other TCP/IP hosts, for the purposes of communication through the transfer of packets. An IP address is expressed in “dotted quad” format, consisting of the decimal values of its four bytes, separated with periods; for example, 127.0.0.1. The first one, two, or three bytes of the IP address identify the network the host is connected to; the remaining bits identify the host itself. The 32 bits of all 4 bytes together can signify $2^{32}$, or roughly 4 billion, hosts. (A few small ranges within that set of numbers are not used.) Also called Internet Protocol number, IP number.
### IP address (Version 4)

The IP Address (version 4) is a logical 32-bit number, divided into 4 bytes of 8 bits, that is configured for all devices communicating on a network using the TCP/IP protocol. Each device, including iSTAR controllers, must have a unique IP address. Example 172.31.101.234.

### IP address (Version 6)

Version 6 IP addresses will support 128-bit numbers. Also known as IPng. IP version 6 consists of 8 groups of 16 bits. Example 22:62457:1:0:0:345:89:7654.

### ipconfig

A Windows command to display the IP addresses of the NIC cards on a computer. Can also be used to release or renew a DHCP lease of an IP address.

### ISO

Short for International Organization for Standardization (often incorrectly identified as an acronym for International Standards Organization), an international association of countries, each of which is represented by its leading standard-setting organization—for example, ANSI (American National Standards Institute) for the United States. The ISO works to establish global standards for communications and information exchange. Primary among its accomplishments is the widely accepted ISO/OSI model, which defines standards for the interaction of computers connected by communications networks. ISO is not an acronym; rather, it is derived from the Greek word isos, which means “equal” and is the root of the prefix “iso.”

### ISO/OSI reference model

Short for International Organization for Standardization Open Systems Interconnection reference model. A layered architecture (plan) that standardizes levels of service and types of interaction for computers exchanging information through a communications network. The ISO/OSI reference model separates computer-to-computer communications into seven protocol layers, or levels, each building—and relying—upon the standards contained in the levels below it. The lowest of the seven layers deals solely with hardware links; the highest deals with software interactions at the application-program level. It is a fundamental blueprint designed to help guide the creation of networking hardware and software. Also called OSI reference model.

### issue code

Field on the access card that indicates how many times the card has been replaced. Is unique per individual and is considered as part of the access decision.
**iSTAR System**
The collection of all iSTAR Controllers that are configured by and report to a host. An intelligent controller system built around the embedded Windows CE operating system. iSTAR is a self operating networked device; a host downloads a database and journal information into the firmware upon initializing.

**journal**
See *historical journal*.

**Keypad Commands**
A feature that allows you to enter commands through a reader keypad. These commands are linked to events which can cause the various event actions to occur. The events that a keypad command is linked to must be downloaded to an iSTAR cluster.

**keypad duress**
A feature that allows a user at a door in a duress situation (being held at gun point, for example) to enter a code that triggers an alarm — if the reader has a keypad. Duress is indicated by entering PIN+1 on the keypad; for example, if the user’s PIN is 1234, enter 1235 on the keypad to indicate duress. See also *duress message*.

**KPC**
See *Key Pad Commands*.

**LAN**
Local Area Network. A network that connects computers that are close to each other, usually in the same building, linked by a cable.

**latency**
Generally, wasted time such as waiting for a disk seek. Also used to define the time it takes to get from one end of a network to the other.

**LBJ**
The jumpers that are used to configure features on iSTAR XL’s, I/8’s, R/8’s, etc. are sometimes referred to as “little black jumpers” or LBJ’s.

**LCD**
Liquid Crystal Display. A display that is used on RM readers, RM-4’s and iSTAR Pro’s.

**LED**
Light Emitting Diode. Display lights that are used in many parts of the hardware. The colors are green, red, and yellow.
**logical Input**

A logical input can be either a physical input triggered by a device or a user-defined message. See also *user defined message*.

**logical network**

A way to describe the topology, or layout, of a computer network. Referring to a logical (rather than physical) topology describes the way information moves through the network—for example in a straight line (bus topology) or in a circle (ring topology). The difference between describing a network as logical or physical is sometimes subtle because the physical network (the actual layout of hardware and cabling) doesn’t necessarily resemble the logical network (the path followed by transmissions). A logical ring, for example, might include groups of computers cabled octopus-like to hardware “collection points” which, in turn, are cabled to one another. In such a network, even though the physical layout of computers and connecting hardware might not visually resemble a ring, the logical layout followed by network transmissions would, indeed, be circular.

**MAG 14 format**

Industry standard magnetic format. Has a facility code, site code, card number, and issue code. Uses Magnetic signaling. Referred to as Mag15 on the 9000.

**manual action**

An action performed by security personnel from the Event Monitor or General Activity Monitor, such as locking or unlocking a door, activating or deactivating an output or event, or disarming an input or event. Manual actions can be programmed beforehand by the C•CURE 800/8000 administrator.

**master controller**

The Master Controller is the iSTAR controller that is responsible for Host communications for a cluster of iSTAR Controllers. Each of the controllers in the cluster is connected to the Master Controller via Ethernet and all communication with the Host is routed through the Master Controller.

**media access control (MAC) address**

MAC addresses are unique hardware addresses that are flashed onto network devices, including iSTAR controllers. They are 48 bit values that are split into 12 nibbles. Example: 00-50-f9-00-10-ab. The first 6 nibbles are known as the vendor portion. All iSTAR’s will have a MAC address of 00-50-f9-nn-nn-nn.

**MIFARE**

A contactless smart card method that operates at 13.56 mHz.
**mode**  
A state variable of a reader on a door that determines, in general, how access requests are processed; the mode can be locked, unlocked, or secure.

**modem**  
An electronic device that converts the computer system’s digital information into analog information and transmits it over a telephone line. When receiving, a modem converts signals from analog to digital. The procedure is known as MOdulate-DEModulate.

**MRM**  
The original RM reader module. Replaced by the RM-4.

**NAT**  
Network Address Translation. A type of gateway that allows computers on one side to communicate to the other side using a public IP address that is common to all of them. The NAT server routes the information to and from the computers using unique TCP ports for each computer.

**NetVideo**  
See *NetVue*.

**NetVue**  
An optional feature of C•CURE 800/8000, integrating both live and stored digital video through a network with C•CURE 800/8000. The integration includes both Software House-provided equipment, such as Intellex, and third-party equipment, such as NICE.

**NetVue action**  
Defined activity performed by the Digital Video System, such as capturing video and real-time recording of events. See also *event*, and *manual action*.

**NetVue mapping**  
Allows the launching of live video at the Monitoring Station from NetVue dome and fixed video camera icons located on a map of the facility (configured in the Administration application). The icon’s shape/color indicates the current state of the dome or fixed camera.

**network**  
A group of computers and associated devices that are connected by communications facilities. A network can involve permanent connections, such as cables, or temporary connections made through telephone or other communication links. A network can be as small as a LAN (local area network) consisting of a few computers, printers, and other devices, or it can consist of many small and large computers distributed over a vast geographic area (WAN or wide area network).
Glossary

**Network Interface card (NIC)**
An interface to a network that has an IP address. Used in the host computer and iSTAR’s. Some computers can have more than one and are then called multi-homed.

**Network port**
A pseudo port that is used to interface an apC to a terminal server.

**Nibble**
A group of 4 bits. Half of a byte.

**Node**
A personal computer on a C•CURE 800/8000 network.

**Not Ready to Arm**
A state of an intrusion zone that indicates that one of the monitored conditions of the intrusion zone is asserted. If the zone were to be armed it would immediately have a violation. When Not Ready to Arm is true, you must either correct the condition or Force Arm the zone. If you Force Arm the zone there will not be a violation but the Not Ready to Arm condition will persist. The reason you might Force Arm is that the monitored device might be faulty and until the device is repaired or replaced you still want to arm the zone.

**Null modem**
A device that provides the required crossover when connecting a DTE device to a DTE device.

**ODBC (open database connectivity)**
ODBC refers to a standard API that allows programmers to access a database using SQL commands. A user of Windows 2000/2003/XP can define ODBC drivers and pre-configured, named ODBC connections from the control panel.

**Odd parity**
An error checking mechanism that requires that the total number of one bits, including the parity bit, is odd. Used to verify the right side of wiegand cards and for each character of a magnetic card.

**Offline**
Pertaining to the operation of a security object. When a security object such as an event is offline, the C•CURE 800/8000 ignores all state changes of the object, including requests to arm it.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>offset value</td>
<td>A feature allowing users to create a card number composed of two or more fields in the card format. Useful when there are multiple cards with the same card numbers and different facility or site codes.</td>
</tr>
<tr>
<td>on-board Flash ROM</td>
<td>Non-volatile storage device on the General Controller Module that stores the iSTAR’s firmware, MAC address, IP address, and IP address of the Gateway router. This firmware is easily upgraded through the host or ICU utility.</td>
</tr>
<tr>
<td>online</td>
<td>Pertaining to the operation of a security object. When a security object such as an apC is online, the C•CURE 800/8000 monitors state changes of the object.</td>
</tr>
<tr>
<td>output</td>
<td>A security object that turns a device on or off when given instructions from the system. Also known as a control point.</td>
</tr>
<tr>
<td>page</td>
<td>To transmit a message to a pager device.</td>
</tr>
<tr>
<td>page message</td>
<td>The message that a user creates and transmits to a pager device.</td>
</tr>
<tr>
<td>paging carrier</td>
<td>The service or device that communicates with a pager to send pages.</td>
</tr>
<tr>
<td>panel</td>
<td>The generic term for the local processor (apC, apC/8X, or apC/L) that performs access control functions, such as granting a cardholder access. See also apC, apC/8X, and apC/L.</td>
</tr>
<tr>
<td>parity card field</td>
<td>A field on the access card allowing the apC to confirm that a reader read the card correctly. This field is relevant only to Wiegand and proximity access cards.</td>
</tr>
<tr>
<td>partitioning</td>
<td>Segmenting the data in a C•CURE database so that users of the system may create and have access only to the data in their assigned segment(s). Access to data in a database partition is limited by the user’s partition assignment followed by their user privileges.</td>
</tr>
<tr>
<td>partition administrator</td>
<td>The person responsible for the configuration and maintenance of all common data in the C•CURE database. The partition administrator is also responsible for creating and monitoring partitions.</td>
</tr>
</tbody>
</table>
passback

A term designating a specific anti-passback violation wherein an access card is presented at an anti-passback reader that accesses the same area/region as the last recorded access for that card. The computer assumes the cardholder has already passed through a reader with the same area assignments, but has not yet been recorded as passing the other way. (On readers with DSMs, the computer only logs the cardholder into the area if the card has been presented and the door opened. For doors without DSMs, the cardholder is automatically logged into the area when the access is granted.) The computer assumes the cardholder from the first presentation already entered the area and that a second cardholder is now trying to enter using the first person’s card, which was “passed back” to them.

PC CARD

Previously referred to as PCMCIA - industry standard interface to small, plug-in peripheral cards, such as modems, memory expansion, and network cards. iSTAR supports a Type III slot.

Personal Identification Number (PIN)

A number assigned to a cardholder by a system administrator. It can be entered on a card reader keypad for further identification.

personnel

A person about whom information, such as name and card number, is stored in a personnel record in C•CURE.

personnel record

A collection of data items, such as name and card number, which identify a person within C•CURE.

personnel view

Personnel record dialog boxes customized for specific users.

physical network

One of two ways of describing the topology, or layout, of a computer network; the other is logical network. A physical network refers to the actual configuration of the hardware forming a network—that is, to the computers, connecting hardware, and, especially, the cabling patterns that give the network its shape. Basic physical layouts include the bus, ring, and star topologies.

Ping

A Windows command that can be used to determine connection to a network device.
PoE  Power Over Ethernet (IEEE 802.3af). A method that uses the CAT 5/6 cable to supply power to the device through the network port. PoE provides 12.95 Watts of power which is equivalent to about 1.1 Amp at 12 VDC.

PoE Plus  Power Over Ethernet Plus (IEEE 802.3at). A method that uses the CAT 5/6 cable to supply power to the device through the network port. PoE provides 25.5 Watts of power which is equivalent to about 2.125 Amp at 12 VDC.

post-alarm time  Defines the stop time for a video segment.

pre-alarm time  Defines the start time for a video segment.

primary communications path  The Primary Communications Path is the first communication path that is used by a controller and a host in an iSTAR cluster.

priority  A method by which the system orders events at the event monitor and resolves conflicts between two or more causes with conflicting actions. If two events affect the same security object, the prevailing action is that of the event with the highest priority.

property  The definition of attributes for a tab control, widget, field, or group of fields. This term is applicable to the configuration layout dialog boxes for personnel.

PSE  Power Sourcing Equipment. The device (Hub, Router, level 3 Switch, Injector) that provides the power for PoE and PoE+. The power is in the form of 48 VAC that is typically converted to DC in the target device.

PTZ  A control that enables remote camera actions Pan, Tilt, or Zoom, to be performed on a NetVue dome camera.

pulse  To activate or deactivate an output for a previously specified length of time.

R/8 Output Module  A Reader-bus Module that controls 8 outputs and monitors 1 tamper input.

Radionics  A brand of alarm system that is integrated with the C•CURE system.
### Glossary

**RAM**

Random access memory.

**RAS/RRAS (Remote Access Service)**

A Windows feature that allows remote users access to the network. Also used by iSTAR for dialup and direct serial connections.

**Reader**

A physical device, also called a read head, that incorporates specific technology to read cards and interacts with an access control card to communicate card reads. Also known as a card reader.

**Reader-bus**

The RS-485 port on an ACM which is used to communicate with reader-bus modules (RM Reader, I/8 and R/8) in a bus topology.

**Reader-bus module**


**receiver**

A major component in a Radionics alarm system that communicates with elements of the alarm system as well as C•CURE. May also be referred to as a gateway or communications receiver.

**receiver number**

Each general purpose receiver has a unique number.

**recipient**

Person to whom an e-mail or page is sent.

**relay**

A component of an output. All Software House outputs have associated relays except for the RM-4 outputs. When using the RM-4 outputs connect an ARM-1 relay module.

**Remote Access Service**

See **RAS/RRAS (Remote Access Service)**.

**request to exit (RTE)**

An exit request made by activating an input. The system ignores (shunts) the associated door’s monitor, and unlocks the door if necessary.
RM  Reader Module used to convert magnetic and Wiegand data from a reader, as well as bi-directional control data, to an RS-485 bit stream to talk to a controller (apC or iSTAR). The board can be housed in RM Readers or externally connected to readers. The RM-4 personality module provides two supervised inputs and two outputs. The RM-4 outputs do not have relays, only the drive circuitry; so an auxiliary relay module, the ARM-1, must be wired within 25ft. of the output. The RM-4E has relay outputs and built in circuitry for maglock doors.

RM Reader Module  A Reader-bus Module with a read head used to read magnetic or Wiegand card data, 2 general purpose supervised inputs, 2 outputs, 1 tamper input, an audible sounder and an optional LCD display and an optional keypad.

RM LCD messages  Messages displayed on an RM reader that indicate different states to cardholders. Users can customize sets of messages for the facility or site.

RoHS  Restriction of Hazardous Substances. A CE directive to prohibit lead and other substances on electronic printed circuit boards.

Roll call report  A report that can be run from either the Administration client or the Monitoring Station indicating who is in a particular area. Typically used in emergencies.

ROM  Acronym for read-only memory. A semiconductor circuit into which code or data is permanently installed by the manufacturing process.

router  A device that finds the best path for a data packet to be sent from one network to another. A router stores and forwards electronic messages between networks, first determining all possible paths to the destination address and then picking the most expedient route, based on the traffic load and the number of hops.

RS-232  An accepted industry standard for serial communications connections. Adopted by the Electrical Industries Association, this Recommended Standard (RS) defines the specific lines and signal characteristics used by serial communications controllers to standardize the transmission of serial data between devices. Used to connect apC’s and Bi-Directional devices to the host. Maximum length is 50 feet without line drivers.
RS-422  A two node serial connection wired the same as RS-485. Not used in the C•CURE but may be seen in terminal servers and American Dynamics equipment.

RS-485  A multi-node bus to connect up to 32 nodes. The method is a differential signal method where the transmit and receive signals have their own ground wire. The bus can be up to 4000 feet. RS-485 (2 wire) is used for all reader busses and RS-485 (4 wire) is used to connect chains of apC’s to the host.

RXD  Short for Receive (rx) Data. A line used to carry received serial data from one device to another, such as from a modem to a computer. Pin 3 is the RXD line in RS-232-C connections.

salvo  A CCTV function that defines a group of cameras that can be called simultaneously to a contiguous group of monitors.

secondary communications path  The Secondary Communications Path is used only if there is a communications failure on the primary communications path between the host and the cluster master. Secondary communication can be direct serial, dialup, or network.

secure door  Sets the door so that it cannot be unlocked. In essence, this action disarms the reader associated with the secured door. This action is reversed by either locking or unlocking the door.

security object  An entity defined or controlled by the system: for example, inputs, outputs, holidays, and time specifications.

sequence  A CCTV function that sequentially displays a selected series of camera video inputs on any monitor for a pre-set amount of time (the dwell time).

serial  Serial means one by one. For example, in serial transmission, information is transferred one bit at a time, and a serial computer has only one arithmetic logic unit, which must execute the whole program one step at a time. RS-232, 422, and 485 are all serial transfer methods.
| **serial connect** | iSTAR master, controller of an iSTAR cluster in continuous communication with the C•CURE host by means of a serial connection (RS-232). The host expects to be in communication with the controller at all times, as contrasted to dialup iSTARS where the contact is periodic. Connection is established using RAS. An interface to a network that has an IP address. Used in the host computer and iSTAR’s. Some computers can have more than one and are then called multi-homed. |
| **serial connection/communication** | The exchange of information between computers or between computers and peripheral devices one bit at a time over a single channel. Serial communications can be synchronous or asynchronous. Both sender and receiver must use the same baud rate, parity, and control information. |
| **serial port** | An input/output location (channel) that sends and receives data to and from a computer's central processing unit or a communications device one bit at a time. Serial ports are used for serial data communication and as interfaces with some peripheral devices, such as mice and printers. A pre-set amount of time (the dwell time). Serial ports typically use RS-232. |
| **server** | The PC that manages the C•CURE security environment, including communications with apCs and with PCs that perform monitoring and administrative functions. The Server also stores and manages the application configuration database and the historical journal. |
| **server time zone** | The time zone for the server PC, set on the Windows 2003/XP Control Panel using the Date/Time icon. |
| **shunt** | To ignore an input. Most common use is to ignore the DSM when the door opens after a legitimate door access or REX. |
| **SIMM** | Single Inline Memory Module. |
| **site code** | Field on an access card that identifies the site for companies that have several sites. |
smart card  A card that can be written to. Some require contact and others are wireless. Smart cards can contain a monetary balance that is deducted from when the card is used to buy something. It is now common for smart cards to be used in access control. In one application, a math model of the cardholders signature is stored on the card thus preventing use of the card if is stolen.

source database  See external database.

split screen  See split window.

split window  Splitting the Monitoring Station window horizontally to display the Event Monitor in the top pane and the General Activity Monitor in the bottom pane. This allows you to view activity on both monitors at the same time.

SQL (structured query language)  A language used to create, maintain, and query relational databases. It is an ISO and ANSI standard. SQL uses regular English words for many of its commands, which makes it easy to use. It is often embedded within other programming languages.

star topology  A network configuration based on a central hub, from which nodes radiate in a star-shaped pattern.

state change  Change of condition in security object: for example, inputs or readers. State changes can be normal and planned or can be the result of other activity: for example, door forced open, rejected access, or duress conditions.

status output  Output that the apC activates while the status of an intrusion zone in disarmed mode is not ready to arm or when an armed intrusion zone is violated.

subnet mask  Subnet masks are used to identify the part of the IP address that is used as the network id by “masking” that part of the address. Subnet masks let you set up internal LANs on your network by “masking” part of the IP address that is typically used for the host id. Masking is the process of moving bits from the host id to the network id.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>supervised input</strong></td>
<td>An input that can detect normal, alert, open, shorted, or line fault circuit states. Line faults typically occur when incorrect resistor values are used.</td>
</tr>
<tr>
<td><strong>supervision error</strong></td>
<td>Informs the system when the status of wiring between an input and an input circuit changes. If the wiring is cut, the system reports an open circuit. If someone tries to jumper the wire (prevent the device from reporting), the system reports a short circuit.</td>
</tr>
<tr>
<td><strong>swipe</strong></td>
<td>To pass a card through a reader. The swipe detects identification data encoded in a card, then refers to the access record defined for that card. Access is granted or withheld based on the data in that record and on whether or not the card number has been configured to have clearance.</td>
</tr>
<tr>
<td><strong>system activities</strong></td>
<td>A pre-defined set of situations that can be identified by the system. You can identify those situations important to your security objectives, and you can customize which of these gets displayed at the Monitoring Station.</td>
</tr>
<tr>
<td><strong>system administrator</strong></td>
<td>The person responsible for the configuration and maintenance of all system hardware as well as all common data in the C•CURE 800/8000 database. The system administrator is also responsible for creating partitions, creating users and assigning them privileges and partition(s), and performing database backups. The system administrator is also a partition administrator if the C•CURE 800/8000 database is partitioned. See also <a href="#">partition administrator</a>.</td>
</tr>
<tr>
<td><strong>system occurrence</strong></td>
<td>Circumstances that indicate state changes to objects the system monitors, such as doors or readers.</td>
</tr>
<tr>
<td><strong>system variables</strong></td>
<td>A dialog box that allows certain system-wide security settings to be configured.</td>
</tr>
<tr>
<td><strong>tab button</strong></td>
<td>The title of a tab page. See <a href="#">tab page</a>.</td>
</tr>
<tr>
<td><strong>tab control</strong></td>
<td>The set of tab pages in the <strong>Layout</strong> area of the <strong>Configure Layout</strong> dialog box. See <a href="#">tab page</a>.</td>
</tr>
</tbody>
</table>
**tab page**
An individual page in the **Layout** area of the **Configure Layout** dialog box that contains the tab button and any combination of widgets, fields, groups of fields on the page. See *tab button*.

**tailgate**
A term designating a specific anti-passback violation wherein an access card is presented from an area/region that the system has no record of the card having entered. The computer assumes the cardholder generating the violation entered the area by following the prior cardholder through an entry door without presenting his or her own card.

**TCP/IP**
TCP/IP is a suite of protocols that allow communications across different network platforms. It is a routable protocol providing access to the Internet and its resources. It consists of several protocols in the Transport layer that operate in the Session layer. Almost all networks support TCP/IP as a protocol.

**TCP port**
TCP/IP communications are typically between two IP addresses using a TCP port. The first 1024 ports are reserved for internal TCP functions. Software House uses some in the 2500 - 2801 range. C•CURE Central uses some in the 6900 range. Sometimes when there are communications problems it is because a firewall or router is blocking the TCP that is required.

**Telnet**
Telnet is an internal TCP function that uses port 23. We sometimes use Telnet to login to a terminal server in order to set it up.

**template**
An object used in exporting and importing personnel records (and in importing asset records); it specifies the exact file format used for export and import.

**thin client**
A connection that executes its program from the computer that it is connect to. The C•CURE 800 client applications can be run as thin clients. The login connections to C•CURE Central are thin client. A thin client is similar to a dumb terminal connecting to a timesharing computer in an earlier architecture.

**time specification**
A security object that specifies a given range of times; used in access control and to automatically cause events to happen during certain time periods.
timestamp field
An external database field which contains a numeric value that increases in magnitude with each external database update. This field is used by the automated import function to retrieve new and modified personnel data from the external database without getting records processed by an earlier import.

time zone
Any of the 24 regions of the globe (loosely divided by longitude) throughout which the same standard time is used.

toggle input
An input whose momentary activation can trigger either the arming or disarming of an intrusion zone depending upon the zone’s prior mode and status. A momentary action key or switch that turns in one direction to activate and then springs back is an example of a toggle input. See also follow input and input.

tracert
A windows command to TRACE the Route to an IP address. It uses a Ping type of method to trace the route.

trailer character
A value that defines the last character in a message from a Bi-Di device. The default value is 13 which is a carriage return.

twain capture
Allows a user to capture an image using the industry standard twain interface. Twain capture involves third party software and devices, such as scanners. After an image is imported using the twain interface, a twain capture dialogue box opens, where the image can be both previewed and edited.

“unacknowledged event” event
An event that is activated when another event has been active and unacknowledged longer than a specified amount of time.

unsupervised input
An input that can detect only normal or alert circuit states in the alarm circuit. For example, if the circuit is normally closed, an open circuit indicates an alarm, but the input cannot detect open or shorted circuit states. The only unsupervised inputs are the eight on a standard apC Star Coupler.

user
A person who has access to the Administration application and/or the Monitoring Station. A user is always personnel, but personnel are not always users.
user defined message
When defined, user defined messages can trigger events on C•CURE 800/8000

user privileges
Software privilege categories which control which functions users can perform in the Administration and Monitoring Station applications. UTC

For all practical purposes, the same as Greenwich Mean Time, which is used for the synchronization of computers on the Internet. Also called coordinated universal time format.

video archiving
The process of relocating video to offline, permanent storage for future retrieval. This process is handled by the digital video server system. Video archiving functions are limited to the features that are currently available on the supported digital video servers. See the product documentation about these servers for more information about archiving capacity.

video event
Live or Recorded Video. A video event is defined by an action (camera record for a set time) associated with an access control event (lock door or open door). The access control event can be configured to trigger the video event based on a pre-defined action (record the door opening for a segment of time). Live video events can be used to monitor a location on a continuous basis in real time.

video segment
The section of the video recording from the time the user starts the video event up to and including the time the user stops the video event. For instance, when a user elects to play recorded video, the Start Date/Time and Stop Date/Time can be entered, allowing the user to view a specific segment of video associated with an event.

video segment ID
A unique index used to obtain a video segment from the video server. A Video Segment Id is used to obtain the section of recording from the time the user starts the video event up to and including the time the user stops the video event. The user can begin recording either manually or by assigning a cause (access control event) to be associated with the video. For example, a door switch monitor can be configured to initiate a video event with a 10-second pre-video time and a 10-second post video time. The Video Segment Id is what is used to access or track that 20 second video segment. Causes that may be associated with video events include any C•CURE 800/8000
event. Video Segment Ids are assigned by the video server and delivered to C•CURE 800/8000. C•CURE 800/8000 uses the Video Segment Id in the appropriate function in order to access the prerecorded video segment.

**video server**
A server designed to deliver digital video and other broadband interactive services over a wide area network or to employees on an intranet, a local area network.

**visitor**
A cardholder assigned a Personnel Type of Visitor. This person is able to access various buildings or areas without an escort.

**WAN**
Wide area network. A network in which computers are connected to each other over a long distance, using telephone lines and satellite communications. See **LAN**.

**widget**
Any single item in the **Layout** area of the **Configure Layout** dialog box. Widgets include objects such as edit fields, labels for edit fields, sets of radio buttons and their labels.

**Wiegand signaling**
An interface method that uses Data1 and Data0 signals.

**Wiegand technology card**
A card that has small magnetic wires embedded in a laminate indicating the ones and zeros.

**Wiegand 26 format**
An HID industry standard that has an 8 bit facility code, a 16 bit card number and 2 parity bits.

**Windows CE**
Microsoft® Windows® CE is a 32-bit, Windows embedded real-time operating system. It is the operating system that is running in the iSTAR GCM.

**WOSA**
Acronym for Windows Open Services Architecture, also known as Windows Open System Architecture. A set of application programming interfaces from Microsoft that are intended to enable Windows-based applications from different vendors to communicate with each other, such as over a network. The interfaces within the WOSA standard include Open Database...
Connectivity (ODBC), the Messaging Application Programming Interface (MAPI), the Telephony Application Programming Interface (TAPI), Windows Sockets (Winsock), and Microsoft Remote Procedure Calls (RPC).

zone

Another term for a Radionics alarm point.
Index
specifying master 3-14
Comm Fail 7-18
Comm Fail status message 7-20
Communications 1-8
  maintaining 3-10
  modem 2-6
  paths 3-9
    Primary communications path. See
    Primary Path
    Secondary communications Path. See
    Secondary Path
specifying methods 3-14
supported by iSTAR Pro 3-2
Compliance 1-9
Configurations
  selecting master in ICU 7-25
Configuring
  controllers using ICU 7-22
  ICU password 7-14
  master using ICU 7-4
  SNMP 7-28
    using Controller Communication
    Information window 7-22
Configuring SNMP 7-28
Connected to alternate master status message 7-20
Connected to Host status message 7-20
Connected to Master status message 7-20
Connections
  specifying parameters for primary path 3-14
Controller Communication Information window 7-23
Controllers 7-17, 7-18, 7-35
  boot date/time (GMT) using web to check 8-6
  checking
    available SDRAM memory capacity 8-9
    if auto DST active via web 8-6
master or host IP address via web 8-5
master or host MAC address via web 8-5
total SDRAM memory capacity 8-9
type (master or member) via web 8-5
Communication Information window 7-22
configuring using ICU 7-22
diagnostic level control reports 8-12
displaying
  in ICU window 7-18
  local date/time via web 8-5
  Object Store Database 8-8
  of GMT via web 8-5
  status 7-20
  the Diagnostic Level Control screen 8-12
  the number of, on network 7-21
  type of 7-19
entering URL 8-2
free memory status 8-6
indicating master 7-25
MAC address identity 7-23
MAC address, check via web 8-5
Password 7-35
specifying for communications with
  C•CURE system host 3-15
status screen via web 8-4
total flash ROM memory 8-6
using web to access 8-2
viewing
  IP address 7-19
  MAC address 7-18
Conventions
  documentation xiv
Current, determining maximum power
  consumption 2-6
D

Danger symbol xiv
Database
   checking
      memory still available for controller 8-9
      size of controller 8-9
      information, viewing 8-8
Diagnostic information, displaying 8-13
Diagnostic LCD 1-12
Diagnostic Level Control screen 8-12
Diagnostic Screens 8-10
Diagnostic status, viewing 8-4
Diagnostic System 7-36
Diagnostic tests
   automatic output 9-7
   card data 9-5
   Ethernet 9-8
   Ethernet and PCMCIA 9-8
   input diagnostics 9-7
   manual output 9-6
   PMB output 9-7
   reader 9-5
   types of 9-5, 9-6
Diagnostic Utility 8-1
   cluster information 8-7
   connecting to 7-34
   database information 8-8
   main screen 8-3
   navigating 8-3
   reader and I/O 8-11
   SID diagnostic levels 8-12
   starting 8-2
   viewing status screens 8-4
Dialup 1-11
Documentation conventions xiv
Door contact, equipment wiring specifications 2-11
Door Map 5-2
Downloading firmware updates 7-39
DRAM
   check capacity 8-9
   check unused capacity 8-9
DRY 6-19
Dry relay 6-19
dry/wet configuration 1-7
DST, controller on or off 8-6

E

Edge Accessories 1-9, 2-3
enable 7-37
Encryption 1-11
Environmental requirements 2-5, 2-7
Equipment Check
   mounting 2-2
Equipment wiring specifications
   readers 2-12
   relay control 2-11
   Request-to-exit 2-11
   RS-485 2-11
   supervised inputs 2-11
ESD
   Power Supply 2-6
Ethernet 5-5
   cluster members 3-6
   diagnostic test 9-8
   options 2-11
Ethernet PHY 4-9
Index

F
F and K input 6-28
FAI 1-7, 1-8, 1-12, 6-27
   Connections 6-27
   Key Supervision State 1-7
   Modes 6-27
   Relay Control 1-7
   Scenarios 6-27
   State of F, K, and Relay Drive 6-31
   Supervision State 1-7
   Supervision Values 6-28
      with Latch followed by Key Unlatch 6-30
      without Latch 6-27, 6-29
FAI Key State 6-33
FAI Key Supervision State 6-33
FAI State 6-33
FAI Supervision State 6-33
Fail-safe mechanism override xv
Fire Alarm Interlock 1-7
Firewalls 3-2
Firmware
   upgrading 7-39
Firmware download 7-40
   setting public IP address 7-14
   setting TCP/IP port 7-14
Flash 1-10
Free memory, controller 8-6

G
Gateways 3-2
GCM
   identifying MAC address 7-18
General Purpose
   inputs 1-6
   relays 1-6
   GMT date/time, controller display via web 8-5
   Grounding Requirements 2-13
   Guidelines for setting up primary path 3-14

H
Help, ICU 7-16
Host
   connections between alternate master and 3-11
      displaying IP address 7-19
   Hosts 1-12
   Housing 1-9

I
I/O 1-6
ICU 7-21, 7-32
   Advanced tab 7-27
      assigning
         cluster member address 7-19
         master IP address 7-19
   Attempting connection message
      for host 7-20
      for master 7-20
   Beaconing
      for Host message 7-20
      for IP Address message 7-20
      for Master message 7-20
   Block Feature 7-9
   broadcast 7-18
   changing password 7-14
   Comm Fail message 7-20
   configuring
      controllers 7-22
iSTAR clusters 7-4
master controller 7-3
Connected to
  alternate master message 7-20
  Host message 7-20
  Master message 7-20
Controller Identity tab 7-25
copying to PC or laptop 7-7
displaying
  host IP address 7-19
  number of active 7-21
  parent IP address 7-19
  type of controller 7-19
Ethernet Adapter tab 7-25
Help 7-16
Host/Master tab 7-27
how cluster information is displayed 7-8
lock 7-9
main window 7-10
main window features 7-15
Not Connected message 7-20
opening
  monitor controller Diagnostic screen 7-16
  Options window 7-14
options, setting 7-12
password, changing 7-14
pinging controllers 7-16
rebooting message 7-20
refreshing
  controller information 7-12
  window 7-16
status of controllers 7-20
troubleshooting tools 7-3
using
  on PC or laptop 7-7, 7-22
  password window 7-10
to manually configure the master 7-4
toolbar 7-15
using out of subnet 7-7
WAN configurations 7-4, 7-5
ICU Block feature 7-9
ICU Block Off 5-7
ICU Block On 5-7
Identifying master or member 7-19
Input diagnostic tests 9-7
input ratings 2-7
Input/Output 1-6
Inputs
  general purpose 1-6
  special purpose 1-7
Installing
  checking site before 2-2
Internet, using for iSTAR Pro diagnostics 8-3
IP address 3-4
  assigning to cluster members 7-19
  assigning to master 7-19
  displaying cluster member 8-7
  parents 7-19
  viewing controller 7-19
  viewing parent 7-19
iSTAR
  comparison 1-10
iSTAR Edge 2-7, 7-18
  Accessories 2-6
  Layout 1-4
  photograph 1-2
  Processor 1-5
  storage 1-5
SW6 6-27
iSTAR Edge/eX cluster 7-4
iSTAR eX 7-17
Index

J

Jumpers 5-6

L

LAN Configurations 7-4
Laptop, using ICU on 7-7, 7-22
LCD 5-3
LCD backlight 4-9
LCD display
  configuring for status and diagnostic messages 9-2
  displaying status messages 9-4
  location 9-2
LCD with backlight 1-8
LED 5-3
LEDs 4-9
Local address management 3-3
Local date/time, controller display 8-5
Logging controller diagnostics 8-12
Low Battery input 4-6
Low battery input 6-33

M

MAC
  address in web diagnostic window 8-3
  address, controller 8-5
  address, description of 7-25
  displaying address 7-25
  GCM label with address 7-18
  viewing address 7-18
Main Power 5-5

Main screen, iSTAR web-based Diagnostic Utility 8-3
Manual output diagnostic tests 9-6
Master Controller 7-3
Master or host
  connection status, using web to check 8-6
  IP address, assigned to master or host 8-5
  MAC address, for controller 8-5
Masters
  about 3-6, 3-8
  assigning IP addresses to 7-19
  cluster members losing connection with 3-12
  displaying IP address 7-19
  indicating 7-25
  primary communications path and 3-8
  specifying for cluster 3-14
  using ICU to manually configure 7-4
Memory
  check controller DRAM 8-9
Menu bar, ICU window 7-21
Modem 2-6
Monitor controller diagnostic screen, opening 7-16
Mounting hardware 2-2

N

Names, controller 7-18
Navigating, iSTAR Web Diagnostic Utility (see Diagnostic Utility) 8-3
NetBIOS
  Fully qualified domain names 3-5
Network
  communicating via TCP/IP 3-2
  Password dialog box 8-2
  platforms 3-2
  requirements 2-5
<table>
<thead>
<tr>
<th>Network Diagnostics</th>
<th>8-10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Connected status message</td>
<td>7-20</td>
</tr>
<tr>
<td>Note symbol</td>
<td>xiv</td>
</tr>
<tr>
<td>Number of controllers, displaying</td>
<td>7-21</td>
</tr>
</tbody>
</table>

**O**

- Object Store Databases screen | 8-8
- On board battery backup | 1-6
- Onboard backup batteries | 4-8
- Onboard Battery Low | 6-33
- Onboard Battery Low input | 4-6
- Onboard controls | 1-8
- Onboard Ethernet | 3-14
- One Wiegand and One RM Reader | 6-4, 6-9
- Options dialog box, opening | 7-14
- Other interactions with the power system include | 4-5
- Output Relay Wet or Dry Jumpers | 5-8

**P**

- Panic hardware | 2-12
- Password
  - configuring for ICU | 7-14
  - iSTAR Configuration dialog box (password) | 7-10
  - network | 7-35
- Path to host, using web to check on | 8-6
- PC, using ICU on | 7-7, 7-22
- PCMCIA
  - diagnostic test | 9-8
- Photograph
  - iSTAR Edge | 1-2
- Physical requirements | 2-5
- PING | 3-3
- Pinging selected controller via ICU | 7-16
- PMB
  - output diagnostic tests | 9-7
- PoE | 1-12
- PoE board | 1-7
- PoE injectors | 4-4
- PoE or PoE Plus Jumper | 5-8
- PoE Present | 4-6
- PoE splitters | 4-4
- PoE system | 1-6
- Power
  - equipment wiring specifications | 2-11
  - ratings
    - RM ports | 2-8
    - Wiegand ports | 2-8
  - requirements | 2-6
  - components | 2-6
  - Software House readers | 2-9
  - third-party readers | 2-10
- Power In | 4-7
- Power in | 4-7
- power LEDs | 1-8
- Power Sourcing Equipment (PSE) | 1-6
- Power specifications | 4-2
- Pre-installation
  - planning | 2-2
- Pre-Installation equipment check | 2-2
- Primary path
  - guidelines for | 3-14
  - main elements | 3-8
  - setting up | 3-14
  - types of connections | 3-8
- Processor | 1-10
Product Comparison 1-10
provides 5-6
Public IP address, setting for firmware downloads 7-14

Q
Queries, broadcasting 7-16
Querying subnet 7-8

R
RAM 1-10
Readers 1-6
and I/O diagnostics 8-11
diagnostic tests 9-5
equipment wiring specifications 2-12
power requirements 2-10
Readers - I8s - R8s 6-24
Real Time Clock 4-9
Rebooting status message 7-20
Refresh ICU window 7-16
Refresh Interval 7-13
Relay control, equipment wiring specifications 2-11
Relay Outputs 5-5
Relays
  general purpose 1-6
Relays onboard 1-11
Reports
  viewing or logging controller diagnostic 8-12
Request-to-exit, (RTE) equipment wiring specifications 2-11
Requirements
ground 2-13
  installation 2-3, 2-5
  modem 2-6
  power 2-6
  system network 2-5
Reset button 5-6
RJ-45
  Ethernet 10BaseT, equipment wiring specifications 2-11
RM Port Termination Switches 5-8
RM Port Terminators 6-5, 6-10
RM ports, power ratings 2-8
RM Readers 6-3, 6-8
RM s Allowed 1-11
Rotary switch 5-7
RS 485 serial port 1-7
RS-485
  wiring specifications 2-11
RS-485 ports 1-5

S
Safety Information 0-xv
Secondary path
  setting up 3-15
  types of connections 3-9
Serial 5-5
Serial host comm 1-11
Single Master Configurations 3-8, 3-10
Site
  checking before installation 2-2
  installation requirements 2-5
SNMP
  communication 7-28
  configuring 7-28
Software House Readers 2-9
Software House readers, power requirements 2-9
Special Purpose inputs 1-7
Special Purpose Inputs 1-7, 6-32, 6-33
Specifications 4-2
  system cabinet 2-5
Speed, MHz 1-10
Starting Diagnostic Utility 7-34, 8-2
Static Electricity 0-xv
Status
  displaying controller 7-20
  using Diagnostic Utility to view controller 8-4
  viewing controller icons 7-18
Status Bar 7-21
Status messages, displaying on the LCD 9-4
Status Tab 6-34
Subnet
  querying 7-8
  using PC or laptop with ICU on 7-7, 7-22
Subsystems, viewing reports for 8-12
Supervised inputs
  equipment wiring specifications 2-11
Switches 5-6
System cabinet, specifications 2-5
System diagnostics
  displaying levels 8-12
  viewing controllers 8-12
System requirements, network 2-5

TCP/IP
  overview 3-2
  port, setting for firmware downloads 7-14
  protocol 3-2
Third Party Readers 2-10
Tip symbol xiv
Toolbar, ICU 7-15
Total memory, controller 8-6
Total object store, database 8-9
Total readers allowed 1-11
Troubleshooting Tools 7-3

UL Listed Panic hardware 2-12
Unsupervised Tamper 1-7
URL, entering controller 8-2
USB Ports 1-7
User message window 7-38

Version
  Win CE 1-10
Viewing
  controller diagnostics 8-12

Wakeup Threshold 4-10
Wakeup threshold 4-5
WAN Configurations 7-5
Warning symbol xiv
Web based iSTAR Diagnostic Utility screen 8-3

Tamper 6-26, 6-32
Index

Web diagnostics 7-37
   controller status screen (also see Diagnostic
   Utility) 8-4
Wet relay 6-19
WET relays 4-9
Wet Relays 1-5
Wiegand
   ports, power ratings of 2-8
Wiegand Reader Ports 2-8
Wiegand Readers 1-11, 6-2, 6-7
Wiegand readers 1-5, 4-9
Win CE Version 1-10
Wiring
   ground requirements 2-13
   requirements 2-11
   specifications
      readers 2-12
      relay control 2-11
      Request-to-exit 2-11
      RS-485 2-11
      supervised inputs 2-11
Wyreless 1-11