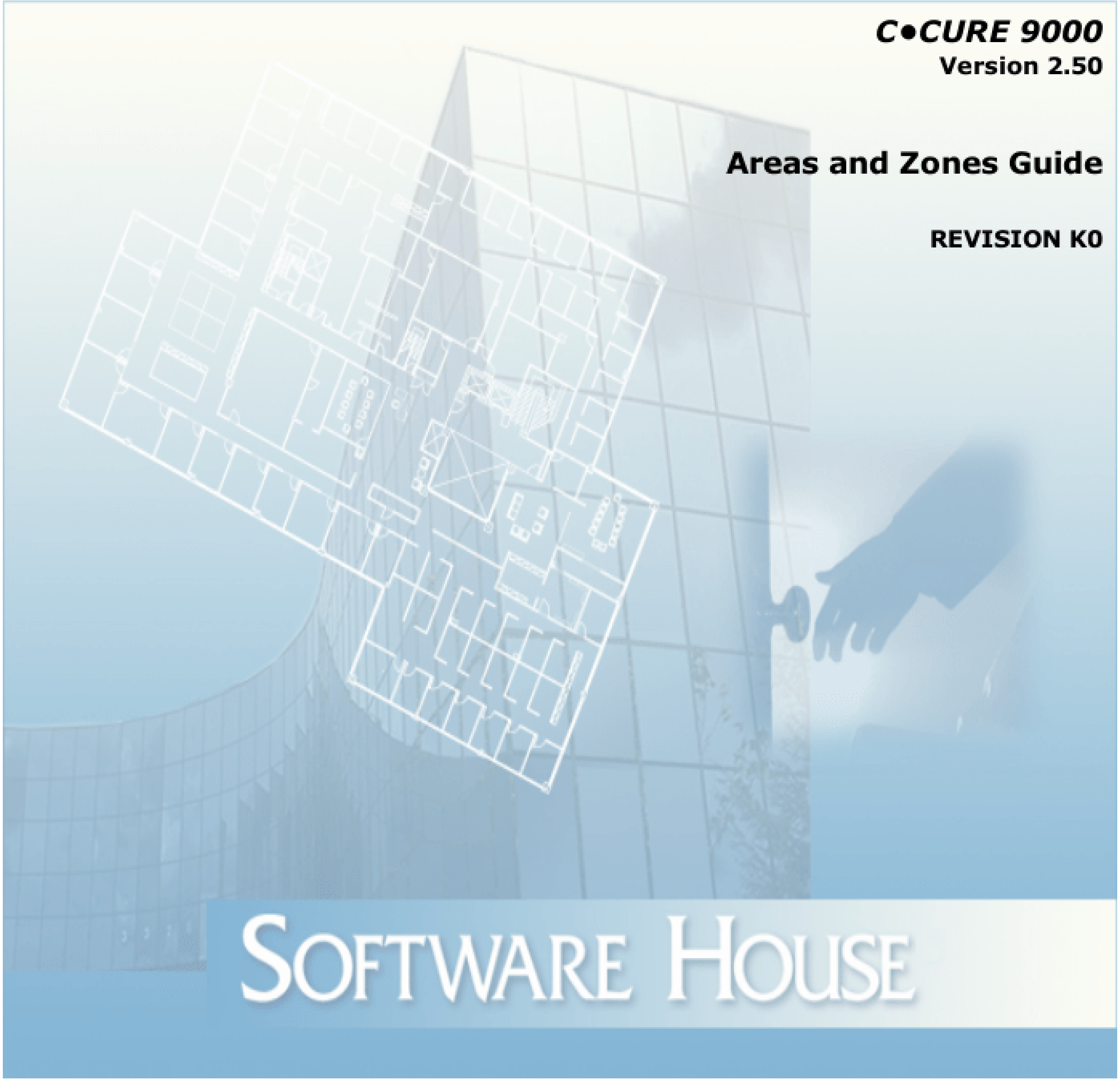
SOFTWARE HOUSE

From Tyco Security Products



C•CURE 9000
Version 2.50

Areas and Zones Guide

REVISION K0

UM-228 K0

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.

Software version: 2.50
Document Number: UM-228
Revision Number: KO
Release Date: December 2015

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

Table of Contents

Preface

This *C•CURE 9000 Areas and Zones Guide* is for new and experienced security system users. The manual describes the software features on the C•CURE 9000 Administration Client Areas and Zones menu and presents procedures for configuring and using them.

You should have read the installation procedures described in the *C•CURE 9000 Installation and Upgrade Guide* and familiarized yourself with the basic C•CURE 9000 information provided in the *C•CURE 9000 Getting Started Guide*.

In this preface

How to Use this Manual

This manual includes the following sections. Turn to the appropriate section for the information you need.

Chapter 1: iSTAR Areas

This chapter describes how to configure iSTAR Cluster Areas, physical regions regulated by C•CURE 9000, and how to use them to control and monitor access in your facility. Areas are used to control Antipassback— Regular and Timed—and with Occupancy Restrictions and also provide the capability to track Personnel.

Chapter 2: iSTAR Intrusion Zones

This chapter describes how to configure iSTAR Intrusion Zones, physical areas delineated by Doors and Inputs and monitored for alarms, and how to use them in C•CURE 9000 to monitor security in your facility.

Chapter 3: Keypad Commands

This chapter describes how to configure and use Keypad Commands that can activate Panel Events.

Finding More Information

You can access C•CURE 9000 manuals and online Help for more information about C•CURE 9000.

Manuals

C•CURE 9000 software manuals are available in Adobe PDF format on the C•CURE 9000 DVD.

You can access the manuals if you copy the appropriate PDF files from the C•CURE 9000 Installation DVD English\Manuals folder.

The available C•CURE 9000 and Software House manuals are listed in the *C•CURE 9000 Installation and Upgrade Guide*, and appear as hyperlinks in the online.pdf file on the C•CURE 9000 DVD English\Manuals folder.

These manuals are also available from the Software House Member Center website ([redacted]).

Online Help

You can access C•CURE 9000 Help by pressing F1 or clicking Help from the menu bar in the Administration/Monitoring Station applications.

Conventions

This manual uses the following text formats and symbols.

Convention	Meaning
Bold	This font indicates screen elements, and also indicates when you should take a direct action in a procedure. Bold font describes one of the following items: • A command or character to type, or • A button or option on the screen to press, or • A key on the keyboard to press • A screen element or name
blue color text	Indicates a hyperlink to a URL, or a cross-reference to a figure, table, or section in this guide.
Regular italic font	Indicates a new term.
<text>	Indicates a variable.

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.
STOP	Indicates a danger. A danger contains information that users must know to avoid death or serious injury.

Software House Customer Support Center

Telephone Technical Support

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

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

Before Calling

Ensure that you:

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

Hours	Normal Support Hours	Monday through Friday, 8:00 [redacted]. to 8:00 [redacted]., EST. Except holidays.
	Emergency Support Hours	24 hours/day, seven days a week, 365 days/year. Requires Enhanced SSA "7 x 24" Standby Telephone Support (emergency) provided to Certified Technicians. For all other customers, billable on time and materials basis. Minimum charges apply – See MSRP.
Phone	For telephone support contact numbers for all regions, see [redacted]	

Software House Customer Support Center

1

iSTAR Areas

This chapter explains how Areas can be used to control and monitor access to physical regions regulated by C•CURE 9000. Areas are used with Global/Cluster Antipassback— Regular and Timed—and with Area Lockout, Muster/De-muster, Occupancy Restrictions, and Escorted Visitor Access. They also provide the capability to track Personnel.

In this chapter

iSTAR Areas Overview

An Area represents a physical region—such as a room, a specific section of a building, or an entire building. Areas are used to control and monitor access to the regions they represent. Maximum control of Areas imposes restrictions on customers that may be impractical, so C•CURE 9000 provides features that allow trade-offs between 'correctness' and 'convenience'.

NOTE C•CURE 9000 currently supports iSTAR Areas only.

- **Control** is defined as actually preventing access based on location information.

  Examples:

  A customer might wish to prevent card holders from using their badges and then passing them to friends so that they can gain entry. To prevent this, the customer can configure Areas with antipassback (APB). In such a configuration, the card holders are admitted, but when the friends present the cards, they are rejected.

  Another customer might want to make sure that a particular Area in the building was accessible to only a certain number of people at one time. To that end, the customer could configure Areas with a Maximum Occupancy Restriction. In this type of configuration, when the maximum number of personnel defined for the Area is reached, no one else can enter—until some personnel leave.

  Still another customer with sensitive laboratories might want personnel who entered/exited one particular Area to be unable to enter another laboratory area for a specified amount of time. The customer can use the Area lockout feature for this purpose.

- **Monitoring** is defined as knowing how many people are in a given area as well as who they are, or which area a given person is in, without actually controlling access to that area.

While Control and Monitoring represent different functionality, they can also be used together.

Reasons for Using Areas

There are various **reasons** for using Areas, including security, safety, and resource management.

- **Security** – The customer's primary concern is to prevent legitimate card holders from entering Areas in an incorrect sequence, to prevent non-cardholders from using someone else's card, to prevent more than a specified number of cardholders from congregating in an area at the same time, or to prevent cardholders from entering a certain Area after being in another Area.

- **Safety** – The customer's primary concern is the safety of employees. Consequently, they want to know where employees are at all times.

  Example:

  The customer might create an evacuation location at the facility where, in an emergency, employees have to present their cards. This location would be monitored, but not controlled.

  On the other hand, access within the facility would be controlled with antipassback—not to prevent cardholders from going wherever they needed, but so the system knows when employees are inside the facility and therefore in possible danger during an emergency.

- **Resource management** – The customer's primary concern is to limit use of a specific facility so that it is appropriately available.

Example:

> The customer might have a parking lot which they do not want employees to let their friends use—by parking their own cars and then handing their cards to friends. In this case, the customer just wants to make sure that there is enough room for the vehicles of the other employees.
>
> The customer might have a high-security laboratory which operates optimally with four personnel present. In this case, the customer could configure that Area with Minimum Occupancy (also known as N-man Rule) specifying the number of personnel who must enter the lab at the same time to gain access, and who also must remain in the Area.

Strict area control and monitoring impose certain restrictions on the customer.

In general, most doors in a facility have a reader on one side and a request-to-exit (RTE), using a motion detector, on the other side. Card holders must present their card to enter, but to exit they just walk up to the door and open it.

Antipassback, however, requires both entry and exit readers because the system must see that a cardholder has left an area before it can let them back in again.

- Having exit readers means that going out through the door is now slower.
  - Personnel might be lining up to go to lunch, where previously they just walked right out.
  - Personnel also have to learn to interact with the system in a new way: to pay attention and present their cards when exiting, even if their friends hold the door open for them. Otherwise, their next access attempts are denied, requiring them to find a system administrator to ‘grace’ them.
- Installing Exit readers also doubles the cost of readers in a new facility and could incur building costs in a retro-fit situation.
- Finally, in systems large enough to spread areas across more than one controller, access decisions may require these controllers to exchange messages over the network. Then if the network is slow or unavailable, ‘correct’ decisions may be impossible to make in a timely fashion. (The controller can guess, but sometimes it will be wrong.)

The preceding issues mean that customers may wish to make trade-offs between correctness and convenience. The following features allow them to do so:

- Timed antipassback
- Non-antipassback areas
- “Local access” failure mode
- Monitoring of card holder location
- Occupancy that counts Personnel numbers without restricting access

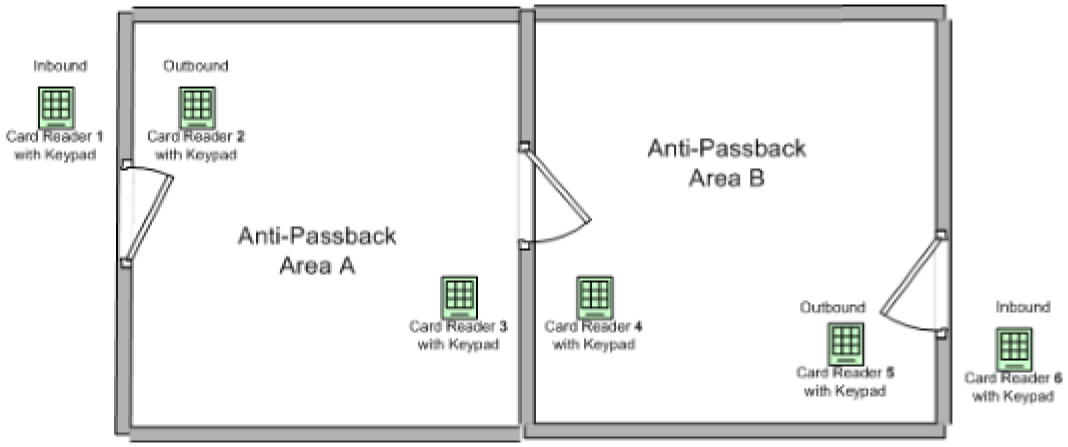
Setting Up Areas

Areas are defined by a set of Doors, Readers, and the Adjacent Areas to which these lead. Doors between Areas require at least one Reader. In some configurations, such as for Antipassback control of the location of Personnel, an entrance Reader and an exit Reader are required. C•CURE 9000 uses Areas to regulate Antipassback control and Occupancy Restrictions.

When high security and reliable tracking of Personnel is required, Areas can be configured to require people to use their badges to both enter and exit an Area. This provides a record of when a person leaves an Area, allowing the system to track the location of a person at any time. C•CURE 9000 uses this information to produce Roll Call Reports, Mustering/De-mustering control and reports, and Antipassback notifications.

Figure 1 on Page 18 presents a simple example of two Areas with Doors and Readers controlling entry and exit.

Figure 1: Areas and Doors with Entry and Exit Readers


Inbound
Card Reader 1 with Keypad
Outbound
Card Reader 2 with Keypad
Anti-Passback Area A
Card Reader 3 with Keypad
Card Reader 4 with Keypad
Anti-Passback Area B
Outbound
Card Reader 5 with Keypad
Inbound
Card Reader 6 with Keypad

You can select from two types of implementation of antipassback on the C•CURE 9000:

- **iSTAR Cluster Antipassback** – Allows each iSTAR Cluster to have its own set of Areas and antipassback does not function across Clusters. Antipassback for iSTAR Cluster Areas means that all Doors, Readers, and adjacent Areas are within the same iSTAR Cluster. The host does not participate in Area access decisions so these continue to function even if host communication is lost.

  When there is a communications failure within the Cluster–between the master Controller and one or more member Controllers, decisions are made according to the failure mode you configure for the Cluster. For more detailed information, see:

  - How the Cluster Antipassback Decision is Made on Page 32
  - How Cluster Antipassback Works During Communications Failure on Page 32.

- **iSTAR Global Antipassback (Cross-Cluster)** – Allows an Area to cross multiple iSTAR clusters to share antipassback information. The Cluster master Controller makes the Antipassback decision when it owns the card being swiped. Otherwise, that master Controller asks the C•CURE 9000 Server to ask the Cluster master Controller that is the card's owner for an antipassback decision. For more detailed information, see:

  - How Global Antipassback Decisions are Made on Page 32
  - How Global Antipassback Works During Communications Failure on Page 33.

You can configure Areas to control and/or monitor access in the following ways or in combinations thereof:

- With no limitation – a person with appropriate clearances can freely enter and exit from an Area.

- Using Antipassback where access is restricted as follows:
  - Regular antipassback – Personnel **cannot** exit an Area they are **not** in, **nor** re-enter an Area without exiting it first.
  - Timed antipassback – Personnel **cannot** re-enter an Area until a specified amount of time has passed.
  - Area Lockout – Personnel can only access a current target location based on their last entrance/exit time from a Lockout Area.
  - Carpool antipassback –
    - Carpool regular antipassback – Personnel in a carpool group **cannot** exit an Area they are **not** in, **nor** re-enter an Area without exiting it first.
    - Carpool timed antipassback – Personnel in a carpool group **cannot** re-enter an Area until a specified amount of time has passed.

NOTE Carpool Areas and Carpool Antipassback can only be configured for iSTAR Cluster Areas. They are not configurable for Cross-Cluster Areas and Global Antipassback.

- Using Maximum or Minimum Occupancy where access is restricted as follows:
  - Personnel **cannot** access an Area:
    - If the number of personnel already in the Area exceeds the **maximum** number defined.
    - If they are not accompanied by the **minimum** number of personnel required to be in the Area at the same time.
  - Personnel **can** access an Area regardless of the Maximum and Minimum Occupancy configured, but their number is counted.
- Using Passthrough, where Personnel must exit an area within a specified amount of time, failing which an Event can activate—if configured to do so. You can configure Passthrough violations independent of antipassback.
- Using Escorted Access, where cardholders designated as Escorted Visitors must be accompanied by cardholders designated as Escorts.
- Using Muster/De-muster, where Personnel gather in a designated Mustering Area in case of emergency. Once the emergency has passed, you can manually de-muster these personnel to a configured de-muster Area. (If a de-muster Area has not been designated, at de-muster time any Personnel in the Mustering Area will be graced and can go to any Area in the facility.

You can monitor access and track a person's location in the following ways:

- By running
  - Roll call reports, which indicate the current location, by Area, for all Personnel at the time the report is generated.
  - Carpool Area Roll call reports, which indicate the current location, by Carpool Area, for all Personnel at the time the report is generated. The report indicates each person's Carpool Group and whether he/she is the driver.

  For information, see Running Area Pre-defined Reports on Page 123.
- By displaying their current Area on the Administration application Personnel Dynamic View (based on the last Area the person entered on a valid admit). For information, see Viewing Area Location of Personnel on Page 119.

- By displaying for any selected Area the Personnel in that Area from both the Administration application Area Dynamic View and the Monitoring Station Area Status List. For information, see Viewing Personnel in an Area on Page 60 and the *C•CURE 9000 Monitoring Station Guide*.

Antipassback

Antipassback (sometimes known as APB) prevents a person from *passing back* a card to another person to use, and detects when someone *tailgates* (follows another person with a valid card admit through a door without using their own card).

Cluster Antipassback/Global Antipassback

- In **Cluster** Antipassback, the antipassback decisions are enforced within one cluster. The cluster members always ask the master for passback information. If the members of this cluster lose communications with the master, they enforce antipassback according to the **Communication Failure Mode** configured for the cluster—whether **No Access** or **Local**.
- **Global** (Cross-Cluster) Antipassback—sometimes referred to as "Host-assisted Antipassback"—works on top of Cluster Antipassback. It allows antipassback information to be shared between multiple iSTAR clusters to enforce the antipassback decisions.

  Appropriate passback requests are forwarded to the Host. The Host retrieves the information from the appropriate owner and then passes it back to the Master to pass back to the member who made the original request. The Master of the cluster to which this member belongs now takes up the ownership of the Personnel card. If the members of this cluster are not in communication, the System Variable user-defined failure mode (iSTAR Driver/iSTAR Global Antipassback Communication Failure Mode) will be enforced. For detailed information, see Table 25 on Page 116 in Setting System Variables That Affect Areas.

Antipassback Types

Antipassback can be either for Personnel or Carpools, and you can configure the following types:

- No Antipassback on Page 21
- Regular Antipassback on Page 22
- Timed Antipassback on Page 22
- Area Lockout on Page 22

No Antipassback

You can configure an Area without antipassback and use it to:

- Designate boundaries.
- Interface with Areas of the antipassback system.
- Monitor access.
- Create Roll Call Reports

Example:

The front Door of a building typically leads from a non-antipassback Area to a controlled antipassback Area. The non-antipassback Area can be either a physical space or a ‘conceptual’ area, such as ‘outside’.

Regular Antipassback

You can use a regular antipassback Area when you need to control the movements of personnel based on their location. Configuring regular antipassback prevents a person from exiting an Area that, according to the system, he/she is **not** in or from entering an Area that, according to the system, he/she is **already** in.

- A **passback violation** occurs when a person enters an Area and then passes the card to another person who uses it to enter the same Area.
- A **tailgate violation** occurs when a person tries to leave an Area that, according to the Controller making the decision, he/she is **not** in. This can occur if the person entered the Area by "tailgating" and then uses his/her card to exit the Area.

You can only enforce antipassback if you have both entry and exit Readers in an Area.

Timed Antipassback

You can use timed antipassback when you are **not** tracking all exits from an Area.

- A timed antipassback violation occurs when a person (identified by their card) tries to access the same Area more than once during a specified period of time.

Examples:

- If a person enters an Area, exits the Area, and then presents his/her card to enter that same Area again—all within the timed antipassback period, a timed antipassback violation occurs.
- Alternatively, if a person enters an Area and then passes his/her card to some one else to use to enter the same Area during the timed antipassback period, a timed antipassback violation occurs. (In this case, the system thinks the same cardholder is trying to access the Area more than once during the specified time period.)

Enforcing timed antipassback does not require exit Readers in an Area, only entry Readers.

Area Lockout

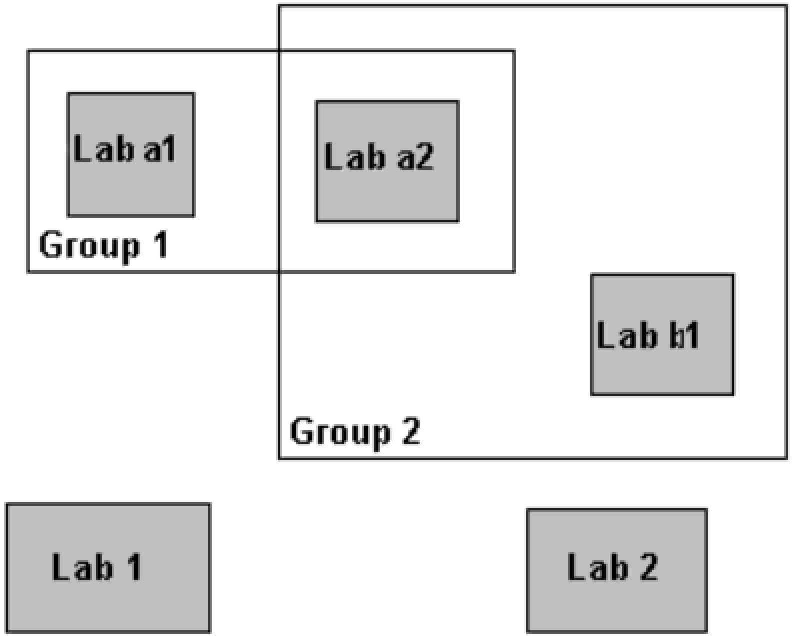
Area Lockout allows you to configure an iSTAR Area in which the presence of Personnel, monitored by the Area's entry and exit Readers, locks the cardholders out of a designated target Area or Group of iSTAR Areas for a specified period of time. A facility with multiple laboratories or highly sensitive manufacturing areas might require this functionality to prevent cross-contamination and a resultant loss of productivity and/or human injury or life.

The iSTAR Area(s) from which the Personnel are locked out can actually be or include the Area being entered. The target locked-out iSTAR Area can be any of the following:

- Same iSTAR Area
- Another iSTAR Area
- iSTAR Area group

A cardholder can be locked out of one and the same target Area due to accessing multiple different Lockout Areas. This can occur because an Area may be in more than one iSTAR Area group specified as a target for lockout. In addition, an iSTAR Area group may be used as a target Area by multiple Lockout Areas. Personnel are locked out of such a common target area for the longest lockout time configured on any of the Lockout Areas, as illustrated in the example shown in Figure 2 on Page 23.

Figure 2: Area Lockout Example



Example:

- In the example in Figure 2 on Page 23, Lockout Area **Lab 1** locks cardholders out of target Area **Group 1** (which contains **Lab a1** and **Lab a2**) for **8** hours. Lockout Area **Lab 2** locks cardholders out of target Area **Group 2** (which contains **Lab b1** and **Lab a2** as well) for **24** hours. Note that **Lab a2** is a Locked-out target Area common to both Lockout Areas, **Lab 1** and **Lab 2**.

  If the cardholder is not currently locked out of any Areas, the following could occur:

  a. The cardholder's entry/exit access in **Lab 1** locks him/her out of **Lab a1** and **Lab a2** for **8** hours.

  b. One hour later, the cardholder's entry/exit access in **Lab 2** locks him/her out of **Lab b1** and **Lab a2** for **24** hours. The cardholder is now locked out of the common target Area **Lab a2** for **24** hours, the longest lockout time, rather than the **7** hours remaining from the first access in **Lab 1**.

  c. Two hours later the cardholder re-enters **Lab 1**. The cardholder is now locked out of **Lab a1** for **8** more hours from this access, but remains locked out of the common target Area **Lab a2** for the **22** hours remaining from the **Lab 2** access in Step b.

  d. If during the lockout times enumerated in Step c—from **Lab a1** for **8** hours and from **Lab a2** for **22** hours—the cardholder is lockout graced, all lockout timers for this person are cleared. The cardholder can now enter any of the labs without waiting for the remaining lockout time to expire.

  e. Other cardholders may enter **Lab a1**, **Lab a2**, or **Lab b1** without triggering lockout restrictions.

The lockout timer starts when Personnel present a card at the entrance or exit Readers of the Lockout Area. If the iSTAR Area doing the locking out and the target Area being locked out are the same, the condition is similar, though not identical, to timed Antipassback where a person cannot present his/her card to enter the same Area through which the most recent access occurred.

An Area Lockout violation can activate an Event, and any Area associated with Area Lockout functionality can be configured with such an Event.

Personnel may exit and re-enter the Lockout Area during the Lockout period as often as they wish (unless it is one of the locked-out target Areas), but every entrance/exit resets the Lockout timer and extends the Lockout time to the full configured period. Personnel can, however, access other non-lockout Areas without affecting the Area Lockout time period. Regular Antipassback can also be used with Lockout Areas, but is not required for Area Lockout functionality.

If Personnel activate a lockout, they cannot enter the locked-out target Area until the Lockout period has passed. If configured via the controller's RM LCD messages, the reader will display a reject "lockout" message with the time remaining in the Lockout period. If Personnel do **not** enter the locked-out target Area until the Lockout period has passed, they can then access this target Area without being rejected.

NOTE An **Area Lockout Grace** is available for gracing individual Personnel separately from the regular Personnel Antipassback **Grace Personnel**. However **Grace All** and **Grace All Partitions**, grace all Personnel for both regular Personnel Antipassback and Area Lockout.

Configuring Antipassback

To configure antipassback, you must configure at least two Areas.

- For Cluster Antipassback, the Areas must be controlled by Readers in the same iSTAR Cluster.
- For Global Antipassback, the Areas can be controlled by Readers on different iSTAR Clusters.

You can use the Area Antipassback tab to set up Regular and Timed Antipassback.

- Configuring Regular Antipassback for iSTAR Areas on Page 76
- Configuring Timed Antipassback for iSTAR Areas on Page 76
- Configuring Lockout for iSTAR Areas on Page 77

Antipassback Events

You can configure triggers to activate Events for antipassback entry/exit violations for an Area for those Personnel with the **Activate Antipassback Event** option selected on the **General** tab of the Personnel Editor.

- Entry events are pulsed on any violation that occurs on a Reader that leads into the Area.
- Exit events are pulsed on any violation on a Reader that leads out of the Area.

The specific cause of the violation does **not** affect which event is pulsed. For information, see:

- iSTAR Area Triggers Tab on Page 94
- Configuring Personnel Antipassback Options on Page 111.

For detailed information on configuring Events, see the Events chapter in the C•*CURE 9000 Software Configuration Guide*.

Antipassback Exempt Personnel

If you select the **Antipassback Exempt** option while configuring a Personnel record, the system allows the person to access Areas without being tested for antipassback.

NOTE The preceding does not apply to personnel in a Carpool Group. They are subject to Carpool Antipassback rules even when their Personnel record is configured with the **Antipassback Exempt** option.

Even if a person is configured as antipassback exempt, you can also choose to configure the **Activate Antipassback Event** option for him/her. In this case, while the person will gain access to the Area, he/she will also trigger any antipassback violation Events configured. For information, see Configuring Personnel Antipassback Options on Page 111.

Carpool Antipassback

Carpool Antipassback provides the capability to designate an Area as a Carpool Area and to organize Personnel into Carpool Groups that use these Areas.

A Carpool Area always enforces antipassback rules, and a Carpool Group always moves into/out of a Carpool Area as a unit. Whenever an entrance to a Carpool Area is accessed by a member of a Carpool Group, all members of the Group are considered to have passed through that entrance. The person who presented the card to enter the Carpool Area is designated as the Group driver.

The system maintains a Carpool Location (Carpool Area) for each Carpool Group in order to report the location for the Group members. When the Carpool Group member swipes at a Carpool entrance or exit, the group's location is moved.

NOTE The Carpool Group member designated as the driver must have Clearance at the Entrance Reader for the group to be given access to the Carpool Area..

Cards and Carpool Groups

Carpool Antipassback allows a Group of Personnel to be moved by a single Card swipe. Antipassback can be enforced on the Group when any Group member's Card is read. This Group of Personnel is known as a 'Carpool Group'.

If you apply Carpool Antipassback to multiple Areas in the same iSTAR cluster, all the Areas together behave as one Carpool system. That is, if a Carpool Group enters one Carpool Area on a cluster, antipassback is enforced for this group on all other Carpool Areas on this cluster.

A Carpool Group can have an unlimited number of Personnel in it, but each person can be in only one Carpool Group.

When a person who is in a carpool group accesses a Carpool Area, the iSTAR will admit or reject based on the Carpool Group’s location and whether or not Carpool Grace has been applied. If the Carpool Group is admitted and the entrance opens, the Carpool Group location for all Personnel in the Carpool Group is changed.

Carpool Regular Antipassback

Carpool regular antipassback works similarly to Personnel regular antipassback, except that is applies to a group of Personnel. It requires the following:

- Carpool Area: an Area that admits all Personnel in a Carpool Group with one card read.
- Carpool Group: a Group of Personnel configured to be admitted into a specified Carpool Area by presenting the card of any member of the Group.

A Carpool antipassback violation occurs when actions occur in the following sequence:

1. A card from the Carpool Group is presented at the entrance Reader.
2. Access is granted.
3. The Carpool location for all Group members is changed to the Area accessed.
4. A card from the same Carpool Group (the same or another card) is presented at the entrance Reader, without an exit read.

A tailgate Carpool Croup violation can occur when:

- A card from the Carpool Group is presented at the entrance Reader.
- Access is granted.
- Another Carpool Group or member of another Carpool Group also enters the Area without presenting their card.
- Anyone from the second group tries to exit the Area. (They are denied egress.)

NOTE Carpool antipassback and regular antipassback are separate features and cannot be configured in the same Area or in Areas adjacent to each other (where the exit Reader from one area is the entrance Reader into another). If the Areas are adjacent, you can have both Areas exit into a 'virtual' common non-antipassback Area.

Carpool Timed Antipassback

A Carpool timed antipassback violation occurs when a Carpool Group member presents a card at any entrance Reader to the same Carpool Area already accessed by that Group within a previously configured time period.

NOTE Both Carpool antipassback and Carpool timed antipassback work only with iSTARs.

Carpool Antipassback Limitations

If you configure Carpool antipassback in multiple areas on the same Cluster, the system considers the Carpool Areas as one Carpool system. You **cannot** enter Carpool Area A if the system thinks you are in Carpool Area B—both on the same Cluster, as long as the two Areas are **not** adjacent.

A Carpool Area may be adjacent to another Carpool Area or a **non**-Carpool Area. However, the following rules apply:

- A Carpool Area **cannot** be configured for:
  - Area Lockout.
  - Area Muster.
- An Area adjacent to a Carpool Area **cannot** be a:
  - Muster Area.
  - Cross-Cluster Area.
- A **non**-Carpool Area adjacent to a Carpool Area **cannot** enforce any form of Antipassback.

Carpool Antipassback Exemptions

Antipassback checking is exempt under the following condition:

- Any Person **not** in a Carpool Group can access a Carpool Antipassback Area if he/she has a valid clearance for this Area. The access does **not** display as a Group access.

However, a Person who is in a Carpool Group is subject to Carpool Antipassback rules even if their Personnel record has the **Antipassback Exempt** option selected.

NOTE To allow Personnel in a Carpool Group to be exempt from antipassback checking, you can either remove them from the Group or apply timed Carpool Grace for the Group. You can also create a Carpool Group with a single person.

Personnel who are **not** in any Carpool Group can be given Clearances for a Carpool Area. They can then enter and exit without any antipassback checking.

Using Personnel Antipassback and Carpool Antipassback

Carpool Antipassback and Personnel Antipassback are separate features. You **cannot** configure them in the same Area, nor in Areas adjacent to each other (where the exit Reader from one Area is the entrance Reader into another). You **cannot** enforce antipassback in the entrance and exit Carpool Areas in certain combinations. See Table 1 on Page 29 for combinations that you **cannot** use.

Table 1: Unallowed Antipassback Combinations

If Entrance Area Enforces...	Exit Area Cannot Enforce...
Regular Antipassback	Carpool Regular Antipassback
Regular Antipassback	Carpool Timed Antipassback
Timed Antipassback	Carpool Regular Antipassback
Timed Antipassback	Carpool Timed Antipassback
Carpool Regular Antipassback	Regular Antipassback
Carpool Regular Antipassback	Timed Antipassback
Carpool Timed Antipassback	Regular Antipassback
Carpool Timed Antipassback	Timed Antipassback
Carpool Regular Antipassback	Muster Area
Carpool Timed Antipassback	Muster Area

NOTE If you use any of these inappropriate combinations, the system displays a warning message and does **not** allow you to continue.

Antipassback Grace

When you *grace* Personnel, it resets their cards' Antipassback/timed antipassback information. Consequently, the first time Personnel use their cards after a grace action, the system does **not** check for Antipassback violations. Once they present their cards and open the door/entrance, the system logs them into the Area. After this move, for all subsequent use of their cards, the system returns to checking for Antipassback violations.

Grace also resets the iSTAR Global Antipassback owners of Personnel cards when the iSTAR owners are not communicating. The first time Personnel use their cards after a reset action, the controllers at which the cards are presented become the owners.

You can grace card(s) from both the Administration application and the Monitoring Station.

- 'Grace Personnel ' clears the antipassback and timed antipassback information for single Personnel.
- 'Person Area Lockout' grace clears all Area lockout timers for single Personnel, allowing entry to all target Areas that he/she is locked out of.
- 'Person Antipassback Reset Card' resets the iSTAR Global Antipassback owner of a single Personnel card; this also graces antipassback and area lockout.
- 'Carpool Grace' clears the antipassback and timed antipassback information for all Personnel in that Carpool Group.

You can apply the preceding types of 'person grace' as follows:

- On the Administration application in several places:
  - Personnel Dynamic View – for one or more selected persons.
  - Carpool Group Dynamic View – for all persons in the Group.
- On the Monitoring Station in several places:
  - Swipe & Show tab – for a single card. (If the card belongs to a person in a Carpool Group, 'Carpool Grace' applies to all Group members.)
  - On the Personnel in Area list – for one or more selected persons.

(For instructions on granting grace, see Gracing Personnel on Page 127.)

Grace All Partitions/Grace All

'Grace All' clears the Antipassback/Area Lockout information for all cards in one or more selected Partition(s), as well as resetting the iSTAR Global Antipassback owners of their cards. Grace All also applies a one-time Carpool Grace that applies to the next access for that Carpool Group. (This is **not** the 'timed' Carpool Grace.)

NOTE In an unpartitioned system, when all Objects are only in one Partition—the 'Default' Partition, Grace All does this for all cards in the system.

Grace All functions as follows:

- On the Administration application:
  - From the Partition Dynamic View – for one or more selected Partitions.
  - By configuring an Event with a Grace All Action.
- On the Monitoring Station Swipe & Show Grace Partition tab:

NOTE This is available **only** on the 'Legacy' Swipe & Show View, **not** on any of the new 'Default' Views.

- Grace All Partition Button – for all Personnel in all Partitions in the system, no matter how many.
- Grace All
  - If the system is **not** partitioned, gracing the Default Partition graces all cards in the database.
  - If the system is partitioned, you can select one or more Partition(s) for which you want to grace all cards.

Carpool Grace

You can grace all Personnel within a Carpool Group for antipassback for a specified time period with set start/end times. For the duration of the configured time, the Carpool Group members can move in and out of Carpool Areas without restriction. During this grace period, the Group's location remains unchanged.

Example:

> A system administrator or guard could configure the grace period for the Carpool Group the day before. Then anyone in the Group could drive his/her own car and park freely in the parking Areas..

The first time a Carpool Group member uses his/her card after the specified time period, the system does **not** check for Carpool antipassback. Once grace is granted, the Carpool Group must move through the entrance (present a card, open the entrance, and move through). After this move—for the next access, their correct location information is recorded, and antipassback is enforced as usual.

- A roll call report run during the grace period may display multiple drivers, since any card swipe will be accepted, and the person swiping the card will be marked as a carpool driver. If a second driver has parked the car in a different location, two locations will show up for this Carpool Group. After the grace time is over, the system reverts to one driver and one location.
- A Carpool Group **cannot** be de-mustered.

Antipassback Decision Making

How decision making works for Antipassback, both under normal conditions and during communications failure, depends on the type of Antipassback that you are using:

- Cluster – see Cluster Antipassback Decision Making on Page 32
- Global – see Global Antipassback Decision Making on Page 32

Cluster Antipassback Decision Making

How the Cluster Antipassback Decision is Made

In iSTAR Clusters, antipassback information is stored on the Cluster master. When an iSTAR member Controller is online and a card is presented at its reader:

- The member sends a request to the master for antipassback information.
- The master replies with the appropriate antipassback information (admit or deny).
- The member reports back to the Master whether or not the door was used.

As long as the communication within the Cluster is good, the Cluster members do not store any antipassback information.

How Cluster Antipassback Works During Communications Failure

When the Cluster members lose communication with the Cluster master, the members begin to enforce antipassback locally according to the **Communication Failure Mode** configured for the Cluster. If the failure mode is:

- **No Access** – Access is denied by any member Controller in the Cluster in communications failure, while member Controllers still in communications with the Master continue to make normal antipassback decisions for entry to the Area.
- **Local** – The Controllers use locally available information to grant or deny access. This information may be insufficient for the Controller to make a **completely correct** decision. In this case, the Controller still admits the person presenting the card.

Restoring Communication for Cluster Antipassback

When communications from member to master is restored, the member waits 16 sec*[size of cluster + 1] before uploading Personnel locations to the master. The master then compares the time recorded in the member with the time recorded on the master, retaining the person's latest recorded location. Once this upload is complete, the member deletes the locally stored antipassback data and resumes requesting this information from the master per the normal operation.

Global Antipassback Decision Making

How Global Antipassback Decisions are Made

iSTAR Global (cross-cluster) Antipassback allows clusters to share antipassback information. In this situation, a cluster master is designated as the owner of a card. The C•CURE 9000 Host maintains a table of all cards and their owner cluster masters and knows which cluster master owns any given card at any given time. When a card is presented at a member:

- If the cluster master of this member is the owner, the antipassback decision is similar to cluster antipassback.
- If the cluster master of this member is not the owner, the Host is requested for antipassback information.
- If there is no owner, the Host designates the requestor as the owner.
- If there is an owner, the Host forwards the request to the owner.
  - If the owner grants access, this reply is sent to the member that requested the information (requestor).
  - The ownership is transferred to the master of the requestor's cluster.
  - If the owner denies access, the message is sent to the requestor and the original owner retains ownership of this card.

How Global Antipassback Works During Communications Failure

When the Host loses connection with an owner cluster master, or a member loses communication with the master, the System Variable user-defined Failure Mode is invoked and antipassback is enforced locally on the cluster in which the card is presented. There are two Failure Modes:

No Access – where non-owners do **not** admit the card if they cannot communicate with the owner.

Local – where the iSTARs decide on antipassback based on information available to the cluster locally. If sufficient information is **not** available, the card is admitted. Relevant local information can include the following:

- Card's movement history
- Layout of doors and areas
- iSTARs that are in communications failure

If you configure the **No Access** failure mode, and a card is denied access because its owner is in communications failure, you can allow access to the part of the system in communication with the Host by resetting the cards antipassback data. The **Antipassback Reset Card** action, accessible from both the Administration application and the Monitoring Station, allows you to force the clusters that continue to communicate with the host to grace the card. After you reset the antipassback, the iSTAR at which the card is next presented becomes the owner of the card.

For the length of the communications failure, this card will have two owners: the old owner who is still in communications failure and the new owner.

NOTE You can use the preceding commands even if the owner is communicating with the Host. In this situation, the owner loses ownership and the card is graced/area lockout graced. The iSTAR at which the card is next presented assumes ownership. (When both owners and non-owners are communicating, a card cannot have two owners.)

Restoring Communication for Global Antipassback

If communication is restored only between the cluster master and the member, then antipassback will only work locally within that cluster. If the communication is restored between the master and the Host, then the antipassback data is synchronized across clusters. If the antipassback of the card was reset during communications failure, the system designates the iSTAR with the most recent antipassback information as the owner.

NOTE

Occupancy and Muster/De-muster information is not shared between clusters. Therefore, you cannot have cross-cluster (global antipassback) Areas with Occupancy restrictions or De-mustering.

However, since you can mix both global APB Areas and cluster Areas at your site, you can have occupancy and/or Muster/De-muster in the cluster Areas with adjacent global APB Areas for the boundaries.

Global Antipassback Configuration Guidelines

This section describes guidelines and limitations for iSTAR configurations that enforce global antipassback.

Performance

Antipassback performance and reliability are impacted by the following:

- Size of the cluster.
- Number of access requests per minute.
- C•CURE 9000 card processing time.
- Network latencies – slower networks result in slower access time.
  - Performance within the cluster depends on network performance between master and members.
  - Performance across clusters depends on network performance between the C•CURE 9000 Host and iSTAR masters.
- Faulty/excessively slow networks can cause communications failures that deny access and activate antipassback failure mode.
- Speed of the C•CURE 9000 Host—impacts configurations requiring a significant amount of access between clusters.

Data Storage

Global antipassback increases the size of the card antipassback record and reduces the amount of space available for card storage. Systems with very large databases might require additional SIMM storage.

Configuration Examples

The following section provides examples of good and poor practices for configuring iSTAR global antipassback.

General Considerations

Global antipassback configurations that optimize performance are designed to:

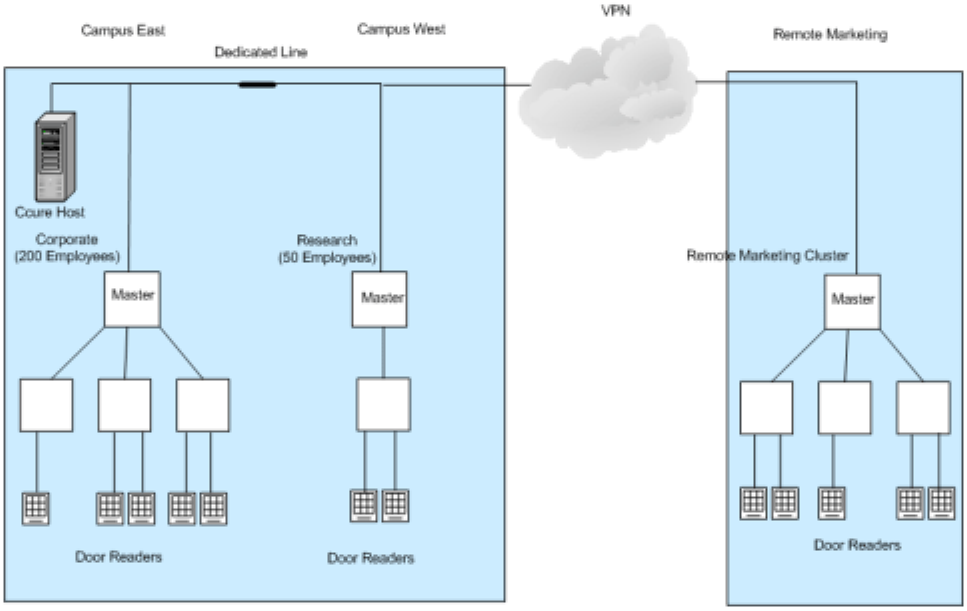
- Maximize processing by the iSTAR master.

  Performance is most efficient when the iSTAR master processes access for personnel within the cluster they access most frequently.
- Minimize access requiring Host intervention.
- Eliminate access across slow/unreliable networks.

High Performance Configuration

Figure 3 on Page 35 shows a configuration that successfully uses global antipassback to enforce area lockout.

Figure 3: A Recommended Configuration



The configuration in Figure 3 on Page 35 optimizes iSTAR performance as follows:

- By using two iSTAR masters:
  - One to control doors in the Corporate facility.
  - Another to control doors in Research.

  Each master processes requests for the doors and cardholders that access it most often.
- By using a fast, dedicated link to facilitate access between clusters.
- By not including doors that reside across a remote (less reliable) link in the global antipassback configuration.

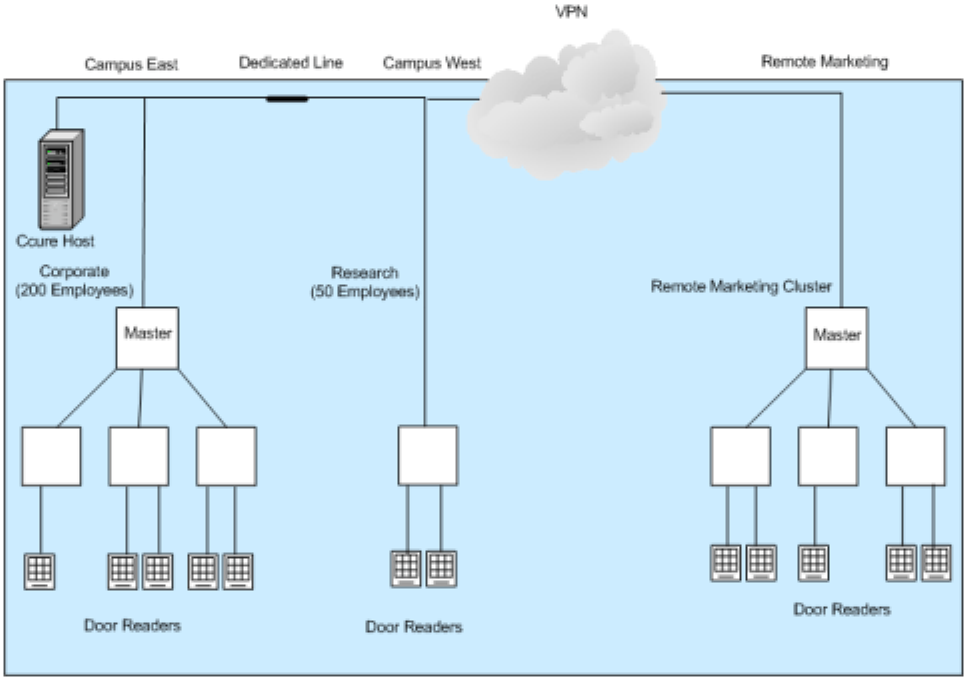
Poor Performance Configuration

The configuration shown in Figure 4 on Page 36 is not recommended. This configuration:

- Minimizes iSTAR efficiency by using a single iSTAR to process doors between two sites.
- Maximizes network inefficiency by using an unreliable network to connect a second global antipassback cluster.

If you use this configuration, you can experience long access delays or denial caused by slow processing and unreliable networks.

Figure 4: A Non-recommended Configuration



Occupancy Restrictions

You can limit access to an Area based on the **maximum** and **minimum** number of personnel present at one time. You can also specify the number of personnel from a group allowed in an Area. (Occupancy rules can also be applied to Carpool Areas. For information, see Carpool Antipassback and Occupancy on Page 38.)

This feature is supported only for iSTAR Areas, and therefore for iSTAR controllers. The doors of an Occupancy-restricted Area can be on multiple iSTARs as long as all are in the same cluster.

NOTE The Occupancy restriction is not supported across iSTAR Clusters.

Maximum occupancy specifies the maximum number of personnel, or personnel from a group, who can access an Area at one time. If at any time the number of personnel in an Area reaches the maximum number and access is restricted, all further access is denied—until personnel leave the area. You can also configure an Event to trigger when an Area reaches its maximum occupancy. A common use of this feature is in parking lots where only a given number of personnel, or personnel from a group, can park in an Area.

In addition, you can configure maximum occupancy to **only** count the number of personnel entering and leaving an Area **without restricting access**.

Minimum occupancy(or **N-man Rule**) specifies that a minimum number of personnel must enter the Area at the **same time** to gain access and must also remain in the specified Area. You can also configure an Event to trigger when an Area reaches its minimum occupancy.

In addition, you can configure minimum occupancy to **only** count the number of personnel entering and leaving an Area **without restricting access**.

NOTE

- Counting for Areas configured for occupancy is performed by the iSTAR Controllers. For Areas without occupancy it is performed by the host. Consequently, to keep the Area count correct if you are going to change an existing occupancy Area to a non-occupancy Area—or vice versa, you should ideally do it when the system is not busy and the Area is empty. Alternatively, if there are Personnel in the Area, you can use the **Set Property** option on the right-click context menu on the Areas Dynamic View to reset the count for the Area.
- A Cluster member Controller that is offline from the Master and host may not enforce occupancy restrictions properly. It may enforce some, but not all, of the restrictions, or it may work as configured.

Carpool Antipassback and Occupancy

Area occupancy restrictions are applied to Carpool Areas in the same manner as for ordinary Person Areas with one difference. The occupancy counts in Carpool Areas are based on the number of Carpool Groups, not the number of individual Personnel. Consequently you can use Occupancy restrictions to limit the maximum number of vehicles in a Carpool Area, as described in the Example below.

NOTE Generally, you would **not** configure minimum occupancy restrictions for a Carpool Area.

Example: Using Occupancy Restrictions with Carpool Antipassback

1. Company A and Company B share a parking lot controlled by an iSTAR Cluster with Readers on automobile access gates. Each company is limited to using 100 parking spots. The lot is defined as a Carpool Area, and each company enforces Carpool Antipassback.
   - All of Company A's Personnel are placed in an 'ordinary' Personnel Group, Group A, and also assigned to Carpool Groups.
   - All of Company B's Personnel are placed in another 'ordinary' Personnel Group, Group B, and also assigned to Carpool Groups.
2. The maximum occupancy allowed in the lot for each company's groups—Group A and Group B—is configured in the **Occupancy Restrictions for Personnel Groups** table on the **Occupancy** tab. In this case, the maximum represents the number of cars allowed. When a driver of a car in Group A or Group B scans a card and enters the lot, one vehicle is counted against the maximum number of spots available for Company A or Company B.

   In addition, Carpool Antipassback is also being enforced (as described in Carpool Antipassback on Page 26). Consequently, when the driver of one of Company A's/Company B's Carpool Groups scans his/her card to get into the parking lot, the count in the Carpool Area increases by one.
3. In this way, the maximum number of vehicles in the parking lot can be limited for each company and Carpool Antipassback also enforced.

Pass-through Areas

Area Pass-through allows you to configure an Area that require a person to exit from it within a specified time interval after entering. A cardholder who enters a Pass-through Area and does **not** exit in the specified time causes a pass-through violation.

The Area Pass-through time can be configured:

- So the interval applies to any cardholder entering the Area. This is known as the Area-wide Pass-through time or interval.
- So the members of a Personnel Group:
  - Have to use the Area-wide interval.
  - Are exempt from any pass-through restriction configured on an Area.
  - Are subject to a custom interval different from the Area-wide interval.

  When a Personnel Group is configured with a pass-through restriction, the configured interval always applies to all Group members.

You configure Area Pass-through on the iSTAR Areas **Occupancy** tab. See iSTAR Area Occupancy Tab on Page 78

Escorted Access

Escorted Access gives C•CURE 9000 the ability to control, track, and report on the movements of Personnel designated as Escorted Visitors. An *Escorted Visitor* is a visitor who can only move around a facility in tandem with an employee designated as an *Escort*.

NOTE A person designated simply as a *Visitor* can move freely around a facility **un**escorted.

Escorted access allows you to do the following:

- Designate a cardholder as the following:
  - An Escorted Visitor, who by default must be accompanied by an Escort to be granted access when presenting a card at a reader.
  - An Escort, a person who can grant access to any Escorted Visitor—as long as other access control rules, such as clearance restrictions, are met.
- Configure an Area:
  - To require an Escorted Visitor to be accompanied by an Escort to enter. (By default, all areas require an Escorted Visitor to have an Escort.)
  - To optionally **not** require an Escort to accompany an entering Escorted Visitor.
  - To optionally require that an Escort must **always be present** with an Escorted Visitor inside that Area.

  Escorted Visitors can only exit an Area without an Escort if the Area they are passing into is configured to not require an Escort for Escorted Visitors. If all Areas in a building are configured to require Escorted Access, Visitors will always require an Escort to move around within the facility.
- To allow an operator to view the count of Escorted Visitors and Escorts in any Area, and to modify the counts if necessary.

If the Doors that lead to an Area are unlocked for any reason, double swipe, for example, then Escorted Visitors are free to enter and leave the Area without an Escort.

If an Area is subject to Occupancy Restrictions, the total number of people entering the area must respect the specified restrictions. If during the Escorted Visitor–Escort sequence the total number of cards presented exceeds the maximum occupancy limit, all Escorted Visitors as well as the Escort are rejected. If an Area has a minimum occupancy restriction greater than one, the number of Escorted Visitors plus the Escort entering an empty Area must be equal to or greater than the minimum requirement; if not, entry is rejected.

There are two modes of Escorted Access: Companion mode and Remote Escort mode.

- In **Companion mode**, multiple Escorted Visitors can be accompanied by one escort, and they all start on the same side of a door. The Escorted Visitors present their cards first, one after another. After all the Escorted Visitors have swiped, the Escort presents his/her card to let the queued up Escorted Visitors through the door. (Companion mode is in effect if the “Readers are continuously active” flag is selected in the iSTAR Door Configuration dialog box.)

  If someone who is neither an Escorted Visitor nor an Escort presents a card before the Escort swipes his or hers, the presented card and all waiting Escorted Visitor and Escort cards are rejected. The Escorted Visitors must now restart the presentation of their cards. However, it is possible, once the Escorted Visitor sequence has started at one side of the door, for an RTE to be made on the other side. In this case, the door can be opened from the RTE side, and it is the Escort's responsibility to keep the Escorted Visitors from aborting their sequence. The Escorted Visitor/Escort sequence continues once the door has closed.

- In **Remote Escort** mode (also called Turnstile mode), the Escorted Visitors and Escort present themselves on opposite sides of the door. An Escorted Visitor presents his/her card first on one side of the door and an Escort then presents his/her card on the other side of the door. Any subsequent Escorted Visitors must do the same—one Escorted Visitor swipe, one Escort swipe. (This mode is in effect if the "Readers are continuously active" flag is **not** selected in the iSTAR Door Configuration dialog box.)

NOTE The time between swipes cannot be greater than that defined in the 'Next Card Time' System Variable.

The maximum number of Escorted Visitors that may travel through a door during one access is defined in System Variable Maximum Visitor Count.

If an Area is subject to Antipassback restrictions:

- In **Companion** mode, Escorted Visitors and Escorts granted access are logged into the Area in the same manner as for regular access.
- In **Remote Escort** mode, the Escorted Visitors' location will be updated, but the Escort's location will not change.

Six pre-defined Reports can be generated to show the access activities of the following:

- Non-escorted Visitors
- Escorts
- Escorted Visitors

Activity messages on the Monitor Station will distinguish:

- Escorted Access messages from other Door/Area access messages.
- Escorted Access violation messages from other Door/Area access violation messages.
- 'Invalid escort' messages from 'escort not present' messages.

NOTE Escorted Access decisions to allow or deny access are made at a Door based on a person's Escorted Visitor/Escort attribute. The iSTAR panel makes that decision regardless of whether or not the Door is part of an Area. In other words, any Door that is not part of an Area will always require Escorted Visitors to have an Escort to gain entry through that Door.

Dynamic Area Manager

This feature requires that a single person at any one time be made responsible for an iSTAR Area—become the Area Manager. This person, who has a Clearance for the Area, must be the first one to enter the Area and then **must be the last person** to leave. If this feature is enabled, when anyone in the Area presents a card to exit, the system checks whether he/she is the Area Manager and whether he/she is the last one left. If it is the Area Manager swiping and he/she is **not** the last person present, the exit is rejected with the reason "unattended".

This feature can also be used in conjunction with Conditional Access. See "iSTAR Door Conditional Access Tab" in the Doors chapter in the C•*CURE 9000 Hardware Configuration Guide*.

Example:

> This feature can be used for security in a bank's cash counting room. It makes sure that one designated person, the first to enter, oversees the entire operation and the other personnel within the room. Consequently, that person, the 'Dynamic Area Manager', must be the last to leave the room after everyone else has exited.

The Area that a Dynamic Area Manager becomes responsible for can be regulated only by iSTAR Pro, eX, Edge, or Ultra Controllers. The iSTAR controller that regulates the Door leading into the Area can be either a master or slave in an iSTAR Cluster, and the Area itself may or may not cross Controller boundaries. Since occupancy is **not** supported within Areas that cross physical Clusters, the C•CURE 9000 system-based Areas impacted by Dynamic Area Manager are contained within a definitive iSTAR Cluster. These Areas use Antipassback control with Occupancy control.

Once Dynamic Area Manager is enabled, the Area counts are tracked by the Panel instead of the Host. Consequently, the feature will work even if the Server is unavailable. The Area User Count will indicate the presence or absence of the 'Area Manager' as well as the number of 'Managed Personnel' inside—all Personnel admitted after the 'Area Manager'.

NOTE An Area for which Dynamic Area Manager is enabled does not support Escorted Access (Escorts/Visitors).

You configure the Dynamic Area Manager feature on the iSTAR Areas **Occupancy** tab. See iSTAR Area Occupancy Tab on Page 78.

Tracking the Location of Personnel

The C•CURE 9000 host maintains a iSTAR Area for each Personnel record—including those of Escorted Visitors and Escorts—as well as the time at which the area was entered.

The current iSTAR Area represents the last known Area the person entered, based on a valid admit: there was a card swipe granting access, and the Door/entry was opened after the access was granted. If the Door/entry is not opened after a valid admit or access is denied, a person's current iSTAR Area is not updated.

The iSTAR Cluster Areas feature allows you to track the current location of Personnel in several different ways:

- Displaying their current Area on the Administration application Personnel Dynamic View. For information, see Viewing Area Location of Personnel on Page 119
- Displaying the Personnel for a selected iSTAR Area from the following:
  - Administration application Area Dynamic View.
  - Monitoring Station Area Status List.
  - Administration application/Monitoring Station Area icon on Map.

  For information, see Viewing Personnel in an Area on Page 60 and the C•*CURE 9000 Monitoring Station Guide*.
- Running one of the pre-defined Reports with information related to Areas:
  - Roll Call or Carpool Roll Call Report to generate a list of Personnel by Area(s) or Area group(s).
  - Carpool Group Report to generate a list of Carpool Groups with their Group members.
  - Visitor/Escort Reports to generate lists of Admitted/Rejected Escorts and/or Visitors.

  You can run these Reports:

  - From the Administration application Report Dynamic View.
  - From the Monitoring Station Report Status List.
  - By configuring an Event whose Action initiates the Report.

  For information, see Running Area Pre-defined Reports on Page 123; Appendix A "Pre-defined Reports, Queries, and Views" in the C•*CURE 9000 Data Views Guide*; the C•*CURE 9000 Monitoring Station Guide*; and the Event chapter in the C•*CURE 9000 Software Configuration Guide*.

Area User Count

The C•CURE 9000 server also maintains a count for each iSTAR Area of Personnel, Escorts and Escorted Visitors, Dynamic Area Manager and Managed Personnel, and Conditionally Admitted Personnel that you can display on either of the following:

- Administration application iSTAR Area Dynamic View.
- Monitoring Station Area Status List.

The count of these different Personnel types in an iSTAR Area can become incorrect due to tailgating, communication failure, or restarting the master controller.

Example:

> When a cardholder tailgates out of an area on which Occupancy Restrictions are configured, the personnel count may become inaccurate if the cardholder is graced to enter another area - the previous area's personnel count

may not decrement.

This problem can be avoided by configuring Occupancy Restrictions on every area. For those areas where Occupancy Restrictions are not desired, the recommended configuration is to set the area **Maximum Occupancy** field to **Allow Access** and set the **Maximum Limit** to a value higher than ever expected.

NOTE For the 'Personnel Count' to be maintained in a Carpool Area, you must configure Occupancy Restrictions. If you do **not** want a **real restriction**, configure a high maximum Occupancy value, as described in the preceding paragraph.

In addition, since counting for iSTAR Areas configured for occupancy is done by iSTAR Controllers, while it is done by the host for non-occupancy Areas, the count can be corrupted if an existing Area is changed from occupancy to non-occupancy—or vice versa. To keep the iSTAR Area counts correct, you should only make such changes when the system is not busy and the Areas are empty.

NOTE A Cluster member Controller that is offline from the Master and host may not enforce occupancy restrictions properly. As a result, when the Controller comes back online, the Area counts may be wrong.

The Count Status for Personnel, Escorts, or Escorted Visitors in an iSTAR Area can be reset to the correct value by an Operator through a property set. The Count Status for Area Manager, Conditionally Admitted Personnel, and Managed Personnel can also be reset—but only to 0 (zero). (However, you should do this only if you are certain that no such Personnel are currently in the iSTAR Area. Otherwise, changing the count to zero could cause unwanted consequences.)

These manual modifications of the iSTAR Area counts are audited, unlike the system updates that are not.

For information, see Viewing a List of iSTAR Areas on Page 56 and Setting a Property for an iSTAR Area on Page 66.

iSTAR Area Configuration Steps

Table 2 on Page 45 shows the C•CURE 9000 Editors and activities that create iSTAR Areas. This table assumes that you have already configured the iSTAR Cluster(s) and Controllers, Doors, and Readers.

Table 2: Creating iSTAR Areas

Task	C•CURE 9000 Editor	Configuration Notes	Additional Information
Configure first basic iSTAR Area and define it for Cluster Antipassback or Global Antipassback	Areas and Zones>iSTAR Area>New>iSTAR Area Editor and General tab	Creates iSTAR Area—and without assigning Doors—defines it as either of following: • Cluster Area – enforcing Cluster Antipassback on specific iSTAR Cluster: - Selects Cluster for Area • Cross-Cluster Area – enforcing Global Antipassback across iSTAR Clusters	See Configuring an iSTAR Area on Page 53, iSTAR Area Editor on Page 67, and iSTAR Area General Tab on Page 67.
Configure iSTAR Area Doors/Readers/Adjacent Areas	Areas and Zones>iSTAR Area>New>iSTAR Area Editor>General tab	Specifies • Access In - Doors - Readers - Adjacent Areas • Access Out (If Access In Door has two Readers) - Doors - Readers - Adjacent Areas	See iSTAR Area General Tab on Page 67.

Creating iSTAR Areas (continued)

Task	C•CURE 9000 Editor	Configuration Notes	Additional Information
Configure iSTAR Area Antipassback	Areas and Zones>iSTAR Area>New>iSTAR Area Editor>Antipassback tab	Specifies • For Antipassback - Antipassback Type: none/regular/timed - For timed APB: options - For Carpool Area: exit options • For Area Lockout - Target Lockout iSTAR Area/iSTAR Area Group - Lockout Time: days/hours/minutes - "Valid card rejection" or "admit unused access" causes lockout	See iSTAR Area Antipassback Tab on Page 74.

Creating iSTAR Areas (continued)

Task	C•CURE 9000 Editor	Configuration Notes	Additional Information
Configure iSTAR Area Occupancy Rules	Areas and Zones>iSTAR Area>New>iSTAR Area Editor>Occupancy tab	Specifies • Occupancy Restrictions for all Personnel - Max/Min: none/allow access/restrict access - Max/Min Limits • Dynamic Area Manager Enabling • Pass-through Restrictions for all Personnel • Occupancy Restrictions for Personnel Groups: - Max/Min - Options • Pass-through Restrictions for Personnel Groups: - Pass-through type NOTE: Occupancy configuration choices also set default Occupancy Mode for Area.	See iSTAR Area Occupancy Tab on Page 78. See iSTAR Area Status Tab on Page 99 and Configuring Event Actions to Affect Areas on Page 114
Configure Escorted Access	Areas and Zones>iSTAR Area>New>iSTAR Area Editor>Escort tab	Specifies • Escort Enforcement Option - Escorted Visitor must have Escort to enter. - Escorted Visitor may enter alone. • Whether or not Escort must always be present with Escorted Visitor in iSTAR Area.	See iSTAR Area Escort Tab on Page 87.

Creating iSTAR Areas (continued)

Task	C•CURE 9000 Editor	Configuration Notes	Additional Information
Configure Muster/De-muster	Areas and Zones>iSTAR Area>New>iSTAR Area Editor>Muster tab	Specifies • Whether or not iSTAR Area is Mustering Area. • Area to De-muster to.	See iSTAR Area Muster Tab on Page 90.
Configure iSTAR Area Triggers	Areas and Zones>iSTAR Area>New>iSTAR Area Editor>Triggers tab	Specifies Event Actions to be activated for various Area violations and Occupancy statuses.	See iSTAR Area Triggers Tab on Page 94.
Change Area State Images	Areas and Zones>iSTAR Area>New>iSTAR Area Editor>State Images tab	Modify Images that indicate Area states on Monitoring Station and Maps.	See iSTAR Area State Images Tab on Page 100 and State Images Tab Tasks on Page 101.
Configure Carpool Group	.Areas and Zones>Carpool Group>New>Carpool Group Editor	Creates Carpool Group and selects Personnel members.	See Configuring a Carpool Group for Carpool Antipassback on Page 102.
Configure APB Comm Fail Modes and Global Antipassback for iSTAR Clusters	Edit the Area's iSTAR Cluster: Hardware> Hardware Tree>iSTAR Cluster>iSTAR Cluster Editor>Area Tab	• Specifies whether or not Cluster enforces Global Antipassback for Areas as well as Cluster Antipassback. • Specifies APB decision-making mode for Area's iSTAR Cluster during communications failure: - No Access or Local	See Configuring iSTAR Clusters for APB Comm Fail Modes and Global Antipassback on Page 105.
Configure Escorted Access Mode for iSTAR Door	Edit the Area's iSTAR Door: Hardware> Hardware Tree>iSTAR Door Editor>General Tab	Specifies Reader setting required for Companion Mode or Remote Access (Turnstile) Mode: whether Reader is continuously active or not.	See Configuring Escorted Access Mode on Page 109.

Creating iSTAR Areas (continued)

Task	C•CURE 9000 Editor	Configuration Notes	Additional Information
Configure Personnel APB Options	Personnel>Personnel> New>Personnel Editor - or - Edit an existing Personnel Record	Specifies that person: • Is exempt from APB rules. - and/or - • Activates APB Events.	See Configuring Personnel Antipassback Options on Page 111.
Configure Personnel Escort Options	Personnel>Personnel> New>Personnel Editor - or - Edit an existing Personnel Record	Specifies person's Escort type: • None • Visitor (non-escorted) • Escorted Visitor • Escort	See Configuring Personnel Escorted Access Options on Page 112.

Creating iSTAR Areas (continued)

Task	C•CURE 9000 Editor	Configuration Notes	Additional Information
Modify System Variable Settings for APB • Changes these values only in consultation with Software House Technical Support Center. Incorrect settings can cause APB comm fail.	Options & Tools>System Variables>iSTAR Driver> • iSTAR APB Max ping round trip • iSTAR APB Ping interval • iSTAR APB response timeout • iSTAR Global Antipassback Communication Failure Mode • Host Global Antipassback Response Timeout • iSTAR Global Antipassback Response Timeout	Variables that fine-tune iSTAR controller behavior for APB functionality.	See "iSTAR Driver Settings" in the System Variables chapter in the *C•CURE 9000 System Maintenance Guide* or Setting System Variables That Affect Areas on Page 116.
Modify System Variable Settings for Occupancy	Options & Tools>System Variables>iSTAR Driver> • Always Track Personnel • Minimum Occupancy Exit Option Options & Tools>System Variables>Hardware Driver> • Next Card Time	Variables that effect controller behavior for Occupancy functionality.	
Modify System Variable Settings for Escorted Access	Options & Tools>System Variables>iSTAR Driver> • Maximum Visitor Count Options & Tools>System Variables>Hardware Driver> • Next Card Time	Variables that affect Controller behavior for Escorted Access functionality.	

Basic iSTAR Area Tasks

The C•CURE 9000 iSTAR Area Editor allow you to accomplish the following tasks:

- Creating an iSTAR Area on Page 52
- Creating an iSTAR Area Template on Page 52
- Configuring an iSTAR Area on Page 53
- Viewing a List of iSTAR Areas on Page 56
- Viewing Personnel in an Area on Page 60
- Viewing Personnel Groups Associated with an Area on Page 60
- Viewing the Status of an iSTAR Area on Page 61
- Viewing Occupancy Mode Causes for an Area on Page 64
- Modifying an iSTAR Area on Page 64
- Deleting an iSTAR Area on Page 65
- Setting a Property for an iSTAR Area on Page 66
- Adding an iSTAR Area to a Group on Page 66

The following tasks related to configuring and using iSTAR Cluster Areas are accomplished through other C•CURE 9000 features:

- Configuring iSTAR Clusters for APB Comm Fail Modes and Global Antipassback on Page 105
- Configuring Escorted Access Mode on Page 109
- Configuring Personnel Antipassback Options on Page 111
- Configuring Personnel Escorted Access Options on Page 112
- Configuring Event Actions to Affect Areas on Page 114
- Setting System Variables That Affect Areas on Page 116
- Viewing Area Location of Personnel on Page 119
- Viewing Area Information on the Door Editor on Page 121
- Running Area Pre-defined Reports on Page 123
- Gracing Personnel on Page 127
- Viewing Area Status with Map Icons on Page 132

Accessing the iSTAR Area Editor

You can access the **iSTAR Area Editor** from the C•CURE 9000 Areas and Zones pane.

To Access the iSTAR Area Editor

1. In the Navigation Pane of the Administration Workstation, click the **Areas and Zones** pane button.
2. Click the Areas and Zones drop-down list and select **iSTAR Area**.
3. Click **New** to create a new Area.

- or -

Click ➡ ▾ to open a Dynamic View showing a list of all existing iSTAR Area Objects, right-click the iSTAR Area you want to change, and click **Edit** from the context menu that appears.

The **iSTAR Area Editor** opens with the **General** tab displayed, as shown in Figure 6 on Page 68.

Creating an iSTAR Area

You can create a new iSTAR Area using the **iSTAR Area Editor**.

This procedure assumes that you have already configured the iSTAR Cluster(s) and Controllers, Doors, and Readers.

To Create an iSTAR Area

1. In the Navigation Pane of the Administration Workstation, click the **Areas and Zones** pane button.
2. Click the **Areas and Zones** drop-down list and select **iSTAR Area**.
3. Click **New** to create a new Area. The **iSTAR Area Editor** opens (see iSTAR Area Editor General Tab on Page 68).
4. You can now configure the new Area.
5. To save your new Area, click **Save and Close**.

   - or -

   Alternatively, if you want to save the Area and then create a new one, click **Save and New**. The current Area is saved and closed, but the **iSTAR Area Editor** remains open ready for a new Area.

Creating an iSTAR Area Template

You can create a new iSTAR Area Template using the **iSTAR Area Editor**. An iSTAR Area template saves you time because you do not have to re-enter the same Area information again.

To Create an iSTAR Area Template

1. In the Navigation Pane of the Administration Workstation, click the **Areas and Zones** pane button.
2. Click the **Areas and Zones** drop-down list and select **iSTAR Area**.
3. Click the down-arrow on the **New** button, and click **Template**.

   The **iSTAR Area Editor** where you can configure the Area template opens (see iSTAR Area General Tab on Page 67).
4. Configure the template to meet your requirements. Any fields that you configure with values become part of the template; then when you subsequently create a new Area from that template, these values are already filled in.
5. In the **Name** field, enter the name you wish to use for the template.

   Example:

   iSTARAreaTemplate1
6. To save the template, click **Save and Close**.

The template will be available as an option on the pull-down menu on the **New** button in the **Areas and Zones** pane.

Configuring an iSTAR Area

This procedure assumes that you have already configured the iSTAR Cluster(s) and Controllers, Doors, and Readers.

NOTE To aid in the configuration process, Software House suggests that you create a basic diagram showing all Doors, Readers, and Areas you need to configure. Then as you perform the configuration of each component, mark the diagram so you know which components are configured and which remain to be configured. Figure 1 on Page 18 is an example of an Area diagram.

- For a **Cluster Area** – The general sequence for creating/configuring an area is to first select the Cluster to control the Area.
- For a **Cross-Cluster** Area – The general sequence for creating/configuring an area is to first configure iSTAR Clusters for Global Antipassback in addition to Cluster Antipassback.

You then add a row to the **Access In** table and select a Door, Reader, and an adjacent Area.

Since each row entry for Door and Reader requires an adjacent Area, the first Area (**Area1**, for example) must be saved without any assigned Doors. You can then configure an adjacent Area (**Area2**, for example) with Door, Reader, and the first Area you created (**Area1**) as the adjacent Area.

The easiest way to do the foregoing is to create the first Area, click **Save and New**, and then create the additional Area(s) as described in the example procedure that follows.

Once you have saved **Area2**, it is automatically entered as the adjacent Area for **Area1**, and **Area2's** Access Out Door and Reader are also entered as the Access In Door and Reader for **Area1**.

To Configure iSTAR Areas

1. Create a new iSTAR Area. (See Creating an iSTAR Area on Page 52.)
2. Type a **Name** and **Description** for the iSTAR Area that sufficiently identifies this Area and its purpose.

   Example:

   iSTARArea1
3. Select the Area type from the drop-down: **Cluster Area** or **Cross-Cluster Area**.
   - If you chose **Cluster Area**, select an iSTAR Cluster for the Area on the **General** tab (shown in Figure 6 on Page 68).
   - If you chose **Cross-Cluster Area**, the system displays **Global Antipassback iSTAR Area**.
4. To save your first 'Doorless' Area and then create an adjacent Area, click **Save and New**.

   The current Area is saved and closed, and the **iSTAR Area Editor** remains open, ready for a new Area.
5. Repeat Step 1 and Step 2 on this page for the second Area.

   Example:

   iSTARArea2
6. If you chose **Cluster Area** for type for Step 3 on this page, select the same iSTAR Cluster you selected in that step.

7. Use the **General** tab (shown in Figure 6 on Page 68) to configure the **Access In** table Doors and Readers for the Area and the adjacent Area. The **Access Out** table is populated automatically based on the **Access In** choices.

8. Use the **Antipassback** tab (shown in Figure 7 on Page 74) to configure:

   - Type of Antipassback for the Area and the related options.
   - Lockout for the Area.

9. Use the **Occupancy** tab (shown in Figure 8 on Page 78) to configure the types of Occupancy for the Area and the related options.

10. Use the **Escort** tab (shown in Figure 10 on Page 88) to configure the type of Escorted Access for the Area.

11. Use the **Muster** tab (shown in Figure 11 on Page 91) to configure the Area as a Mustering Area and to select its De-muster Area.

12. Use the **Triggers** tab (shown in Figure 12 on Page 94) to configure triggers that can activate Event Actions when the Area's different Violation properties and Occupancy statuses have a certain value.

    Examples:

    APB Entry Violation or APB Exit Violation

    At or Over Maximum or At or Under Minimum

13. Use the **State Images** tab (shown in Figure 14 on Page 101) to modify the Images that indicate Area states on the Monitoring Station for this Area.

14. To save **Area2** as configured, click **Save and Close**.

15. Open **iSTARArea1** in the **iSTAR Area Editor** to finish configuring it:

    a. Select **iSTAR Area** from the **Areas and Zones** drop-down list and click ➡ ▾ to open the Dynamic View list of the two iSTAR Areas.

    b. Double-click **iSTARArea1**.

16. On the **General** tab, view the system-entered Doors, Readers, adjacent Area (**Area2**) in the **Access In** and **Access Out** table rows.

17. Configure Antipassback, Occupancy, State Images, and Trigger options for **iSTARArea1**, as needed.

18. Click **Save and Close**.

    - or -

    Alternatively, if you want to save this Area and then create another one, click **Save and New**.

Configuring an iSTAR Carpool Area for Carpool Antipassback

This procedure assumes that you have already configured the iSTAR Cluster and Controllers, Doors, and Readers.

NOTE To aid in the configuration process, Software House suggests that you create a basic diagram showing all Doors (Entrances), Readers, and Areas you need to configure. Then as you perform the configuration of each component, mark the diagram so you know which components are configured and which remain to be configured. Figure 1 on Page 18 is an example of an Area diagram.

The general sequence for creating/configuring a Carpool Area is to first select the Cluster to control the Area. (A Carpool Area **cannot** be a Cross-Cluster Area.)

You then add a row to the **Access In** table and select a Door (Entrance), Reader, and an adjacent Area.

Since each row entry for Door (Entrance) and Reader requires an adjacent Area, the first Area (**Area1**, for example) must be saved without any assigned Doors (Entrances). You can then configure an adjacent Area (**Area2**, for example) with Door (Entrance), Reader, and the first Area you created (**Area1**) as the adjacent Area.

The easiest way to do the foregoing is to create the first Area, click **Save and New**, and then create the additional Area(s) as described in the example procedure that follows.

NOTE The Area adjacent to a Carpool Area can be either a Carpool Area or a **non**-Carpool Area. An adjacent **non**-Carpool Area, however, **cannot** enforce any form of Antipassback, **nor** can it be a Muster or Cross-Cluster Area.

Usually, you configure the Area adjacent to a Carpool Area as a 'virtual' Area, designated as 'Outside'. You can also configure several Carpool Areas adjacent to each other.

Once you have saved **Area2**, it is automatically entered as the adjacent Area for **Area1**, and **Area2's** Access Out Door (Entrance) and Reader are also entered as the Access In Door (Entrance) and Reader for **Area1**.

To Configure an iSTAR Carpool Area

1. Create a new iSTAR Area, whether a Carpool Area or a 'regular' Area. (See Creating an iSTAR Area on Page 52.)
2. Type a **Name** and **Description** for the Area that sufficiently identifies it and its purpose.

   Examples:

   OutsideAreaRear1 or **iSTARCarpoolAreaRear1**
3. Select the Area type from the drop-down: **Cluster Area**.
4. Select an iSTAR Cluster for the Area on the **General** tab (shown in Figure 6 on Page 68).
5. To save your first 'Doorless' Area and then create an adjacent Area, click **Save and New**.

   The current Area is saved and closed, and the **iSTAR Area Editor** remains open, ready for a new Area.
6. Repeat Step 2 and Step 3 on this page for the second Area, giving it an appropriate name and description.

   Examples:

   iSTARCarpoolAreaRear1 or **iSTARCarpoolAreaRear2**
7. Select the same iSTAR Cluster you selected in Step 4.
8. Use the **General** tab (shown in Figure 6 on Page 68) to configure the **Access In** table Doors (Entrances) and Readers for the Area and the adjacent Area. The **Access Out** table is populated automatically based on the **Access In** choices.
9. Use the **Antipassback** tab (shown in Figure 7 on Page 74) to configure Carpool Antipassback for the Area with its related options.
10. Use the **Occupancy** tab (shown in Figure 8 on Page 78) to configure the Occupancy restrictions for the Carpool Area.
11. Use the **Triggers** tab (shown in Figure 12 on Page 94) to configure triggers that can activate Event Actions when the Carpool Area's different Violation properties and Occupancy statuses have a certain value.

Examples:

APB Entry Violation or APB Exit Violation

At or Over Maximum

12. Use the **State Images** tab (shown in Figure 14 on Page 101) to modify the Images that indicate Area states on the Monitoring Station for this Carpool Area.

13. To save **Area2** as configured, click **Save and Close**.

14. Open **iSTARArea1** in the **iSTAR Area Editor** to finish configuring it:

    a. Select **iSTAR Area** from the **Areas and Zones** drop-down list and click ➡ to open the Dynamic View list of the two iSTAR Areas.

    b. Double-click **iSTARArea1**.

15. On the **General** tab, view the system-entered Doors (Entrances), Readers, adjacent Area (**Area2**) in the **Access In** and **Access Out** table rows.

16. Configure Antipassback, Occupancy, State Images, and Trigger options for **iSTARArea1**, as needed.

17. Click **Save and Close**.

    - or -

    Alternatively, if you want to save this Area and then create another one, click **Save and New**.

Now, to successfully use this Area for Carpool Antipassback, you should create Carpool Groups. For directions, see Configuring a Carpool Group on Page 103.

Viewing a List of iSTAR Areas

You can display a list of the iSTAR Areas you have created by opening a Dynamic View of iSTAR Areas.

NOTE The Dynamic Views information refreshes automatically, showing items that have changed values and new items that were not included before.

To View a List of iSTAR Areas

1. In the **Navigation** Pane of the Administration Workstation, click **Areas and Zones** to open the **Areas and Zones** pane.

2. Select **iSTAR Area** from the **Areas and Zones** drop-down list.

3. Click ➡ to open a Dynamic View listing all iSTAR Area Objects. (You can also click the down-arrow of this button to either view the list in the current tabbed view or open a new tabbed view.)

    - You can sort, filter, and group items in the list.
    - You can right-click an iSTAR Area in the list to open the iSTAR Area Context menu and perform any of the functions on that menu. (See Viewing Personnel in an Area on Page 60.)
    - You can right-click any column heading to open a context menu of all possible Area fields that can display as columns and add/remove fields to view status information. (For more detailed information, see Viewing iSTAR Area Status on the Dynamic View on Page 61.)

For more information on using Dynamic Views, see the Dynamic Views chapter in the *C•CURE 9000 Data Views Guide*.

iSTAR Area List Context Menu

The context menu that opens when you right-click an iSTAR Area in the iSTAR Area Dynamic View includes the selections described in Table 3 on Page 57.

Table 3: iSTAR Area List Context Menu

Menu Selection	Description
Edit	Click this menu selection to edit the selected iSTAR Area. The **iSTAR Area Editor** opens (with the addition of a **Groups** tab, which displays any Groups that this Area belongs to). You can rename the iSTAR Area, change the description and any other attributes, with the exception of the iSTAR Cluster(s) to which the Area is assigned.
Delete	Click this menu selection to delete the selected iSTAR Area. A prompt appears asking you to confirm that you want to delete the iSTAR Area. Click **Yes** to delete the iSTAR Area or **No** to cancel the deletion.
Add to Group	You can add one or more selected iSTAR Areas to a Group of iSTAR Areas. When you click this menu choice, a dialog box appears for you to select the Group to which to add the iSTAR Area(s). When you click a Group of iSTAR Areas in the list, the selected iSTAR Area(s) are added to the Group.
Set property	Click this menu selection to change the value of the selected properties in the selected Cluster Area(s). See Using Set Property on Page 58.
Export selection	Click this menu selection to Open an Export...to XML or CSV file dialog box to export one or more of the selected iSTAR Area records to either an XML or a CSV file. This allows you to quickly and easily create XML/CSV reports on the selected data. NOTE: Although XML is the initial default file type, once you choose a type in the **Save as type** field, whether XML or CSV, that becomes the default the next time this dialog box opens. CSV-formatted exports **cannot** be imported. If you require importing functionality, export to XML. • When you export to an XML file, all available data for the selected object(s), whether displayed in the Dynamic View or not—as well as all the child objects of the selected record(s), is exported. • When you export to a CSV file, only data in the columns displaying in the Dynamic View is exported, and in the order displayed. This allows you to both select and arrange data fields for your report. In addition, exporting to a CSV file allows you to view the exported data in an Excel spreadsheet and further manipulate it for your use. For more information, see the Dynamic Views chapter in the *C•CURE 9000 Data Views Guide*. NOTE: When you click **Export Selection**, you are running the export on the client computer. Consequently, the system does not use the Default Export Directory Path—which is on the server. It opens a directory on the client, reverting to the last directory used. You can navigate to the default export server directory, if you wish. Or to avoid confusion or use the same destination folder for both client and server computers, you can use UNC (Universal Naming Convention) paths, for example: \\Computer Name\Program Files\Software House\SWHouse\SWHSystem\Export.
Find in Audit Log	Click this menu selection to Open a **Query Parameters** dialog box in which you can enter prompts and/or modify the Query criteria to search for entries in the Audit Log that reference the selected iSTAR Area. When found the results display in a separate Dynamic View.
Find in Journal	Click this menu selection to Open a **Query Parameters** dialog box in which you can enter prompts and/or modify the Query criteria to search for entries in the Journal that reference the selected iSTAR Area. When found the results display in a separate Dynamic View.
Monitor	Click this menu selection to view activity for the selected iSTAR Area(s), and any Door and Trigger-with-target-Event children, on an Admin Monitor Activity Viewer. For more information, see "Monitoring an Object from the Administration Station" in the *C•CURE 9000 Getting Started Guide*.

iSTAR Area List Context Menu (continued)

Menu Selection	Description
Display Personnel in Area	Click this menu selection to open the **Personnel in Area** Dynamic View. This list includes: • For a 'regular' Area – All of the Personnel currently in the Area. By default, shows the Person's name and the Area Name. • For a Carpool Area – All of the Carpool Group Personnel currently in the Carpool Area. By default, shows the Person's name, Carpool Group, Carpool Driver, and the Carpool Area Name. (See Viewing Personnel in an Area on Page 60.) You can also right-click any column heading to view a list of other available Personnel fields that can display as columns. For more information, see the Dynamic Views chapter in the *C•CURE 9000 Data Views Guide*.
Display Occupancy Personnel Groups	Click this menu selection to open the **Personnel Groups for Area** Dynamic View. This list includes all of the Personnel Groups currently configured for the Area. By default, the Dynamic View shows the Personnel Group name, Personnel Count, Maximum and Minimum Occupancy Limits, and Area Name. (See Viewing Personnel Groups Associated with an Area on Page 60.) You can also use the **Set Property** option on the right-click context menu to reset the Personnel Count for an Area Personnel Group. For more information, see the Dynamic Views chapter in the *C•CURE 9000 Data Views Guide*.
Clear Area Counts	Click this menu selection to return the Personnel count for all selected Areas, including in Area Personnel Groups, to 0 (zero).
Show Occupancy Mode Causes	Click this menu selection to open an Occupancy Mode Cause List dialog box for the Area. (See Viewing Occupancy Mode Causes for an Area on Page 64.)
De-muster Area	Click this menu selection to de-muster Mustering Area(s) when the emergency is over. The system updates the Area counts to reflect the number of Personnel being moved from the Mustering Area(s) to the De-muster Area(s). NOTE: This action requires a confirmation. This action is **not** available for Carpool Areas.
Remove All Personnel from Area	Click this menu selection to clear all Personnel from the Area(s), returning all Personnel, Visitor, and Escort counts to 0 (zero). NOTE: This action requires a confirmation, but does **not** grace the Personnel removed from the Area. In addition, it warns you that: - Counts may not be accurate if there are actually personnel in the Area(s) when you perform the action. - The action may cause unexpected results if the Area(s) is configured for Occupancy or antipassback.
Show Association	Click this menu selection to view a list of Security Objects associated with this iSTAR Area. For more information, see "Showing Associations for an Object" in the *C•CURE 9000 Getting Started Guide*.

Using Set Property

Click the Set Property menu selection to change the value of the selected properties in the selected iSTAR Area(s).

A dialog box appears asking you to select a property to change. Click ... to open a selection list and click the property you wish to change. You can then change the value of the following properties:

NOTE The counts for Area Manager, Conditionally Admitted Personnel, and Managed Personnel can **only be reset to 0 (zero)**. However, you should do this **only** if you are certain that no such Personnel are currently in the iSTAR Area. Otherwise, changing the count to zero could cause unwanted consequences.

- **Area Manager Count** – You can reset the count for the Dynamic Area Manager in the iSTAR Area to 0 (zero) by selecting this property and typing in that value. (The count could have become incorrect due to loss of Host-to-Controller communications.)
- **Conditionally Admitted Count** – You can reset the count for Personnel admitted conditionally to the iSTAR Area to 0 (zero) by selecting this property and typing in that value. (The count could have become incorrect due to loss of Host-to-Controller communications.)
- **Description** – You can change the textual description of the iSTAR Area(s) by selecting this property and typing in a new value.
- **Enforce Timed APB Only** – You can determine whether or not the iSTAR Area(s) is/are subject **only** to the timed antipassback rules —**not** to the regular antipassback rules—by selecting this property and selecting/clearing the **Value** check box.
- **Escort Count** – You can reset the count of Escorts in the iSTAR Area(s) by selecting this property and typing in a new value. (The count could have become incorrect due to tailgating or loss of Host-to-Controller communications.)
- **Escort Enforcement Option** – You can determine whether or not the iSTAR Area(s) require(s) an Escort to swipe his/her card for an Escorted Visitor to enter by selecting this property and selecting the appropriate value.
- **Escort Required in Area** – You can determine whether or not the iSTAR Area(s) require(s) an Escort to remain in the Area with the Escorted Visitor(s) at all times by selecting this property and selecting/clearing the **Value** check box.
- **Escorted Visitor Count** – You can reset the count of Escorted Visitors in the iSTAR Area(s) by selecting this property and typing in a new value. (The count could have become incorrect due to tailgating or loss of Host-to-Controller communications.)
- **Managed Personnel Count** – You can reset the count for Personnel admitted to the iSTAR Area by the Dynamic Area Manager to 0 (zero) by selecting this property and typing in that value. (The count could have become incorrect due to loss of Host-to-Controller communications.)
- **Personnel Count** – You can reset the count of Personnel in the iSTAR Area(s) by selecting this property and typing in a new value. (An Area's count could have become incorrect due to tailgating or loss of Host-to-Controller communications.)
- **Personnel Group Access Limited** – You can determine whether or not the iSTAR Area(s) limit access to the Area only to Personnel with Clearance belonging to any Groups configured for the Area(s) by selecting this property and selecting/clearing the **Value** check box.
- **Personnel Group Count Access** – You can determine whether or not the iSTAR Area(s) **allow** Personnel with Clearance from any Groups configured for the Area(s) to enter and exit the Area even though the numbers entered in the Maximum/**Minimum** fields have or have not been reached by selecting this property and selecting/clearing the **Value** check box.
- **Valid Exit Clears Timed APB** – You can determine whether or not the iSTAR Area(s) allow a person's valid exit to clear the timed antipassback rules (permitting this person to immediately re-enter the Area) by selecting this property and selecting/clearing the **Value** check box.

Viewing Personnel in an Area

You can select an existing iSTAR Area or Carpool Area on the Dynamic View and display a list of the Personnel currently in the Area.

- For a 'regular' Area, the list displays all of the Personnel currently in that Area.
- For a Carpool Area, the list displays all of the Carpool Group Personnel currently in that Carpool Area.

To View the Personnel in an Area

1. On the **iSTAR Area** Dynamic View, right-click a 'regular' iSTAR Area in the list to open the iSTAR Area Context menu. (See iSTAR Area List Context Menu on Page 57.)
2. Click **Display Personnel in Area**. A list of the Personnel currently in the Area displays.

   By default, the Dynamic View is titled "Personnel in Area" and shows the Person's name and the Area Name.

   You can also right-click any column heading to view a list of other available Personnel fields that can display as columns, such as Antipassback Event, Antipassback Exempt, or Escort Option status.

   If new Personnel are granted access and enter the Area or other Personnel leave while this Dynamic View is open, the list updates automatically.

   For more information, see the Dynamic Views chapter in the *C•CURE 9000 Data Views Guide*.

To View the Carpool Group Personnel in a Carpool Area

1. On the **iSTAR Area** Dynamic View, right-click a Carpool Area in the list to open the iSTAR Area Context menu. (See iSTAR Area List Context Menu on Page 57.)
2. Click **Display Personnel in Area**. A list of the Carpool Group Personnel currently in the Carpool Area displays.

   By default, the Dynamic View is titled "Carpool Members in Area" and shows **only** the Person's name, Carpool Group, Carpool Driver, and the Carpool Area Name.

   If new Carpool Group Personnel are granted access and enter the Carpool Area or other Personnel leave while this Dynamic View is open, the list updates automatically.

Viewing Personnel Groups Associated with an Area

You can select an existing iSTAR Area on the Dynamic View and display a list of the Personnel Groups currently configured for the Area—including Carpool Groups for Carpool Areas .

To View the Personnel Groups for an Area

1. On the **iSTAR Area** Dynamic View, right-click an iSTAR Area in the list to open the iSTAR Area Context menu (see iSTAR Area List Context Menu on Page 57).
2. Click **Display Occupancy Personnel Groups**. A list of the Personnel Groups configured for the Area displays. (For Carpool Areas, the list includes its associated Carpool Groups.)

   By default, the Dynamic View shows the Personnel Group's name, the Personnel Count, the Maximum and Minimum Occupancy Limits, and the Area Name. You can also use the **Set Property** option on the right-click context menu to reset the Personnel Count for an Area Personnel Group.

   For more information, see the Dynamic Views chapter in the *C•CURE 9000 Data Views Guide*.

Viewing the Status of an iSTAR Area

You can view basic status information about an Area in three different places:

- Administration application
  - Viewing iSTAR Area Status on the Dynamic View on Page 61.
  - Viewing Occupancy Mode Causes for an Area on Page 64.
  - Viewing Area Status on the Status Tab on Page 100.
- Monitoring Station: **Explorer Bar>Non-Hardware Status> Areas>Status List - Area** – see the Monitoring Status chapter in the *C•CURE 9000 Monitoring Station Guide*.

Viewing iSTAR Area Status on the Dynamic View

This section briefly describes procedures for displaying iSTAR Area status information on the iSTAR Area dynamic view. However, these changes are only in effect while you have the View open. To actually change the View permanently, you need to configure the view and save your changes. For information, see the Dynamic Views chapter in the *C•CURE 9000 Data Views Guide*.

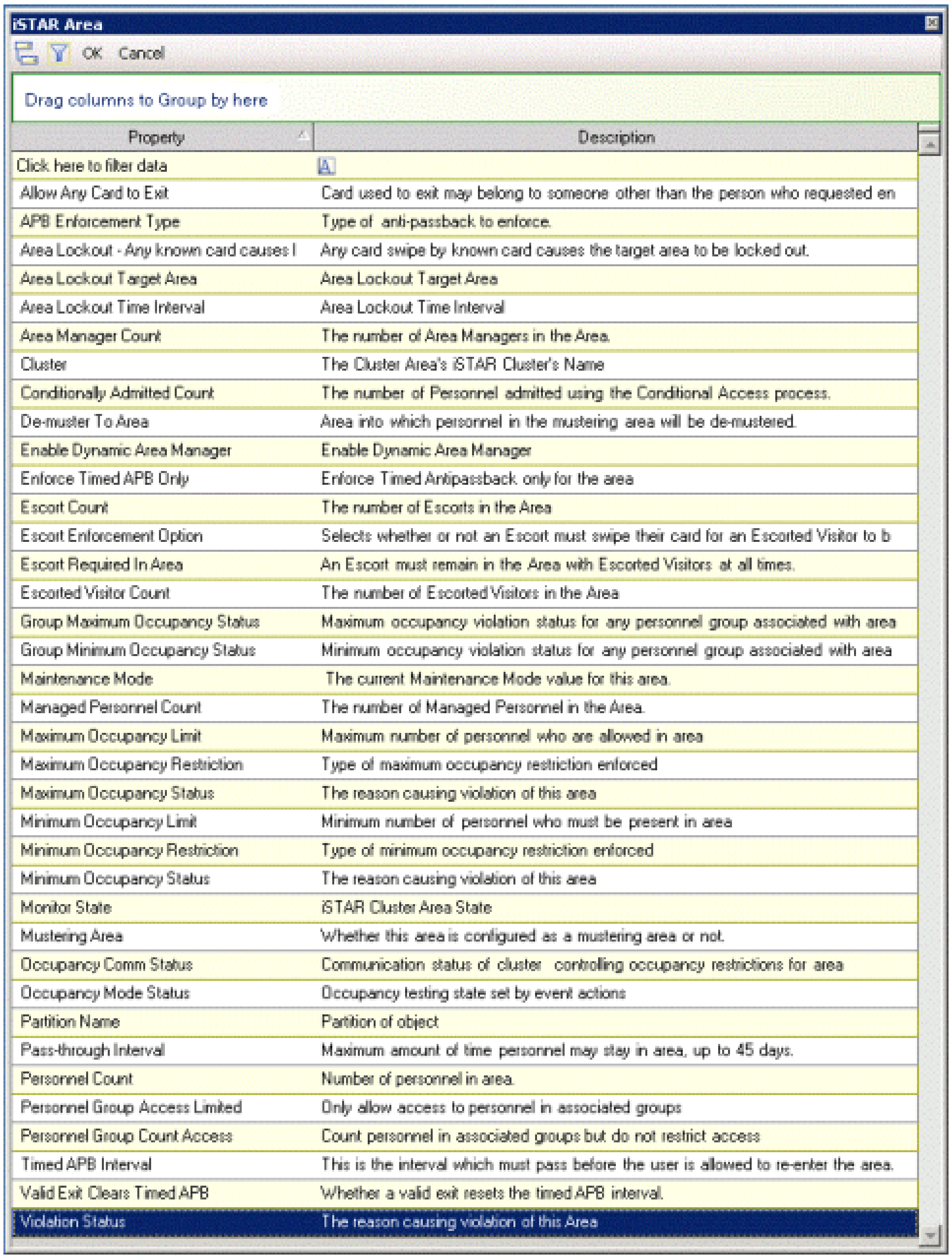
To View iSTAR Area Status Information

1. On the **iSTAR Area** Dynamic View, right-click any column heading.

   A context menu appears with a short list of Area fields—some that display as column headings and some that do not. Fields that are currently displayed in the view are marked with a ☑.

2. Click **More columns...** at the bottom of the list.

   A list of all available iSTAR Area fields that can display as columns appears.



Property	Description
Click here to filter data	A
Allow Any Card to Exit	Card used to exit may belong to someone other than the person who requested en
APB Enforcement Type	Type of anti-passback to enforce.
Area Lockout - Any known card causes l	Any card swipe by known card causes the target area to be locked out.
Area Lockout Target Area	Area Lockout Target Area
Area Lockout Time Interval	Area Lockout Time Interval
Area Manager Count	The number of Area Managers in the Area.
Cluster	The Cluster Area's iSTAR Cluster's Name
Conditionally Admitted Count	The number of Personnel admitted using the Conditional Access process.
De-muster To Area	Area into which personnel in the mustering area will be de-mustered.
Enable Dynamic Area Manager	Enable Dynamic Area Manager
Enforce Timed APB Only	Enforce Timed Antipassback only for the area
Escort Count	The number of Escorts in the Area
Escort Enforcement Option	Selects whether or not an Escort must swipe their card for an Escorted Visitor to b
Escort Required In Area	An Escort must remain in the Area with Escorted Visitors at all times.
Escorted Visitor Count	The number of Escorted Visitors in the Area
Group Maximum Occupancy Status	Maximum occupancy violation status for any personnel group associated with area
Group Minimum Occupancy Status	Minimum occupancy violation status for any personnel group associated with area
Maintenance Mode	The current Maintenance Mode value for this area.
Managed Personnel Count	The number of Managed Personnel in the Area.
Maximum Occupancy Limit	Maximum number of personnel who are allowed in area
Maximum Occupancy Restriction	Type of maximum occupancy restriction enforced
Maximum Occupancy Status	The reason causing violation of this area
Minimum Occupancy Limit	Minimum number of personnel who must be present in area
Minimum Occupancy Restriction	Type of minimum occupancy restriction enforced
Minimum Occupancy Status	The reason causing violation of this area
Monitor State	iSTAR Cluster Area State
Mustering Area	Whether this area is configured as a mustering area or not.
Occupancy Comm Status	Communication status of cluster controlling occupancy restrictions for area
Occupancy Mode Status	Occupancy testing state set by event actions
Partition Name	Partition of object
Pass-through Interval	Maximum amount of time personnel may stay in area, up to 45 days.
Personnel Count	Number of personnel in area.
Personnel Group Access Limited	Only allow access to personnel in associated groups
Personnel Group Count Access	Count personnel in associated groups but do not restrict access
Timed APB Interval	This is the interval which must pass before the user is allowed to re-enter the area.
Valid Exit Clears Timed APB	Whether a valid exit resets the timed APB interval.
Violation Status	The reason causing violation of this Area

3. To add fields as columns to view status information, select one or more fields from the list using CTRL+Left-click or SHIFT+Left-click and then click **OK**.

Example:

Escort Enforcement Option/Escort Required in Area/Group Maximum Occupancy Status/Group Minimum Occupancy Status/Maximum Occupancy Limit/Maximum Occupancy Restriction/Maximum Occupancy Status

4. To remove a field as a column in the Dynamic View, click a field in the list that has a ✓.
5. To change the left/right order of the columns to your liking, click any column heading and drag that column to a new position. The Dynamic View columns are adjusted to the new column order you established.
6. To change the column width:

a. move the cursor to the edge of the column heading you wish to resize. The cursor changes to ↔.

b. Drag this cursor to the left or right and release the mouse button to make the column wider or narrower.

Viewing Occupancy Mode Causes for an Area

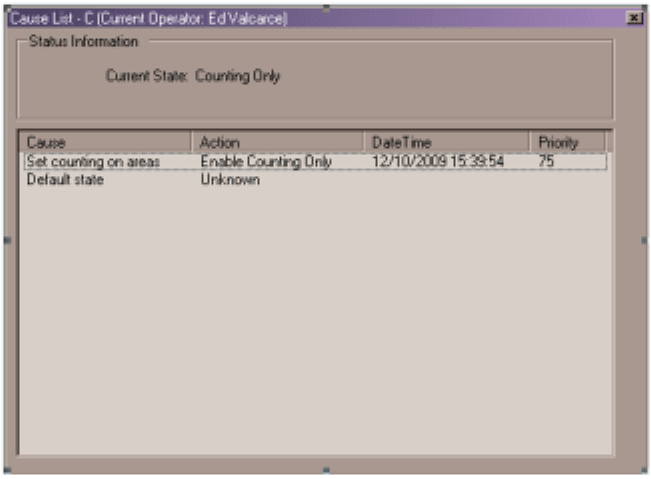
You can select an existing iSTAR Area on the Dynamic View and display a list of the causes for the Area's current Occupancy Mode. For more information about Occupancy mode, see:

- How Area Occupancy Configuration Affects Occupancy Mode on Page 81
- iSTAR Area Status Tab on Page 99
- Configuring Event Actions to Affect Areas on Page 114

To View the Occupancy Mode Causes for an Area

1. On the **iSTAR Area** Dynamic View, right-click an iSTAR Area in the list to open the iSTAR Area Context menu.
2. Click **Show Occupancy Mode Causes**. A list such as that shown in the example in Figure 5 on Page 64 displays.

Figure 5: Occupancy Mode Cause List for iSTAR Area



Cause List - C (Current Operator: Ed Valcarce)

Status Information

Current State: Counting Only

Cause	Action	DateTime	Priority
Set counting on areas	Enable Counting Only	12/10/2009 15:39:54	75
Default state	Unknown		

By default, the Dynamic View shows the Cause, the Action, the Date and Time, and the Priority of the Action. The causes are listed in order of priority, except when the priorities are equal—in which case they are listed by time.

Modifying an iSTAR Area

- For a **Cluster Area** – You can do the following:
  - Change the Area's Cluster **only** if you remove all the Doors from the **Access In** table.
  - Change the Area to a Cross-Cluster type Area.
- For a **Cross-Cluster Area** – You cannot change it into a Cluster type Area.

In addition, while you cannot change the Doors, Readers, and Adjacent Areas on an existing row, you can remove the relevant table row and make new selections.

NOTE Because counting for Areas configured for occupancy is done by iSTAR Controllers, while it is done by the host for non-occupancy Areas, you can corrupt the count if you change an existing Area from occupancy to non-occupancy—or vice versa. To keep the Area counts correct, you should only make such changes to Areas when the system is not busy and the Areas are empty. Alternatively, if there are Personnel in the Area, you can use the **Set Property** option on the right-click context menu on the Areas Dynamic View to reset the count for the Area.

To Modify an iSTAR Area

1. In the **Navigation** Pane of the Administration Workstation, click **Areas and Zones** to open the **Areas and Zones** pane.
2. Select iSTAR Area from the **Areas and Zones** drop-down list.
3. Click ➡ ▾ to open a Dynamic View showing all iSTAR Area Objects.
4. Right-click the iSTAR Area in the list that you want to change and select **Edit** from the context menu that appears.

   - or -

   Double-click the iSTAR Area you want to change.

   The **iSTAR Area Editor** opens for you to edit the Area making changes as you wish in the fields on the top of the editor, and on any of the tabs. (The Editor now includes a **Groups** tab that displays any Groups to which this iSTAR Area belongs.)

NOTE On the **General** tab:

- To change the Cluster selection for a **Cluster Area**, you **must remove** all the Doors from the **Access In** table.
- To change the Doors, Readers, and Adjacent Areas, remove the relevant table row and make new selections.

5. To save the modified Area, click **Save and Close**.

   - or -

   If you want to save the Area and then create a new one, click **Save and New**. The current iSTAR Area is saved and closed, but the **iSTAR Area Editor** remains open ready for a new iSTAR Area.

Deleting an iSTAR Area

You can delete an iSTAR Area, if you also have **Edit** permission for any Personnel who may currently be in the Area. Deleting an Area with assigned Doors removes the association between the Area and the assigned Doors and Readers.

NOTE You cannot delete an Area if it is configured as the de-mustering Area for a Muster Area.

To Delete an iSTAR Area

1. In the **Navigation** Pane of the Administration Workstation, click **Areas and Zones** to open the **Areas and Zones** pane.

2. Select iSTAR Area from the **Areas and Zones** drop-down list.
3. Click ➡ ▾ to open a Dynamic View showing all iSTAR Area Objects.
4. Right-click the iSTAR Area in the list that you want to delete and select **Delete** from the context menu that appears.
5. Click **Yes** on the "Are you sure you want to delete the selected iSTAR Area?" message box.

Setting a Property for an iSTAR Area

You can use **Set Property** to quickly set a property for an iSTAR Area without opening the **iSTAR Area Editor**. You use Set Property for mass updates. See Table 3 on Page 57 for the properties that can be changed.

To Set a Property for iSTAR Areas

1. In the **Navigation** Pane of the Administration Workstation, click **Areas and Zones** to open the **Areas and Zones** pane.
2. Select **iSTAR Area** from the **Areas and Zones** drop-down list.
3. Click ➡ ▾ to open a Dynamic View showing all iSTAR Area Objects.
4. Right-click the iSTAR Area in the list for which you want to set the property and select **Set Property** from the context menu.
5. Specify the property for the Area. Click the drop-down button to see a list of properties.
6. Enter the value for the property and click **OK**.
7. Click **OK** on the **Setting Properties of iSTAR Area** message box.

Adding an iSTAR Area to a Group

You can use **Add To Group** to add the iSTAR Area Object to a Group.

To Add iSTAR Areas To a Group

1. Make sure that the Group is already configured for the iSTAR Area to be added to it.
2. In the **Navigation** Pane of the Administration Workstation, click **Areas and Zones** to open the **Areas and Zones** pane.
3. Select **iSTAR Area** from the **Areas and Zones** drop-down list.
4. Click ➡ ▾ to open a Dynamic View showing all iSTAR Area Objects.
5. Right-click the Area in the list that you want to add to a Group and select **Add To Group** from the context menu.
6. When the **Group** list displays, select the Group you want to add the iSTAR Area to.

   The name and description of the Group display on the **Groups** tab of the **iSTAR Area** Editor.

iSTAR Area Editor

The **iSTAR Area Editor**, shown in Figure 6 on Page 68, in C•CURE 9000 lets you create and modify iSTAR Area Objects.The **iSTAR Area Editor** displays the following tabs for configuring Areas:

- iSTAR Area General Tab on Page 67
- iSTAR Area Antipassback Tab on Page 74
- iSTAR Area Occupancy Tab on Page 78
- iSTAR Area Escort Tab on Page 87
- iSTAR Area Muster Tab on Page 90
- iSTAR Area Triggers Tab on Page 94
- iSTAR Area Status Tab on Page 99
- iSTAR Area State Images Tab on Page 100
- iSTAR Area Groups Tab on Page 98 (when editing an existing Area)

The **iSTAR Area Editor** has the buttons described in Table 4 on Page 67.

Table 4: iSTAR Area Editor Buttons

Button	Description
Save and Close	Click this button when you have completed any changes to the iSTAR Area and wish to save those changes. The iSTAR Area closes.
Save and New	Click this button when you have completed any changes to the iSTAR Area and wish to save those changes and also create a new iSTAR Area. The iSTAR Area you were editing is saved, and a new iSTAR Area opens (either blank or including template information if you were using a template to create the new iSTAR Area).
☒	Click this button when you want to close the **iSTAR Area Editor** without saving your changes. A warning appears asking whether or not you want to save your changes before closing the editor. Click **Yes** to exit and save and **No** to exit and cancel your changes.

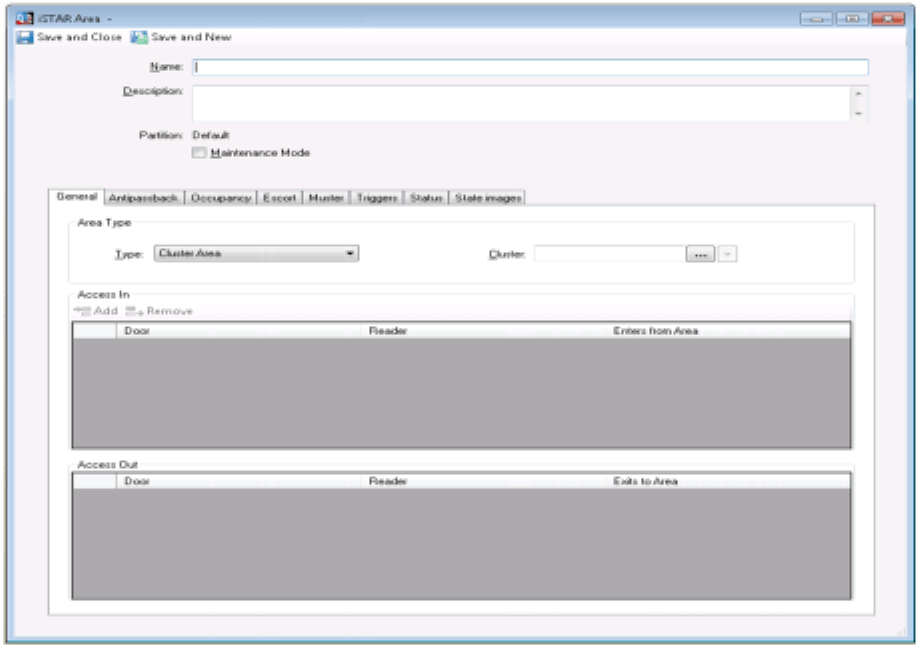
iSTAR Area General Tab

The **iSTAR Area General** tab, shown in Figure 6 on Page 68, lets you determine whether the Area is a Cluster Area or a Cross-Cluster Area and then define the Area's Doors, Readers, and adjacent Areas.

Definitions for this tab are provided in:

- iSTAR Area Editor Definitions on Page 68.
- iSTAR Area General Tab Definitions on Page 69.

Figure 6: iSTAR Area Editor General Tab



Partition: Default

□ Maintenance Mode

Type: Cluster Area

General Tab Tasks

You use the General tab to accomplish the tasks listed below, needed to configure an iSTAR Area. The procedural steps for each task are detailed in the following subsections.

- Configuring iSTAR Area Doors, Readers, and Adjacent Areas on Page 70
- Deleting iSTAR Area Doors, Readers, and Adjacent Areas on Page 72
- Configuring a Global Antipassback Area on Page 72

iSTAR Area Editor Definitions

The **iSTAR Area Editor** has the fields shown in Table 5 on Page 68.

Table 5: iSTAR Area Fields

Fields/Buttons	Description
Name	Enter a unique name, up to 100 characters, to identify the iSTAR Area.
Description	Enter a description of the iSTAR Area, up to 255 characters.
Partition	A read-only field displaying the name of the Partition to which this iSTAR Area belongs. (This field is visible only if the C•CURE 9000 system is partitioned.) • A Cluster Area has the same Partition as its selected iSTAR Cluster. If the Cluster's Partition changes, then the Area's Partition changes accordingly. • A Cross-Cluster Area (Global Antipassback iSTAR Area) has the same Partition as the 'New Object Partition' in which it was created. The iSTAR Clusters can be in any Partitions.

iSTAR Area Fields (continued)

Fields/Buttons	Description
Maintenance Mode	Select this check box to put this Area into Maintenance Mode so whether or not Events, Status, and Activity related to this Area display on the Monitoring Station depends on the Operator's Privilege and the Application Layout assigned. For detailed information, see the Maintenance Mode chapter in the *C•CURE 9000 Hardware Configuration Guide*.

iSTAR Area General Tab Definitions

The **iSTAR Area General** tab has the buttons shown in Table 6 on Page 69 (in the **Access In** table) and the fields shown in Table 7 on Page 69.

Table 6: iSTAR Area Editor - General Tab Buttons

Button	Description
Add	Click this button to add a new blank row to the **Access In** table. Each new row is added after the last.
Remove	Click this button to remove a selected row from the **Access In** table. You have to click the row selector ▶ to select a row to remove. If **no** row is selected, this button is **not** available.

Table 7: iSTAR Area Editor - General Tab Fields

Fields/Buttons	Description
Area Type	
Type	Click the down-arrow to select the type of Area you want this Area to be from the drop-down list: • **Cluster Area** – Select to limit this Area to a single iSTAR Cluster • **Cross-Cluster Area** – Select to allow this Area to cross iSTAR Clusters and enforce Global Antipassback. If you select Cross-Cluster Area, the **Cluster** field is replaced with the read-only label, **Global Antipassback iSTAR Area**, and the **Add** button in the **Access In** table becomes immediately available. NOTE: Once you configure and save a Cross-Cluster Area, you cannot change it back to a Cluster Area. You can, however, change a Cluster Area into a Cross-Cluster Area.
Cluster	For a Cluster Area Type Area, select the iSTAR Cluster that controls the Area. NOTE: The **Add** button in the **Access In** table becomes available when you select the Cluster. Once you select the Cluster and add Doors to the Area, you **cannot** change the Cluster. Conversely, if you remove all Doors from the table, the Cluster field becomes available and you can make another selection.

iSTAR Area Editor - General Tab Fields (continued)

Fields/Buttons	Description
Access In	
Door	Click in the **Door** field to display ..., and then click this button to select an Entry Door from the dialog box that appears. • For a **Cluster Area**, the Door must belong to the selected Cluster and not yet be assigned to any Area (The list displays only valid Doors.) • For a **Cross-Cluster Area**, the Door can belong to any Cluster in the system that enforces Global Antipassback as well as Cluster Antipassback. It cannot belong to a Cluster configured for Cluster Antipassback only. (The list displays only valid Doors.) Once a Door is selected, the **Areas & Zones** tab on the **Door Editor** displays read-only Area information. See Viewing Area Information on the Door Editor on Page 121. NOTE: Once a Door is selected for a row, it **cannot** be changed, although the entire row can be removed.
Reader	Click in the **Reader** field to display ..., and then click this button to select an Entry Reader from the dialog box that appears. Each Door must have at least one Reader. NOTE: If you selected a Door in the first field, **only** Readers configured for that Door appear in the list and can be associated with the Area. If you did **not** select a Door, the Reader list is not filtered and includes all the Readers in the system—both Readers on iSTAR Clusters configured **only** for Cluster Antipassback and Global-Antipassback-enabled iSTAR Clusters. However, the system will not let you save the Area with an invalid Reader.) You can change the Reader selection until this Area configuration is saved. After that the Reader **cannot** be changed, although the entire row can be removed. The **Access In** Reader for a given Area will always be the **Access Out** Reader for the adjacent Area. **Example:** If a Door and its single Reader are configured as **Access In** to Area A, the editor for the adjacent Area B shows the Door and Reader as **Access Out** to Area A.
Enters from Area	Click in this field to display ..., and then click this button to select an adjacent Area from the dialog box that appears.
Access Out	This table is populated automatically when an entry is made to the Access In table.
Door	• If a Door selected in the **Access In** table has two Readers, the system automatically enters the same Door and adjacent Area in this **Access Out** table. The Reader shown in this table is the other Reader on the Door. • If a Door selected in the **Access In** table has **only one** Reader, **no** entry is made for that Door in this **Access Out** table.
Reader	
Exits to Area	

Configuring iSTAR Area Doors, Readers, and Adjacent Areas

- For a **Cluster Area**, this procedure assumes that you have already
  - Selected the iSTAR Cluster for the Area.
  - Configured iSTAR Doors and Readers for the Cluster.
- For a **Cross-Cluster Area**, this procedure assumes that you have already
  - Configured iSTAR Clusters for Global Antipassback in addition to Cluster Antipassback.
  - Configured iSTAR Doors and Readers for the Clusters.

To Configure iSTAR Area Doors, Readers, and Adjacent Areas

1. Create or modify an iSTAR Area. See:
   - Configuring an iSTAR Area on Page 53
   - Modifying an iSTAR Area on Page 64
2. On the **General** tab of the **iSTAR Area Editor** in the **Access In** box, click **Add** to create a new row.
3. Click in the **Door** field to display ... and click this button.

   A selection list opens with the Doors available for iSTAR Areas.
4. Click a Door to add it to the row.

   Example:

   ClusterProController1 Door1
5. Click in the **Reader** field to display ... and click this button.

   A selection list opens with the Readers available for iSTAR Areas.
6. Click a Reader to add it to the row.

   Example:

   iSTAR Reader1-ACM1-iSTARProCluster1Controller1

   As soon as the Reader is selected, if it was one of two Readers on the selected Door, the system populates the row in the **Access Out** box with the same Door and the other Reader.

   Example:

   Door: ClusterProController1 Door1

   Reader: iSTAR Reader2-ACM1-iSTARProCluster1Controller1
7. Click in the **Enters from Area** field to display ... and click this button.

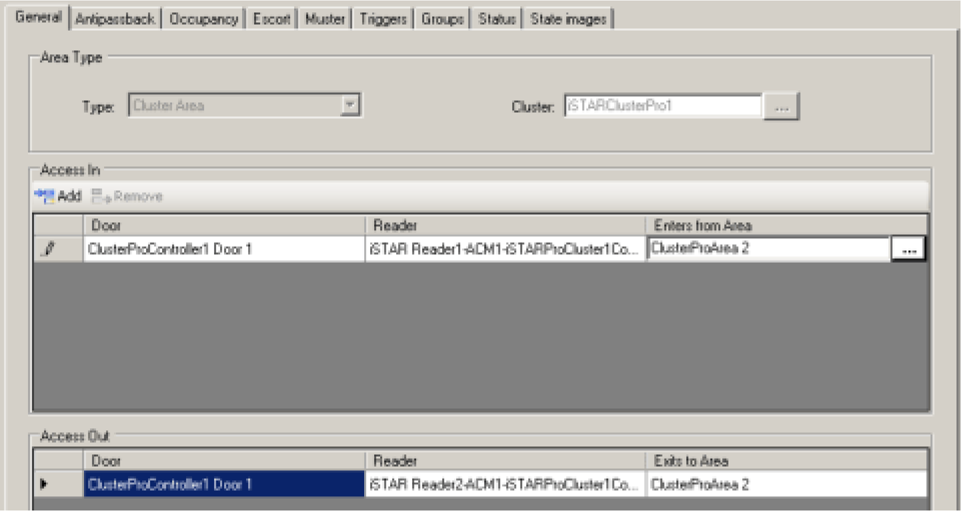
   A selection list opens with the iSTAR Areas available to be the adjacent Area.
8. Click an Area to add it to the row.

   Example:

   ClusterProArea2

   The selected adjacent Area is now entered **not only** as the **Enters from** Area for the **Access In** table, but has **also** been entered by the system as the **Exits To** Area for the row in the **Access Out** table.

The General tab now appears as shown in the following example:



Type: Cluster Area

Cluster: iSTARClusterPro1

Access In

	Door	Reader	Enters from Area
✎	ClusterProController1 Door 1	iSTAR Reader1-ACM1-iSTARProCluster1Co...	ClusterProArea 2

Access Out

	Door	Reader	Exits to Area
▶	ClusterProController1 Door 1	iSTAR Reader2-ACM1-iSTARProCluster1Co...	ClusterProArea 2

9. To configure more Doors for this iSTAR Area, click **Add** in the **Access In** box and repeat the preceding steps.

Deleting iSTAR Area Doors, Readers, and Adjacent Areas

Once you have selected a Door for a row, it **cannot** be changed. In addition once you have selected a Reader and an adjacent Area for a row, you can modify them **only until** you save the Area. After that you **cannot** modify any Object in a row. You can, however, delete the entire row—thus removing the Door, Reader, and Adjacent Area from the Area configuration.

To Delete an iSTAR Area Door

1. On the **General** tab of the **iSTAR Area Editor** in the **Access In** box, click a row to select it.
2. Click **Remove** to delete the Door/Reader row.

   The row is deleted. If the deleted Door had two Readers, the system also deletes the related row in the **Access Out** box.

NOTE While you can actually select a row in the **Access Out** box, the **Remove** button remains unavailable. Consequently, you **cannot** delete the row directly, only by deleting the related row in the **Access In** box.

Configuring a Global Antipassback Area

To Configure a Global Antipassback Area

1. First create an iSTAR Cluster that enforces Global Antipassback.

   a. In the Navigation Pane of the Administration Workstation, click the **Hardware** pane button.

   b. Click the **Hardware** drop-down list, select **iSTAR Cluster**, and click **New**.

   - or -

   Click ➡ ▾ to open a Dynamic View showing a list of all existing iSTAR Clusters or expand the Hardware Tree, and in the Dynamic View list/Tree, select the iSTAR Cluster you want to configure and click **Edit** from the context menu that appears.

   c. On the **iSTAR Cluster Editor**, click to open the **Area** Tab.

   d. In the **Global Antipassback** box, click to select the **Cluster enforces iSTAR Global antipassback as well as iSTAR Cluster antipassback** option.

2. Configure Doors and Readers for this iSTAR Cluster.

3. Create or modify an iSTAR Area. See:
   - Configuring an iSTAR Area on Page 53
   - Modifying an iSTAR Area on Page 64.

4. On the **General** tab of the **iSTAR Area Editor** in the **Area Type** box, click the down-arrow and select the **Cross-Cluster Area**.

5. In the **Access In** box, click **Add** to create a new row.

6. Click in the **Door** field to display ... and click this button.

   A selection list opens with the Doors available for iSTAR Cross-Cluster Areas. (Only Doors on iSTAR Clusters enabled for Global Antipassback and Cluster Antipassback are included in this list.)

7. Click a Door to add it to the row.

8. Click in the **Reader** field to display ... and click this button.

   A selection list opens with the Readers available for iSTAR Areas.

NOTE

> If you selected a Door in the first field, only Readers configured for that Door appear in the list to be associated with the Area. Consequently, these will be Readers on Global-Antipassback-enabled iSTAR Clusters.
>
> If you did **not** select a Door first, the Reader list is **not** filtered and includes all the Readers in the system—even those on iSTAR Clusters configured **only** for Cluster Antipassback. The system, however, will **not** allow you to save the Area with an invalid Reader.

9. Click a Reader to add it to the row.

   As soon as the Reader is selected, if it was one of two Readers on the selected Door, the system populates the row in the **Access Out** box with the same Door and the other Reader.

10. Click in the **Enters from Area** field to display ... and click this button.

    A selection list opens with the iSTAR Areas available to be the adjacent Area. This list includes all the Areas in the system because you can enter a Cross-Cluster Area from Cluster Areas as well as from other Cross-Cluster Areas.

11. Click an Area to add it to the row.

    The selected adjacent Area is now entered **not only** as the **Enters from** Area for the **Access In** table, but has **also** been entered by the system as the **Exits To** Area for the row in the **Access Out** table.

iSTAR Area Antipassback Tab

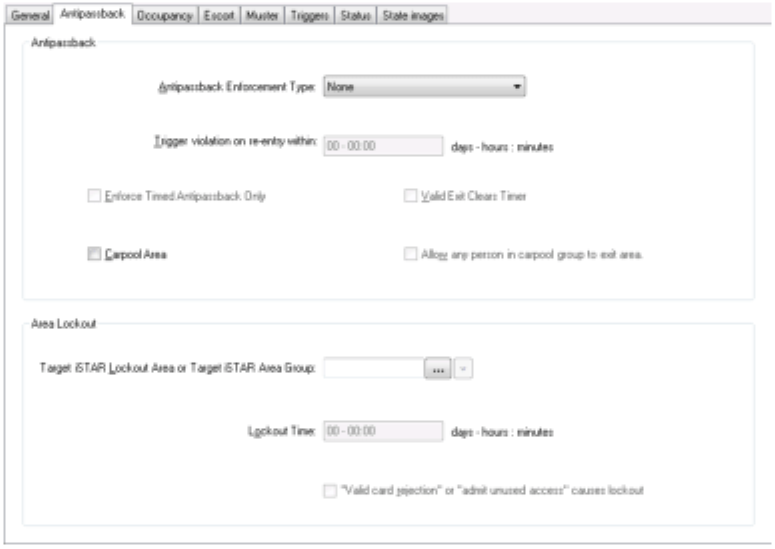
The **iSTAR Area Antipassback** tab, shown in Figure 7 on Page 74, lets you define the type of Antipassback for the iSTAR Area and its related options as well as the parameters for Area Lockout. You can also use this tab to configure the iSTAR Area as a Carpool Area instead of a Personnel Area. (Carpool Areas **cannot** be Cross-Cluster.)

To configure antipassback you need at least two iSTAR Areas controlled by Readers—both an Access In Reader and an Access Out Reader.

- For Cluster Antipassback – the readers must be on the same Cluster.
- For Global Antipassback (Cross-Cluster) – the readers can be on any Clusters that are configured for Global APB as well as for Cluster APB.

Definitions for this tab are provided in iSTAR Area Antipassback Tab Definitions on Page 74.

Figure 7: iSTAR Area Editor Antipassback Tab



Antipassback

Antipassback Enforcement Type: None

Trigger violation on re-entry within: 00 - 00:00 days - hours : minutes

□ Enforce Timed Antipassback Only

□ Valid Exit Clears Timer

□ Carpool Area

□ Allow any person in carpool group to exit area.

Area Lockout

Target iSTAR Lockout Area or Target iSTAR Area Group:

Lockout Time: 00 - 00:00 days - hours : minutes

□ "Valid card rejection" or "admit unused access" causes lockout

Antipassback Tab Tasks

You use the **Antipassback** tab to accomplish the tasks listed below, to configure an iSTAR Area. The procedural steps for each task are detailed in the following subsections.

- Configuring Regular Antipassback for iSTAR Areas on Page 76
- Configuring Timed Antipassback for iSTAR Areas on Page 76
- Configuring Carpool Antipassback for iSTAR Areas on Page 77
- Configuring Lockout for iSTAR Areas on Page 77

To configure how antipassback is enforced when the Cluster is in communications failure, see Configuring iSTAR Clusters for APB Comm Fail Modes and Global Antipassback on Page 105.

iSTAR Area Antipassback Tab Definitions

The **iSTAR Area Antipassback** tab has the fields shown in Table 8 on Page 75.

Table 8: iSTAR Area Editor - Antipassback Tab Fields

Fields/Buttons	Description
Antipassback	
Antipassback Enforcement Type	Click the down-arrow to select from the drop-down list the type of Antipassback for the Area. **None** – **No** antipassback checking is enforced. Personnel may enter and exit the Area if they have valid clearance. This is the default. **Antipassback** – Regular antipassback checking is enforced. Antipassback violations occur when Personnel try to enter the Area they currently occupy (according to the system) or any non-adjacent Area. **Timed Antipassback** – Timed antipassback checking is enforced. Timed APB violations occur when Personnel try to re-enter the Area they currently occupy (according to the system) within a specified time period. After the specified time has elapsed, Personnel are allowed to re-enter the Area, even if they have **not** exited validly. (However, for tracking purposes, Personnel are considered to be in the area until they exit validly—even if the antipassback timer period has elapsed.) NOTE: By default, Timed APB Areas also enforce Regular APB rules. Personnel must exit an Area before entering a non-adjacent Area.
Trigger violation on re-entry within: days - hours: minutes	NOTE: This field is available only if **Timed Antipassback** is selected in the preceding field as the Enforcement type. Enter in days, hours, and minutes the time to elapse before the person can re-enter the Area. (The maximum allowed interval is **seven** days.)
Enforce Timed Antipassback Only	NOTE: This field is available only if **Timed Antipassback** is selected as the Enforcement type. Select this check box to indicate that **only** the timed APB rule should be enforced on this Area, **not** the regular APB rules. The default is cleared. Thus, when Personnel attempt to **exit/enter** an Area configured with this option: • Regular APB **exit** rules are **not** checked and they can exit. • Regular APB **entrance** rules are **not** checked— so if the APB timer period has already elapsed for the person, they can enter. NOTE: If regular APB is configured on an adjacent Area, that Area still enforces the regular APB rules before granting either entry/exit.
Valid Exit Clears Timer	NOTE: This field is available only if **Timed Antipassback** is selected as the Enforcement type. Select this check box to indicate that if Personnel validly exit this Area, their APB time period is cancelled so they can re-enter the Area at once. The default is cleared.
Carpool Area	NOTE: This field is available only if this a Cluster Area and not a Cross-Cluster Area. Select this check box to designate the Area as a Carpool Area. NOTE: If this option is selected, making this a Carpool Area, you must select an **Antipassback Enforcement Type** on the top of the tab: either **Antipassback** (regular) or **Timed Antipassback**. (The re-entry time limit for Timed Antipassback is the same for a Carpool Area as for a non-Carpool Area—a maximum of 7 days.)
Allow any person in carpool group to exit area	Select this option if you want to allow Personnel to use different cards from the same Carpool Group for entering and exiting the Carpool Area. (This means that even if cardholder one's card was used to enter the Area, cardholder two, three, or four from the same Carpool Group can use his/her card to exit.)
Area Lockout	
Target iSTAR Lockout Area or Target iSTAR Area Group	Click ... to display a dialog box with a list of iSTAR Areas/iSTAR Area Groups and select the iSTAR Area or iSTAR Area Group that you want as the Lockout target Area.

iSTAR Area Editor - Antipassback Tab Fields (continued)

Fields/Buttons	Description
Lockout Time	Enter the time in days, hours, and minutes that must elapse before the person can enter the target Area after accessing this Lockout Area. The default value is 0 [zero] indicating that Area Lockout is not configured for this iSTAR Area. The maximum allowed interval is **five** days.
Valid card rejection or admit unused access causes lockout	NOTE: This option is available only if a target iSTAR Area/iSTAR Area Group is selected in the first field in the **Area Lockout** box. Select this option to indicate that any card swipe, even it results in a reject or with a valid admit but an unopened door, causes the person to be locked out of the target iSTAR Area/iSTAR Area Group.

Configuring Regular Antipassback for iSTAR Areas

To Configure Regular Antipassback for an Area

1. Create or modify an iSTAR Area. See:
   - Configuring an iSTAR Area on Page 53
   - Modifying an iSTAR Area on Page 64
2. On the **iSTAR Area Editor**, click the **Antipassback** tab to open.
3. Click the down-arrow in the **Antipassback Enforcement Type** field to display a drop-down list with three choices: Antipassback, Timed Antipassback, and None. (The default is None.)
4. Click **Antipassback** to have regular antipassback enforced for this iSTAR Area.

Configuring Timed Antipassback for iSTAR Areas

To Configure Timed Antipassback for an Area

1. Create or modify an iSTAR Area. See:
   - Configuring an iSTAR Area on Page 53
   - Modifying an iSTAR Area on Page 64
2. On the **iSTAR Area Editor**, click the **Antipassback** tab to open.
3. Click the down-arrow in the **Antipassback Enforcement Type** field to display a drop-down list with three choices: Antipassback, Timed Antipassback, and None. (The default is **None**.)
4. Click **Timed Antipassback** to have timed antipassback enforced for this iSTAR Area.

   When you select **Timed Antipassback**, the **Trigger violation on re-entry within....** field and the **Enforce Timed Antipassback Only** and the **Valid Exit Clears Timer** check boxes become available.
5. In the **Trigger violation on re-entry within: days - hours: minutes** field, enter the time period that must elapse after a person enters the Area before he/she can re-enter.
6. To configure this iSTAR Area so it does **not** enforce regular antipassback rules as usual (the default), **only** timed antipassback rules, select the **Enforce Timed Antipassback Only** check box.

7. To configure this iSTAR Area so that a person who validly exits has their APB Timer period erased, click to select the **Valid Exit Clears Timer** check box. This allows such a person to immediately re-enter the Area.

Configuring Carpool Antipassback for iSTAR Areas

To Configure Carpool Antipassback for an Area

1. Create or modify an iSTAR Area. See:
   - Configuring an iSTAR Area on Page 53
   - Modifying an iSTAR Area on Page 64
2. On the **iSTAR Area Editor**, click the **Antipassback** tab to open.
3. Click to select the **Carpool Area** check box to make this a Carpool Area.
4. To configure this Carpool Area so anyone in the Carpool Group can validly swipe to exit the Area, not only the driver, click to select the **Allow any person in carpool group to exit area** check box.
5. Click the down-arrow in the **Antipassback Enforcement Type** field to display a drop-down list with three choices: Antipassback, Timed Antipassback, and None. (The default is **None**.)
6. Click **Antipassback** to have regular antipassback enforced for this Carpool Area.

   - Or -

   Click **Timed Antipassback** to have timed antipassback enforced for this Carpool Area.
7. If you select **Timed Antipassback**, the **Trigger violation on re-entry within....** field and the **Enforce Timed Antipassback Only** and the **Valid Exit Clears Timer** check boxes become available. Configure them as required:

   a. In the **Trigger violation on re-entry within: days - hours: minutes** field, enter the time period that must elapse after a Carpool Group enters the Area before the Group can re-enter.

   b. To configure this Carpool Area so it enforces **only** timed antipassback rules—**not** the usual, regular antipassback rules (the default), select the **Enforce Timed Antipassback Only** check box.

   c. To configure this Carpool Area so a validly exiting Carpool Group has their APB Timer period erased, click to select the **Valid Exit Clears Timer** check box. This allows such a Carpool Group to immediately re-enter the Area.

Configuring Lockout for iSTAR Areas

To Configure Lockout for an iSTAR Area

1. Create or modify an iSTAR Area. See:
   - Configuring an iSTAR Area on Page 53
   - Modifying an iSTAR Area on Page 64
2. On the **iSTAR Area Editor**, click the **Antipassback** tab to open.
3. Click … next to the **Target iSTAR Lockout Area or Target iSTAR Area Group** field to display a selection list with the iSTAR Areas and iSTAR Area Groups available as lockout targets.

NOTE You can only select groups for Lockout that were configured with a Group Type of 'iSTAR Area'.

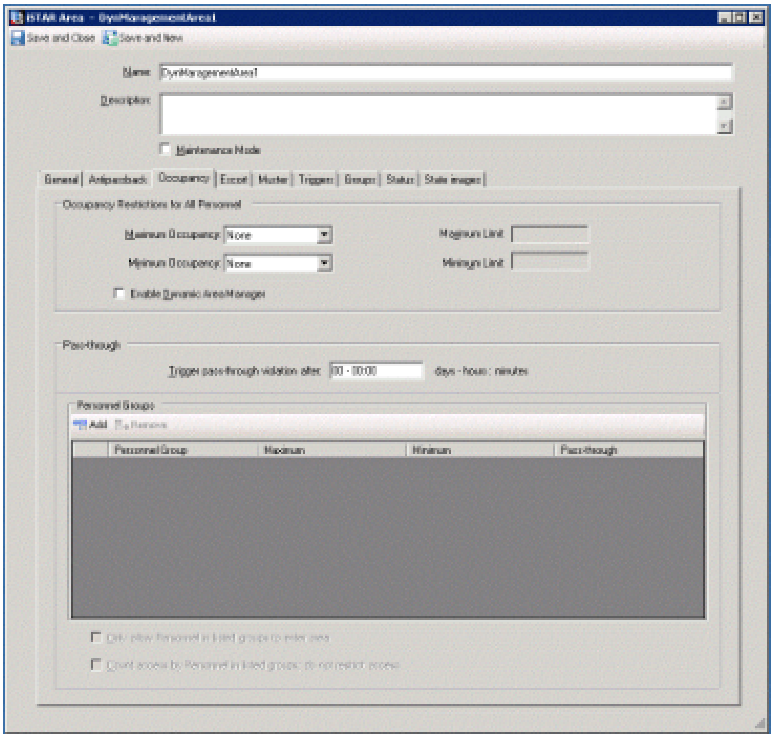
4. Click an iSTAR Area/iSTAR Area Group to select it as the target.
5. In the **Lockout Time** field, enter the time in days, hours, and minutes that the cardholder will be locked out of the specified target iSTAR Area after accessing this Lockout Area.
6. Select the optional **Valid card rejection or admit unused access causes lockout** option if you want any and every card swipe at the Lockout Area reader to cause the person to be locked out of the target Area.
7. On the **Area** tab of the **iSTAR Cluster Editor** for the Area's Cluster, select **No access** as the Cluster Antipassback Communication Failure Mode. For information, see the *C•CURE 9000 Hardware Guide.*

NOTE If you want the remaining Lockout Time to display on a Reader LCD, you must create a custom RM Reader LCD Message Set and associate it with the Controllers configured for the Lockout Area. For information on creating Reader LCD Message Sets, see the *C•CURE 9000 Hardware Guide.*

iSTAR Area Occupancy Tab

The **iSTAR Area Occupancy** tab, shown in Figure 8 on Page 78, lets you define the Occupancy restrictions for the Area for both Personnel in general and for Personnel in Personnel Groups. The tab also allows you to configure Dynamic Area Manager for the Area as well as Area Pass-through for both Personnel and Personnel Groups.

Figure 8: iSTAR Area Editor Occupancy Tab



Name: DynManagementArea1

Description:

□ Maintenance Mode

Occupancy Restrictions for All Personnel

Maximum Occupancy: None

Minimum Occupancy: None

Maximum Limit:

Minimum Limit:

□ Enable Dynamic Area Manager

Pass-through

Trigger pass-through violation after: 00 - 00:00 days - hours : minutes

Personnel Groups

	Personnel Group	Maximum	Minimum	Pass-through

□ Only allow Personnel in listed groups to enter area

□ Count access by Personnel in listed groups; do not restrict access

Definitions for this tab are provided in iSTAR Area Occupancy Tab Definitions on Page 79.

The following topics provide more information about the Occupancy tab:

- Configuring Area Occupancy Restrictions for All Personnel on Page 84.
- Rules for Area Occupancy Access on Page 82.

Occupancy Tab Tasks

You use the Occupancy tab to accomplish the tasks listed below, needed to configure an iSTAR Area. The procedural steps for each task are detailed in the following subsections.

- Configuring Area Occupancy Restrictions for All Personnel on Page 84.
- Configuring Dynamic Area Manager on Page 85.
- Configuring Pass-through Areas on Page 86.
- Configuring Area Occupancy Restrictions for Personnel Groups on Page 85.
- Deleting a Personnel Group from an iSTAR Area on Page 87.

iSTAR Area Occupancy Tab Definitions

The **iSTAR Area Occupancy** tab has the buttons shown in Table 9 on Page 79 and the fields shown in Table 10 on Page 79.

Table 9: iSTAR Area Editor Occupancy Tab Buttons

Button	Description
Add	Click this button to add a new blank row to the **Personnel Groups** table. Each new row is added after the last.
Remove	Click this button to remove a selected row from the **Personnel Groups** table. You must click the row selector ► to select a row to remove. If **no** row is selected, this button is **not** available.

Table 10: iSTAR Area Editor - Occupancy Tab Fields

Fields/Buttons	Description
Occupancy Restrictions for All Personnel Occupancy restrictions/limit counts for **All Personnel** work in conjunction with Occupancy restrictions/limit counts for **Personnel Groups**. See Rules for Area Occupancy Access on Page 82 for detailed information and examples.	
Maximum Occupancy*	Click the down-arrow to select the type of Maximum Occupancy for the Area from the drop-down list. **None** – No Maximum Occupancy Restriction is enforced. Personnel may enter and exit the Area if they have valid clearance. This is the default. (When this option is selected, the **Maximum Limit** field is blank and unavailable.) **Allow Access**– Maximum Occupancy Restriction is set, but the system allows Personnel to enter the Area even though the number entered in the **Maximum Limit** field (required) has been reached. The system sends a message to the Monitoring Station when this occurs and triggers any Occupancy Events configured for the Area. **Restrict Access** – Maximum Occupancy Restriction is enforced. The system uses the number entered in the **Maximum Limit** field (required) to restrict access to the Area.

iSTAR Area Editor - Occupancy Tab Fields (continued)

Fields/Buttons	Description
Maximum Limit	Enter the maximum number of Personnel allowed in the area at one time. By default, this field is blank and unavailable. It becomes available, and requires an entry, when either **Allow Access** or **Restrict Access** are selected as the Maximum Occupancy type. NOTE: If values are set for both Maximum and Minimum Limits, the maximum value must be equal to/greater than the minimum value.
Minimum Occupancy*	Click the down-arrow to select from the drop-down list the type of Minimum Occupancy for the Area. **None** – No Minimum Occupancy Restriction is enforced. Personnel may enter and exit the Area if they have valid clearance. This is the default. (When this option is selected, the **Minimum Limit** field is blank and unavailable.) **Allow Access**– Minimum Occupancy Restriction is set, but the system allows Personnel to enter and exit the Area even though the number entered in the **Minimum Limit** field (required) has not been reached. The system sends a message to the Monitoring Station when this occurs and triggers any Occupancy Events configured for the Area. **Restrict Access** – Minimum Occupancy Restriction is enforced. The system uses the number entered in the **Minimum Limit** field (required) to restrict access to and exit from the Area. To be allowed access, the minimum number of personnel must enter within a certain time frame. Once the minimum number entering the Area is reached, personnel will not be allowed to exit the Area unless they all exit at one time. NOTE: The time interval for Minimum occupancy restrictions is set by the **Next Card Time** System Variable in the Hardware Driver category. The variable default is 15 seconds, so personnel will always have a minimum of 15 seconds to present the next card. For more information, see Setting System Variables That Affect Areas on Page 116.
Minimum Limit	Enter the minimum number of Personnel allowed and required to be in the area at one time.
Enable Dynamic Area Manager	Select this option to make the first person who enters the Area the 'Dynamic Area Manager', the one responsible for this Area. This person must also be the last one to exit the Area. For more information, see Dynamic Area Manager on Page 42. NOTE: When this option is selected, the following is true: • The **Minimum Occupancy** drop-down list is set to **Allow Access**. • The **Minimum Limit** field is set to "1" and is unavailable. • The options on the **Escort** tab are set in a specific way. (For information, see iSTAR Area Escort Tab Definitions on Page 88
Pass-through	
Trigger pass-through violation after: days - hours : minutes	Enter the time interval in days, hours, and minutes after which a pass-through violation will be triggered for this Area. A Pass-though restriction means that personnel have to enter and exit the Area within the time specified in this field. If the value is 0, no pass-through restriction is configured. The maximum amount of time you can enforce pass-through restriction is 45 days.

iSTAR Area Editor - Occupancy Tab Fields (continued)

Fields/Buttons	Description
Occupancy Restrictions for Personnel Groups Occupancy restrictions/limit counts set for **Personnel Groups** work in conjunction with the Occupancy restrictions/limit counts set for **All Personnel**. So be careful when configuring these options for the Area. See Rules for Area Occupancy Access on Page 82 for detailed information and examples.	
Personnel Group	Click in the **Personnel Group** field to display ..., and then click this button to select a Personnel Group for association with this Area from the dialog box that appears. NOTE: If a person is a member of more than one Personnel Group selected for the same Area, the Occupancy counts for the Groups are not maintained correctly when the person accesses the Area. For this reason, Software House recommends avoiding this type of configuration.
Maximum*	Enter the maximum number of Personnel from this Group allowed in the Area at one time. NOTE: If values are set for both Group Maximum and Group Minimum, the maximum value must be equal to/greater than the minimum value. The value you enter in this field will apply to Personnel in this Group separately from any other configured Group.
Minimum*	Enter the minimum number of Personnel from this Group allowed and required to be in the Area at one time. NOTE: The value you enter in this field will apply to Personnel in this Group separately from any other configured Group. In addition, if values are set for both Group and All Personnel Minimum Limits, whichever if the higher minimum will apply.
Pass-through	Click in the **Pass-through** field to display ..., and then click this button to open the **Group Pass-through Configuration** editor. See Configuring Pass-through Areas on Page 86 especially To Configure Pass-through Areas Applying to Personnel Groups on Page 86.
Only allow Personnel in listed groups to enter area	NOTE: This check box is available only if there is at least one Personnel Group in the list. Select this option to limit access to the Area **only** to Personnel (with Clearance) in any of the listed Groups. This means that Personnel **not** in one of these group are denied access.
Count access by Personnel in listed groups; do not restrict access*	NOTE: This check box is available only if there is at least one Personnel Group in the list. Select this option to **allow** Personnel (with Clearance) from any Group in the list to enter and exit the Area whether or not the numbers entered in the Maximum/Minimum fields have been reached. The system sends a message to the Monitoring Station when this occurs and triggers any Occupancy Events configured for the Area.
*The occupancy restrictions that you configure for this Area set the initial default Occupancy Mode for the Area, as detailed in How Area Occupancy Configuration Affects Occupancy Mode on Page 81.	

How Area Occupancy Configuration Affects Occupancy Mode

The current Occupancy Mode for an Area—displayed on the Area **Status** tab (see iSTAR Area Status Tab on Page 99)—is initially set by the way you configure the Occupancy restrictions for the Area, as described in Table 11 on Page 82.

Any one higher level Occupancy restriction, whether for 'All Personnel' or for a 'Personnel Group,' raises the Occupancy Mode level.

Example:

The Minimum and Maximum Occupancy for the Area for 'All Personnel' is **None**, which would equal an Occupancy Mode of 'No Occupancy Testing'. However, a Personnel Group is configured for the Area with a Maximum limit of **5** and a Minimum limit of 2. As a result, the default setting for the Area's Occupancy Mode is 'Counting for Events and Access Restriction.'

The Occupancy Mode can also be reset by Event Actions. For more information, see Configuring Event Actions to Affect Areas on Page 114.

Table 11: Relation Between Area Occupancy Tab Settings and Occupancy Mode

Area Occupancy Tab Field	Setting	Default Occupancy Mode
Occupancy Restrictions for All Personnel		
Maximum Occupancy/Minimum Occupancy	None	No Occupancy
	Allow Access	Counting for Events
	Restrict Access	Counting for Events and Access Restriction
Occupancy Restrictions for Personnel Groups		
No Personnel Group		No Occupancy
Personnel Group Entered	No entries for Maximum/Minimum	No Occupancy
	Maximum/Minimum entered	Counting for Events and Access Restriction
Count access by Personnel in listed groups; do not restrict access	Selected	Counting for Events

Rules for Area Occupancy Access

For any particular Area Occupancy configuration, whether a person is admitted or not is straightforward:

If any condition would deny access to the individual, then access is **not** granted.

The limits and restrictions configured for 'All Personnel' apply to the individual whether or not he/she belongs to a Personnel Group configured in the **Occupancy Restrictions for All Personnel Groups** box.

Examples:

The following example cases in Table 12 on Page 83 and Table 13 on Page 83 show configurations for All personnel and for Personnel Groups.

For a group:

- "Restrict access" means that the **Count access by Personnel in listed groups; do not restrict access** check box is **not** selected.
- "Allow access" means that the aforementioned check box is selected.

Table 12: Minimum Occupancy Configurations

Conditions		Area Count	Activity	Result
Case 1				
All Personnel	Min = 3; Allow Access	0	1 Group A member presents card	Access denied (based on Group)
Personnel Group A	Min = 2; Restrict Access	0		
Case 2				
All Personnel	Min = 3; Allow Access	0	2 Group A members present cards	Access granted (based on Group)
Personnel Group A	Min = 2; Restrict Access	0		
Case 3				
All Personnel	Min = 3; Restrict Access	0	2 Group A members present cards	Access denied (based on All Personnel)
Personnel Group A	Min = 2; Restrict Access	0		
Case 4				
All Personnel	Min = 2; Allow Access	0	1 Group A member presents card	Access denied
Personnel Group A	Min = 3; Restrict Access	0		
Case 5				
All Personnel	Min = 2; Allow Access	0	2 Group A members present cards	Access denied (based on Group)
Personnel Group A	Min = 3; Restrict Access	0		
Case 6				
All Personnel	Min = 2; Restrict Access	0	2 Group A members present cards	Access denied (based on Group)
Personnel Group A	Min = 3; Restrict Access	0		

Table 13: Maximum Occupancy Configurations

Conditions		Area Count	Activity	Result
Case 1				
All Personnel	Max = 4; Restrict Access	3 from GroupA	Group A member presents card	Access denied (based on Group)
Personnel Group A	Max = 3; Restrict Access		Non-Group A member presents card	Access granted (no condition denies access)

Maximum Occupancy Configurations (continued)

Conditions		Area Count	Activity	Result
Case 2				
All Personnel	Max = 3; Restrict Access	3 from GroupA	Group A member presents card	Access granted (based on All Personnel)
Personnel Group A	Max = 4; Restrict Access*			
Case 3				
All Personnel	Max = 3; Allow Access	3 from GroupA	Group A member presents card	Access granted (no condition denies access)
Personnel Group A	Max = 4; Restrict Access	4 from GroupA	Group A member presents card	Access denied (based on Group)
			Non-Group A member presents card	Access granted (no condition denies access)
*This configuration is **not** recommended because 4 Group A members will **not** be allowed to enter the Area.				

Configuring Area Occupancy Restrictions for All Personnel

To Configure Occupancy Restrictions for All Personnel for an Area

1. Create or modify an iSTAR Cluster Area. See:
   - Configuring an iSTAR Area on Page 53
   - Modifying an iSTAR Area on Page 64
2. On the **iSTAR Area Editor**, click the **Occupancy** tab to open.
3. In the **Occupancy Restrictions for All Personnel** box, click the down-arrow in the **Maximum Occupancy** field to display a drop-down list and select one of the three Maximum Occupancy types: None, Allow Access, or Restrict Access. (The default is **None**.)
4. In the **Maximum Limit** field, which becomes available and requires an entry if you selected either **Allow Access** or **Restrict Access**, enter the maximum number of Personnel allowed in the area at one time.
5. Click the down-arrow in the **Minimum Occupancy** field to display a drop-down list and select one of the three Minimum Occupancy types: None, Allow Access, or Restrict Access. (The default is **None**.)
6. In the **Minimum Limit** field, which becomes available and requires an entry if you selected either **Allow Access** or **Restrict Access**, enter the minimum number of Personnel allowed/required in the area at one time.

NOTE If values are set for both the Maximum and Minimum Limits, the maximum value must be equal to or greater than the minimum value.

Configuring Area Occupancy Restrictions for Personnel Groups

To Configure Occupancy Restrictions for Personnel Groups for an Area

1. Create or modify an iSTAR Cluster Area. See:
   - Configuring an iSTAR Area on Page 53
   - Modifying an iSTAR Area on Page 64
2. On the **iSTAR Area Editor**, click the **Occupancy** tab to open.
3. In the **Occupancy Restrictions for Personnel Groups** box, click **Add** to create a new row.
4. Click in the **Personnel Group** field to display ... and click this button.

   A selection list opens with the Personnel Groups available for iSTAR Cluster Areas.
5. Click a Group to add it to the row.

   Example:

   Personnel Group 3
6. In the **Maximum** field enter the maximum number of Personnel from this Group allowed in the Area at one time.
7. In the **Minimum** field enter the minimum number of Personnel from this Group both allowed and required to be in the Area at one time.

NOTE If values are set for both the Maximum and Minimum Limits, the maximum value must be equal to or greater than the minimum value.

8. To configure more Personnel Groups for this iSTAR Cluster Area, click **Add** and repeat the preceding steps.
9. To limit access to the Area only to Personnel (with the appropriate Clearance) in any of the Groups listed in the box, click to select the **Only allow Personnel in listed groups to enter area** check box.
10. To allow Personnel (with the appropriate Clearance) from any of the Groups listed in the box to enter and exit the Area whether or not the numbers entered in the Maximum/Minimum fields have been reached, click to select the **Count access by Personnel in listed groups; do not restrict access** check box. In this situation, the system sends a message to the Monitoring Station and triggers any Occupancy Events configured for the Area.

NOTE If a person is a member of more than one Personnel Group selected for the same Area, the Occupancy counts for the Groups are not maintained correctly when the person accesses the Area. For this reason, Software House recommends avoiding this type of configuration.

Configuring Dynamic Area Manager

To Configure Dynamic Area Manager for an Area

1. Create or modify an iSTAR Cluster Area. See:
   - Configuring an iSTAR Area on Page 53
   - Modifying an iSTAR Area on Page 64
2. On the **iSTAR Area Editor**, click the **Occupancy** tab to open.

3. Click to select the **Enable Dynamic Area Manager** option. (The default is unselected.)

   Once you select this option, the following settings are made in the **Occupancy Restrictions for All Personnel** box:

   - The **Minimum Occupancy** drop-down list is set to **Allow Access**.
   - The **Minimum Limit** field is set to "1" and becomes unavailable.

   In addition, the options on the **Escort** tab are set in a specific way. (For information, see iSTAR Area Escort Tab Definitions on Page 88.)

Configuring Pass-through Areas

You can configure Area Pass-through restrictions that apply system-wide to all Personnel or only to the members of one or more Personnel Groups.

For Personnel Groups, you can configure Pass-through so the Group members are:

- Exempt from any Area-wide Pass-through time.
- Subject to the Area-wide Pass-through time.
- Subject to a custom Pass-through time different from the Area-wide time.

To Configure a Pass-through Area Applying to All Personnel

1. Create or modify an iSTAR Cluster Area. See:
   - Configuring an iSTAR Area on Page 53
   - Modifying an iSTAR Area on Page 64
2. On the **iSTAR Area Editor**, click the **Occupancy** tab to open.
3. In the **Trigger pass-through violation after** field in the **Pass-through** box, enter the time interval—in days, hours, and minutes—that the cardholder has to go in and then out of the Area—without causing a violation.

To Configure Pass-through Areas Applying to Personnel Groups

1. Follow Steps 1, 2, and 3, as described in the preceding task
2. In the **Personnel Groups** table in the **Occupancy Restrictions for Personnel Groups** box, click **Add** to create a new row.

   (Once a new row appears, the **Pass-through** field displays the default, **Exempt**.)
3. Click in the **Personnel Group** field to display ... and click this button.

   A selection list opens with the Personnel Groups available for iSTAR Cluster Areas.
4. Click a Group to add it to the row.

   Example:

   Personnel Group 3
5. In the **Pass-through** field, if you do **not** want the Personnel Group you selected to be subject to the Area-wide Pass-through time, leave the default entry, **Exempt**.

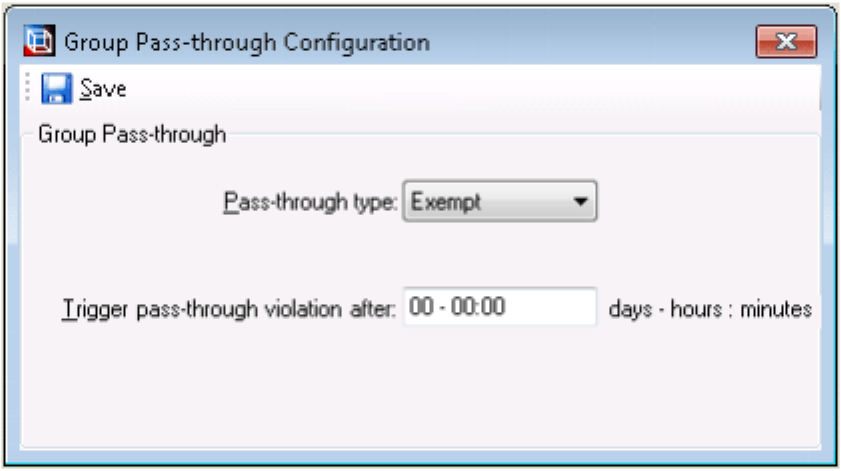
   - or -

   To configure a different Pass-through option:

a. Click in the **Pass-through** field to display ... and click this button.

The **Group Pass-through Configuration** dialog box, shown in Figure 9 on Page 87, opens with **Exempt** displayed in the **Pass-through type** field.

Figure 9: Group Pass-through Configuration Dialog Box



Pass-through type: Exempt

Trigger pass-through violation after: 00 - 00:00 days - hours : minutes

b. Click the down-arrow in the **Pass-through type** field to display the other types: **Area Wide** and **Custom**.

c. To make this Personnel Group subject to the Area-wide Pass-through time entered in the **Trigger pass-through violation after** field in the **Pass-through** box in the middle of the **Occupancy** tab, click **Area Wide** and then click **Save**.

- or -

To make this Personnel Group subject to a different Pass-through time, click **Custom**, enter the time interval (in days, hours, and minutes) in the **Trigger pass-through violation after** field in this dialog box, and then click **Save**.

The **Group Pass-through Configuration** dialog box closes.

6. To configure Pass-through for more Personnel Groups for this iSTAR Cluster Area, click **Add** and repeat the preceding steps.

Deleting a Personnel Group from an iSTAR Area

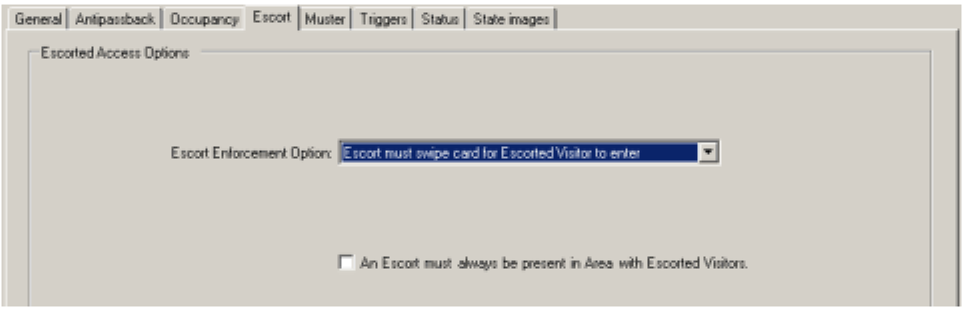
To Delete an iSTAR Area Personnel Group

1. In the **Occupancy Restrictions for Personnel Groups** box on the **Occupancy** tab, click a Personnel Group row to select it.
2. Click **Remove** to delete the row.

iSTAR Area Escort Tab

The **iSTAR Area Escort** tab, shown in Figure 10 on Page 88, lets you define the Escorted Access option for the Area.

Figure 10: iSTAR Area Editor Escort Tab



Escorted Access Options

Escort Enforcement Option: Escort must swipe card for Escorted Visitor to enter

☐ An Escort must always be present in Area with Escorted Visitors.

Definitions for this tab are provided in iSTAR Area Escort Tab Definitions on Page 88.

The following topic provides more information about the Escort tab:

How Area Escort Configuration Affects Escorted Access on Page 90.

Escort Tab Task

You use the Escort tab to accomplish the task listed below, needed to configure an iSTAR Area. The procedural steps for the task are detailed in the following subsection.

- Configuring Escorted Access for iSTAR Areas on Page 89.

iSTAR Area Escort Tab Definitions

The **iSTAR Area Escort** tab has the fields shown in Table 14 on Page 88.

Table 14: iSTAR Area Editor - Escort Tab Fields

Fields/Buttons	Description
Escorted Access Options	
Escort Enforcement Type	Click the down-arrow to select the type of escort enforcement for the Area from the drop-down list. **Escort must swipe card for Escorted Visitor to enter** – Escorted Access is enforced. Escorted Visitors may enter the Area only if an Escort has presented a valid card. This is the default. **Escorted Visitor may enter without an Escort swiping card**– Escorted Access is not enforced. Escorted Visitors may enter the Area without any Escort. NOTE: If this Area is configured for Dynamic Area Manager (on the **Occupancy** tab), **Escorted Visitor may enter without an Escort swiping card** is selected in the drop-down list and the drop-down list is **unavailable**.

iSTAR Area Editor - Escort Tab Fields (continued)

Fields/Buttons	Description
An Escort must always be present in Area with Escorted Visitors	Select this option to require an Escort to remain in the Area with the Escorted Visitors. In other words, the last Escort in the Area will be denied access to leave as long as there are Escorted Visitors in the Area. If this check box is **not** selected, Escorted Visitors can stay in the Area unescorted, and all Escorts can leave the Area. NOTE: • If this Area is configured for Remote Escort (Turnstile) mode, Software House recommends **not** selecting this option. • If this Area is configured for Muster/De-muster as well as for Escorted Access, this option **must not be** selected. • If this Area is configured for Dynamic Area Manager (on the **Occupancy** tab), this option is **not** selected and is **unavailable**.

Configuring Escorted Access for iSTAR Areas

To Configure Escorted Access for an Area

1. Create or modify an iSTAR Cluster Area. See Configuring an iSTAR Area on Page 53 or Modifying an iSTAR Area on Page 64.
2. On the **iSTAR Area Editor**, click the **Escort** tab to open.
3. In the **Escorted Access Options** box, click the down-arrow in the **Escort Enforcement Type** field to display the drop-down. Select one of the following two types to configure the Area to require Escorted Access for entry or to not require it.
   - Escort must swipe card for Escorted Visitor to enter (the default).
   - Escorted Visitor may enter without an Escort swiping card.

NOTE If this Area is configured for Dynamic Area Manager (on the **Occupancy** tab), **Escorted Visitor may enter without an Escort swiping card** is selected in the drop-down list and the drop-down list is **unavailable**.

4. To configure this Area so Escorted Visitors can remain inside without an Escort, leave the **An Escort must always be present in Area with Escorted Visitors** option unselected (the default). To require the Escorted Visitors to always have an Escort present with them in this Area, select this option.

NOTE

- If this Area is configured for Remote Escort (Turnstile) mode, Software House recommends that you leave this option **unselected**.
- If the Area is configured for Muster/De-muster as well as for Escorted Access, the option **must not be selected.**
- If this Area is configured for Dynamic Area Manager (on the Occupancy tab), this option is **not** selected and is **unavailable**.

How Area Escort Configuration Affects Escorted Access

The restrictions that apply to Escorted Visitors' access to an Area depend on the way you configure the Area's Escort options.There are four possible combinations, as described in Table 15 on Page 90.

Table 15: Area Escorted Access Configurations

Options	Conditions	Result
Case 1		
Escort Enforcement Option —	Escort must swipe card for Escorted Visitor to enter. (The default setting.)	An Escort must be present and swipe at the Door for the Escorted Visitor to enter the Area, but after that the Escorted Visitor can be left alone inside the Area. This means that all Escorts may leave the Area at any time.
An Escort must always be present in Area with Escorted Visitors check box —	Unselected. (The default setting.)	
Case 2		
Escort Enforcement Option —	Escort must swipe card for Escorted Visitor to enter. (The default setting.)	An Escort must be present and swipe at the Door for the Escorted Visitor to enter the Area, and at least one Escort must remain in the Area with the Escorted Visitor. This is the most restrictive combination.
An Escort must always be present in Area with Escorted Visitors check box —	Selected.	
Case 3		
Escort Enforcement Option —	Escorted Visitor may enter **without** an Escort swiping card.	An Escorted Visitor can enter the Area without an Escort swiping, and the Escorted Visitor can be left alone inside the Area. This means that all Escorts may leave the Area at any time. This is the way to configure an Area so that Escorted Visitors may enter and leave without any Escort restrictions. This is the least restrictive combination.
An Escort must always be present in Area with Escorted Visitors check box —	Unselected. (The default setting.)	
Case 4		
Escort Enforcement Option —	Escorted Visitor may enter **without** an Escort swiping card.	An Escorted Visitor can enter the Area without an Escort swiping as long as an Escort is already present in the Area. At least one Escort must remain in the Area with the Escorted Visitor.
An Escort must always be present in Area with Escorted Visitors check box —	Selected.	

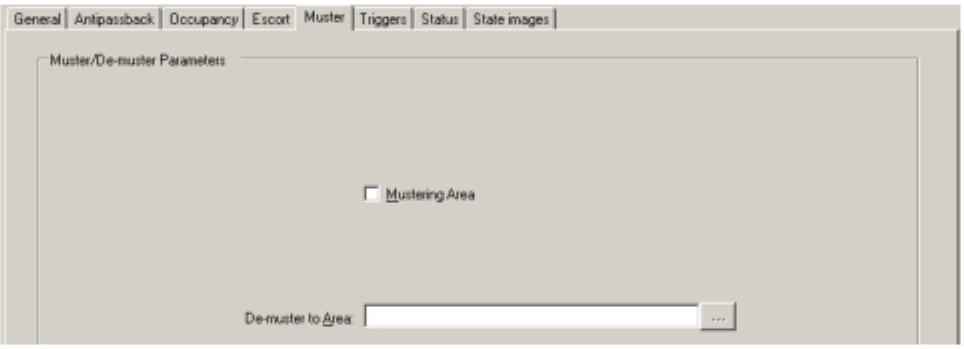
iSTAR Area Muster Tab

The **iSTAR Area Muster** tab, shown in Figure 11 on Page 91, lets you define whether or not this Area is a Mustering Area, and if it is, what Area it de-musters to.

NOTE

> When you configure Muster/De-muster, you **must** also configure **both** Areas either **for Occupancy** or **without Occupancy**. This is to keep the Area count correct since counting for Areas configured for occupancy is performed by the iSTAR Controllers, while it is performed by the host for Areas without occupancy. The system does not validate for this, but if you do not follow this rule, your counts can become corrupted.
>
> In addition, to keep the Area count correct for Personnel Groups, you must configure both the Mustering Area and the De-muster Area with the same Groups. For information, see Configuring Muster/De-muster Areas for Personnel Groups on Page 92.
>
> (If you are going to change an existing occupancy Area to a non-occupancy Area—or vice versa, you should ideally do it when the system is not busy and the Area is empty. Alternatively, if there are Personnel in the Area, you can use the **Set Property** option on the right-click context menu on the Areas Dynamic View to reset the count for the Area.)

Figure 11: iSTAR Area Editor Muster Tab



Definitions for this tab are provided in iSTAR Area Muster Tab Definitions on Page 91.

Muster Tab Tasks

You use the **Muster** tab to accomplish the tasks listed below to configure an iSTAR Area. The procedural steps for the tasks are detailed in the following subsections.

- Configuring a Muster Area on Page 92.
- Configuring Muster/De-muster Areas for Personnel Groups on Page 92.

iSTAR Area Muster Tab Definitions

The **iSTAR Area Muster** tab has the fields shown in Table 16 on Page 92.

Table 16: iSTAR Area Editor - Muster Tab Fields

Fields/Buttons	Description
Muster/De-muster Parameters	
Mustering Area	Select this check box to indicate this Area is a Mustering Area in which Personnel gather in an emergency. Once the emergency is over and the Area is de-mustered, Personnel are de-mustered to another Area. NOTE: A Mustering Area can also be configured for Antipassback and Occupancy, but they are not required for Muster/De-muster functionality. For more information, see iSTAR Area Muster Tab on Page 90 If this Area is configured for Escorted Access as well as for Muster/De-muster, do **not** select the **An Escort must always be present in Area with Escorted Visitors** option on the **Escort** tab. For information, see iSTAR Area Escort Tab Definitions on Page 88.
De-muster to Area	NOTE: This field is available only if you have selected the previous option and made this Area a Mustering Area. Click ... and select an Area to act as the De-mustering location for this Area from the list of available iSTAR Areas. • The list can include any Area in the system except the following: - Areas currently configured as Mustering Areas. - Areas not in the same iSTAR Cluster if this Mustering Area is **not** configured for Global Antipassback. • Multiple iSTAR Areas can be configured to de-muster to the same De-mustering Area. NOTE: When Muster/De-muster is configured, both Areas **must** either be configured for Occupancy or configured **without** Occupancy. If you leave this field blank (do not enter a De-muster Area), at de-muster time any Personnel in this Mustering Area will be graced.

Configuring a Muster Area

To Configure an Area as a Mustering Area

1. Create or modify an iSTAR Area. See
   - Configuring an iSTAR Area on Page 53
   - Modifying an iSTAR Area on Page 64
2. On the **iSTAR Area Editor**, click the **Muster** tab to open.
3. Select the **Mustering Area** check box to make this a Mustering Area.
4. Click ... next to the **De-muster to Area** field to display a selection list with all the iSTAR Areas in the system available for de-mustering to.
5. Click an Area to select it as De-muster Area.

Configuring Muster/De-muster Areas for Personnel Groups

To keep Personnel Group counts correct between a Mustering Area and the Area it de-musters to, you must configure the Areas in a particular way.

A Muster Area can only report the Personnel Group counts that need to be added to its De-muster Area if it knows about the Groups. So you must configure these Groups in the **Personnel Groups** list on the Muster Area's **Occupancy** tab. Then you must add the same Personnel Groups to the related De-muster Area on its **Occupancy** tab.

For the Muster Area, you should also configure a **high** Maximum limit for each Personnel Group with **no** Minimum limit and select the **Count access by Personnel in listed groups; do not restrict access** option.

Once you have configured both your Muster and De-muster Areas as described, the following happens:

1. When Personnel swipe into the Muster Area, the Area keeps count of total Personnel as well as Personnel in the listed Groups.
2. Then when the system de-musters, all these counts transfer correctly.

NOTE The following procedure details the steps to properly configure your Muster/De-muster Areas, but you do not need to perform them in the order given here.

To Configure Muster/De-muster Areas for Personnel Groups

1. Create or modify an iSTAR Area to be the Muster Area. See Configuring an iSTAR Area on Page 53 or Modifying an iSTAR Area on Page 64.
2. On the **iSTAR Area Editor**, click the **Occupancy** tab to open.
3. In the **Occupancy Restrictions for Personnel Groups** box, click **Add** to create a new row.
4. Click in the **Personnel Group** field to display ... and click this button.

   A selection list opens with the Personnel Groups available for iSTAR Cluster Areas.
5. Click a Group to add it to the row.
6. In the **Maximum** field enter a very high figure for maximum number of Personnel from this Group allowed in the Area at one time.
7. Leave the **Minimum** field empty.
8. Click to select the **Count access by Personnel in listed groups; do not restrict access** check box.

NOTE If a person is a member of more than one Personnel Group selected for the same Area, the Occupancy counts for the Groups are not maintained correctly when the person accesses the Area. For this reason, Software House recommends avoiding this type of configuration.

9. Click the **Muster** tab to open.
10. Select the **Mustering Area** check box to make this a Mustering Area and then click **Save and New**.

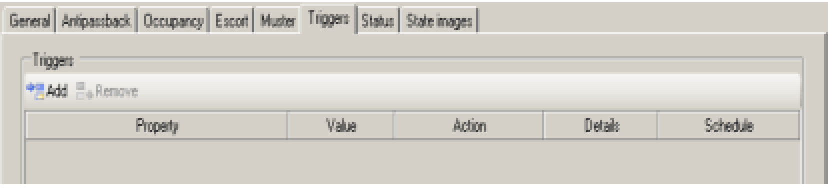
    The system saves your Muster Area and opens the **iSTAR Area Editor** for you to create the related De-muster Area.
11. Click to open the **Occupancy** tab and repeat Step 3 and Step 4 on Page 93.
12. When the selection list opens with the available Personnel Groups, select the same Group you configured for the Muster Area in Step 5 on Page 93.
13. Click **Save and Close**.
14. Re-open the Mustering Area you created first and open the **Muster** tab.
15. Click ... next to the **De-muster to Area** field to display a selection list with the iSTAR Areas in the system available for de-mustering.
16. Click to select the second Area you created as the De-muster Area.

17. Click **Save and Close**.

iSTAR Area Triggers Tab

The **iSTAR Area Triggers** tab, shown in Figure 12 on Page 94, allows you to set up **Triggers**, configured procedures used by C•CURE 9000 to activate specific actions when a particular predefined condition occurs.

Figure 12: iSTAR Area Editor Triggers Tab



Definitions for this tab are provided in iSTAR Area Triggers Tab Definitions on Page 95.

The following topics provide more information about the Triggers tab:

- How to Use the Triggers Tab on Page 94.

Triggers Tab Tasks

You use the Triggers tab to accomplish the tasks listed below, needed to configure an iSTAR Area. The procedural steps for each task are detailed in the following subsections.

- Configuring Triggers for iSTAR Areas on Page 96.
- Deleting a Trigger from an iSTAR Area on Page 98.

How to Use the Triggers Tab

The tab contains one Action, **Activate Event**, that can be linked to a specific value of an Area-related violation or state and to any panel or host Event configured in the system. Once the Area's state matches one of these values, the linked **Activate Event** Action is triggered and the user-specified Event is set to an active state (if allowed by the Event, which should be armed at the time). Violation Status Events (such as APB Entry/Exit Violations—representing antipassback violations—and Access over Maximum/under Minimum Occupancy Violations) are momentarily activated, while Maximum and Minimum Occupancy Status Events are persistent.

You could use the activated Event to display a Reader LCD Message saying "Lot Full" when a Parking Lot Area's **Maximum Occupancy Status** becomes "At or Over Maximum".

By creating new rows and selecting different values for each row, each value of the **Violation Status** field can trigger its own Event. It is also possible to trigger two different Events for the same violation state value by creating two rows with the same value and then linking each row to its own Event.

NOTE However, each violation state value can activate **only one** panel Event.

iSTAR Area Triggers Tab Definitions

The **iSTAR Area Triggers** tab has the buttons shown in Table 17 on Page 95 and the fields shown in Table 18 on Page 95.

Table 17: iSTAR Area Editor Triggers Tab Buttons

Button	Description
Add	Click this button create a new row in the **Triggers** table. You have to configure all the fields in the row and select an Event to complete the Add operation.
Remove	Click this button to remove a selected row from the **Triggers** table. You have to click the row selector ▶ to select a row to remove. If **no** row is selected, this button is **not** available.

Table 18: iSTAR Area Editor - Triggers Tab Fields

Field	Description
Property	Click in the **Property** field to display ... and then click this button to display a dialog box with available properties. Double-click a Property to select it. For detailed information about the relationships between the available properties, their corresponding values, the Event types, and Scheduling, see Table 19 on Page 96.
Value	Click the down-arrow to select a value from the drop-down list or for the Personnel Count Property, enter 0 (zero) or 1 (one). When the Area's Violation Status matches this value, the Event you specify in the **Event** field is activated.
Action	Click the down-arrow to select **Activate Event** (the only type available) from the drop-down list. This Action will be executed when the value of the Area's Status matches that selected in the **Value** field.
Details	The name of the Event configured for this row (read-only) is entered by the system once you make a selection in the **Event** field.
Event	Click ... in this field to select the Event to be activated if the Area's Violation Status for the current row on the grid has the specified value. For each Violation Status value, you can select **multiple** host Events, but only **one** panel Event. NOTE: Switching rows in the grid updates this field with the user-selected Event so that each row can have its own Event to activate.
Schedule	Click in the **Schedule** field to display ... and then click this button to display a dialog box with available Schedules. Double-click a Schedule to select it. • For panel Events, the **Schedule** field is set to **Always** and **cannot** be modified. • For host Events, this field is modifiable.

Table 19: iSTAR Area Triggers Table Details

Property	Possible Values	Event Type	Schedule Type
Group Maximum Occupancy Status	At or Over Maximum	Panel Host	Always only Modifiable
Group Minimum Occupancy Status	At or Under Minimum		
Maximum Occupancy Status	At or Over Maximum		
Minimum Occupancy Status	At or Under Minimum		
Personnel Count	Enter 0 (zero) or 1 (one)		
Violation Status	APB Entry Violation/APB Exit Violation (Antipassback violations)		
	Access over Maximum Occupancy Violation/Exit under Minimum Occupancy Violation		
	Additional Card Violation (Violations that occur when multiple Card swipe requirements for Area access are **not** met.) NOTE: Due to the complexity of Area configuration, some situations that seem to be Additional Card Violations may not trigger the configured Event. You should verify that your particular Area configuration activates the desired violation Event.		
	Lockout Violation		
	Pass-through Violation		
	Group Pass-through Violation		

Configuring Triggers for iSTAR Areas

You can create as many triggers as you wish for any iSTAR Area.

To Configure Area Triggers

1. Create or modify an iSTAR Cluster Area. See:
   - Configuring an iSTAR Area on Page 53
   - Modifying an iSTAR Area on Page 64
2. On the **iSTAR Area Editor**, click the **Triggers** tab to open.
3. Click **Add** to create a new trigger row.

4. Click in the **Property** field to display ... and click this button.

   A selection list opens with the available properties.

5. Click a property to add it to the row.

   Example:

   Violation Status

6. Click the down-arrow in the **Value** field to display a drop-down list of values for the property you selected.

7. Click the **Value** you want to activate the event for this trigger to add it to the row.

   Example:

   APB Exit Violation

8. Click the down-arrow in the **Action** field to display a drop-down list containing **Activate Event** as the only available Action. Click **Activate Event** to add it to the row as the action that will be executed when the Cluster Area's state matches that selected in the **Value** field.

   The **Event** field displays on the bottom of the tab.

9. Click ... in the **Event** field to display a selection list of all Events currently configured in the C•CURE 9000 system, and then click an Event to select it.

   The system enters the name of the Event you select in the **Details** field for the row when you click anywhere outside the **Event** field. This Event will be activated whenever the **Violation State** for the current row on the grid matches the value specified in that row.

   The **Schedule** field contains the default entry **Always**. (This is the **only** schedule valid for Panel Events. You **can** select a different schedule for a Host Event.)

10. Click ... in the **Schedule** field to display a selection list of schedules configured in the C•CURE 9000 system.

11. Click a Schedule to select it.

12. To create more triggers for this iSTAR Area, repeat the above steps for each trigger you want.

    Switching rows in the grid updates the **Event** field with the user-selected event so that each row can have its own event to activate.

Deleting a Trigger from an iSTAR Area

To Delete an iSTAR Area Trigger

1. On the **Triggers** tab, click a row to select it.
2. Click **Remove** to delete the trigger row.

iSTAR Area Groups Tab

The iSTAR Area **Groups** tab lists the iSTAR Area Groups to which this Area belongs.

NOTE This tab does **not** display on the **iSTAR Area Editor** when you are configuring a new Area. It displays when you are editing an existing Area.

The Groups table on this tab is a Dynamic View that you can filter, group, print, and view in Card View, using the buttons described in Table 20 on Page 98.

Definitions for the icons and columns on the Groups tab are provided in iSTAR Area Groups Tab Definitions on Page 98.

You can select any of the iSTAR Area Groups in the list and double-click ▶ to edit it or right-click to display the Groups Context menu (described in the Groups chapter in the *C•CURE 9000 Software Configuration Guide*). You can also right-click in the **Name** or **Description** field of an iSTAR Area Group row to display a standard edit menu.

iSTAR Area Groups Tab Definitions

The **iSTAR Area Groups** tab has the buttons and fields shown in Table 20 on Page 98.

Table 20: iSTAR Cluster Area Editor Groups Tab Fields/Buttons

Fields/Buttons	Name	Description
📄	Card View	Click to display the list of iSTAR Area Groups in Card View
🖨	Print	Click to print the list of iSTAR Area Groups.
▤	Group	Click to enable Grouping of the list. You can drag a column heading to the area labeled **Drag columns to group by here to** group the list by that heading
▽	Filter	Click to display the filter bar. You can click in the filter bar to add filtering criteria to any column of the list. For more information about Filtering, see the Dynamic Views chapter in the *C•CURE 9000 Data Views Guide*.
Name		Name of the Group, up to 100 characters.
Description		Description of the Group.

iSTAR Area Status Tab

The **iSTAR Area Status** tab, shown in Figure 13 on Page 100, provides a read-only listing of critical information about the dynamic status of this iSTAR Area, including:

- Maximum Occupancy Status– shows whether or not the Maximum Occupancy limit was reached: Unknown, At or Over Maximum, or Normal.
- Minimum Occupancy Status – shows whether or not the Minimum Occupancy limit was reached: Unknown, At or Under Minimum, or Normal.
- Current Occupancy Testing Mode – displays the last reported mode: Unknown, No Occupancy Testing, Counting Only, Counting for Events, or Counting for Events and Access Restriction.

NOTE An Area's initial Occupancy Testing mode depends on the way in which the Area was configured on the **Occupancy** tab, described in How Area Occupancy Configuration Affects Occupancy Mode on Page 81. You can reset the mode through Event Actions, described in Configuring Event Actions to Affect Areas on Page 114. (The 'Counting Only' mode can **only** be set with an Event Action.)

- Group Maximum Occupancy Status – shows whether or not the Maximum Occupancy limit was reached: Unknown, At or Over Maximum, or Normal.
- Group Minimum Occupancy Status – shows whether or not the Minimum Occupancy limit was reached: Unknown, At or Under Minimum, or Normal.
- Communication Status – displays the comm state of the Cluster Area: Normal, Communication Failure, or Partial Connectivity.

NOTE *PartialConnectivity* indicates that Occupancy is not being enforced for the Area because some iSTAR Controller with Readers in the Area is in Comm Fail. In this situation, the iSTAR continues to collect Occupancy information and when communication is restored, all information is synchronized.

- Personnel Count – displays the number of Personnel currently in this Area.
- Escort Count – displays the number of Personnel designated as Escorts who are currently in this Area.
- Escorted Visitor Count – displays the number of Personnel designated as Escorted Visitors who are currently in this Area.
- Area Manager Count – shows whether or not the Dynamic Area Manager is currently present in the Area.
- Managed Personnel Count – displays the number of Personnel currently in the Area with the Dynamic Area Manager. (This number includes all Personnel admitted into the Area **after** the Dynamic Area Manager—both those admitted with Clearances and those admitted 'conditionally'.)

NOTE The Area Manager and Managed Personnel Counts display only if the Area is configured for Dynamic Area Manager. For information, see Dynamic Area Manager on Page 42.

In addition, when the Area is so configured, the Escort and Escorted Visitor Counts do **not** display. The system does **not** support the Escort and Dynamic Area Manager features at the same time for any one Area.

- Conditionally Admitted Count – displays the number of Personnel currently in the Area who were admitted 'conditionally'. See "iSTAR Door Conditional Access Tab" in the Doors chapter in the C•*CURE 9000 Hardware Configuration Guide*.

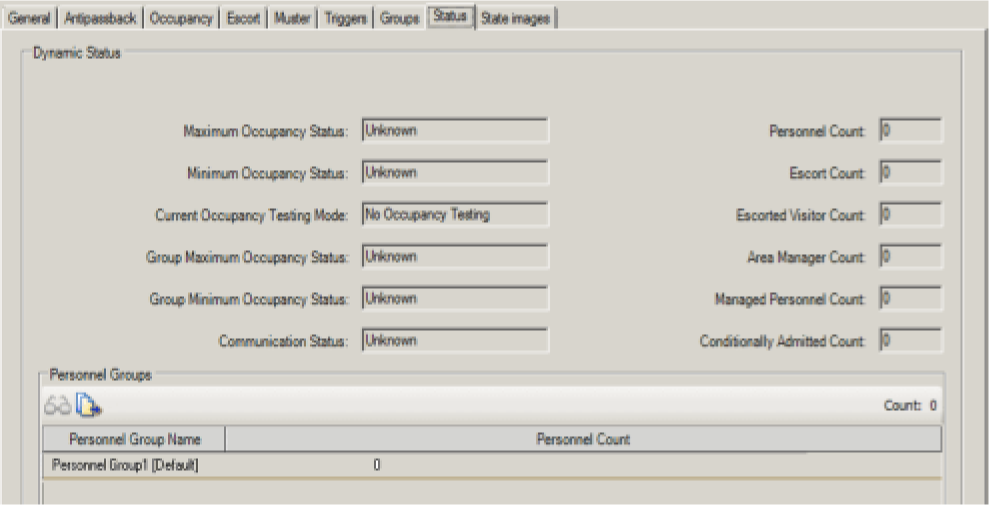
- Personnel Groups – if any configured for Area – displays:
  - Personnel Group Name
  - Personnel Count

Viewing Area Status on the Status Tab

To View Status on the iSTAR Area Editor

1. In the Navigation Pane of the Administration Workstation, click the **Areas and Zones** pane button.
2. Click the **Areas and Zones** drop-down list and select **iSTAR Area**.
3. Click to open a Dynamic View showing a list of all existing iSTAR Area Objects.
4. Right-click the iSTAR Area whose status you want to view and click **Edit** from the context menu that appears. The **iSTAR Area Editor** opens with the **General** tab displayed.
5. Click the **Status** tab to open, as shown in Figure 13 on Page 100.

Figure 13: iSTAR Area Editor Status Tab



Maximum Occupancy Status: Unknown
Minimum Occupancy Status: Unknown
Current Occupancy Testing Mode: No Occupancy Testing
Group Maximum Occupancy Status: Unknown
Group Minimum Occupancy Status: Unknown
Communication Status: Unknown

Personnel Count: 0
Escort Count: 0
Escorted Visitor Count: 0
Area Manager Count: 0
Managed Personnel Count: 0
Conditionally Admitted Count: 0

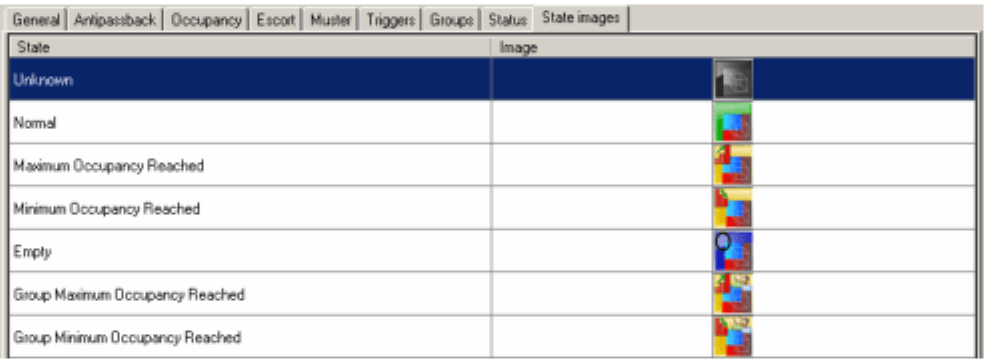
Count: 0

Personnel Group Name	Personnel Count
Personnel Group1 [Default]	0

iSTAR Area State Images Tab

The **iSTAR Area State Images** tab, shown in Figure 14 on Page 101, provides a means to change the default images used to indicate states for the iSTAR Area on the Monitoring Station. You can select other images to display for this Area or return to the default images, as described in State Images Tab Tasks on Page 101.

Figure 14: iSTAR Area Editor State Images Tab



State	Image
Unknown	
Normal	
Maximum Occupancy Reached	
Minimum Occupancy Reached	
Empty	
Group Maximum Occupancy Reached	
Group Minimum Occupancy Reached	

State Images Tab Tasks

To Change an Image

1. Double-click the default image in the tab to open a Windows file selection dialog box.
2. If necessary, navigate to find the new image.
3. Select the desired replacement image and click **Open**. The new image replaces the default image and displays in the **State Images** tab.

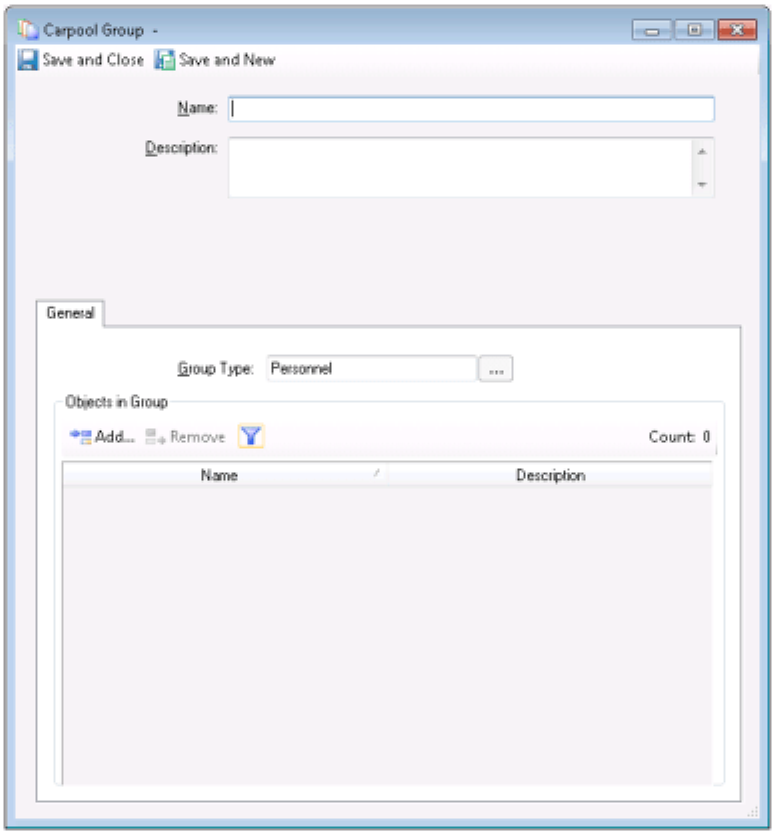
To Restore the Default Image

- Right-click the replacement image in the Area **State Images** tab and select **Restore Default**.

Configuring a Carpool Group for Carpool Antipassback

The **Carpool Group Editor**, shown in Figure 15 on Page 102, lets you configure Carpool Groups and their member Personnel.

Figure 15: Carpool Group Editor



Definitions for this tab are provided in Carpool Group Editor Definitions on Page 102.

Information about using the **Carpool Group Editor** is provided in Carpool Group Editor Tasks on Page 103.

Carpool Group Editor Definitions

The **Carpool Group Editor** has the fields shown in Table 21 on Page 102.

Table 21: Carpool Group Editor Fields

Fields/Buttons	Description
Name	Enter a unique name, up to 100 characters, to identify the Carpool Group.
Description	Enter a description of the Carpool Group, up to 255 characters.
Partition.	A read-only field displaying the name of the Partition to which this Carpool Group belongs. (This field is visible only if the C•CURE 9000 system is partitioned.)

The **Carpool Group Editor** General tab has the buttons and fields shown in Table 22 on Page 103 .

Table 22: Carpool Group General Tab Buttons/Fields

Fields/Buttons	Description
Group Type	Displays Personnel, the default type.
Objects in Group	
Add	Click this button to open the **Object Selection** dialog box where you can select one or more Personnel as members of this Carpool Group. (A person can only belong to one Carpool Group at a time.) NOTE: You can select multiple Personnel at one time. Once you have made your selection, the system enters the Personnel in the **Objects in Group** table—one person to a row.
Remove	Click this button to remove a selected row from the **Objects in Group** table. You must click the row selector ▸ to select a row to remove. If **no** row is selected, this button is **not** available.
Name	The name of the person who is a member of this Carpool Group.
Description	Enter a description of the person, up to 500 characters.

Carpool Group Editor Tasks

You use the Carpool Group Editor General tab to accomplish the tasks listed below, needed to configure a Carpool Group. The procedural steps for each task are detailed in the following subsections.

- Configuring a Carpool Group on Page 103.
- Deleting a Person from a Carpool Group on Page 104.

Configuring a Carpool Group

To Create a Carpool Group

1. In the Navigation Pane of the Administration Workstation, click the **Areas and Zones** pane button.
2. Click the **Areas and Zones** drop-down list and select **Carpool Group**.
3. Click **New** to create a new Carpool Group. The **Carpool Group Editor** opens with **Personnel** displaying as the default **Group Type** (see Figure 15 on Page 102).
4. Click **Add** in the **Objects in Group** box.

   A **Name Selection** dialog box opens for you to select the Personnel you want for this Carpool Group.
5. Click the check box next to names of one or more persons and then click **OK**.
6. The **Carpool Group Editor** displays with the Personnel you selected added to the **Objects in Group** table.
7. To save your new Carpool Group, click **Save and Close**.

   - or -

   Alternatively, if you want to save the Carpool Group and then create a new one, click **Save and New**. The current Carpool Group is saved and closed, but the **Carpool Group Editor** remains open ready for you to configure a new Carpool Group.

Deleting a Person from a Carpool Group

To Delete a Carpool Group

1. On the **Carpool Group Editor**, click anywhere on a person row to select it.
2. Click **Remove** to delete the person from the Group.

Configuring iSTAR Clusters for APB Comm Fail Modes and Global Anti-passback

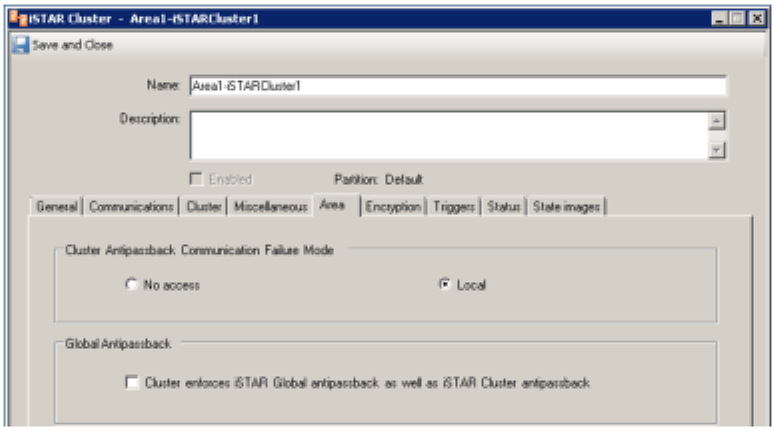
On the **Area** tab of the **iSTAR Cluster Editor**, as shown in Figure 16 on Page 105, you can configure the following:

- How Cluster Antipassback works during a communications failure when the Cluster members lose communication with the Cluster master. See To Configure Cluster Antipassback Communications Failure Mode on Page 107.
- Whether or not the Cluster is configured for both Global Antipassback and Cluster Antipassback or solely for Cluster Antipassback. See To Configure the Cluster for both Global Antipassback and Cluster Antipassback on Page 107.

NOTE Modifying either of these options can only be done if the Cluster is **not** Enabled.

(You configure how Global Antipassback works during communications failure with a system variable in the iSTAR Driver section, iSTAR Global Antipassback Communication Failure Mode. See To Configure Cluster Antipassback Communications Failure Mode on Page 107.)

Figure 16: iSTAR Cluster Editor – Area Tab



iSTAR Cluster - Area1-iSTARCluster1

Name: Area1-iSTARCluster1

Description:

□ Enabled

Partition: Default

Cluster Antipassback Communication Failure Mode

○ No access

● Local

Global Antipassback

□ Cluster enforces iSTAR Global antipassback as well as iSTAR Cluster antipassback

Cluster Antipassback Communications Failure Mode

During a communications failure, the Cluster members (the Controllers) begin to enforce antipassback locally, based on the Failure Mode you configure for the Cluster. By default the **No Access** option is cleared (not set), while the **Local** option is selected (set).

NOTE A Cluster that has an Alternate Master configured supports only **Local** Failure Mode. Consequently, once a secondary Controller is selected for the Cluster, **No access** Mode is unavailable.

Global Antipassback for the Cluster

iSTAR Global Antipassback gives a higher level of security, but also means that when a person's card moves from one Cluster to another, it must be transferred through the Host. Transfer through the Host is slower than within a Cluster. It also requires Cluster to Host network connections to be good. Access within a Cluster is faster: it only relies on member-to-master network connections. (Alternate masters are **not** supported in Global Antipassback Clusters.)

By default the **Cluster enforces iSTAR Global antipassback as well as iSTAR Cluster antipassback** check box is **not** selected, indicating that **only** Cluster Antipassback is enforced for the Area. In addition, the systems upgraded from previous versions of C•CURE 9000 set all Clusters with this default value.

The value of this check box must be compatible with the Area type of all Areas on all the Doors on all the Controllers in the Cluster as shown in Table 23 on Page 106.

Table 23: Cluster/Area Type Compatibility

Cluster enforces:	All areas on all doors on all Cluster's panels must have type:
iSTAR Cluster Antipassback **Only**	Cluster
iSTAR Cluster **AND** Global Antipassback	Cluster **OR** Cross-Cluster

Anytime you change this check box, you must check all the Areas on all the Doors on all the Cluster's Controllers. If there is an incompatibility, the system displays an error message and does not allow the change until the Areas in question are removed from the Doors. You must perform the same check every time an iSTAR is added to a Cluster since the iSTAR might already have Areas attached.

Area Tab Field Definitions

The **Area** tab has the fields shown in Table 24 on Page 106.

Table 24: iSTAR Cluster Editor — Area Tab Fields

Fields	Description
Cluster Antipassback Communication Failure Mode The options in this box are available only if the **Cluster enforces iSTAR Global antipassback as well as iSTAR Cluster antipassback** option in the **Global Antipassback** box is **not** selected.	
No access	Select this option to configure **No access** as the Communications Failure mode for this Cluster. • Access is denied by any member Controller in the Cluster in communications failure. • Member Controllers still in communications with the Master continue to request normal antipassback decisions for entry to the Area. • Master Controllers need no communication to make antipassback decisions and always do so regardless of host or member communication. (In this mode, the person is presumed to be **in violation**, unless proven otherwise.) NOTE: This mode is **unavailable** if the Cluster has an Alternate Master.
Local	Select this option to configure **Local** as the Communications Failure mode for this Cluster. • The Controller uses locally available information to grant or deny access. Even if this information is insufficient, the Controller admits the person presenting the card. (In this mode, the person is presumed **not-in-violation**, unless proven otherwise.) When **Local** mode is configured, the person is allowed in unless the Controllers making the decision determine beyond doubt that he/she is guilty of an antipassback violation.

iSTAR Cluster Editor — Area Tab Fields (continued)

Fields	Description
Global Antipassback	
Cluster enforces iSTAR Global antipassback as well as iSTAR Cluster antipassback	Select this check box to indicate that this Cluster shares data with all the other Clusters that use iSTAR Global Antipassback. The default is cleared indicating that the Cluster does not share data with any other Clusters. NOTE: When this option is selected, the **Cluster Antipassback Communication Failure** Mode box options become unavailable.

To Configure Cluster Antipassback Communications Failure Mode

1. In the Navigation Pane of the Administration Workstation, click the **Hardware** pane button.
2. Click the **Hardware** drop-down list, select **iSTAR Cluster**, and click ➡ ▾ to open a Dynamic View showing a list of all existing iSTAR Clusters.

   - or -

   Expand the Hardware Tree.
3. In the Dynamic View list/Tree, select the iSTAR Cluster for which you want to set the Antipassback Communications Failure Mode, right-click, and click **Edit** from the context menu that appears.
4. On the **iSTAR Cluster Editor**, click to open the **Area** Tab.
5. In the **Cluster Antipassback Communication Failure Mode** box, click to select either the **No access** or **Local** option.

To Configure the Cluster for both Global Antipassback and Cluster Antipassback

1. In the Navigation Pane of the Administration Workstation, click the **Hardware** pane button.
2. Click the **Hardware** drop-down list, select **iSTAR Cluster**, and click ➡ ▾ to open a Dynamic View showing a list of all existing iSTAR Clusters.

   - or -

   Expand the Hardware Tree.
3. In the Dynamic View list/Tree, select the iSTAR Cluster that you want to configure and click **Edit** from the context menu that appears.
4. On the **iSTAR Cluster Editor**, click to open the **Area** Tab.
5. In the **Global Antipassback** box, click to select the **Cluster enforces iSTAR Global antipassback as well as iSTAR Cluster antipassback** option.

To Configure Global Antipassback Communications Failure Mode

1. In the Administration Station, on the Options & Tools pane, select **System Variables**.
2. On the **General** tab, expand the **iSTAR Driver** category.
3. In the **Name** column, locate the **iSTAR Global Antipassback Communication Failure Mode** system variable.

4. Double-click on the row.

   - or -

   Right-click in the row and then click **Edit** from the Context menu that appears.

   The **System Variables** Editor appears with the **Global Antipassback Communication Failure Mode** system variable on the **iSTAR Variables** tab.

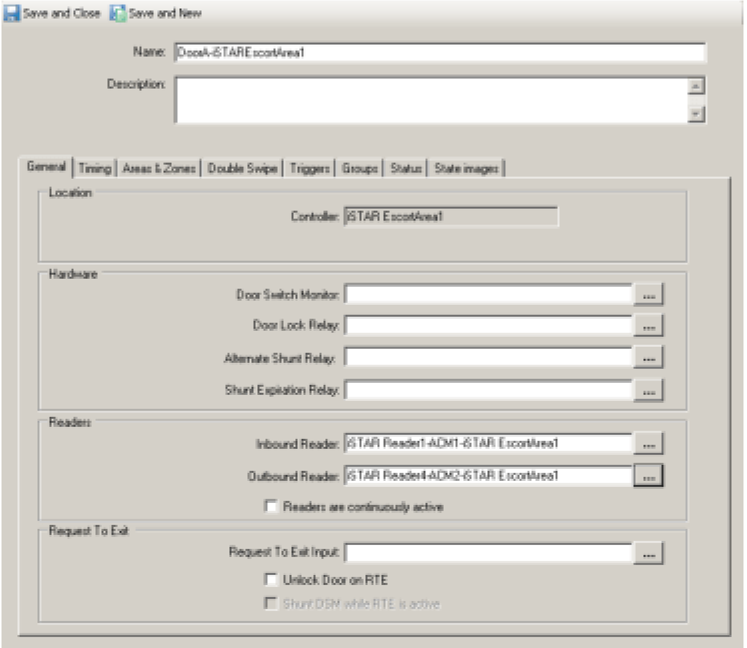
5. Click the down-arrow in the **Mode** field to display the drop-down. Select one of the following:

   - **No Access** – Non-owners do not admit unless they can communicate with the iSTAR owner Controller. (Sets the variable to 0.)
   - **Local** – iSTAR Controllers make a decision based on locally available information or admit if that information is insufficient. (Sets the variable to 1.)

Configuring Escorted Access Mode

The mode that Escorted Access operates in—whether Companion mode or Remote Escort (Turnstile) mode—requires the correct setting of the **Readers are continuously active** check box in the Readers box on the iSTAR Door Configuration dialog box, as shown in Figure 17 on Page 109.

Figure 17: iSTAR Door Configuration Dialog Box – General Tab



Name: DoorA-iSTAREscortArea1

Description:

Controller: iSTAR EscortArea1

Door Switch Monitor:

Door Lock Relay:

Alternate Shunt Relay:

Shunt Expiration Relay:

Inbound Reader: iSTAR Reader1-ACM1-iSTAR EscortArea1

Outbound Reader: iSTAR Reader4-ACM2-iSTAR EscortArea1

☐ Readers are continuously active

Request To Exit Input:

☐ Unlock Door on RTE

☐ Shunt DSM while RTE is active

By default the **Readers are continuously active** option is cleared (not set).

In **Companion Mode** – Doors must be configured to permit multiple accesses through the Door on each access cycle. In this way an Escort can provide access to multiple Escorted Visitors with one swipe of the Escort's card.

In **Remote Access Mode** – Doors must be configured to disable access of more than one person on one access cycle. The system will then accept and process only one card on each side of the Door at a time: first an Escorted Visitor, then the Escort, then another Escorted Visitor, then the Escort, etc.

To Configure the Mode for Escorted Access

1. In the Navigation Pane of the Administration Workstation, click the **Hardware** pane button.
2. Click the **Hardware** drop-down list, select **iSTAR Door**, and click ➔ ▾ to open a Dynamic View showing a list of all existing iSTAR Doors.

   - or -

   Expand the Hardware Tree.
3. In the Dynamic View list/Tree, select the iSTAR Door for which you want to set the Escorted Access mode, right-click, and click **Edit** from the context menu that appears.

4. On the **iSTAR Door Editor** in the **Readers** box:
   - To configure Companion mode, click to select the **Readers are continuously active** option.
   - To configure Remote Access mode, clear the **Readers are continuously active** option.

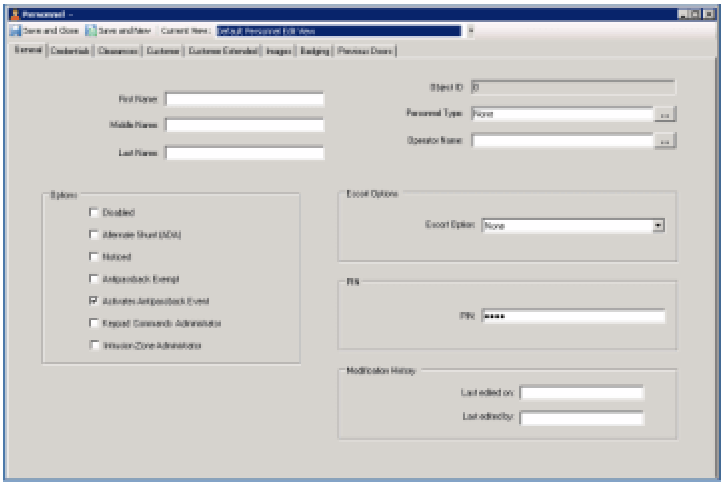
Configuring Personnel Antipassback Options

You can configure a person to be exempt from antipassback rules (both regular and timed) for all Areas so that he/she is permitted entry to/exit from an antipassback Area regardless of a violation. In such cases, no violation message are generated/logged, but access activity is logged as usual.

In addition, you can specify that a person activate antipassback events, whether or not he/she is antipassback exempt, if the access/exit would ordinarily cause a violation.

You configure these options in the **Options** box on the **Personnel Editor General** tab, shown in Figure 18 on Page 111. By default the **Antipassback Exempt** option is cleared (not set), while the **Activate Antipassback Event** option is selected (set).

Figure 18: Personnel Editor General Tab



Personnel -

Save and Close | Save and New | Current View: Default Personnel Edit View

General | Credentials | Clearances | Customer | Customer Extended | Images | Badging | Previous Doors

First Name:

Middle Name:

Last Name:

Object ID: 0

Personnel Type: None

Operator Name:

Options

□ Disabled

□ Alternate Shunt (ADA)

□ Noticed

□ Antipassback Exempt

☑ Activate Antipassback Event

□ Keypad Commands Administrator

□ Intrusion Zone Administrator

Escort Options

Escort Option: None

PIN

PIN: ****

Modification History

Last edited on:

Last edited by:

To Configure a Person To Be Antipassback Exempt

1. In the Navigation Pane of the Administration Workstation, click the **Personnel** pane button.
2. Click the **Personnel** drop-down list and select **Personnel**.
3. Click **New** to create a new Personnel record.

   - or -

   Click to open a Dynamic View showing a list of all existing Personnel Objects, right-click the Personnel record you want to change, and click **Edit** from the context menu that appears.

   The **Personnel Editor** opens with the **General** Tab displayed.
4. In the **Options** box, click to select the **Antipassback Exempt** option.
5. To save the Personnel record, click **Save and Close**.

To Configure a Person To Always Activate Antipassback Events

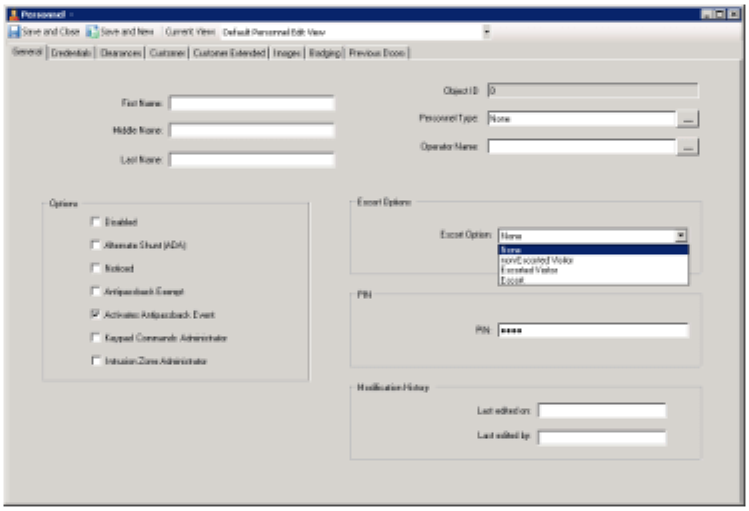
1. Open a Personnel Record on the **Personnel Editor General** Tab.
2. In the **Options** box, click to select the **Activate Antipassback Event** option.
3. To save the Personnel record, click **Save and Close**.

Configuring Personnel Escorted Access Options

You can configure a person's Escort option—None, Non-escorted Visitor, Escorted Visitor, Escort—which controls how he/she is able to move around a facility, through its Doors and into and out of Areas.

You configure this option in the **Escort Options** box on the **Personnel Editor General** tab, as shown in Figure 19 on Page 112. By default the **Escort Option** combo box is set to **None**.

Figure 19: Personnel Editor General Tab – with Escort Options Box



Personnel

Save and Close | Save and New | Current View: Default Personnel Edit View

General | Credentials | Clearances | Customer | Customer Extended | Images | Badging | Previous Doors

First Name:

Middle Name:

Last Name:

Object ID: 0

Personnel Type: None

Operator Name:

Options

- ☐ Disabled
- ☐ Alternate Shunt (ADA)
- ☐ Noticed
- ☐ Antipassback Exempt
- ☑ Activates Antipassback Event
- ☐ Keypad Commands Administrator
- ☐ Intrusion Zone Administrator

Escort Options

Escort Option: None

- None
- nonEscorted Visitor
- Escorted Visitor
- Escort

PIN

PIN: ••••

Modification History

Last edited on:

Last edited by:

To Configure a Person's Escort Option

1. Click the **Personnel** drop-down list and select **Personnel**.
2. Click **New** to create a new Personnel record.

   - or -

   Click ➔ ▾ to open a Dynamic View showing a list of all existing Personnel Objects, right-click the Personnel record you want to change, and click **Edit** from the context menu that appears.

   The **Personnel Editor** opens with the **General** Tab displayed.
3. In the **Escort Options** box, click the down-arrow next to the combo box to select the **Escort Option** you want for this Personnel record:
   - **None** (the default).
   - **Non-escorted Visitor** – A Visitor to the company who is permitted to go through the facility without an Escort.
   - **Escorted Visitor** – A Visitor to the company who must be accompanied by an employee designated as an Escort in order to move through the facility.
   - **Escort** – an Employee trained in using the visitor management policies of the company, who knows what to do in any of the following situations:
     - Escorted Visitor's card fails for clearance.
     - An employee wants to cut in front of or in the middle of the Escorted Visitor queue.

4. To save the Personnel record, click **Save and Close**.

Configuring Event Actions to Affect Areas

You can configure an Event with Actions related to iSTAR Areas.

Example:

> You can reset the current Occupancy Mode for an iSTAR Area—set by default by the original Occupancy configuration. Such an Event Action can change an Area's Occupancy mode to 'Counting Only', which cannot be set by the Area configuration. You can also use an Event Action to clear the Area counts for 'All Personnel' and 'Personnel Groups'.

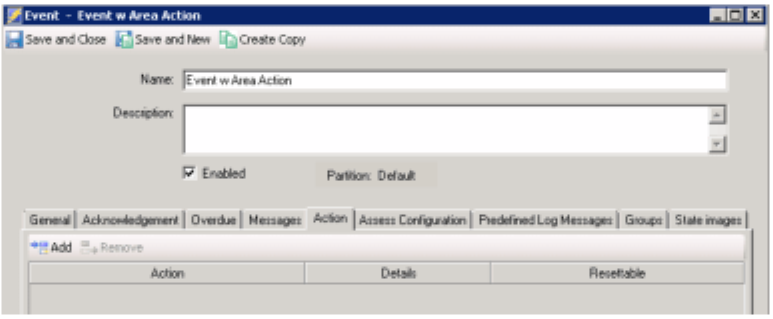
The following Event Actions pertain in some way to Areas:

- Allow Conditional Access Cycle
- Clear Area Counts
- De-muster Area
- Enable Counting for Access Restriction
- Enable Counting for Event
- Enable Counting Only
- Grace All
- Grace All Partitions
- Remove All Personnel from Area

To Configure Events with an Action to Affect an Area

1. Click **Configuration** to open the Configuration pane.
2. Select **Event** from the Configuration Pane drop-down list.
3. Click **New** on the **Configuration** Pane. The **Event Editor** opens.
   a. Type a name for this **Event** in the **Name** field.
   b. Type a **Description** in the **Description** field.
   c. Click **Enabled** to make the Event available to C•CURE 9000 Operators.
4. On the Event **General** tab, choose the settings that you want for the Event.
5. Click the **Action** tab to open, as shown in Figure 20 on Page 114.

Figure 20: Event Editor – Action Tab



Event - Event w Area Action

Name: Event w Area Action

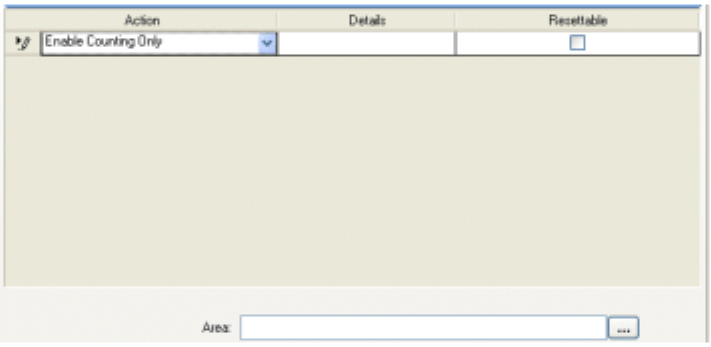
Description:

☑ Enabled

Partition: Default

6. On the **Action** tab, click **Add** to add an Action row.
7. Click the down-arrow in the **Action** field and then scroll down in the drop-down list to select the Action you want.

   An **Area**, **Partition**, or **Carpool Group** field displays on the bottom of the screen depending on the Action, as shown in the following example.

Action	Details	Resettable
Enable Counting Only		□

   Area:

   (For the **Grace All** and **Grace All Partitions** Actions, the **Partition** field displays, while the **Area** field displays for all the other Actions.

8. Click ... in the **Area** or **Partition** field to display a selection list of all Areas or Partitions currently configured in the C•CURE 9000 system, and then click to select the one you want as the recipient of the Action.

   The system enters the name of the object you select in the **Details** field for the row.
9. Select the **Resettable** check box if you want an operator responding to the Event to be able to reset the Action without acknowledging the Event.

Setting System Variables That Affect Areas

Four System Variables described in Table 25 on Page 116 have an impact on Areas functionality.

Table 25: System Variables that Affect Schedules

Category/ System Variable	Description	Default Setting
Hardware Driver		
Next Card Time	Maximum length of time (in seconds) allowed between card presentations for features that require the presentation of multiple cards for access (Escorted Visitor Access or into/out of Minimum Occupancy Areas, for example). The value must be between 15 and 300. NOTE: Software House recommends setting this value to at least 30 seconds if cardholders need time to present a card with biometric and/or PIN information.	15
iSTAR Driver		
Always Track Personnel	If **True**, the Area location of Personnel is **always** tracked at the Controller/Panel. If **False**, the Area location of Personnel is **not** tracked at the Controller/Panel, unless Antipassback is configured.	False
Minimum Occupancy Exit Option	Enables personnel to exit an Area configured for restricted Minimum Occupancy if the iSTAR resets, which will reset the Area count to 0 (zero). If **True**, the iSTAR permits the personnel inside the Area to exit. If **False**, the iSTAR does not permit the personnel inside the Area to exit, unless the Area count is reset correctly. In either case, the Area may have an incorrect count that should be reset manually	False
Maximum Visitor Count	Indicates the maximum number of Escorted Visitors who may be escorted by a single designated Escort. The value must be between 0 and 100. NOTE: You must stop and restart the iSTAR driver to have any changes you make to this variable take effect.	10
iSTAR APB maximum ping round trip	Number of milliseconds ping response must arrive after ping sent for APB link to be declared “fast” again. Must be larger than minimum time required for a round trip message over link during normal utilization of network; otherwise comm **cannot** be restored. Must be larger than 250. The value must be between 250 and 1800000. NOTE: Change this value **only** in consultation with the Software House Customer Support Center. **Incorrect settings can cause APB comm fail**.	500
iSTAR APB ping interval	Number of milliseconds iSTAR and host wait before sending APB ping on “slow” APB link (to master or host). This is also the minimum amount of time the iSTAR and host will wait before attempting to re-establish APB comm over a link that has timed out. The value must be between 1000 and 600000. NOTE: Change this value **only** in consultation with the Software House Customer Support Center. **Incorrect settings can cause APB comm fail**.	10000

System Variables that Affect Schedules (continued)

Category/ System Variable	Description	Default Setting
iSTAR APB response timeout	Number of milliseconds iSTAR member waits for APB response from master. This is the amount of time a person will see "Please Wait" displayed at the Reader. Must be larger than minimum time required for 3 round-trip messages over link during normal utilization of network; otherwise comm **cannot** be restored. Must be larger than 1000. The value must be between 1000 and 600000. NOTE: Change this value **only** in consultation with the Software House Customer Support Center. **Incorrect settings can cause APB comm fail**.	5000
iSTAR Global Antipassback Communication Failure Mode	Global Antipassback operation when the controllers are in communication failure mode. Double-click on row to edit. (For procedural information, see To Update System Variables on the System Variables Editor on Page 118and To Configure Global Antipassback Communications Failure Mode on Page 107.) The value must be between 0 and 2. • **No Access** Mode = 0 – Non-owner iSTAR Controllers do not admit unless they can communicate with the iSTAR owner Controller. • **Local** Mode = 1 – iSTAR Controllers make a decision based on locally available information or admit if that information is insufficient.	0
Host Global Antipassback Response Timeout	Number of milliseconds iSTAR master waits for Global Antipassback response from iSTAR . • Must be less than 'iSTAR Global Antipassback response timeout'. • Must be larger than minimum time required for a round trip message over link during normal utilization of network. Otherwise, communications cannot be restored. • Must be larger than 1000. The value must be between 1000 and 60, 000. NOTE: Change this value **only** in consultation with the Software House Customer Support Center. **Incorrect settings can cause APB comm fail**.	2000
iSTAR Global Antipassback Response Timeout	Number of milliseconds iSTAR master waits for Global Antipassback response from Host. • Must be less than 'iSTAR APB response timeout'. • Must be larger than minimum time required for 2 round trip messages over link during normal utilization of network. Otherwise, communications cannot be restored. • Must be larger than 1000. The value must be between 1000 and 60, 000. NOTE: Change this value **only** in consultation with the Software House Customer Support Center. **Incorrect settings can cause APB comm fail**.	4000

To Change the Value for an Area-related System Variable

1. In the Administration Station, on the Options & Tools pane, select **System Variables**.
2. On the **General** tab, expand the Hardware or iSTAR Driver category, as needed.
3. In the **Name** column, locate the system variable you want to update.
4. Read the text in the **Description** column for the relevant system variable.
   - If the text says, "Double-click on row to edit", see To Update System Variables on the System Variables Editor on Page 118.

5. In the **Value** column, enter a new value.
6. If necessary, stop and restart the drivers to have your changes take effect.

   For a list of variables and allowable values in this category, see Table 25 on Page 116.

To Update System Variables on the System Variables Editor

1. To update a system variable when the **Description** column for the relevant system variable says, “Double-click on row to edit”:

   Double-click on the row.

   - or -

   Right-click in the row and then click **Edit** from the Context menu that appears.

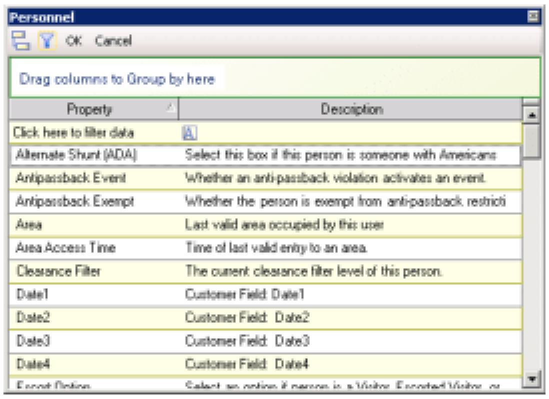
   The **System Variables** Editor appears with the system variable on the **iSTAR Variables** tab.
2. Change the values in these fields as necessary.
3. Click **Save and Close** when you are finished editing the system variables.

Viewing Area Location of Personnel

You can view the current Area that Personnel are in by opening the default Dynamic View for Personnel records on the Administration application.

To View a Person's Current Area

1. In the Navigation Pane of the Administration Workstation, click the **Personnel** pane button.
2. Select **Personnel** from the Personnel pane drop-down list.
3. Click to open a Dynamic View listing all Personnel objects. (You can also click the down-arrow of this button to either view the list in the current tabbed view or open a new tabbed view.)
   - You can sort, filter, and group items in the list.
   - You can right-click a Personnel record in the list to open the context menu (for information, see the Personnel chapter in the *C•CURE 9000 Personnel Guide*) and perform any of the functions on that menu. See the Dynamic Views chapter in the *C•CURE 9000 Data Views Guide* for more information on using Dynamic Views.
4. Right-click any column heading to open the context menu with additional Personnel fields that can display as columns.
5. Click **More Columns** to open a dialog box listing all the other possible Personnel fields that can display as columns.

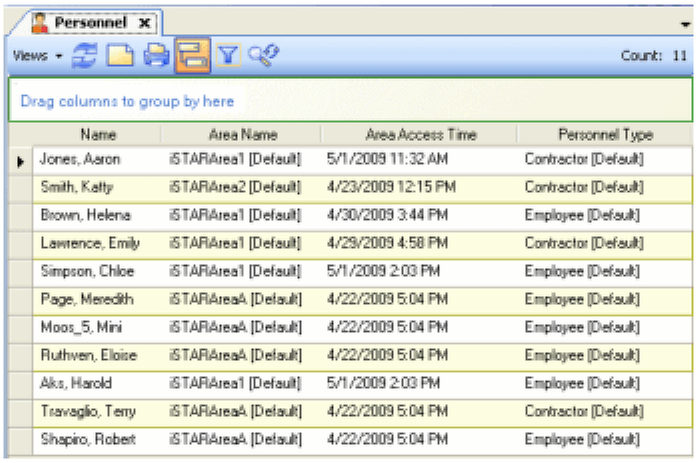


Property	Description
Click here to filter data	
Alternate Shunt (ADA)	Select this box if this person is someone with Americans
Antipassback Event	Whether an anti-passback violation activates an event.
Antipassback Exempt	Whether the person is exempt from anti-passback restricti
Area	Last valid area occupied by this user
Area Access Time	Time of last valid entry to an area.
Clearance Filter	The current clearance filter level of this person.
Date1	Customer Field: Date1
Date2	Customer Field: Date2
Date3	Customer Field: Date3
Date4	Customer Field: Date4
Escort Option	Select an option if person is a Visitor, Escorted Visitor, or

6. Select **Area Name** and **Area Access Time** from the list and click **OK** on the top of the dialog box.

   The Personnel Dynamic View now includes a column for **Area Name** and **Area Access Time** populated with the current location for each person in the list and the time he/she entered the Area, as shown in Figure 21 on Page 120.

Figure 21: Personnel Dynamic View with Area Location



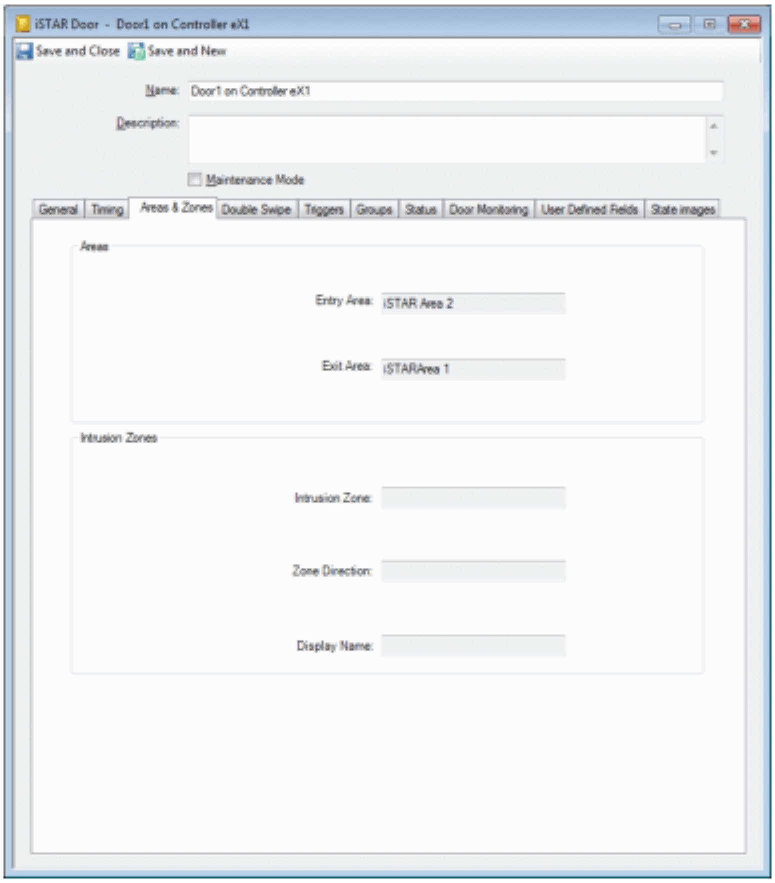
Name	Area Name	Area Access Time	Personnel Type
Jones, Aaron	iSTARArea1 [Default]	5/1/2009 11:32 AM	Contractor [Default]
Smith, Katty	iSTARArea2 [Default]	4/23/2009 12:15 PM	Contractor [Default]
Brown, Helena	iSTARArea1 [Default]	4/30/2009 3:44 PM	Employee [Default]
Lawrence, Emily	iSTARArea1 [Default]	4/29/2009 4:58 PM	Contractor [Default]
Simpson, Chloe	iSTARArea1 [Default]	5/1/2009 2:03 PM	Employee [Default]
Page, Meredith	iSTARAreaA [Default]	4/22/2009 5:04 PM	Employee [Default]
Moos_5, Mini	iSTARAreaA [Default]	4/22/2009 5:04 PM	Employee [Default]
Ruthven, Eloise	iSTARAreaA [Default]	4/22/2009 5:04 PM	Employee [Default]
Aks, Harold	iSTARArea1 [Default]	5/1/2009 2:03 PM	Employee [Default]
Travaglio, Terry	iSTARAreaA [Default]	4/22/2009 5:04 PM	Contractor [Default]
Shapiro, Robert	iSTARAreaA [Default]	4/22/2009 5:04 PM	Employee [Default]

Viewing Area Information on the Door Editor

A Door assigned to an iSTAR Area displays read-only assignment information on the **Door Editor** on the **Areas & Zones** tab, as shown in Figure 22 on Page 121.

NOTE If this Door is **not** assigned to an Area, the **Areas** box is blank.

Figure 22: Door Editor — Areas & Zones Tab



Name: Door1 on Controller eX1

Entry Area: iSTAR Area 2

Exit Area: iSTARArea 1

The **Areas & Zones** tab has the read-only fields shown in Table 26 on Page 121.

Table 26: Door Editor — Areas & Zones Tab Fields

Fields	Description
Entry Area	Name of Area to which this Door is an 'Access In' Door.
Exit Area	Name of Area to which this Door is an 'Access Out' Door.

To View a Door's Area Information

1. In the Navigation Pane of the Administration Workstation, click the **Hardware** pane button.
2. Expand the Hardware Tree and navigate to the iSTAR Door whose information you want to view.

3. Select the Door and right-click to display the context menu.
4. Click **Edit**.
5. When the **iSTAR Door Editor** appears, click to open the **Areas & Zones** Tab and review the Area information.

Running Area Pre-defined Reports

C•CURE 9000 allows you to generate Software House pre-defined Reports with information related to Areas:

- **Roll Call Report** (SWH20 - Roll Call) – gives a view of where personnel are located at the time the report is started, the iSTAR Area/iSTAR Area Group, and can assist in the emergency evacuations of buildings.

  C•CURE 9000 tracks the current location, or iSTAR Area, of all Personnel as they move through Doors controlled by access Readers. This tracking is independent of the antipassback restrictions of an Area, so antipassback does not have to be enforced for Roll Call Reports to be used.

  iSTAR Area Groups, which can contain one or more iSTAR Areas, also support the generation of Roll Call Reports (with the exception of the system default "All Areas" Group). An iSTAR Area may be assigned to several iSTAR Area groups; the Areas assigned to an iSTAR Area Group may also span multiple iSTAR Controllers. For information on iSTAR Area Groups, see the Groups chapter in the *C•CURE 9000 Data Views Guide*.
- **Carpool Roll Call Report** (SWH21 - Carpool Area Roll Call) – gives the last known Carpool Area for Personnel, by Carpool Group, at the time the report is started. This is the last Carpool Area that the person entered. However, if they exited to an adjacent Area **not** a Carpool Area, their Carpool Area location is **not** changed.

  C•CURE 9000 tracks the current location of all Personnel parked in each Carpool Area, along with their Carpool Group and whether they are the Group Driver.
- **Carpool Group Report** (SWH22 - Carpool Group) – gives a list of Carpool Groups with the names of the corresponding Personnel members.
- **Visitor/Escort Reports** (SWH50 - SWH55) – give lists of Admitted/Rejected Escorts and/or Visitors. For detailed information about these Reports, see the table in the "Pre-defined Reports" section of Appendix A in the *C•CURE 9000 Data Views Guide*.

NOTE These are some of the many pre-defined Reports provided by Software House. While you **cannot** alter the original Report, you can make a copy and then modify it to your liking. For information, see Appendix A in the *C•CURE 9000 Data Views Guide*.

These Reports can be initiated in different ways:

- Running Area Reports from the Administration Report Dynamic View on Page 123.
- Running Area Reports from the Monitoring Station Report Status List on Page 125
- Using an Event to Run an Area Report on Page 126

Running Area Reports from the Administration Report Dynamic View

This procedure for running Area Reports uses the Roll Call Report as an example for all the Area-related Reports.

To Run an Area Report from the Report Dynamic View

1. In the Navigation Pane of the Administration Workstation, click the **Data Views** pane button.
2. Click the **Data Views** drop-down list and select **Report**.
3. Click ➡ ▾ to open a Dynamic View listing all Reports, both the Software House pre-defined Reports and Reports you've created. (You can also click the down-arrow of this button to either view the list in the current tabbed view or open a new tabbed view.)

4. Use the right-hand scroll bar to scroll through the list and find one of the Area Reports, such as SWH20 - Roll Call or SWH21 - Carpool Roll Call.
5. Double-click the Report to run it as a new tab in the C•CURE 9000 content area.

   - or -

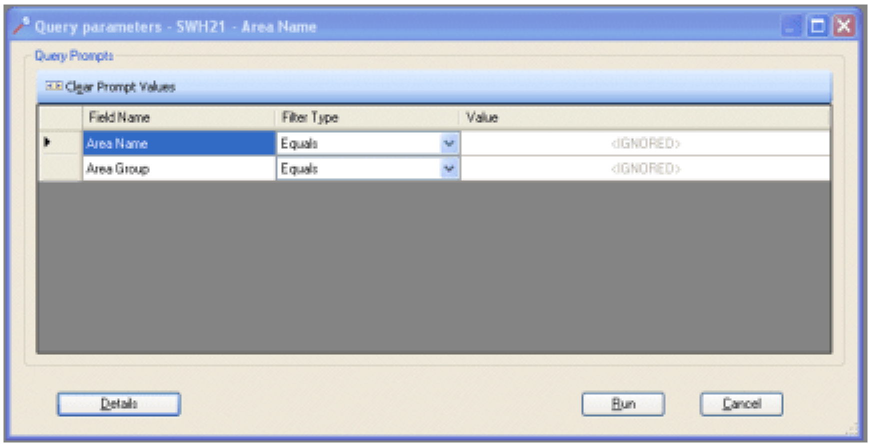
   Right-click the Report to open the Report Context menu and take one of the following actions:

   - Click **View** to run the Report as a new tab in the C•CURE 9000 content area.
   - Click **Popup View** to run the Report and view it in a separate popup window.
   - Click **View in Current Tab** to run the Report in the current tab in the C•CURE 9000 content area (replacing the Reports Dynamic View).
   - Click **Run on Server** to start the Report running in the back ground. (The finished report is saved and is accessible from the Report Result Dynamic View.)

NOTE A system variable in the Reporting category allows you to set limits on the maximum page count of the reports generated in your C•CURE 9000 system. For information, see the System Variables chapter in the C•*CURE 9000 System Maintenance Guide*.

A **Query Parameters** dialog box appears, as shown in the example for the Roll Report in Figure 23 on Page 124. (For more information about queries, see the Query chapter in the C•*CURE 9000 Data Views Guide*.)

Figure 23: Roll Call Report Query Parameters Dialog Box



Field Name	Filter Type	Value
Area Name	Equals	<IGNORED>
Area Group	Equals	<IGNORED>

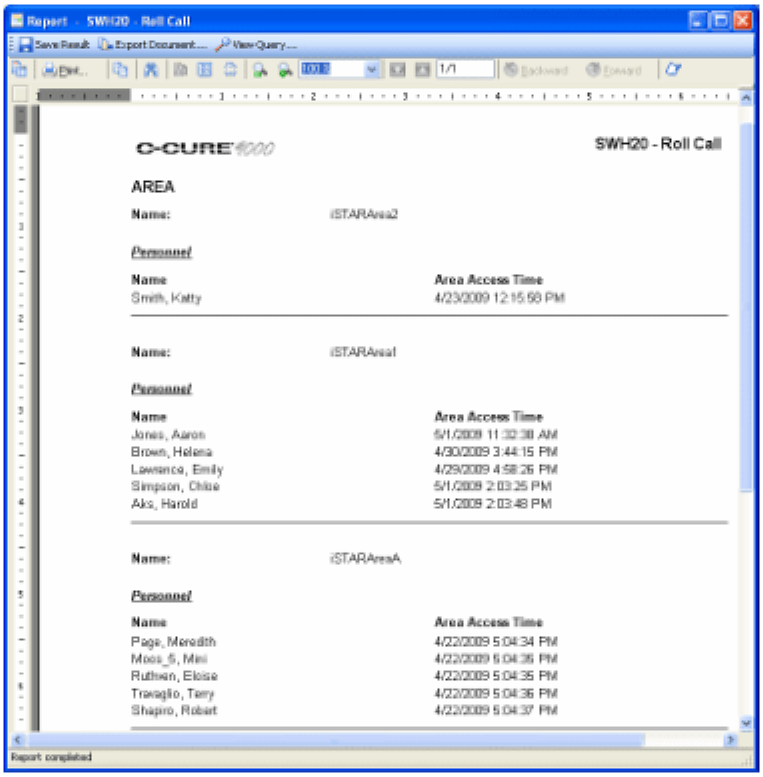
6. To view all the information about the query's search criteria, click **Show Query Detail**.
7. Enter values for the **Area Name** and/or **Area Group** parameters and then click **Execute Query** to retrieve data for the Report.

   The progress of the report generation displays on the Status bar.

   Once the status bar shows the number of records being processed, a **Cancel Report** button on the top of the screen becomes available for use.

   When the report processing is completed, the Roll Call Report appears on the **Report Viewer**, as shown in the example in Figure 24 on Page 125. The **Cancel Report** button disappears and the **Save Result** and **Export Document** buttons become available.

Figure 24: Roll Call Report on Report Viewer



C-CURE 9000

SWH20 - Roll Call

AREA

Name: iSTARArea2

Personnel

Name	**Area Access Time**
Smith, Katty	4/23/2009 12:15:58 PM

Name: iSTARArea1

Personnel

Name	**Area Access Time**
Jones, Aaron	5/1/2009 11:32:38 AM
Brown, Helena	4/30/2009 3:44:15 PM
Lawrence, Emily	4/29/2009 4:58:26 PM
Simpson, Chloe	5/1/2009 2:03:25 PM
Aks, Harold	5/1/2009 2:03:48 PM

Name: iSTARAreaA

Personnel

Name	**Area Access Time**
Page, Meredith	4/22/2009 5:04:34 PM
Moss_5, Mini	4/22/2009 5:04:35 PM
Ruthven, Eloise	4/22/2009 5:04:35 PM
Traviaglio, Terry	4/22/2009 5:04:36 PM
Shapiro, Robert	4/22/2009 5:04:37 PM

Running Area Reports from the Monitoring Station Report Status List

This procedure for running Area Reports uses the Roll Call Report as an example for all the Area-related Reports.

To Run an Area Report from the Monitoring Station

1. On the Explorer Bar of the Monitoring Station, click **Reports** in the **Non Hardware Status** Menu.

   The **Report Status List** dialog box opens with a list of all Reports in the system, both the Software House canned Reports and Reports you've created.

2. Click the **Data Views** drop-down list and select **Report**.

3. Use the right-hand scroll bar to scroll down through the list and find one of the Roll Call Reports, such as SWH20 - Roll Call or SWH21 - Carpool Roll Call.

4. Right-click the Report to open the Report Context menu and take one of the following actions:
   - Click **Popup View** to run the Report and view it in a separate popup window.
   - Click **Run on Server** to start the Report running in the background. The finished report is saved and is accessible from the Report Result Dynamic View.)

NOTE A system variable in the Reporting category allows you to set limits on the maximum page count of the reports generated in your C•CURE 9000 system. For information, see the System Variables chapter in the C•*CURE 9000 System Maintenance Guide*.

A **Query Parameters** dialog box appears with the appropriate prompts, in this example for the Roll Call Report, as shown in Figure 23 on Page 124. (For more information about queries, see the Query chapter in the *C•CURE 9000 Data Views Guide*.)

5. To view all the information about the query's search criteria, click **Show Query Detail**.
6. Enter values for the **Area Name** and/or **Area Group** parameters and then click **Execute Query** to retrieve data for the Report.

   The progress of the report generation displays on the Status bar.

   Once the status bar shows the number of records being processed, a **Cancel Report** button on the top of the screen becomes available for use.

   When the report processing is completed, the Roll Call Report appears on the **Report Viewer**, as shown in the example in Figure 24 on Page 125.

Using an Event to Run an Area Report

You can configure an Event with an Action that runs an Area Report. For information, see "Scheduling a Report" in the Reports chapter in the *C•CURE 9000 Data Views Guide*.

Gracing Personnel

You can choose to grace Personnel denied access to an Antipassback/Area Lockout/Carpool Area from both the Administration application and the Monitoring Station. The first time personnel use their cards after a grace action, the system does not check for Antipassback violations and also allows them into Areas from which they would otherwise be locked out. For all subsequent use of their cards, the system returns to checking for Antipassback violations and enforcing Area Lockouts.

You can also reset the iSTAR Global Antipassback owner of a person's card when the iSTAR owner is not communicating.

- The following apply to one or more selected persons.
  - Grace Personnel
  - Antipassback Reset Card
  - Area Lockout Grace
  - Grace Carpool Group – applies to all personnel in the group and can be applied in two different ways:
    - To the Carpool Group.
    - To any person who is a member of the Carpool Group
- Grace All – applies to all Personnel and Carpool Groups in one or more selected Partitions. (In an unpartitioned system, since all Security Objects are in the 'Default' Partition, applying **Grace All** to the Default Partition graces all Personnel and all Carpool Groups in the C•CURE 9000.)
- Grace All Partitions – applies to all Personnel and all Carpool Groups in all Partitions in the system—regardless of how many partitions there are.

NOTE

- Grace Carpool Group is a 'timed' grace for which you must enter start/end times. Everyone in the Carpool Group then gets free access to the Carpool Area for that time period. (**And** after the period expires, they get one free access.)
- Grace All and Grace All Partitions, on the other hand, apply a 'one-time' grace for the Carpool that goes away after the first swipe, similar to regular Antipassback gracing.

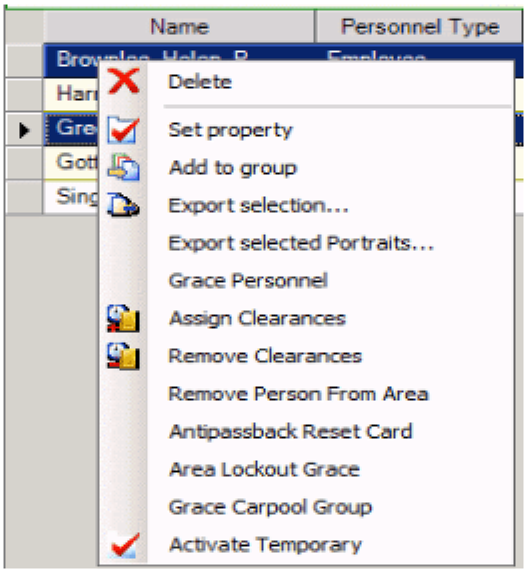
The methods for 'gracing' are as follows:

- Gracing One or More Selected Personnel
  - From the Administration Application – see To Grace Selected Personnel from the Administration Application on Page 128.
  - From the Monitoring Station – see To Grace Selected Personnel from the Monitoring Station on Page 128.
- Gracing All Personnel
  - From the Administration Application – see To Grace 'All' Personnel from the Administration Application on Page 129.
  - From the Monitoring Station – see To Grace 'All' Personnel from All Partitions from the Monitoring Station on Page 130.
  - Using an Event – see To Grace 'All' Personnel Using an Event on Page 130.
- Gracing Personnel from Selected Partitions
  - From the Monitoring Station – see To Grace Personnel from Selected Partitions from the Monitoring Station on Page 131.

To Grace Selected Personnel from the Administration Application

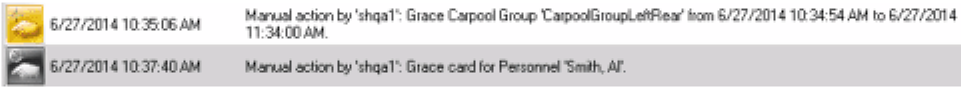
1. In the Navigation Pane of the Administration Workstation, click the **Personnel** pane button.
2. Select **Personnel** from the Personnel pane drop-down list.
3. Click ➡ ▾ to open a Dynamic View listing all Personnel objects, as shown in the examples in Figure 21 on Page 120 and Figure 21 on Page 120. (You can also click the down-arrow of this button to either view the list in the current tabbed view or open a new tabbed view.)
4. Click to select one or more Personnel in the list and then right-click to display the Context menu.

NOTE If you select more than 100 Personnel, the **Grace Personnel**, **Antipassback Reset Card**, **Area Lockout Grace**, and **Grace Carpool Group** selections are **not** available.



5. Click **Grace Personnel**, **Antipassback Reset Card**, **Area Lockout Grace**, or **Grace Carpool Group**.

   The selected Personnel are graced and are displayed on the Monitoring Station Activity Viewer.



6/27/2014 10:35:06 AM	Manual action by 'shqa1': Grace Carpool Group 'CarpoolGroupLeftRear' from 6/27/2014 10:34:54 AM to 6/27/2014 11:34:00 AM.
6/27/2014 10:37:40 AM	Manual action by 'shqa1': Grace card for Personnel 'Smith, Al'.

To Grace Selected Personnel from the Monitoring Station

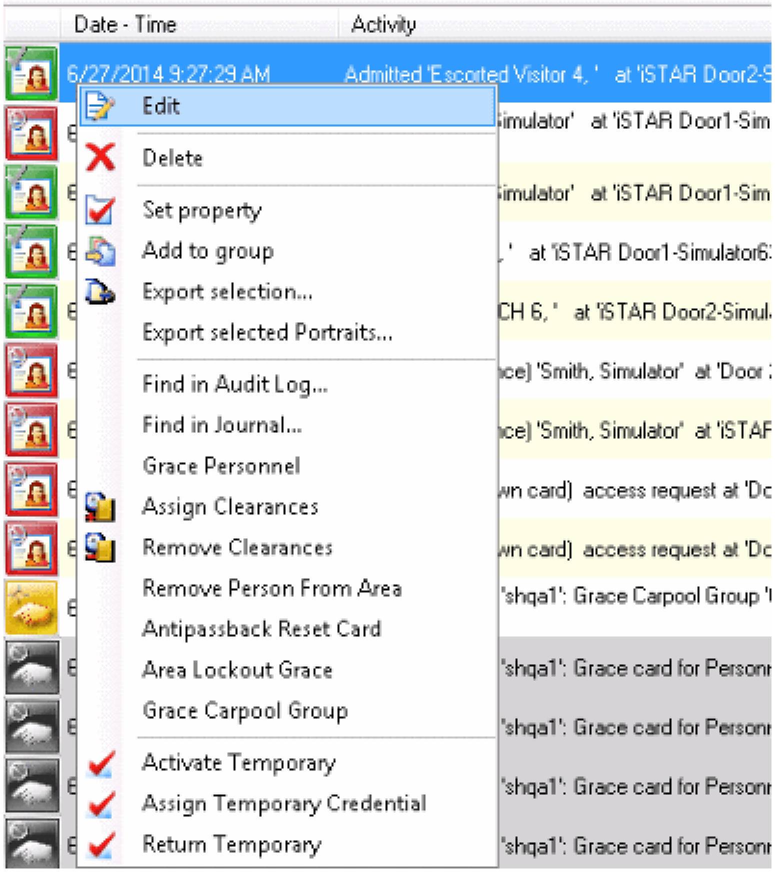
NOTE The look of the Swipe & Show Viewer depends on whether you are using the 'Legacy' View or one of the new 'Default' Views. For information, see "Swipe and Show Viewer" in the Application Layout chapter of the *C•CURE 9000 Software Configuration Guide* and Chapter 6 Monitoring Access in the *C•CURE 9000 Monitoring Station Guide*.

1. Open the **Swipe & Show** Viewer of the Monitoring Station.

   - or -

   On the Monitoring Station **Activity Viewer** in rows showing Personnel accesses, click to select a row, and right-click to display the context menu.

NOTE If you select more than 100 Personnel, the **Grace Personnel**, **Antipassback Reset Card**, **Area Lockout Grace**, and **Grace Carpool Group** selections are **not** available.


Date - Time
Activity
6/27/2014 9:27:29 AM
Admitted 'Escorted Visitor 4, ' at 'iSTAR Door2-S
imulator' at 'iSTAR Door1-Sim
imulator' at 'iSTAR Door1-Sim
' at 'iSTAR Door1-Simulator6
CH 6, ' at 'iSTAR Door2-Simul
ce) 'Smith, Simulator' at 'Door
ce) 'Smith, Simulator' at 'iSTAF
wn card) access request at 'Dc
wn card) access request at 'Dc
'shqa1': Grace Carpool Group '
'shqa1': Grace card for Personn
'shqa1': Grace card for Personn
'shqa1': Grace card for Personn
'shqa1': Grace card for Personn
Edit
Delete
Set property
Add to group
Export selection...
Export selected Portraits...
Find in Audit Log...
Find in Journal...
Grace Personnel
Assign Clearances
Remove Clearances
Remove Person From Area
Antipassback Reset Card
Area Lockout Grace
Grace Carpool Group
Activate Temporary
Assign Temporary Credential
Return Temporary

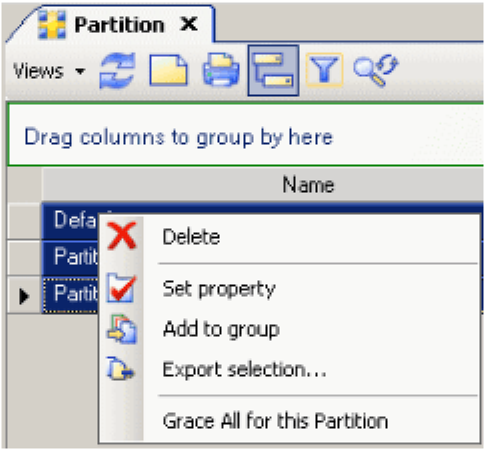
2. Click the **Grace Personnel**, **Antipassback Reset Card**, **Area Lockout Grace**, or **Grace Carpool Group** button on the **Swipe & Show** Viewer.

   - or -

   Click **Grace Personnel**, **APB Reset Card**, **Area Lockout Grace**, or **Grace Carpool Group** on the **Activity Viewer** context menu.

To Grace 'All' Personnel from the Administration Application

1. In the **Navigation** Pane of the Administration Workstation, click the **Configuration** pane button.
2. Select **Partition** from the Configuration pane drop-down list.
3. Click ➔ ▾ to open a Dynamic View with all the Partition Objects your Privileges allow you to see. (You can also click the down-arrow of this button to either view the list in the current tabbed view or open a new tabbed view.)
4. Click to select one, several, or all Partitions in the list and then right-click to display the Context menu.



5. Click **Grace All for this Partition**.

   All the Personnel in the selected Partition(s) are graced. (If the system was **not** partitioned so **only** the Default Partition displayed in the list, or if you selected all the Partitions in the system, the command would grace all system Personnel.)

To Grace 'All' Personnel from All Partitions from the Monitoring Station

1. Open the **Swipe & Show** Viewer of the Monitoring Station and click to open the **Grace Partition** tab.
2. Click the **Grace All Partitions** button.

   All Personnel in all the Partitions in the system are graced—whether there is only one, the Default Partition, or many Partitions.

To Grace 'All' Personnel Using an Event

1. Configure an event with an appropriate name and description according to the information in the Events chapter in the *C•CURE 9000 Software Configuration Guide*.
2. Click to open the Action tab.
3. Click **Add** to create a new Action row.

   a. Click the down-arrow in the **Action** field to display a drop-down list containing available Actions. Use the scroll bar to scroll down to find **Grace All** and click to add it to the row as the Action that will be executed by this Event.

   Once you select **Grace All**, the **Partition** field displays on the bottom of the tab.

   b. Click ... in the **Partition** field to display a selection list of all Partitions currently configured in the C•CURE 9000 system, and then click an Partition to select it.

   When you click anywhere outside the **Partition** field, the system enters the name of the Partition you selected in the **Details** field for the row.

   The Grace All Action will be applied to all Personnel in the selected Partition, Partition A, whenever this Event is activated. (If the system was **not** partitioned, **only** the Default Partition could be selected. In that case, the command would grace all system Personnel.)

   c. Leave the **Resettable** check box unselected. Resetting an Event Action is **not** applicable to a Grace All Action.

4. Finish configuring the other appropriate settings for this Event, remembering to select the **Enabled** check box to activate the Event.

To Grace Personnel from Selected Partitions from the Monitoring Station

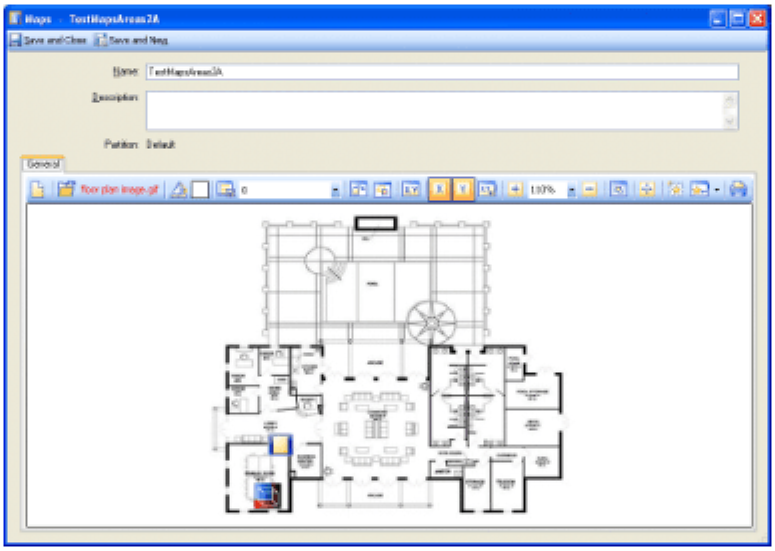
1. Open the **Swipe & Show** Viewer of the Monitoring Station and click to open the **Grace Partition** tab, as shown in on Page 127.
2. Click to select one or more Partitions in the list and then right-click to display the Context menu.
3. Click **Grace All**.

   All the Personnel in the selected Partition, Partition A, are graced. (If the system was **not** partitioned, **only** the Default Partition would display in the list. In that case, the command would grace all system Personnel.)

Viewing Area Status with Map Icons

The **Map Editor** in C•CURE 9000, as shown in the example in Figure 25 on Page 132, lets you display your facility's floor or site plan and place clickable icons that permit you to monitor the state of iSTAR Areas and, if desired, their related Doors.

Figure 25: Map Editor with Area and Door Icons



Name: TestMapsAreas2A

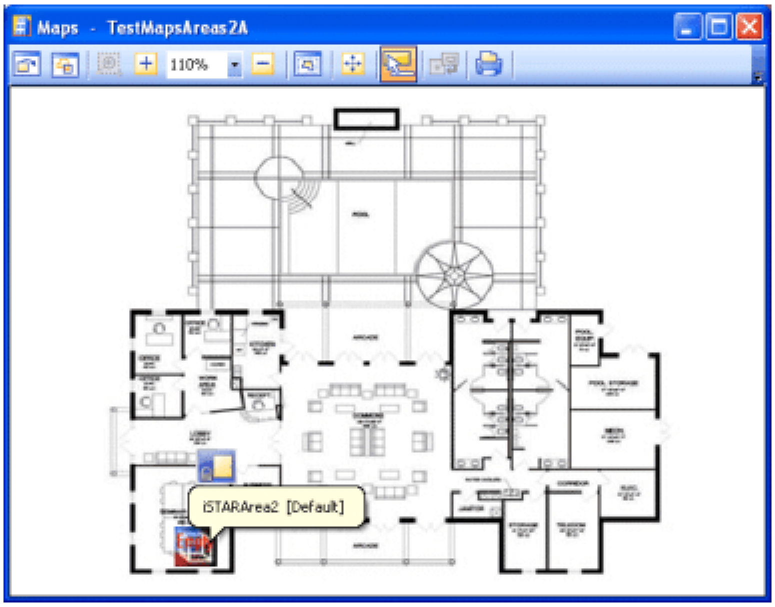
Description:

Partition: Default

For detailed information on creating Maps, see the Maps chapter in the C•*CURE 9000 Data Views Guide* and the "Adding an Object Icon to the Map" section in particular.

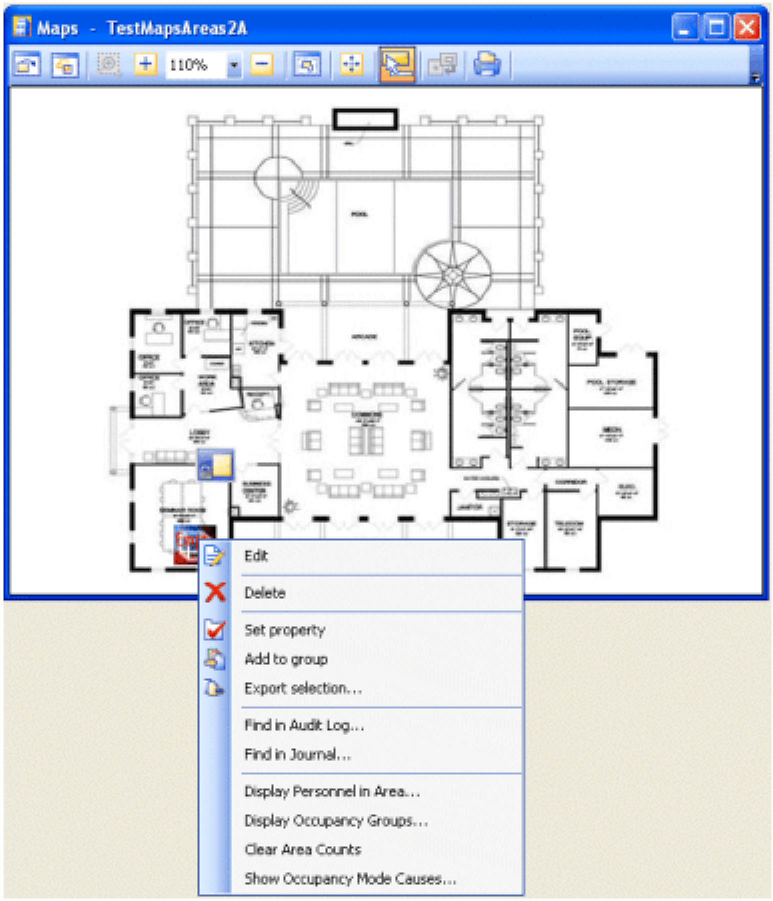
The **Map Viewer**, accessed from the context menu that displays when you right-click a specific Map row in either the Maps **Dynamic View** on the Administration Application or the Maps **Status List** on the Monitoring Station, allows you to view such a Map in real time. The Area and Door icons on the Map show the current status of the Objects they represent, as shown in the example in Figure 26 on Page 133.

Figure 26: Map Popup View with Area and Door Icons



You can also right-click any icon on the **Map Popup** View to display another context menu pertinent to the specific Object type, as shown in the example for the Area icon in Figure 27 on Page 134 (if the **Show context menu on right click** option was selected in the **Maps Icon Properties** dialog box when you configured the Map).

Figure 27: Map Popup View with Area Icon Context Menu



The iSTAR Area icon context menu has the same options as the context menu for iSTAR Areas in the Dynamic View, described in Table 3 on Page 57.

2

iSTAR Intrusion Zones

This chapter includes conceptual information about iSTAR Intrusion Zones and describes the procedures you use to create them.

In this chapter

Introduction

An *iSTAR Intrusion Zone* is a user-defined group of Doors and Inputs on the same local Controller that delineates a physical area monitored for alarms—thus protecting that area. The Inputs you assign to an iSTAR Intrusion Zone—such as motion detectors, glass break sensors, etc.—monitor security inside the zone. The Doors you assign to an iSTAR Intrusion Zone define the entrance and exit points for the zone.

Grouping Doors and Inputs into an iSTAR Intrusion Zone allows easy Arming and Disarming of groups of alarm monitoring points (Inputs), as well as Locking and Unlocking groups of doors, while displaying their current mode and status. The local Controller is responsible for monitoring the Doors and Inputs, reporting the state of the Intrusion Zone as a whole, and controlling the Door access modes and Input Arm/Disarm states. The use of Intrusion Zones is optional.

In addition Triggers can be defined to link the Intrusion Zone's current mode and status (such as when a zone is violated) to Events whose Actions sound an alarm or send an e-mail or page, for example.

iSTAR Intrusion Zone Modes and States

An Intrusion Zone is always in one of two modes:

- Armed
- Disarmed

An iSTAR Intrusion Zone in Armed mode can be in either of the following two states:

- Violated
- Not Violated

Regardless of its Mode and Violated state, an iSTAR Intrusion Zone's Ready To Arm State may be either:

- Ready to Arm
- Not Ready to Arm – the iSTAR Intrusion Zone has offnormal Inputs or open Doors (whether it is Armed or Disarmed)

You can view the mode/state of an iSTAR Intrusion Zone in three places:

- Administration application
  - **iSTAR Intrusion Zone** Dynamic View – see Viewing Intrusion Zone Status on the Dynamic View on Page 161.
  - **iSTAR Intrusion Zone Editor Status** tab– see Viewing Intrusion Zone Status on the Status Tab on Page 189.
- Monitoring Station: **Explorer Bar>Non-Hardware Status> Intrusion Zones>Status List - iSTAR Intrusion Zones** – see the Monitoring Status chapter in the *C•CURE 9000 Monitoring Station Guide*.

Armed

If the zone is *Armed*, the area is protected. You cannot enter an Armed Intrusion Zone without using Doors, activating Inputs, and causing an Intrusion Zone Violation.

When you arm an Intrusion Zone, the iSTAR reports the Armed status to the C•CURE server. If the Arming method included presenting a card, the hardware reports the Personnel access. The iSTAR also reports tamper, input supervision errors, and communication failures.

For five seconds after an Intrusion Zone is armed, the zone's readers display "Area Armed" in the LCD area. This message is followed by the current date and time. If there is an Event assigned to the Armed mode, the iSTAR activates the Event while the Intrusion Zone is Armed.

Disarmed

If the zone is *Disarmed*, the Inputs assigned to that Intrusion Zone do not generate Intrusion Zone Violations when activated (when people enter the zone, for example).

When you disarm an Intrusion Zone, the iSTAR reports the Disarmed status to the C•CURE server. If the Disarm method included presenting a card, the hardware reports the Personnel access. For five seconds after an Intrusion Zone is disarmed, the system displays Disarm status messages on all Readers within the zones. If there is an Event assigned to the Disarmed mode, the iSTAR activates the Event while the Intrusion Zone is Disarmed.

The iSTAR processes access requests at the Intrusion Zone Doors during the Disarmed state. You can gain access at the locked Doors through the usual means: valid card, valid card and pin, or RTE. The iSTAR also reports tamper, input supervision errors, and communication failures.

Violated

An Intrusion Zone changes from Normal to *Violated* when the system detects an Intrusion Zone Violation. Violations include:

- Hardware tamper or communication failure.
- Supervision errors for Intrusion Zone Inputs or tamper Inputs.
- Inputs that activate while the zone is armed. (If the zone is disarmed within the entrance delay, the Violation does **not** occur.)
- Doors that open while the zone is armed. (If the zone is disarmed within the entrance delay, the Violation does **not** occur.)

When the system detects an Intrusion Zone Violation, the iSTAR changes the status of the Intrusion Zone to **Violated** and notifies C•CURE 9000 of the Violation. The server records the Violation in the journal and generates an activity message at the Monitoring Station.

If the Intrusion Zone includes an action, such as flashing lights, configured on the **Triggers** tab for the Event to be activated if the Zone is in a Violated state, the system initiates the action while the Intrusion Zone is Violated.

The Intrusion Zone status remains Violated—whether or not the object causing the Violation returns to the Normal state—until you change the mode of the Intrusion Zone to **Armed** or **Disarmed**.

You can change the mode to **Armed** via key-press/active input and card swipe, Keypad Command Action, or an **Arm selected** Direct Action from the Administration application Dynamic View or Monitoring Station Status List.

You can only disarm a Violated iSTAR Intrusion Zone if you have selected the **Allow Disarm While Violated** option on the **iSTAR Intrusion Zone Arm - Disarm** tab. (If this option is not selected, you must first clear the Violation by deactivating the appropriate Inputs and re-arming the zone, or by force-arming the zone.

You can change the mode to **Disarmed** via card swipe, key-press/active input and card swipe, Keypad Command Action, or a **Disarm selected** Direct Action from the Administration application Dynamic View or Monitoring Station Status List.

For instructions on Arming and Disarming a zone, see Controlling Intrusion Zone Mode on Page 140.

Ready to Arm/Not Ready to Arm

The status of the Intrusion Zone may be either *Ready to arm* or *Not ready to arm*.

Ready to Arm

You can arm an Intrusion Zone whose status is Ready to arm. The intrusion zone is ready to arm when:

- All objects assigned to the Intrusion Zone are in a Normal state
- Intrusion Zone Inputs are **not** active
- Intrusion Zone Doors are closed

Not Ready to Arm

The status of an Intrusion Zone is Not ready to arm when:

- Any object assigned to the Intrusion Zone is **not** functioning normally
- An Intrusion Zone Input is active
- An Intrusion Zone Door is open

When the Intrusion Zone status is Not ready to arm, you cannot change the mode of the zone from Disarmed to Armed unless you use the "force armed" feature.

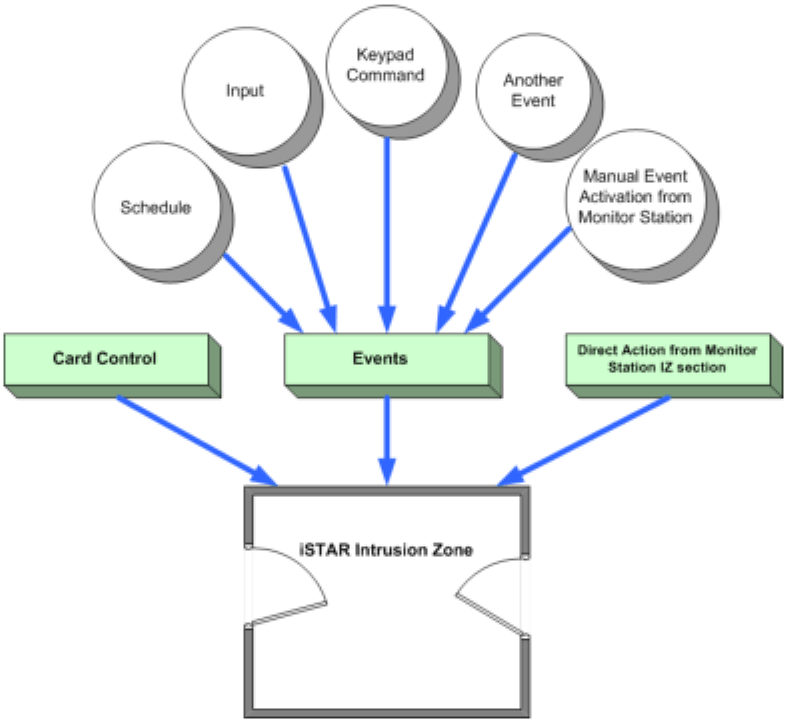
You can force arm an intrusion zone with a normal Event Action, a local Keypad Command Action, or a Direct Action from the Administration application Dynamic View or Monitoring Station Status List. A force arm is necessary when one or more Intrusion Zone Inputs are active, causing a Not ready to arm state. You can also force arm an Intrusion Zone, to intentionally disregard an active monitoring point.

Controlling Intrusion Zone Mode

The Arming/Disarming mode of an iSTAR Intrusion Zone can be controlled by the following methods, illustrated in Figure 28 on Page 140:

- Card Control
- Event Control
  - C•CURE 9000 Events
  - Keypad Command Events
  - Monitoring Station Manual Event Activation
- Manual Control (Direct Actions from Monitoring Station)

Figure 28: Controlling iSTAR Intrusion Zone Modes


Input
Keypad Command
Another Event
Schedule
Manual Event Activation from Monitor Station
Card Control
Events
Direct Action from Monitor Station IZ section
iSTAR Intrusion Zone

When the Intrusion Zone is **armed**, all the Intrusion Zone Inputs are armed, Intrusion Zone Doors are set to an armed state, and the Intrusion Zone's Trigger-linked armed Event is active. If Intrusion Zone Inputs activate while the Intrusion Zone is armed and the Intrusion Zone is not disarmed before the Entrance Delay expires, the Intrusion Zone goes into a Violated state and triggers the violated event.

When the Intrusion Zone is **disarmed**, all Intrusion Zone Inputs (except for Protected Inputs) are disarmed, Intrusion Zone doors are set to a disarmed state, and the Intrusion Zone's Trigger-linked disarmed Event is active.

If Inputs activate while the Intrusion Zone is armed or disarmed, the Intrusion Zone becomes not-ready-to-arm and triggers the not-ready-to-arm event.

The various methods can be combined.

Example:

You can arm an Intrusion Zone via Card Control—a card read, but disarm it with Event Control—an event triggered by a Keypad Command.

Card Control

Card Control provides the methods shown in Table 27 on Page 141 to arm or disarm a zone.

Table 27: Card Control Options

Disarm	Arm
Credential Only (with valid Clearance)	Key-press* and Credential (with valid Clearance)
Credential (with valid Clearance) and Active Input**	Active Input** and Credential (with valid Clearance)
Credential (with valid Clearance) and Personnel Group	Key-press*, Credential (with valid Clearance), and Personnel Group
Credential (with valid Clearance), Active Input**, and Personnel Group	Active Input**, Credential (with valid Clearance), and Personnel Group
*To **key-press**, press the CMD/ENT key twice; and then present a valid Credential within ten seconds.	
An **Active Input is any available input of the iSTAR. It is common to use a key-activated switch as the Active Input. The switch must be active prior to the presentation of the Credential.	

When arming or disarming an Intrusion Zone by Card Control, the behavior of the zone and the Door is affected by the location of the Reader, whether outside the zone or inside the zone.

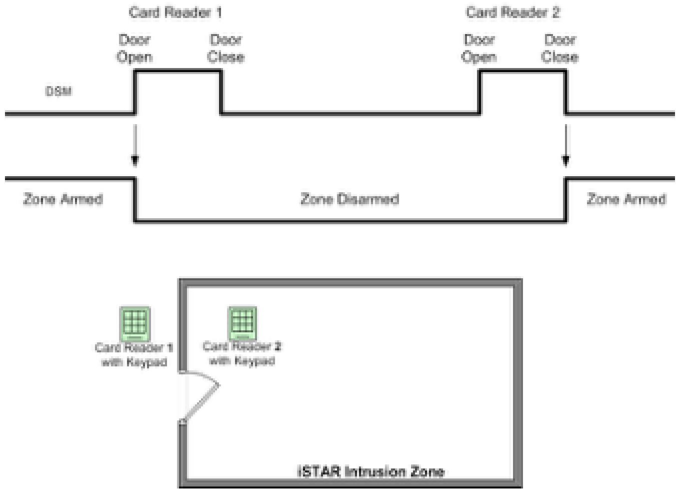
When the Intrusion Zone is armed from an **outside** Reader, the door strike is not activated when the valid Credential is read. The system determines that the zone is being armed because either the Active Input is active or CMD/ENT has been pressed twice (a **key-press**). Since you are already outside the Intrusion Zone, there is no need to activate the door strike. If you arm the Intrusion Zone from an **inside** Reader, then the door strike does activate.

Example:

Figure 29 on Page 142 illustrates the use of the Door State Monitor (DSM) when controlling an Intrusion Zone by card control:

- The diagram begins with the zone armed.
- A person then disarms the Intrusion Zone using card control at Reader 1. (Notice that when the door opens after the valid card read, the zone immediately disarms.)
- Later, the person arms the Intrusion Zone from the inside using card control at Reader 2. (Notice that the Intrusion Zone does **not** arm until the person leaves the Intrusion Zone by opening and then closing the door.)

Figure 29: Use of a Door State Monitor with Card Control



For more information about outside/inside Readers, see Door Behavior for Entrance and Exit Doors on Page 151.

When card control is used, the person must have a valid Clearance at the door where the card is presented. As documented in Table 27 on Page 141, card control can be further qualified by requiring the person to be a member of a particular Personnel Group.

NOTE Personnel designated as Intrusion Zone Administrators do **not** have to be included in the required Personnel Group, but must have valid Clearance at the door. For more information, see Configuring a Person to Arm/Disarm Intrusion Zones on Page 192.

Event Control

There are Event Actions that control the mode of iSTAR Intrusion Zones. Some can be used by any Event and others are restricted to Keypad Command Events.

The Event Actions in the following list can be used by any Event and can control any of the iSTAR Intrusion Zones. They can be either Cluster- or Host-based, unless they are linked to a Keypad Command—in which case they must be downloaded to an iSTAR Controller in a Cluster.

- Arm Intrusion Zone
- Disarm Intrusion Zone
- Force arm Intrusion Zone
- Toggle Intrusion Zone mode

The Event Actions in the following list are restricted to Keypad Commands. These actions must be downloaded to the iSTAR Controller where the Intrusion Zone is configured. The Keypad Reader must be associated with a Door that is part of the Intrusion Zone.

- Show Intrusion Zone Offnormal Points
- Show Intrusion Zone Status
- Arm Local Intrusion Zone
- Disarm Local Intrusion Zone

- Force Arm Local Intrusion Zone
- Show Local Intrusion Zone Offnormal Points
- Show Local Intrusion Zone Status
- Toggle Local Intrusion Zone

Event Caused by Schedule

A Schedule can be configured to cause an Event that can automatically control the Intrusion Zone based on date and time.

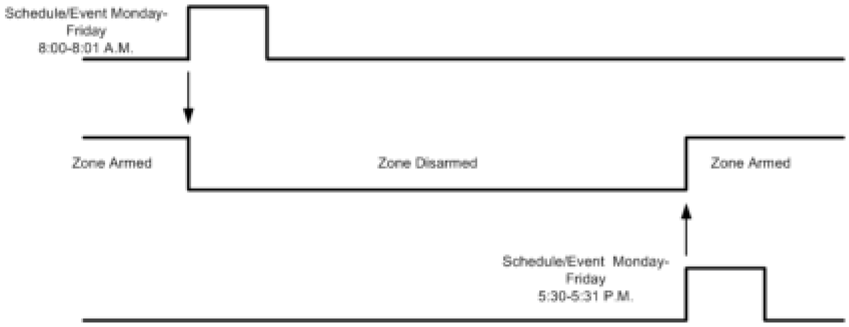
Example:

> Disarming an Intrusion Zone during normal work hours.

Controlling Intrusion Zones with Schedules is different from controlling other C•CURE 9000 Objects. Arming/disarming is done on the leading edge of the Schedule Event. The arm state does **not** follow the state of the Schedule or the Event.

Use a one-minute Schedule-caused Event to arm the Intrusion Zone and another one-minute Schedule-caused Event to disarm it, as shown in the example in Figure 30 on Page 143.

Figure 30: Scheduled Events controlling Intrusion Zone Mode



Event Caused by an Input

Any Input (except those with a special use, such as a Door State Monitor) can be used to activate an Event which then controls the Intrusion Zone. For instance, a switch inside the Intrusion Zone can be used to toggle the Intrusion Zone between the armed and disarmed states. If an Input is used in this way, the Intrusion Zone configuration permits Entrance and Exit Delays to allow time to get in or out of the Intrusion Zone before an alarm is triggered.

Event Caused by Another Event

C•CURE 9000 Event capability permits linking other Events to the Events that control the Intrusion Zone.

Example:

> The Intrusion Zone can be immediately armed and secured if a duress condition or door forced alarm occurs anywhere in the building.

Event Caused by a Keypad Command

Use the Keypad Command capability of the C•CURE 9000 to activate Events that control Intrusion Zones from Reader Keypads.

An important point to understand about Keypad Command Events is that these events live until overridden. An action is required to undo or override a Keypad Command Event. Software House recommends constructing Keypad Commands in pairs; use one Keypad Command to activate an Object, and another Keypad Command to deactivate the Object.

There are various ways these Keypad Command pairs can be configured.

Any event caused by a Keypad Command must be downloaded to an iSTAR Controller that is part of the same Cluster where the Intrusion Zone is configured.

It is also possible to activate Events in another Cluster by using 'indirection'—have the Keypad Event activate an Event in the Cluster which then activates a further Event that is in either the Host or another Cluster.

Local – Some Intrusion Zone Event Actions are local—the Keypad Command must come from a Reader on a Door in the Intrusion Zone. The Event triggered by that Keypad Command must be downloaded to the iSTAR Controller that includes the Intrusion Zone.

Manual Event Activation from the Monitoring Station

Any Event can be activated from the Monitoring Station by a Manual Action. You define the time and date the activation will start and end.

NOTE Remember that the arming and disarming is edge-triggered, so you want one Event to arm the Intrusion Zone and another Event to disarm the Intrusion Zone.

Direct Action at the Monitoring Station

You can manually **Disarm**, **Arm**, or **Force-arm** a selected Intrusion Zone from the Monitoring Station Status List for Intrusion Zones. These actions do **not** need a start/end date and time. If the Action is allowed, it occurs immediately.

Some situations where such an action is or is not allowed follow:

- You cannot **Disarm** an armed Intrusion Zone that is in **violation** unless the **Allow Disarm While Violated** option is selected. (See iSTAR Intrusion Zone Arm - Disarm Tab on Page 177.)
- You cannot **Arm** a disarmed Intrusion Zone if the Intrusion Zone is **not ready to arm** (the Intrusion Zone contains one or more activated Inputs). However, in such a situation you can **Force-arm** the Intrusion Zone. When an Intrusion Zone is force-armed, the latter inputs do not cause a **violation**, but continue to cause a **not ready to arm** state.

Inputs

An iSTAR Intrusion Zone can have three types of Inputs:

- Controlled Inputs
- Protected Inputs
- Monitored Inputs

Controlled Inputs

These are the regular inputs that are configured to be part of the Intrusion Zone. These Inputs are configured to be armed and disarmed as the Intrusion Zone is armed and disarmed. The Intrusion Zone monitors these Inputs and does not allow arming if they are active, and if these Inputs become active while the Intrusion Zone is armed, the zone becomes Violated.

Protection Inputs

These Inputs are configured to be monitored by an Intrusion Zone **without** being disarmed and armed by the zone. The Intrusion Zone monitors these Inputs and does **not** allow normal arming if they are active. These Inputs are **not** controlled by the Intrusion Zone, **nor** are they normal monitored Inputs of the zone. However, these Inputs are configured as part of the Intrusion Zone and have option flags set to indicate that they are protection Inputs. If these Protection Inputs become active while the Intrusion Zone is armed, the zone becomes Violated.

Monitored Inputs

These Inputs, which are monitored by the Intrusion Zone but **not** armed or disarmed by the Intrusion Zone, are **not** specifically configured as part of the Intrusion Zone—they are **not** in the Intrusion Zone selected Inputs list. Instead, these Inputs are automatically derived from the Controller, Doors, Arm/Disarm Inputs, Protection Inputs, and Controlled Inputs that are configured for the Intrusion Zone. The Monitored Inputs monitor the health of the Intrusion Zone's configured Controlled/Protection Inputs and Doors. The list of Monitored Inputs includes the Controller cabinet tamper and all the tampers and comm fail Inputs for the Hardware that controls the Inputs and Doors configured to be in the iSTAR Intrusion Zone, as well as supervision errors for all Intrusion Zone Hardware.

Activation of these Inputs causes an armed Intrusion Zone to become violated and prevents normal Intrusion Zone arming. Force arming over an active Monitored Input allows the Intrusion Zone to arm, without affecting the state of the Monitored Input. Subsequent new activation of the Monitored Input causes the armed zone to become violated.

When Monitored Inputs are activated, they appear on the Reader LCD of Intrusion Zone Doors if these Doors are configured for 'Status' display mode.

The following list includes all the groups of Inputs that are monitored by iSTAR Intrusion Zones:

NOTE Most of the Monitored Inputs **cannot** be removed from the Intrusion Zone Monitored Inputs list, but if the Input is **not** configured in the system at all, then the physical/logical Input will **not** be monitored by the Intrusion Zone.

The first two Monitored Inputs in the list, the iSTAR cabinet tamper and the door open state for the Doors, have special behavior. The others from #3 onward have the common behavior of preventing arming and causing immediate violation of an armed Intrusion Zone.

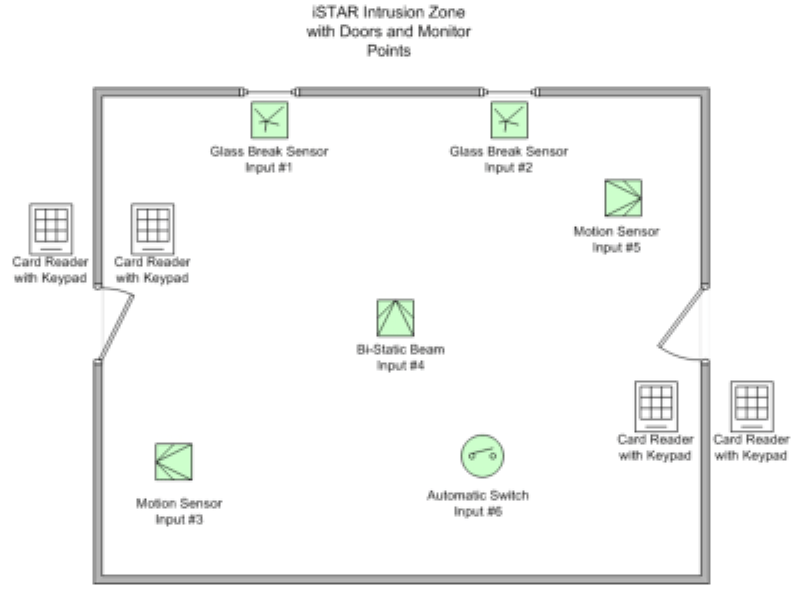
1. iSTAR Cabinet Tamper – The cabinet tamper for the iSTAR Controller is a Monitored Input for all Intrusion Zones on that iSTAR. This is the only such Input that can be removed from the Monitored Input list through a system variable. (For information, see the "iSTAR Driver" section in the System Variables chapter in the *C•CURE 9000 System Maintenance Guide*.)
2. Door Open Status – This is the door open state for Doors configured to be part of the iSTAR Intrusion Zone. An open Door prevents normal arming. A Door on an armed Intrusion Zone that opens either starts an entrance delay or if there is **no** entrance delay, causes the Intrusion Zone to be violated.

3. DSM/RTE Supervision Errors – Supervision errors on DSMs and RTEs for Doors configured to be part of the Intrusion Zone.
4. Controlled Input Supervision Errors – Supervision errors for Controlled Inputs that are part of the Intrusion Zone.
5. Other Inputs – Supervision errors for the arm/disarm Inputs that may be configured for the Intrusion Zone.
6. Reader Tamper and Reader Comm. Fail – Reader tamper and reader comm. fail Inputs—if configured—for Readers on Doors that are in the Intrusion Zone. Also includes:
   - Reader tamper and reader comm. fail Inputs—if configured—for Readers that contain Controlled Inputs for the Intrusion Zone even if the Reader is **not** on any Door or is on a Door that is not part of the Intrusion Zone.
   - Reader tamper and reader comm. fail Inputs—if configured—for Readers that contain any arm or disarm Inputs for the Intrusion Zone or for Readers that may contain any advanced door monitoring Inputs for Doors controlled by the Intrusion Zone.
   - Reader tamper and reader comm. fail Inputs for Readers that may contain any Outputs used by Doors controlled by the Intrusion Zone.
7. I/8 Input Board Tamper and Comm. Fail – Tamper and comm. fail Inputs—if configured—for I/8 Input boards that contain Controlled Inputs for the Intrusion Zone. Also includes I/8 Input Board Tamper and Comm. Fail Inputs for I/8 boards that contain Intrusion Zone arm/disarm Inputs.
8. R/8 Output Board Tamper and Comm. Fail – Tamper and comm. fail Inputs—if configured—for R/8 Output boards that contain any Outputs used by Doors controlled by the Intrusion Zone.
9. Tamper and Comm. Fail for Protection Inputs – the tamper and comm. fail inputs—if configured—for the Readers and I/8 Input boards that contain the Protection Inputs.
10. Protection Input Supervision Errors – Supervision errors of Protection Inputs are also treated as Monitored Inputs.

Figure 31 on Page 147 shows a basic iSTAR Intrusion Zone with two doors and six Inputs. The Inputs are switch contacts that indicate situations such as glass breakage, motion sensing, etc.

- If any Input is active (excluding an entrance delay or a shunt) when the Intrusion Zone is armed, there is a **violation**.
- If any Input is active when the Intrusion Zone is disarmed, the zone is considered to be **not ready to arm**.

Figure 31: Example of iSTAR Intrusion Zone: Two Doors and Six Inputs



A Controlled Input can optionally be configured either to be **shunted** during an entrance delay or to be **shunted** and also to **trigger** an entrance delay**.**

Shunt Example:

When a switch inside the Intrusion Zone controls arming and disarming and the switch area is monitored by a motion sensor, you would want the motion sensor (Input) to be shunted during the entrance delay.

Entrance Delay Example:

When a perimeter Door of the Intrusion Zone is either key-operated or has a combination lock, you would want an Input monitoring the Door to trigger an entrance delay. This would allow a person time to disarm the Intrusion Zone after entering. This Input would also be shunted during the entrance delay.

Protection Input Example:

The Glass Break Sensor Inputs #1 and #2 are Protected Inputs that are always armed (24/7). They are **never** shunted during an entrance delay, **nor** do they trigger an entrance delay.

- If these Protected Inputs activate while the Intrusion Zone is **armed**, the zone becomes **violated**.
- If these Protected Inputs activate while the Intrusion Zone is **disarmed**, the Inputs report their Input state and the zone becomes **not ready to arm**.

Intrusion Zone Status Triggers

Triggers allow you to configure the activation of Events that both display the Intrusion Zone mode and respond to the state of the Intrusion Zone. The Events can be configured to activate when the iSTAR Intrusion Zone is in the following modes/states:

- While **disarmed**
- While **armed**
- When **ready to arm**

- When **not ready to arm**
- When **violated**
- When **not violated**

You can also configure a Trigger ('arm check status') that activates an Event if it finds that the Intrusion Zone is **not** armed during a specified Schedule.

Events indicating an **Armed** or **Disarmed** mode are usually used to activate status indicators that indicate the Intrusion Zone's mode.

A **Not ready to arm** state exists when the zone is disarmed and any Input in the zone is active. The **Not ready to arm** state is asserted even when an approved person opens the door. A typical use of the event is to activate an indicator light.

A **Zone violated** state can use an event to sound an alarm and cause other actions in response to the violation.

Some of these Events may be either Panel-based (Controller) or Host-based. Others are either Host only or Panel only. The actions of these events can link to any system Objects, Events, or iSTAR Clusters.

Table 28 on Page 148 shows the effect of **off normal points** on **not ready to arm** and **violated** Events. The **Property Value: Violated** column indicates if the Intrusion Zone is in violation after any entrance/exit delay expires.

Table 28: Intrusion Zone Mode and Effect of Off Normal Points

Case	Intrusion Zone Mode	Any Off Normal Points	Property Value: Ready to Arm*	Property Value: Violated**
1	Armed	No	Yes	No
2	Disarmed	No	Yes	No
3	Armed	Yes	No	Yes
4	Armed	Not now, but one existed previously	Yes	Yes
5	Disarmed	Yes	No	No
6***	Force Armed	Input(s) active when Force armed, remain active.	No	No
7***	Force Armed	Input(s) active when Force armed, remain active. Additional input(s) active.	No	Yes
*A **ready to arm** state means **no** Inputs are **off normal**.				
A **violated state means at least one Input is active/was active. This state can only occur with the Intrusion Zone in **Armed** mode.				

Intrusion Zone Mode and Effect of Off Normal Points (continued)

<table>
<tr><th>Case</th><th>Intrusion Zone Mode</th><th>Any Off Normal Points</th><th>Property Value: Ready to Arm*</th><th>Property Value: Violated**</th></tr>
<tr><td colspan="5">***Cases 6-7 explain a <b>Force Armed</b> situation. You can force arm an Intrusion Zone with a normal Event Action/ Local Keypad Command Action/ Direct Action from the Monitoring Station. A force arm is necessary when one or more Intrusion Zone Inputs are active due to a fault, causing a <b>not ready to arm</b> state.
• In case 6, with the Intrusion Zone force armed with an active Input, the zone is in <b>Armed</b> mode, in a <b>not ready to arm</b> state, and <b>not</b> violated. If the active Input goes non-active, the <b>not ready to arm</b> state deactivates. The effect of force arming is to ignore any active Inputs at the time of the force arm to indicate a violation.
• In case 7, the Intrusion Zone is force armed with an active Input as in case 6, but another Input goes active; therefore, the Intrusion Zone is in <b>Armed</b> mode, in a <b>not ready to arm</b> state, and is <b>violated</b>.</td></tr>
</table>

Doors

When configuring the doors that define an iSTAR Intrusion Zone, you must consider the values for the following optional fields:

- Arm state and Disarm state
- Card Control
- Display
- Entrance or Exit Door

Arm Mode and Disarm Mode

When an Intrusion Zone is in either **Armed/Disarmed** mode, an Intrusion Zone Door has three possible states.

In Armed mode - The three possible Door states are:

- **Locked** – The Door is locked. A Card access with a valid Clearance is required to enter. If a card is presented, it must immediately disarm the zone by Card control or coincide with a disarm of the Intrusion Zone by other methods within the Entrance Delay Time.
- **Secured** – The Door is secured. The Door Reader does not allow a card access, but can be used for Card control and Keypad Commands. The Door status must be changed to Locked or Unlocked before it can be used for access. Typically, Disarming the Intrusion Zone changes the Door to Locked or Unlocked.
- **Unlocked** – It is unlikely to want a perimeter Door of the Intrusion Zone left unlocked. However, there could be a Door within the Intrusion Zone that is left unlocked for safety reasons.

In Disarmed mode - The three possible door states are:

- **Locked** – The Door is locked. A card access with a valid Clearance is required.
- **Secured** – The Door is secured. The Door Reader does not allow a card access, but can be used for card control and Keypad Commands. Before the Door can be used for access, its state must be changed to "Locked" or "Unlocked".

NOTE This state is **not** often used in a **Disarmed** Intrusion Zone. There could be a case, however, where a Door in the zone leading to a store room (or something similar) is left secured even though the Intrusion Zone is Disarmed.

- **Unlocked** – The Door is open. No card access is required.

Card Control

This option controls whether the Card control methods, described in Card Control on Page 141, are allowed at this Door.

If Card control methods are configured, Card reads are allowed even if the Door state is **unlocked** or **secure**. In the latter cases, the card reads are **not** used for access but for **Card swipe arm/disarm** of the Intrusion Zone. If the system determines that the Card read is **not** being used for arm or disarm, the Card reads will be ignored.

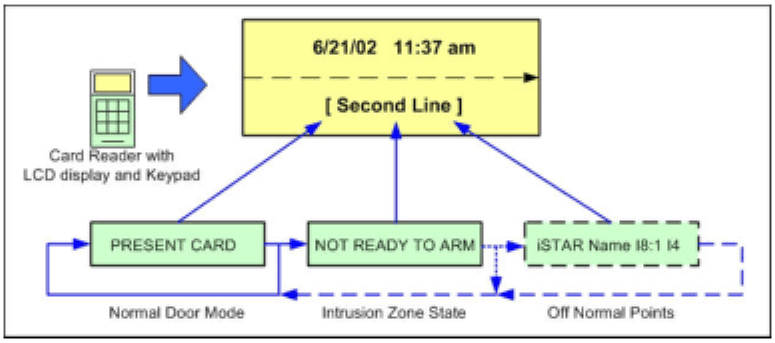
Display

This option controls whether or not status information about this Intrusion Zone is shown on the LCD display on the door reader(s).

- Display flag is set to **blank**. The first line of the Reader's LCD shows date and time, while the second line momentarily shows or mode change status/access control messages.
- Display flag is set to **Status**. The first line of the Reader's LCD shows date and time, while the second line alternates between normal door modes/actions, Intrusion Zone modes/actions, and off normal point(s)—if there are any. If there is more than one off normal point, each successive display shows the next one in sequence.

Figure 32 on Page 150 illustrates a situation where Input number 4 of the first I8 board is active.

Figure 32: Sample of LCD Second Line Status Display – with Off Normal Point



Entrance/Exit Door

Whether a Door is an Entrance or an Exit Door relates to whether or not the inbound Reader of the Door leads into the Intrusion Zone.

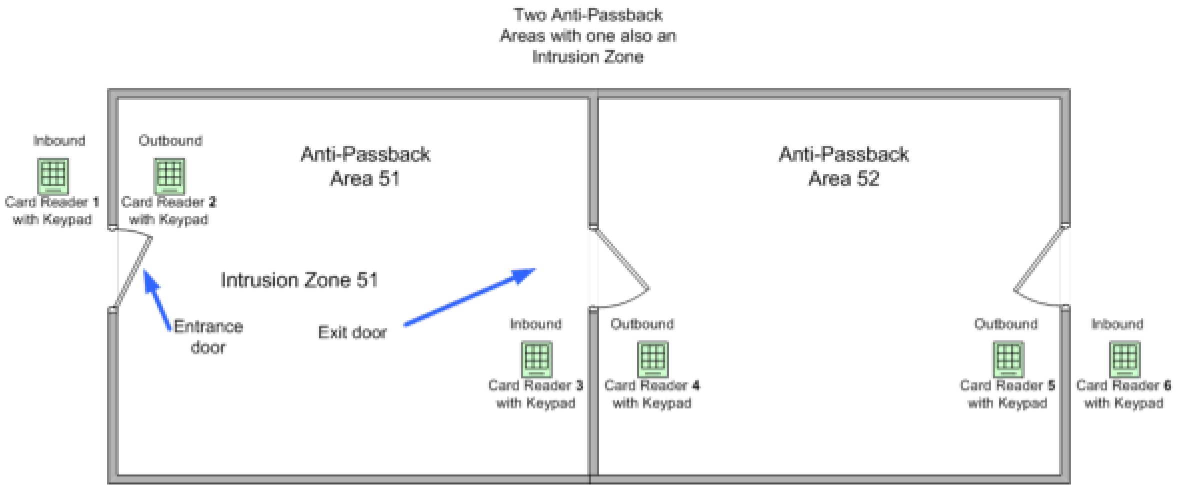
The purpose is to allow the Intrusion Zone to decide whether a person is physically inside or outside of the zone.

- If they are outside when they disarm the zone, then the Door strike needs to be opened.
- If they are outside when they arm the zone, there is **no** need to activate the strike.

In most cases, the inbound Reader leads into the Intrusion Zone and the outbound Reader leads out of the zone. In these cases, designate the door as an **Entrance** Door.

The **Exit Door** designation is rarely used. The **Exit Door** designation relates to an Intrusion Zone that is also part of, or abutting, an antipassback (APB) area. Figure 33 on Page 151 shows two APB areas, with one of them also being an Intrusion Zone.

Figure 33: iSTAR Intrusion Zone Also an Antipassback Area



Example:

> Assume that the APB Areas in Figure 33 on Page 151 above were created prior to the Intrusion Zone. When defining AP Area 52 the middle door was defined with Reader 3 as the **inbound** Reader to AP Area 52 and Reader 4 as the **outbound** Reader from AP Area 52 to AP Area 51.
>
> Later when the Intrusion Zone was configured, the left-side door was configured as an **Entrance** Door since the **inbound** Reader brought you into the Intrusion Zone. The middle door was configured as an **Exit** door since the **outbound** reader brought you into the IZ.

Designating a Door as an **Exit** Door reverses the actions and effects of the Door strike and the Door State Monitor (DSM), as described in the following section, Door Behavior for Entrance and Exit Doors. The **inbound** Reader of an **Entrance** Door behaves exactly the same as the **outbound** Reader of an **Exit** door, and vice versa.

Door Behavior for Entrance and Exit Doors

You control how the Door strike behaves, and the DSM is interpreted with the **Entrance** and **Exit** selection. (When the door strike is active and a DSM exists, you must open, and sometimes close, the Door for actions to take effect.)

Table 29 on Page 151 shows all the meaningful situations that you may encounter with Entrance/Exit Doors.

Table 29: Entrance and Exit Door Behavior

Case	Door Type	Door Reader	Zone State	Door Action	Door Strike Active	DSM Required
1[a]	Entrance	Inbound	Armed	Disarm	Yes	Yes - disarms when door opens
2[b]	Entrance	Inbound	Not Armed	Arm	No	No
3[c]	Entrance	Outbound	Not Armed	Arm	Yes	Yes - arms when door opens and closes
4[d]	Entrance	Outbound	Armed	Disarm	No	No

Entrance and Exit Door Behavior (continued)

Case	Door Type	Door Reader	Zone State	Door Action	Door Strike Active	DSM Required
5[a]	Exit	Outbound	Armed	Disarm	Yes	Yes - disarms when door opens
6[b]	Exit	Outbound	Not Armed	Arm	No	No
7[c]	Exit	Inbound	Not Armed	Arm	Yes	Yes - arms when door opens and closes
8[d]	Exit	Inbound	Armed	Disarm	No	No

[a] Cases 1 and 5 represent approaching the armed Intrusion Zone from outside and **disarming** it with Card control. The zone disarms and you are granted access. If a DSM is configured, the zone does **not** disarm until the Door opens and activates the DSM.

[b] Cases 2 and 6 represent **arming** the Intrusion Zone by Card control from the Reader physically outside the zone.

NOTE: The Card arms the zone, but does **not** activate the strike.

If you simply present your Card with **no** attempt to arm the zone, it is treated as a normal Door access and activates the strike. The system can differentiate between a Door access and an attempt to arm: to indicate that you want to arm the zone, you must have either pressed CMD/ENT twice or have an active Input.

[c] Cases 3 and 7 represent approaching the inside Reader and **arming** the Intrusion Zone.

NOTE: The door strike is activated to allow exit.

You should also configure an exit delay for these cases. If a DSM is configured, the zone does **not** arm until the Door opens and closes.

[d] Cases 4 and 8 represent **disarming** the Intrusion Zone from an inside Reader. (For security reasons, this zone may be configured to **only** be armed or disarmed from inside.) You gain access through the Door with an entrance delay, enter, and then disarm the zone. Any motion sensor Inputs covering entrance areas during this time **must** be shunted.

NOTE: The strike does **not** activate in these cases because you are already in the zone.

NOTE

To arm an Intrusion Zone from the outbound reader (for a double-reader door), an **Exit Delay** time of 4 seconds or greater must be configured on the Intrusion Zone Arm - Disarm tab.

iSTAR Intrusion Zone Configuration Steps

Table 30 on Page 153 shows the C•CURE 9000 Editors and activities that create iSTAR Intrusion Zones. This table assumes that you have already configured the iSTAR Cluster and Controller.

Table 30: Creating iSTAR Intrusion Zones

Task	C•CURE 9000 Editor	Configuration Notes	Additional Information
Disable/Enable the Intrusion Zone Cabinet Tamper (optional)	Options & Tools>System Variables>iSTAR Driver Category> Disable the Intrusion Zone Cabinet Tamper	Whether to disable the use of the Intrusion Zone Cabinet Tamper or not. The default value is false – the Intrusion Zone Cabinet Tamper is enabled. NOTE: You must stop and restart the iSTAR driver to have any changes you make to this variable take effect.	See "iSTAR Driver Settings" in the System Variables chapter in the *C•CURE 9000 System Maintenance Guide*.
Configure a Personnel Group (optional, depending on arming/disarming method)	Configuration>Group> New>Group Editor - or - Edit an existing Personnel Group	Creates a Personnel Group to whose members arming/disarming the Intrusion Zone with the card swipe methods can be limited.	See the Groups chapter in the *C•CURE 9000 Software Configuration Guide*.
Configure the iSTAR Intrusion Zone	Areas and Zones>iSTAR Intrusion Zone>New>iSTAR Intrusion Zone Editor and General tab	Creates an iSTAR Intrusion Zone and selects a Controller for it.	See Basic Intrusion Zone Tasks on Page 155 and iSTAR Intrusion Zone Editor on Page 165.
Configure Intrusion Zone Doors	Areas and Zones>iSTAR Intrusion Zone>New>iSTAR Intrusion Zone Editor>General tab	Specifies • Entrance/exit Doors • Door state • Card control access • Reader display mode • Display name	See iSTAR Intrusion Zone General Tab on Page 166.
Configure Intrusion Zone Inputs	Areas and Zones>iSTAR Intrusion Zone>New>iSTAR Intrusion Zone Editor>Inputs tab	Specifies • Controlled Inputs that cause entrance delays or are shunted during entrance delay. • Protection Inputs that are monitored 24/7. • Input Display name Displays Monitored Inputs	See iSTAR Intrusion Zone Inputs Tab on Page 172.
Configure Intrusion Zone Arm/Disarm Methods	Areas and Zones>iSTAR Intrusion Zone>New>iSTAR Intrusion Zone Editor>Arm - Disarm tab	• Specifies arming/disarming methods • Defines exit/entrance delays	See iSTAR Intrusion Zone Arm - Disarm Tab on Page 177.
Configure Intrusion Zone Triggers	Areas and Zones>iSTAR Intrusion Zone>New>iSTAR Intrusion Zone Editor>Triggers tab	Specifies Event Actions to be activated for iSTAR Intrusion Zone modes/states.	See iSTAR Intrusion Zone Triggers Tab on Page 183.

Creating iSTAR Intrusion Zones (continued)

Task	C•CURE 9000 Editor	Configuration Notes	Additional Information
Change Intrusion Zone State Images	Areas and Zones>iSTAR Intrusion Zone>New>iSTAR Intrusion Zone Editor>State Images tab	Modify Images that indicate iSTAR Intrusion Zone states on the Monitoring Station.	See iSTAR Intrusion Zone State Images Tab on Page 191 and State Images Tab Tasks on Page 191.
Configure Personnel	Personnel>Personnel> New>Personnel Editor - or - Edit an existing Personnel Record	Enables a specific person **not necessarily** in the iSTAR Intrusion Zone Personnel Group to arm/disarm the Intrusion Zone with the Card swipe methods.	See Configuring a Person to Arm/Disarm Intrusion Zones on Page 192.

Basic Intrusion Zone Tasks

The C•CURE 9000 iSTAR Intrusion Zones Editor allow you to accomplish the following tasks:

- Creating an iSTAR Intrusion Zone on Page 155
- Creating an iSTAR Intrusion Zone Template on Page 156
- Configuring an iSTAR Intrusion Zone on Page 157
- Viewing a List of iSTAR Intrusion Zones on Page 157
- Viewing Doors/Inputs for an Intrusion Zone on Page 159
- Viewing the Status of an iSTAR Intrusion Zone on Page 161
- Modifying an iSTAR Intrusion Zone on Page 162
- Deleting an iSTAR Intrusion Zone on Page 163
- Setting a Property for an iSTAR Intrusion Zone on Page 163
- Adding an iSTAR Intrusion Zone to a Group on Page 164

The following tasks related to configuring and using iSTAR Intrusion Zones are accomplished through other C•CURE 9000 features:

- Configuring a Person to Arm/Disarm Intrusion Zones on Page 192
- Viewing Intrusion Zone Information on the Door Editor on Page 193
- Viewing Intrusion Zone Information on the Input Editor on Page 195

Accessing the iSTAR Intrusion Zone Editor

You can access the **iSTAR Intrusion Zone Editor** from the C•CURE 9000 **Areas and Zones** pane.

To Access the iSTAR Intrusion Zone Editor

1. In the Navigation Pane of the Administration Workstation, click the **Areas and Zones** pane button.
2. Click the **Areas and Zones** drop-down list and select **iSTAR Intrusion Zone**.
3. Click **New** to create a new Intrusion Zone.

   - or -

   Click ➡ ▾ to open a Dynamic View showing a list of all existing iSTAR Intrusion Zone Objects, right-click the iSTAR Intrusion Zone you want to change, and click **Edit** from the context menu that appears.

   The **iSTAR Intrusion Zone Editor** opens with the **General** tab displayed, as shown in Figure 35 on Page 166.

Creating an iSTAR Intrusion Zone

You can create a new iSTAR Intrusion Zone using the **iSTAR Intrusion Zone Editor**.

This procedure assumes that you have already configured the iSTAR Cluster and Controller and if required by validation type, have also configured at least one Personnel Group.

To Create an iSTAR Intrusion Zone

1. In the Navigation Pane of the Administration Workstation, click the **Areas and Zones** pane button.
2. Click the **Areas and Zones** drop-down list and select **iSTAR Intrusion Zone**.
3. Click **New** to create a new Intrusion Zone. The **iSTAR Intrusion Zone Editor** opens.

   You can now configure the new Intrusion Zone.
4. To save your new Intrusion Zone, click **Save and Close**.

   - or -

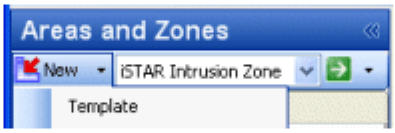
   Alternatively, if you want to save the Intrusion Zone and then create a new one, click **Save and New**. The current Intrusion Zone is saved and closed, but the **iSTAR Intrusion Zone Editor** remains open ready for a new Intrusion Zone.

Creating an iSTAR Intrusion Zone Template

You can create a new template for an iSTAR Intrusion Zone. An iSTAR Intrusion Zone template saves you time because you do not have to re-enter the same Intrusion Zone information again.

To Create an iSTAR Intrusion Zone Template

1. In the **Navigation** Pane of the Administration Workstation, click the **Areas and Zones** pane button.
2. Click the **Areas and Zones** drop-down list and select **iSTAR Intrusion Zone**.
3. Click the down-arrow on the **New** button, and click **Template**.

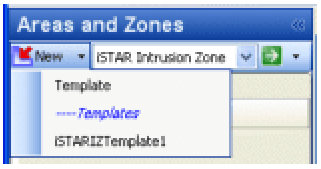


   The **iSTAR Intrusion Zone Editor** where you can configure the Intrusion Zone template opens (see Figure 35 on Page 166).
4. Configure the template to meet your requirements. Any fields you configure values for become part of the template; then when you subsequently create a new Intrusion Zone from that template, these values are already filled in.
5. In the **Name** field, enter the name you wish to use for the template

   Example:

   iSTARIZTemplate1
6. To save the template, click **Save and Close**.

   The template will be available as an option on the pull-down menu on the **New** button in the **Areas and Zones** pane.



Configuring an iSTAR Intrusion Zone

This procedure assumes that you have already configured the iSTAR Cluster and Controller and if required by validation type, have also configured at least one Personnel Group.

To Configure an iSTAR Intrusion Zone

1. Create a new iSTAR Intrusion Zone or modify an existing iSTAR Intrusion Zone.

> **NOTE** If you are modifying an existing Intrusion Zone, you **cannot** change the iSTAR Controller field.

2. Type a **Name** and **Description** for the iSTAR Intrusion Zone that sufficiently identifies this Intrusion Zone and its purpose.
3. Select an iSTAR Controller for the Intrusion Zone on the **General** tab (shown in Figure 35 on Page 166).
4. Use the **General** tab (shown in Figure 35 on Page 166) to configure the Doors that lead into and out of the Intrusion Zone and the options that affect the use and operation of these doors.
5. Use the **Inputs** tab (shown in Figure 36 on Page 172) to configure Inputs that are controlled/monitored by the Intrusion Zone—including Inputs that are protected 24/7.
6. Use the **Arm-Disarm** tab (shown in Figure 37 on Page 177) to configure the local methods for arming/disarming the Intrusion Zone, the related options, and the exit/entrance delays.
7. Use the **Triggers** tab (shown in Figure 38 on Page 183) to configure triggers that can activate Event Actions when the Intrusion Zone's mode or state has a certain value (for example, armed/disarmed or ready to arm/not ready to arm).
8. Use the **State Images** tab (shown in Figure 41 on Page 191) to change the default images used to indicate states for the iSTAR Intrusion Zone on the Monitoring Station, or to return to the default images.

Viewing a List of iSTAR Intrusion Zones

You can display a list of the iSTAR Intrusion Zones you have created by opening a Dynamic View of iSTAR Intrusion Zones.

> **NOTE** The information in Dynamic Views is dynamically updated.

To View a List of iSTAR Intrusion Zones

1. In the **Navigation** Pane of the Administration Workstation, click **Areas and Zones** to open the **Areas and Zones** pane.
2. Select **iSTAR Intrusion Zone** from the **Areas and Zones** drop-down list.
3. Click ➡ ▾ to open a Dynamic View listing all iSTAR Intrusion Zone Objects. (You can also click the down-arrow of this button to either view the list in the current tabbed view or open a new tabbed view.)
   - You can sort, filter, and group items in the list.
   - You can right-click an iSTAR Intrusion Zone in the list to open the iSTAR Intrusion Zone Context menu (see Table 31 on Page 158) and perform any of the functions on that menu.

(See Viewing Doors/Inputs for an Intrusion Zone on Page 159.)

- You can right-click any column heading to open a context menu of all possible Intrusion Zone fields that can display as columns and add/remove fields to view status information. See Viewing Intrusion Zone Status on the Dynamic View on Page 161.

For more information on using Dynamic Views, see the Dynamic Views chapter in the *C•CURE 9000 Data Views Guide*.

iSTAR Intrusion Zone List Context Menu

The context menu that opens when you right-click an iSTAR Intrusion Zone in the iSTAR Intrusion Zone Dynamic View includes the selections described in Table 31 on Page 158.

Table 31: iSTAR Intrusion Zone List Right-Click Context Menu Options

Menu Selection	Description
Edit	Click this menu selection to edit the selected iSTAR Intrusion Zone. The **iSTAR Intrusion Zone Editor** opens (with the addition of a **Groups** tab, which displays any Groups that this zone belongs to). You can rename the iSTAR Intrusion Zone, change the description and any other attributes with the exception of the iSTAR Controller.
Delete	Click this menu selection to delete the selected iSTAR Intrusion Zone. A prompt appears asking you to confirm that you want to delete the iSTAR Intrusion Zone. Click **Yes** to delete the iSTAR Intrusion Zone or **No** to cancel the deletion.
Set property	Click this menu selection to change the value of the selected properties in the selected iSTAR Intrusion Zone(s). A dialog box appears asking you to select a property to change. Click ... to open a selection list and click the property you wish to change. You can then change the value of the following properties: • **Allow Disarm While Violated**– You can determine whether or not the iSTAR Intrusion Zone(s) can be disarmed while in Violated mode by selecting this property and selecting/clearing the **Value** check box. • **Description** – You can change the textual description of the iSTAR Intrusion Zone(s) by selecting this property and typing in a new value. • **Enabled** – You can determine whether or not the iSTAR Intrusion Zone(s) are activated on the system by selecting this property and selecting/clearing the **Value** check box.
Add to Group	You can add one or more selected iSTAR Intrusion Zones to a Group of iSTAR Intrusion Zones. When you click this menu choice, a dialog box appears for you to select the Group to which to add the iSTAR Intrusion Zone(s). When you click a Group of iSTAR Intrusion Zones in the list, the selected iSTAR Intrusion Zone(s) are added to the Group.

iSTAR Intrusion Zone List Right-Click Context Menu Options (continued)

Menu Selection	Description
Export selection	Click this menu selection to Open an Export...to XML or CSV file dialog box to export one or more of the selected iSTAR Intrusion Zone records to either an XML or a CSV file. This allows you to quickly and easily create XML/CSV reports on the selected data. NOTE: Although XML is the initial default file type, once you choose a type in the **Save as type** field, whether XML or CSV, that becomes the default the next time this dialog box opens. CSV-formatted exports **cannot** be imported. If you require importing functionality, export to XML. • When you export to an XML file, all available data for the selected object(s), whether displayed in the Dynamic View or not—as well as all the child objects of the selected record(s), is exported. • When you export to a CSV file, only data in the columns displaying in the Dynamic View is exported, and in the order displayed. This allows you to both select and arrange data fields for your report. In addition, exporting to a CSV file allows you to view the exported data in an Excel spreadsheet and further manipulate it for your use. For more information, see the Dynamic Views chapter in the *C•CURE 9000 Data Views Guide*. NOTE: When you click **Export Selection**, you are running the export on the client computer. Consequently, the system does not use the Default Export Directory Path—which is on the server. It opens a directory on the client, reverting to the last directory used. You can navigate to the default export server directory, if you wish. Or to avoid confusion or use the same destination folder for both client and server computers, you can use UNC (Universal Naming Convention) paths, for example: \\Computer Name\Program Files\Software House\SWHouse\SWHSystem\Export.
Find in Audit Log	Click this menu selection to Open a **Query Parameters** dialog box in which you can enter prompts and/or modify the Query criteria to search for entries in the Audit Log that reference the selected iSTAR Intrusion Zone. When found the results display in a separate Dynamic View.
Find in Journal	Click this menu selection to Open a **Query Parameters** dialog box in which you can enter prompts and/or modify the Query criteria to search for entries in the Journal that reference the selected iSTAR Intrusion Zone. When found the results display in a separate Dynamic View.
Arm	Click this menu selection to arm the selected Intrusion Zone. NOTE: This menu option is available only if the iSTAR Intrusion Zone's Controller is enabled.
Disarm	Click this menu selection to disarm the selected Intrusion Zone. NOTE: This menu option is available only if the iSTAR Intrusion Zone's Controller is enabled.
Force Arm	Click this menu selection to force arm the selected Intrusion Zone. NOTE: This menu option is available only if the iSTAR Intrusion Zone's Controller is enabled.
Monitor	Click this menu selection to view activity for the selected Intrusion Zone(s), and any Door, Input, and Trigger-with-target-Event children, on an Admin Monitor Activity Viewer. For more information, see "Monitoring an Object from the Administration Station" in the *C•CURE 9000 Getting Started Guide*.
Display Doors and Inputs	Click this menu selection to open the **Doors and Inputs of [selected Intrusion Zone]** Dynamic View. These lists include respectively all of the selected Intrusion Zone's Doors and its Controlled and Monitored Inputs. By default, the Dynamic Views show the name of the Door(s)/Input(s) and their Intrusion Zone Status. (See Viewing Doors/Inputs for an Intrusion Zone on Page 159.) You can also right-click any column heading to view a list of other available Door/Input fields that can display as columns. For more information, see the Dynamic Views chapter in the *C•CURE 9000 Data Views Guide*.

Viewing Doors/Inputs for an Intrusion Zone

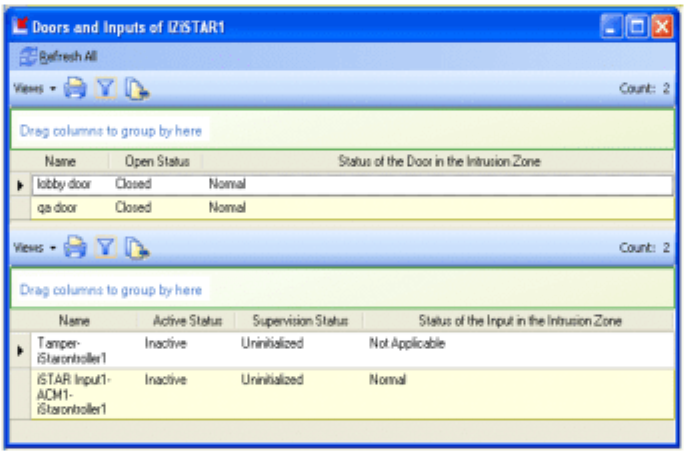
You can select an existing Intrusion Zone on the Dynamic View and display lists of its Doors and Inputs with relevant Intrusion Status and other information.

NOTE	The Dynamic Views for both iSTAR Doors and iSTAR Inputs allow you to add a column that names the Intrusion Zone to which the Doors/Inputs belong.

To View an Intrusion Zone's Doors/Inputs

1. On the **iSTAR Intrusion Zone** Dynamic View, right-click an iSTAR Intrusion Zone in the list to open the iSTAR Intrusion Zone Context menu (see Table 31 on Page 158).
2. Click **Display Door and Inputs**. The lists such as those shown in the example in Figure 34 on Page 160 display.

Figure 34: Doors and Inputs List for iSTAR Intrusion Zone


Doors and Inputs of IZiSTAR1
Refresh All
Views
Count: 2
Drag columns to group by here
Views
Count: 2
Drag columns to group by here

Name	Open Status	Status of the Door in the Intrusion Zone
lobby door	Closed	Normal
qa door	Closed	Normal

Name	Active Status	Supervision Status	Status of the Input in the Intrusion Zone
Tamper-iStarontroller1	Inactive	Uninitialized	Not Applicable
iSTAR Input1-ACM1-iStarontroller1	Inactive	Uninitialized	Normal

The screen displays a Dynamic View list of the selected Intrusion Zone's Doors on the top and a Dynamic View list of its Controlled/Monitored Inputs on the bottom. By default, the Dynamic Views show the name of the Door (s)/Input(s) and their Intrusion Zone Status. The Dynamic Views have the fields described in Table 32 on Page 160.

- You can sort, filter, and group items in the lists.
- You can also right-click any column heading to view a list of other available Door/Input fields that can display as columns.

If new Doors/Inputs are added to the zone while this Dynamic View is open, the list updates automatically.

For more information, see the Dynamic Views chapter in the C•CURE 9000 *Data Views Guide*.

Table 32: Doors and Inputs of iSTAR Intrusion Zone Fields

Fields	Description
(Doors)	
Name	Door system name
Open Status	Open Closed
Status of the Door in the Intrusion Zone	Normal Offnormal (would violate zone if zone were armed) Not Applicable (host may not be communicating with Controller)

Doors and Inputs of iSTAR Intrusion Zone Fields (continued)

Fields	Description
(Inputs – Controlled & Monitored)	
Name	Input system name
Active Status	Active Inactive
Supervision Status	Uninitialized Supervision Error or specific error, such as Open Loop, Line Fault, etc.
Status of the Input in the Intrusion Zone	Controlled Input: Normal Offnormal (would violate zone if zone were armed) Not Applicable (host may not be communicating with Controller) Monitored Input: always Not Applicable

Viewing the Status of an iSTAR Intrusion Zone

You can view basic status information about an Intrusion Zone in three different places:

- Administration application
  - **iSTAR Intrusion Zone** Dynamic View – see Viewing Intrusion Zone Status on the Dynamic View on Page 161.
  - **iSTAR Intrusion Zone Editor Status** tab – see Viewing Intrusion Zone Status on the Status Tab on Page 189.
- Monitoring Station: **Explorer Bar>Non-Hardware Status> Intrusion Zones>Status List - iSTAR Intrusion Zones** – see the Monitoring Status chapter in the *C•CURE 9000 Monitoring Station Guide*.

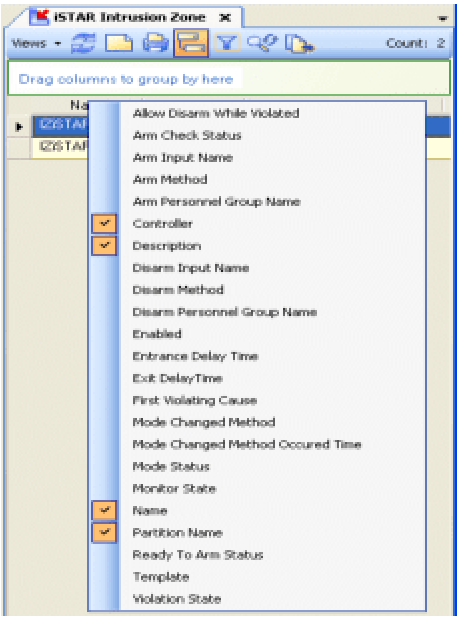
Viewing Intrusion Zone Status on the Dynamic View

This section briefly describes procedures for displaying Intrusion Zone status information on the iSTAR Intrusion Zone dynamic view. However, these changes are only in effect while you have the View open. To actually change the View permanently, you need to configure the view and save your changes. For information, see the Dynamic Views chapter in the *C•CURE 9000 Data Views Guide*.

To View Intrusion Zone Status Information

1. On the **iSTAR Intrusion Zone** Dynamic View, right-click any column heading.

   A context menu of all available Intrusion Zone fields that can display as columns appears.



Fields that are currently displayed in the view are marked with a ✓.

2. To add fields as columns to view status information, click anywhere on that field in the list.

   Example:

   First Violating Cause/Mode Changed Method/Mode Changed Method Occurred Time/Mode Status/Ready To Arm Status

3. To remove a field as a column in the Dynamic View, click a field in the list that has a ✓.

4. To change the left/right order of the columns to your liking, click any column heading and drag that column to a new position. The Dynamic View columns are adjusted to the new column order you established.

5. To change the column width:

   a. Move the cursor to the edge of the column heading you wish to resize. The cursor changes to ↔.

   b. Drag this cursor to the left or right and release the mouse button to make the column wider or narrower.

Modifying an iSTAR Intrusion Zone

You can modify an existing iSTAR Intrusion Zone by editing it using the **iSTAR Intrusion Zone Editor**.

To Modify an iSTAR Intrusion Zone

1. In the **Navigation** Pane of the Administration Workstation, click **Areas and Zones** to open the **Areas and Zones** pane.

2. Select iSTAR Intrusion Zone from the **Areas and Zones** drop-down list.

3. Click ➔ to open a Dynamic View showing all iSTAR Intrusion Zone Objects.

4. Right-click the iSTAR Intrusion Zone in the list that you want to change and select **Edit** from the context menu that appears.

   - or -

Double-click the iSTAR Intrusion Zone you want to change.

The **iSTAR Intrusion Zone Editor** opens for you to edit the Intrusion Zone making changes as you wish in the fields on the top of the editor, and on any of the tabs (with the exception of the iSTAR Controller). (The Editor now includes a **Groups** tab that displays any Groups to which this iSTAR Intrusion Zone belongs.)

5. To save the modified Intrusion Zone, click **Save and Close**.

   - or -

   Alternatively, if you want to save the Intrusion Zone and then create a new one, click **Save and New**. The current iSTAR Intrusion Zone is saved and closed, but the **iSTAR Intrusion Zone Editor** remains open ready for a new iSTAR Intrusion Zone.

Deleting an iSTAR Intrusion Zone

You can delete an iSTAR Intrusion Zone.

To Delete an iSTAR Intrusion Zone

1. In the **Navigation** Pane of the Administration Workstation, click **Areas and Zones** to open the **Areas and Zones** pane.
2. Select iSTAR Intrusion Zone from the **Areas and Zones** drop-down list.
3. Click ➡ ▾ to open a Dynamic View showing all iSTAR Intrusion Zone Objects.
4. Right-click the iSTAR Intrusion Zone in the list that you want to delete and select **Delete** from the context menu that appears.
5. Click **Yes** on the "Are you sure you want to delete the selected iSTAR Intrusion Zone?" message box.

Setting a Property for an iSTAR Intrusion Zone

You can use **Set Property** to quickly set a property for an iSTAR Intrusion Zone without opening the **iSTAR Intrusion Zone Editor**. You use Set Property for mass updates. See on Page 157 for the properties that can be changed.

To Set a Property for iSTAR Intrusion Zones

1. In the **Navigation** Pane of the Administration Workstation, click **Areas and Zones** to open the **Areas and Zones** pane.
2. Select **iSTAR Intrusion Zone** from the **Areas and Zones** drop-down list.
3. Click ➡ ▾ to open a Dynamic View showing all iSTAR Intrusion Zone Objects.
4. Right-click the iSTAR Intrusion Zone in the list for which you want to set the property and select **Set Property** from the context menu.
5. Specify the property for the Intrusion Zone. Click the drop-down button to see a list of properties.
6. Enter the value for the property and click **OK**.
7. Click **OK** on the **Setting Properties of iSTAR Intrusion Zone** message box.

Adding an iSTAR Intrusion Zone to a Group

Use **Add To Group** to add the iSTAR Intrusion Zone Object to a Group.

To Add iSTAR Intrusion Zones To a Group

1. Make sure that the Group is already configured for the iSTAR Intrusion Zone to be added to it.
2. In the **Navigation** Pane of the Administration Workstation, click **Areas and Zones** to open the **Areas and Zones** pane.
3. Select **iSTAR Intrusion Zone** from the **Areas and Zones** drop-down list.
4. Click ➡ ▾ to open a Dynamic View showing all iSTAR Intrusion Zone Objects.
5. Right-click the Intrusion Zone in the list that you want to add to a Group and select **Add To Group** from the context menu.
6. When the **Group** list displays, select the Group you want to add the iSTAR Intrusion Zone to. The name and description of the Group now display on the **Groups** tab of the **iSTAR Intrusion Zone** Editor.

iSTAR Intrusion Zone Editor

The **iSTAR Intrusion Zone Editor**, shown in Figure 35 on Page 166, in C•CURE 9000 lets you create and modify iSTAR Intrusion Zone Objects. The **iSTAR Intrusion Zone Editor** displays the following tabs for configuring Intrusion Zones:

- iSTAR Intrusion Zone General Tab on Page 166
- iSTAR Intrusion Zone Inputs Tab on Page 172
- iSTAR Intrusion Zone Arm - Disarm Tab on Page 177
- iSTAR Intrusion Zone Triggers Tab on Page 183
- iSTAR Intrusion Zone Groups Tab on Page 188 (when editing an existing Intrusion Zone)
- iSTAR Intrusion Zone Status Tab on Page 189
- iSTAR Intrusion Zone State Images Tab on Page 191

The **iSTAR Intrusion Zone Editor** has the buttons described in Table 33 on Page 165.

Table 33: iSTAR Intrusion Zone Editor Buttons

Button	Description
Save and Close	Click this button when you have completed changes to the iSTAR Intrusion Zone and wish to save those changes. The iSTAR Intrusion Zone closes.
Save and New	Click this button when you have completed any changes to the iSTAR Intrusion Zone and wish to save those changes and also create a new iSTAR Intrusion Zone. The iSTAR Intrusion Zone you were editing is saved, and a new iSTAR Intrusion Zone opens (either blank or including template information if you were using a template to create the new iSTAR Intrusion Zone).
☒	Click this button when you want to close the **iSTAR Intrusion Zone Editor** without saving your changes. A warning appears asking whether or not you want to save your changes before closing the editor. Click **Yes** to exit and save and **No** to exit and cancel your changes.

iSTAR Intrusion Zone General Tab

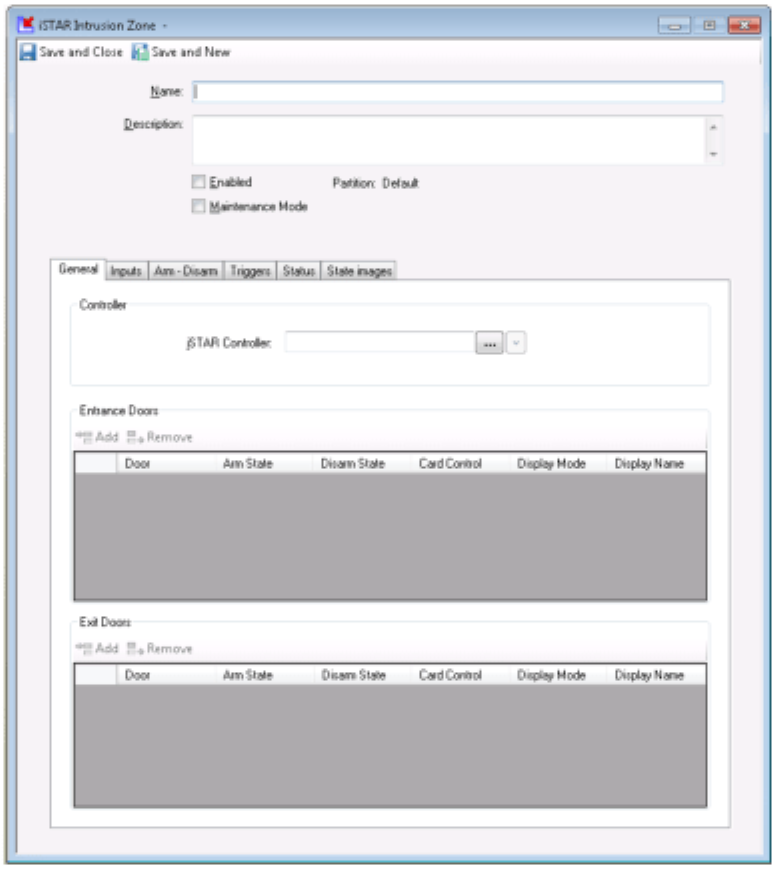
The **iSTAR Intrusion Zone General** tab, shown in Figure 35 on Page 166, lets you define the doors for the Intrusion Zone.

Definitions for this tab are provided in iSTAR Intrusion Zone General Tab Definitions on Page 167.

You can perform the following tasks from the **iSTAR Intrusion Zone General** tab:

- Configuring iSTAR Intrusion Zone Entrance/Exit Doors on Page 169
- Deleting iSTAR Intrusion Zone Entrance/Exit Doors on Page 171

Figure 35: iSTAR Intrusion Zone Editor General Tab



□ Enabled

□ Maintenance Mode

Partition: Default

iSTAR Intrusion Zone Editor Definitions

The **iSTAR Intrusion Zone Editor** has the fields shown in Table 34 on Page 166.

Table 34: iSTAR Intrusion Zone Editor Fields

Fields/Buttons	Description
Name	Enter a unique name, up to 100 characters, to identify the iSTAR Intrusion Zone.

iSTAR Intrusion Zone Editor Fields (continued)

Fields/Buttons	Description
Description	Enter a description of the iSTAR Intrusion Zone, up to 255 characters.
Enabled	Select this check box to activate the iSTAR Intrusion Zone.
Partition	A read-only field displaying the name of the Partition to which this iSTAR Intrusion Zone belongs. (This field is visible only if the C•CURE 9000 system is partitioned.) NOTE: The Intrusion Zone derives its Partition from the selected iSTAR Controller. If the Controller's Partition changes—the Partition of the Cluster to which the Controller belongs is changed, then the Intrusion Zone's Partition changes accordingly.
Maintenance Mode	Select this check box to put this Intrusion Zone into Maintenance Mode so whether or not Events, Status, and Activity related to this Intrusion Zone display on the Monitoring Station depends on the Operator's Privilege and the Application Layout assigned. For detailed information, see the Maintenance Mode chapter in the *C•CURE 9000 Hardware Configuration Guide*.

iSTAR Intrusion Zone General Tab Definitions

The **iSTAR Intrusion Zone General** tab has the buttons shown in Table 35 on Page 167 (in the **Entrance Doors** and **Exit Doors** tables) and the fields shown in Table 36 on Page 167.

Table 35: iSTAR Intrusion Zone Editor - General Tab Buttons

Button	Description
Add	Click this button to add a new blank row to the **Entrance Doors** or **Exit Doors** table. Each new row is added after the last. To add a new row after a specific existing row, click the row selector ▶ to select a row and then click Add.
Remove	Click this button to remove a selected row from the **Entrance Doors** or **Exit Doors** table. You have to click the row selector ▶ to select a row to remove. If **no** row is selected, this button is **not** available.

Table 36: iSTAR Intrusion Zone Editor - General Tab Fields

Fields/Buttons	Description
Controller	
iSTAR Controller	Select the controller for the Intrusion Zone. NOTE: The **Add** and **Remove** buttons in the **Entrance Doors** and **Exit Doors** tables become available when you select the Controller. Once you select the Controller and add either a Door or an Input, you **cannot** change the Controller.
Entrance Doors	

iSTAR Intrusion Zone Editor - General Tab Fields (continued)

Fields/Buttons	Description
Door	Click in the **Door** field to display ..., and then click this button to select a Door from the dialog box that appears. The Door must belong to the selected Controller and not yet be assigned to any Intrusion Zone. Once a Door is selected, the **Door Editor Areas & Zones** tab displays read-only Intrusion Zone information. See Viewing Intrusion Zone Information on the Door Editor on Page 193. NOTE: Once a Door is selected for a row, it **cannot** be changed, although its attributes can be changed, and the entire row can be removed.
Arm State	Click the down-arrow to select from the drop-down list the mode that this door is set to when the Intrusion Zone is **Armed**: **Locked**, **Secured**, or **Unlocked** (For detailed Door state information, see Doors on Page 149.)
Disarm State	Click the down-arrow to select from the drop-down list the mode that this door is set to when the Intrusion Zone is **Disarmed**: **Locked**, **Secured**, or **Unlocked** (For detailed Door state information, see Doors on Page 149.)
Card Control	Click to select this check box to allow this Door to use the Card Arm/Disarm method to arm or disarm the Intrusion Zone. The default is cleared.
Display Mode	Click the down-arrow to select the display mode for the LCDs on this Door's Reader from the drop-down list. **Blank** – The LCD displays date/time and the normal Door information with momentary displays of Intrusion Zone mode changes. This is the default. **Status** – The LCD displays date/time on the first line and the second line displays dynamically changing information about the Intrusion Zone's state. For more detailed information and an illustrative graphic, see Display on Page 150.
Display Name	Click in this field and type the name that you want displayed on the Reader LCD display for the Door—up to 16 characters (restricted to printable ASCII characters and the "space"). NOTE: This field allows you to create an LCD display name for this Intrusion Zone Door. If you do not enter a name here, the system will use the rightmost 16 characters of the Door's name. The Display Name is used whenever the Intrusion Zone needs to display this door as an 'offnormal' point on the Reader LCD. (This name does not have to be 'unique.')
Exit Doors	
Door	Click in the **Door** field to display ..., and then click this button to select a Door from the dialog box that appears. The Door must belong to the selected Controller and not yet be assigned to any Intrusion Zone. Once a Door is selected, the **Door Editor Areas & Zones** tab displays read-only Intrusion Zone information. See Viewing Intrusion Zone Information on the Door Editor on Page 193. NOTE: Once a Door is selected for a row, it **cannot** be changed, although its attributes can be changed, and the entire row can be removed.
Arm State	Click the down-arrow to select from the drop-down list the mode that this door is set to when the Intrusion Zone is **Armed**: **Locked**, **Secured**, or **Unlocked** (For detailed Door state information, see Doors on Page 149.)
Disarm State	Click the down-arrow to select from the drop-down list the mode that this door is set to when the Intrusion Zone is **Disarmed**: **Locked**, **Secured**, or **Unlocked** (For detailed Door state information, see Doors on Page 149.)
Card Control	Click to select this check box to allow this Door to use the Card Arm/Disarm method to arm or disarm the Intrusion Zone. The default is cleared.

iSTAR Intrusion Zone Editor - General Tab Fields (continued)

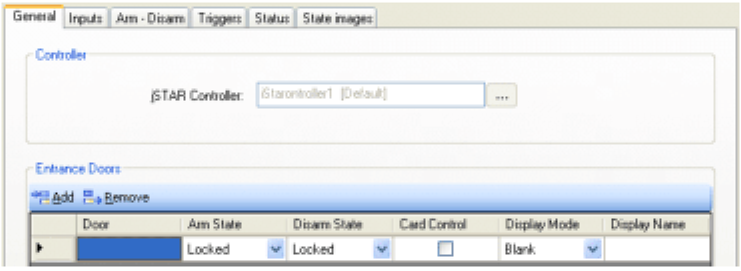
Fields/Buttons	Description
Display Mode	Click the down-arrow to select the display mode for the LCDs on this Door's Reader from the drop-down list. **Blank** – The LCD displays date/time and the normal Door information with momentary displays of Intrusion Zone mode changes. This is the **default**. **Status** – The LCD displays date/time on the first line and the second line displays dynamically changing information about the Intrusion Zone's state.
Display Name	Click in this field and type the name that you want displayed on the Reader LCD display for the Door—up to 16 characters (restricted to printable ASCII characters and the "space"). NOTE: This field allows you to create an LCD display name for this Intrusion Zone Door. If you do not enter a name here, the system will use the rightmost 16 characters of the Door's name. The Display Name is used whenever the Intrusion Zone needs to display this door as an 'offnormal' point on the Reader LCD. (This name does not have to be 'unique.')

Configuring iSTAR Intrusion Zone Entrance/Exit Doors

This procedure assumes that you have already selected the iSTAR Controller for the Intrusion Zone and have configured Doors and Readers.

To Configure iSTAR Intrusion Zone Entrance/Exit Doors

1. Create or modify an iSTAR Intrusion Zone. See:
   - Creating an iSTAR Intrusion Zone on Page 155
   - Modifying an iSTAR Intrusion Zone on Page 162
2. On the **General** tab of the **iSTAR Intrusion Zone Editor** in the **Entrance Doors** box or the **Exit Doors** box, click **Add** to create a new row, as shown in the following example for the Entrance Doors.

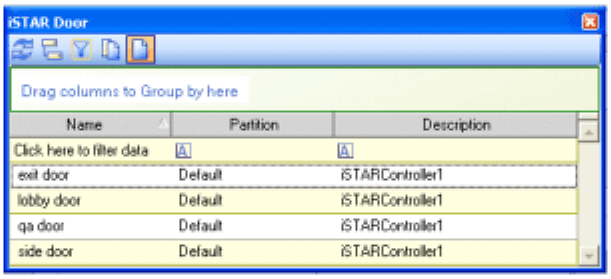


iSTAR Controller: iStarontroller1 [Default]

	Door	Arm State	Disarm State	Card Control	Display Mode	Display Name
▸		Locked	Locked	□	Blank	

3. Click in the **Door** field to display ... and click this button.

   A selection list opens with the Doors available for iSTAR Intrusion Zones.



iSTAR Door

Drag columns to Group by here

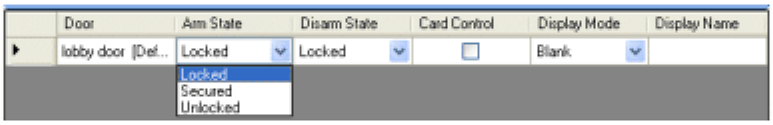
Name	Partition	Description
Click here to filter data	A	A
exit door	Default	iSTARController1
lobby door	Default	iSTARController1
qa door	Default	iSTARController1
side door	Default	iSTARController1

4. Click a Door to add it to the row.

   Example:

   lobby door

5. Click the down-arrow in the **Arm State** field to display a drop-down list of access control modes: Locked/Secured/Unlocked. (The default entry is Locked.)



Door	Arm State	Disarm State	Card Control	Display Mode	Display Name
lobby door (Def...	Locked	Locked	□	Blank	

6. Click the **Mode** you want set for this Door when the Intrusion Zone is in the Armed state to add it to the row.

   Example:

   Locked

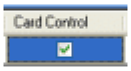
7. Click the down-arrow in the **Disarm State** field to display a drop-down list of access control modes: also Locked/Secured/Unlocked. (The default entry is Locked.)

8. Click the **Mode** you want set for this Door when the Intrusion Zone is in the Disarmed state to add it to the row.

   Example:

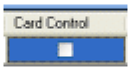
   Unlocked

9. To allow the Intrusion Zone to be armed/disarmed using card methods at this Door, click to select the check box in the **Card Control** field. (The default entry is cleared.)

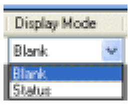


- or -

To **not** allow card method Arming/Disarming at this door, do not select the check box.



10. Click the down-arrow in the **Display Mode** field to display the mode drop-down list: Blank/Status. (The default entry is Blank.)



11. Click the LCD-type **Display Mode** you want for this Door's Reader to add it to the row.

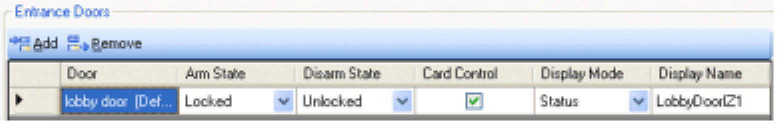
Example:

Status

12. Click in the **Display Name** field and type the name you want displayed for this Door on its Reader's LCD display—up to 16 characters.

NOTE If you do **not** enter a name here, the system uses the 16 rightmost characters of the Door's name.

The row now appears as shown in the following example for an Entrance Door:



Door	Arm State	Disarm State	Card Control	Display Mode	Display Name
lobby door [Def...	Locked	Unlocked	☑	Status	LobbyDoorIZ1

13. To configure more Entrance/Exit Doors for this iSTAR Intrusion Zone, click **Add** in the appropriate box and repeat the preceding steps.

Deleting iSTAR Intrusion Zone Entrance/Exit Doors

Once you have selected a Door for a row, it cannot be changed. You can, however, delete the entire row, removing that Door from the Intrusion Zone.

NOTE If you need to completely delete a Door from the system, you must first make sure to remove it from any Intrusion Zone to which it is assigned.

To Delete an iSTAR Intrusion Zone Entrance/Exit Door

1. On the **General** tab of the **iSTAR Intrusion Zone Editor** in the **Entrance Doors** box or the **Exit Doors** box, click a row to select it.

2. Click **Remove** to delete the Door row.

iSTAR Intrusion Zone Inputs Tab

The **iSTAR Intrusion Zone Inputs** tab, shown in Figure 36 on Page 172, lets you define Inputs to be controlled/monitored by the iSTAR Intrusion Zone as follows:

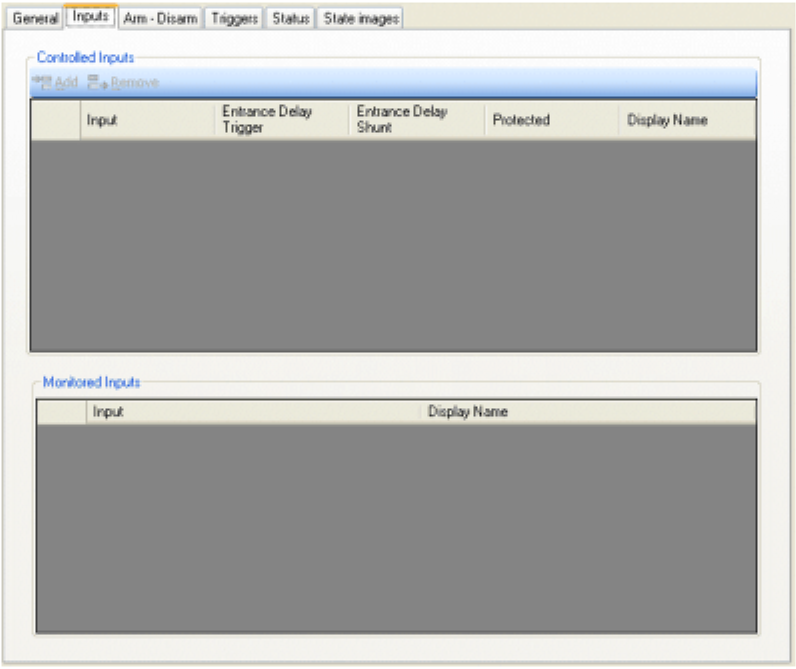
- Set the Controlled/Monitored Inputs that:
  - Cause the Entrance Delay to start.
  - Are shunted during the Entrance Delay.
  - Cause immediate violation of the Intrusion Zone when armed without starting the Entrance Delay.
- Define the Inputs monitored by the Intrusion Zone that are armed 24/7 (Protection Inputs).
- View Monitored Inputs and modify Display Name.

Definitions for this tab are provided in iSTAR Intrusion Zone Inputs Tab Definitions on Page 172.

You can perform the following tasks from the **iSTAR Intrusion Zone Inputs** tab:

- Configuring iSTAR Intrusion Zone Controlled/Protected Inputs on Page 174
- Configuring Display Names for iSTAR Intrusion Zone Monitored Inputs on Page 176
- Deleting iSTAR Intrusion Zone Controlled/Protected Inputs on Page 176

Figure 36: iSTAR Intrusion Zone Editor Inputs Tab



iSTAR Intrusion Zone Inputs Tab Definitions

The **iSTAR Intrusion Zone Inputs** tab has the buttons shown in Table 37 on Page 173 (in the **Controlled Inputs** table) and the fields shown in Table 38 on Page 173.

Table 37: iSTAR Intrusion Zone Editor Inputs Tab Buttons

Button	Description
Add	Click this button to add a row to the **Controlled Inputs** table. Each new row is added after the last. To add a new row after a specific existing row, click the row selector ▸ to select a row and then click Add.
Remove	Click this button to remove a selected row from the **Controlled Inputs** table. You have to click the row selector ▸ to select a row to remove. If **no** row is selected, this button is **not** available.

Table 38: iSTAR Intrusion Zone Editor - Inputs Tab Fields

Fields/Buttons	Description
Controlled Inputs	
Input	Click in the **Input** field to display ..., and then click this button to select an Input from the dialog box that appears. The Input must belong to the selected Controller and not yet be assigned to any Intrusion Zone. Once you select an Input for the Intrusion Zone, the following happens on the **Input Editor**: • On the **General** tab, the value in the **Type** field changes from **General** to **Intrusion Zone**. • The **Intrusion Zone** tab becomes available, displaying read-only information on the Intrusion Zone to which the Input now belongs and the Input's display name. For Information, see Viewing Intrusion Zone Information on the Input Editor on Page 195.
Entrance Delay Trigger	Click this check box to select this Input as an Entrance Delay Trigger for the Intrusion Zone. The default is cleared. If selected, activation of this Input while the Intrusion Zone is armed starts the Entrance Delay and gives the person entering the zone time to disarm the Intrusion Zone. NOTE: The Entrance Delay Trigger must also be selected as Entrance Delay Shunt.
Entrance Delay Shunt	Click this check box to select this Input to be shunted during the Entrance Delay for the Intrusion Zone. The default is cleared.
Protected	Click to select this check box to indicate that this Input is Protected. The default is cleared. Once you make this a Protected Input for the Intrusion Zone, the value in the **Type** field on the **General** tab of the **Input Editor** changes to **Intrusion Zone** - Protected. The **Intrusion Zone** tab becomes available, displaying read-only information on the Intrusion Zone to which the Input now belongs and the Input's display name. For Information, see Viewing Intrusion Zone Information on the Input Editor on Page 195.
Display Name	Click in this field and type the name that you want displayed on the Reader LCD display for the Input—up to 16 characters (restricted to printable ASCII characters and the "space"). NOTE: This field allows you to create an LCD display name for this Intrusion Zone Controlled Input. If you do not enter a name here, the system will use the rightmost 16 characters of the Input's name. The Display Name is used whenever the Intrusion Zone needs to display this door as an 'offnormal' point on the Reader LCD. (This name does not have to be 'unique.')

iSTAR Intrusion Zone Editor - Inputs Tab Fields (continued)

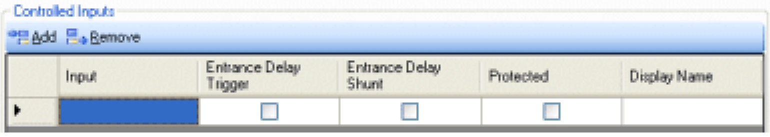
Fields/Buttons	Description
Monitored Inputs	The system automatically populates this table based on the Doors, Controlled Inputs, and Arming/Disarming Inputs configured for the Intrusion Zone. (For these Monitored Inputs to display in the table they have to have been configured on the iSTAR Controller.) The Monitored Inputs displayed in this table change dynamically if you change the zone's assigned Doors, Controlled Inputs, or Arming/Disarming Inputs. NOTE: The iSTAR Cabinet Tamper Input will automatically be entered here to be monitored by this Intrusion Zone (and all other Intrusion Zones on this Controller) unless its use has been disabled by a System Variable. For more information, see "iSTAR Driver Settings" in the System Variables chapter in the *C•CURE 9000 System Maintenance Guide*.
Input	Input system name
Display Name	Click in this field and type the name that you want displayed on the Reader LCD display for the Input—up to 16 characters (restricted to printable ASCII characters and the "space"). NOTE: This field allows you to create an LCD display name for this Monitored Input. The Display Name is shared between all Intrusion Zones on the same Controller. If you do not enter a name here, the system will use the rightmost 16 characters of the Input's name. The Display Name is used whenever the Intrusion Zone needs to display this Input as an 'offnormal' point on the Reader LCD. (This name does not have to be 'unique.')

Configuring iSTAR Intrusion Zone Controlled/Protected Inputs

This procedure assumes that you have already selected the iSTAR Controller for the Intrusion Zone and have configured Doors, Readers, and Inputs.

To Configure iSTAR Intrusion Zone Controlled/Protected Inputs

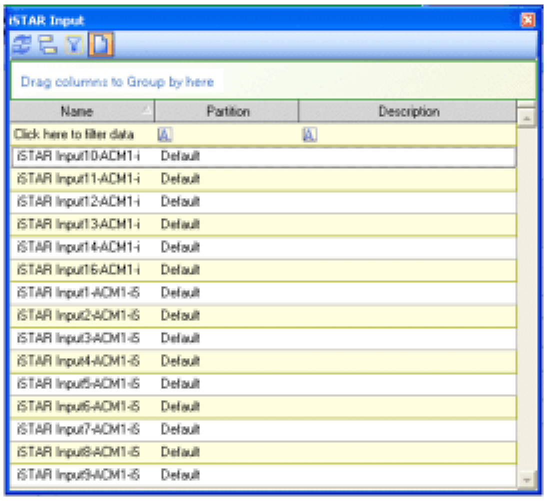
1. Create or modify an iSTAR Intrusion Zone. See
   - Creating an iSTAR Intrusion Zone on Page 155
   - Modifying an iSTAR Intrusion Zone on Page 162
2. On the **iSTAR Intrusion Zone Editor**, click the **Inputs** tab to open.
3. In the **Controlled Inputs** box, click **Add** to create a new row.



	Input	Entrance Delay Trigger	Entrance Delay Shunt	Protected	Display Name
▶		□	□	□	

4. Click in the **Input** field to display ... and click this button.

   A selection list opens with the Inputs available for iSTAR Intrusion Zones.



iSTAR Input

Drag columns to Group by here

Name	Partition	Description
Click here to filter data		
iSTAR Input10-ACM1-i	Default	
iSTAR Input11-ACM1-i	Default	
iSTAR Input12-ACM1-i	Default	
iSTAR Input13-ACM1-i	Default	
iSTAR Input14-ACM1-i	Default	
iSTAR Input16-ACM1-i	Default	
iSTAR Input1-ACM1-iS	Default	
iSTAR Input2-ACM1-iS	Default	
iSTAR Input3-ACM1-iS	Default	
iSTAR Input4-ACM1-iS	Default	
iSTAR Input5-ACM1-iS	Default	
iSTAR Input6-ACM1-iS	Default	
iSTAR Input7-ACM1-iS	Default	
iSTAR Input8-ACM1-iS	Default	
iSTAR Input9-ACM1-iS	Default	

5. Click an Input to add it to the row.

   Example:

   iSTAR Input1-ACM1-iSTARontroller1

6. To make this Input an Entrance Delay Trigger for the Intrusion Zone, click to select the check box in the **Entrance Delay Trigger** field. (The default entry is cleared.)
7. To select this Input to be shunted during Entrance Delays for the Intrusion Zone, click to select the check box in the **Entrance Delay Shunt** field. (The default entry is cleared.)
8. To configure this Input to be protected 24/7, click to select the check box in the **Protected** field. (The default entry is cleared.)

NOTE A **Protected** Input **cannot** be an Entrance Delay Trigger, **nor** can it be shunted during Entrance Delay.

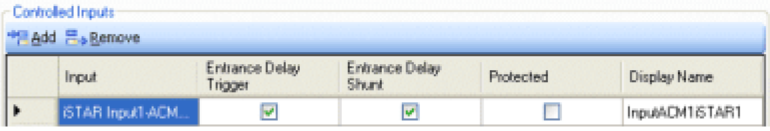
9. Click in the **Display Name** field and type the name you want displayed for this Input on the Reader's LCD display—up to 16 characters.

   Example:

   Zone5

NOTE If you do **not** enter a name here, the system uses the 16 rightmost characters of the Input's name. (This name does not have to be 'unique.')

The row now appears as shown in the following example:



Controlled Inputs

Add Remove

	Input	Entrance Delay Trigger	Entrance Delay Shunt	Protected	Display Name
▸	iSTAR Input1-ACM...	☑	☑	☐	InputACM1iSTAR1

10. To configure more Controlled Inputs for this iSTAR Intrusion Zone, click **Add** in the appropriate box and repeat the preceding steps.

Configuring Display Names for iSTAR Intrusion Zone Monitored Inputs

This procedure assumes that you have already selected the iSTAR Controller for the Intrusion Zone and have configured Doors, Readers, and Inputs.

To Configure iSTAR Intrusion Zone Monitored Input Display Names

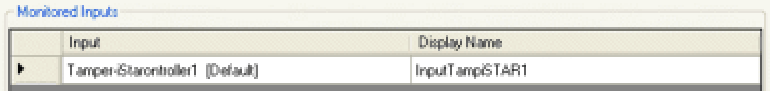
1. Create or modify an iSTAR Intrusion Zone. See:
   - Creating an iSTAR Intrusion Zone on Page 155
   - Modifying an iSTAR Intrusion Zone on Page 162
2. Click in the **Display Name** field and type the name you want displayed whenever the Intrusion Zone needs to display this Input as an 'offnormal' point on the Reader LCD—up to 16 characters. (This Display Name is shared between all Intrusion Zones on the same Controller.)

   Example:

   Input1TampiSTAR1

   NOTE If you do **not** enter a name here, the system uses the 16 rightmost characters of the Input's name. (This name does not have to be 'unique.')

   The row now appears as shown in the following example:

   Monitored Inputs

	Input	Display Name
▸	Tamper-iStarontroller1 (Default)	InputTampiSTAR1

3. To enter Display Names for any other Monitored Inputs for this iSTAR Intrusion Zone, repeat the preceding step.

Deleting iSTAR Intrusion Zone Controlled/Protected Inputs

Once you have selected a Controlled Input for a row, it cannot be changed. You can, however, delete the entire row, removing that Input from the Intrusion Zone.

NOTE If you need to completely delete a Controlled/Protected Input from the system, you must first make sure to remove it from any Intrusion Zone to which it is assigned.

To Delete an iSTAR Intrusion Zone Controlled/Protected Input

1. On the **Inputs** tab of the **iSTAR Intrusion Zone Editor** in the **Controlled Inputs** box, click a row to select it.
2. Click **Remove** to delete the Input row.

iSTAR Intrusion Zone Arm - Disarm Tab

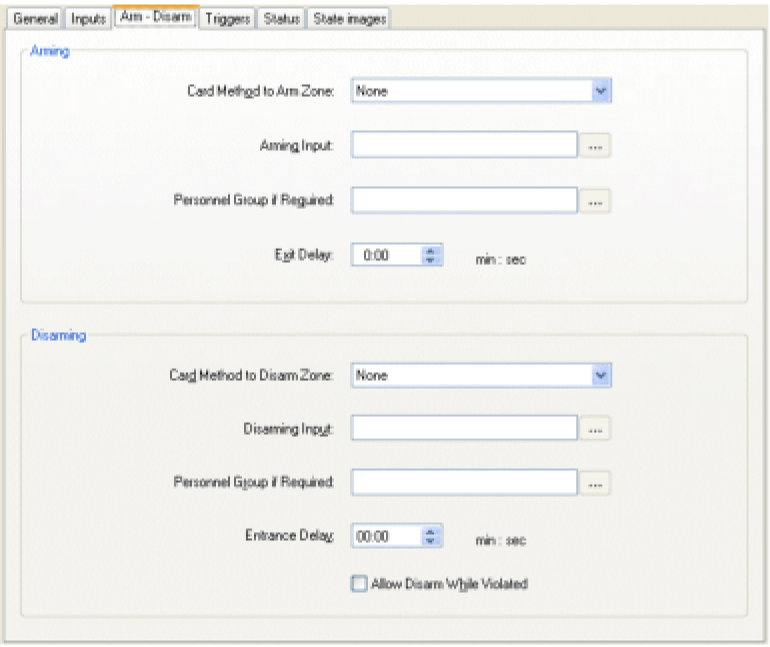
The **iSTAR Intrusion Zone Arm - Disarm** tab, shown in Figure 37 on Page 177, lets you define the local methods for arming and disarming the Intrusion Zone, the related options, and the exit and entrance delays. Definitions for this tab are provided in iSTAR Intrusion Zone Arm - Disarm Tab Definitions on Page 177.

You can perform the following tasks from the **iSTAR Intrusion Zone Arm - Disarm** tab:

- Configuring Arming for an iSTAR Intrusion Zone on Page 179
- Configuring Disarming for an iSTAR Intrusion Zone on Page 181

> **NOTE** Other methods that can be used to arm/disarm an Intrusion Zone include:
>
> - Host manual actions (guard privileges control this)
> - Keypad Commands
> - Event Actions (activated by Triggers)

Figure 37: iSTAR Intrusion Zone Editor Arm - Disarm Tab



Card Method to Arm Zone: None

Arming Input:

Personnel Group if Required:

Exit Delay: 0:00 min : sec

Card Method to Disarm Zone: None

Disarming Input:

Personnel Group if Required:

Entrance Delay: 00:00 min : sec

□ Allow Disarm While Violated

iSTAR Intrusion Zone Arm - Disarm Tab Definitions

The **iSTAR Intrusion Zone Arm - Disarm** tab has the fields shown in Table 39 on Page 178.

Table 39: iSTAR Intrusion Zone Editor - Arm - Disarm Tab Fields

Fields/Buttons	Description
Arming	
Card Method to Arm Zone	Click the down-arrow to select from the drop-down list the Card method required to arm the Intrusion Zone. **None** – **No** Card swipe is allowed to arm the Intrusion Zone. This is the default. (Typically selected to arm with an Event.) **Key Press and Credential** – The person **must** press CMD/ENT twice and then swipe a card with Clearance. **Active Input and Credential** – The person **must** press an Active Input (selected in the **Arming Input** field—a key activated switch, for example) and then swipe a card with Clearance. **Key Press, Credential and Personnel group** – The person **must** press CMD/ENT twice and then swipe a card with Clearance, and must also belong to the Personnel group designated in the **Personnel Group if Required** field. NOTE: Personnel with the **Intrusion Zone Administrator** option selected (**Personnel General** tab) who have clearance to the door do **not** have to be in the Personnel Group to validly use the command. **Active Input, Credential and Personnel Group** – The person **must** press an Active Input (selected in the **Arming Input** field—a key activated switch, for example) and then swipe a card with Clearance, and must also belong to the Personnel group designated in the **Personnel Group if Required** field.
Arming Input	NOTE: This field is available only if the Card Method selected in the preceding field specifies an Active Input. Click ... and select an Input from the dialog box to act as the Active Input to arm this Intrusion Zone. The same Input can be used for both arming and disarming the Intrusion Zone. (Only Inputs on the Controller not yet assigned to any other function and not configured on the Intrusion Zone **Inputs** tab as a Controlled Input display in the list.) The Input you select has its type changed from 'General' to Intrusion Zone' once you save the Intrusion Zone configuration.
Personnel Group if Required	NOTE: This field is available only if the Card Method selected in the **Card Method to Arm Zone** field specifies a Personnel Group. Click ... and select a **Personnel Group** from the dialog box that appears. NOTE: Personnel with the **Intrusion Zone Administrator** option selected (**Personnel General** tab) can always arm the Intrusion Zone without being in the specified Personnel Group—if they have clearance to the door.
Exit Delay min:sec	Click the up- and down-arrows to set the Exit Delay time in minutes and seconds. The range is from 00:00 to 2:00 (min:sec). If an Exit Delay time is set, when arming of the Intrusion Zone is activated by the selected method, the Exit Delays starts, giving the person exiting the zone time to leave without the Intrusion Zone going into Violation.
Disarming	
Card Method to Disarm Zone	Click the down-arrow to select from the drop-down list he Card method required to disarm the Intrusion Zone. **None** – No Card swipe is allowed to disarm the Intrusion Zone. This is the default. (Typically selected to disarm with an Event) **Credential Only** – The person **must** swipe a card with Clearance. **Active Input and Credential** – The person **must** press an Active Input (selected in the **Input** field—a key activated switch, for example) and then swipe a card with Clearance. **Credential and Personnel group** – The person **must** swipe a card with Clearance and must also belong to the Personnel group designated in the **Personnel Group if Required** field. NOTE: Personnel with the **Intrusion Zone Administrator** option selected (**Personnel General** tab) who have clearance to the door do **not** have to be in the Personnel Group to validly disarm the Zone. **Active Input, Credential and Personnel Group** – The person **must** press an Active Input (selected in the **Input** field—a key activated switch, for example) and then swipe a card with Clearance, and must also belong to the Personnel group designated in the **Personnel Group if Required** field.

iSTAR Intrusion Zone Editor - Arm - Disarm Tab Fields (continued)

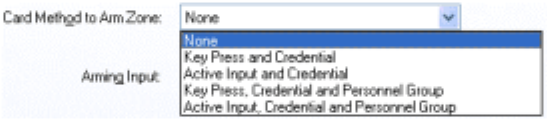
Fields/Buttons	Description
	NOTE: This field is available only if the Card Method selected in the preceding field specifies an Active Input. Click ... and select an Input from the dialog box to act as the Active Input to disarm this Intrusion Zone. The same Input can be used for both arming and disarming the Intrusion Zone. (Only Inputs on the Controller not yet assigned to any other function and not configured on the Intrusion Zone **Inputs** tab as a Controlled Input display in the list.) The Input you select has its type changed from 'General' to Intrusion Zone' once you save the Intrusion Zone configuration.
Personnel Group if Required	NOTE: This field is available only if the Card Method selected in the **Card Method to Disarm Zone** field specifies a Personnel Group. Click ... and select a **Personnel Group** from the dialog box that appears. NOTE: Personnel with the **Intrusion Zone Administrator** option selected (**Personnel General** tab) can always disarm the Intrusion Zone without being in the specified Personnel Group—if they have clearance to the door.
Entrance Delay min:sec	Click the up- and down-arrows to set the Entrance Delay time in minutes and seconds. The range is from 00:00 to 20:30 (min:sec). If an Entrance Delay time is set, a person entering an armed Intrusion Zone activates any Entrance Delay Trigger Input(s) and is given the time to disarm the Intrusion Zone.
Allow Disarm While Violated	Click to select this check box to permit this Intrusion Zone to be disarmed while in Violated mode. The default is cleared. NOTE: If you want the person who disarms an Intrusion Zone at the start of the work day to be aware before the disarm that the zone has been violated during the night, leave this option cleared (not set).

Configuring Arming for an iSTAR Intrusion Zone

This procedure assumes that you have already selected the iSTAR Controller for the Intrusion Zone and have configured Doors, Readers, and Inputs.

To Configure Arming for an iSTAR Intrusion Zone

1. Create or modify an iSTAR Intrusion Zone. See:
   - Creating an iSTAR Intrusion Zone on Page 155
   - Modifying an iSTAR Intrusion Zone on Page 162
2. On the **iSTAR Intrusion Zone Editor**, click the **Arm - Disarm** tab to open.
3. In the **Arming** box, click the down-arrow in the **Card Method to Arm Zone** field to display a drop-down list of card arming methods. (The default is None.)



Card Method to Arm Zone: None

Arming Input:

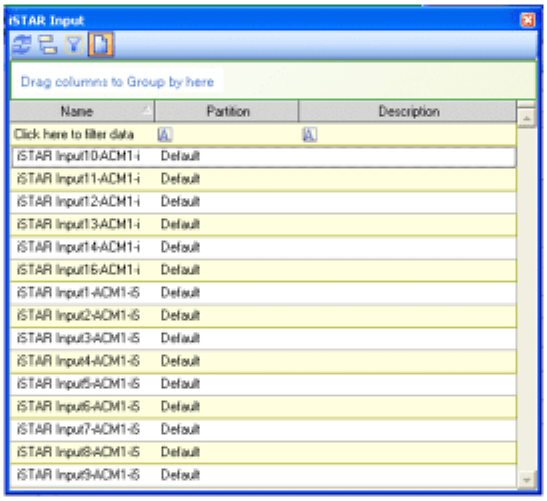
None
Key Press and Credential
Active Input and Credential
Key Press, Credential and Personnel Group
Active Input, Credential and Personnel Group

4. Click the local method you want to be used to arm this Intrusion Zone.

If you select a method requiring an Active Input, the **Arming Input** field becomes available and requires an entry. If you select a method requiring a Personnel Group, the **Personnel Group if Required** field becomes available and requires an entry.

5. If required, click ... next to the **Arming Input** field.

   A selection list opens with the Inputs available for arming iSTAR Intrusion Zones.



iSTAR Input

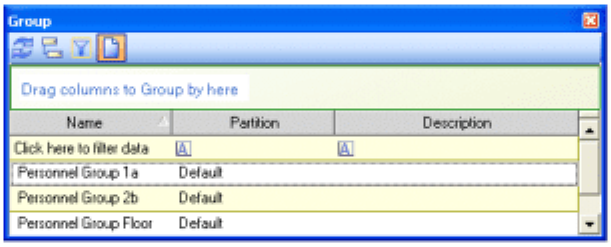
Drag columns to Group by here

Name	Partition	Description
Click here to filter data	A	A
iSTAR Input10-ACM1-i	Default	
iSTAR Input11-ACM1-i	Default	
iSTAR Input12-ACM1-i	Default	
iSTAR Input13-ACM1-i	Default	
iSTAR Input14-ACM1-i	Default	
iSTAR Input16-ACM1-i	Default	
iSTAR Input1-ACM1-i5	Default	
iSTAR Input2-ACM1-i5	Default	
iSTAR Input3-ACM1-i5	Default	
iSTAR Input4-ACM1-i5	Default	
iSTAR Input5-ACM1-i5	Default	
iSTAR Input6-ACM1-i5	Default	
iSTAR Input7-ACM1-i5	Default	
iSTAR Input8-ACM1-i5	Default	
iSTAR Input9-ACM1-i5	Default	

6. Click an Input to select it. (The same Input can be used to both arm and disarm the zone, but it **cannot** be a Controlled Input.)

7. If required, click ... next to the **Personnel Group if Required** field.

   A selection list opens with the available Personnel Groups.



Group

Drag columns to Group by here

Name	Partition	Description
Click here to filter data	A	A
Personnel Group 1a	Default	
Personnel Group 2b	Default	
Personnel Group Floor	Default	

8. Select the Personnel Group to which the person must belong in order to arm the Intrusion Zone.

NOTE Personnel who have the **Intrusion Zone Administrator** option selected on their record and have clearance to the door can always arm the Intrusion Zone even if they are **not** in the selected Personnel Group. For information, see Configuring a Person to Arm/Disarm Intrusion Zones on Page 192.

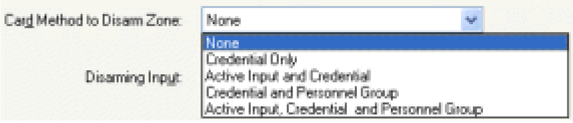
9. In the **Exit Delay** field, click the up- and down-arrows to set the time in minutes and seconds that the person arming the zone by the selected method has to exit before the zone violates. The range is from 00:00 to 2:00 (min:sec).

Configuring Disarming for an iSTAR Intrusion Zone

This procedure assumes that you have already selected the iSTAR Controller for the Intrusion Zone and have configured Doors, Readers, and Inputs.

To Configure Disarming for an iSTAR Intrusion Zone

1. Create or modify an iSTAR Intrusion Zone. See:
   - Creating an iSTAR Intrusion Zone on Page 155
   - Modifying an iSTAR Intrusion Zone on Page 162
2. On the **iSTAR Intrusion Zone Editor**, click the **Arm - Disarm** tab to open.
3. In the **Disarming** box, click the down-arrow in the **Card Method to Disarm Zone** field to display a drop-down list of card disarming methods. (The default is None.)



Card Method to Disarm Zone: None

Disarming Input:

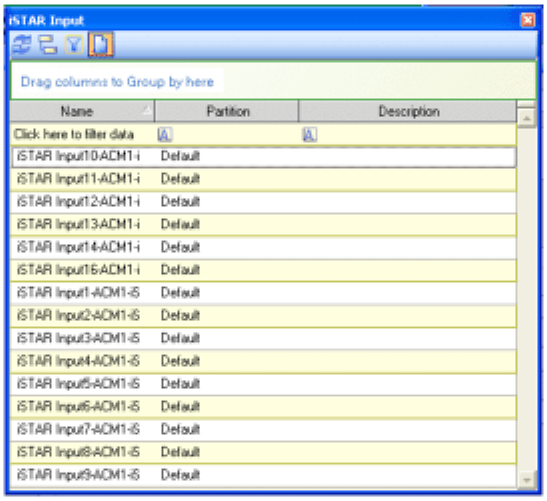
- None
- Credential Only
- Active Input and Credential
- Credential and Personnel Group
- Active Input, Credential and Personnel Group

4. Click the local method you want to be used to disarm this Intrusion Zone.

   If you select a method requiring an Active Input, the **Disarming Input** field becomes available and requires an entry. If you select a method requiring a Personnel Group, the **Personnel Group if Required** field becomes available and requires an entry.

5. If required, click ... next to the **Disarming Input** field.

   A selection list opens with the Inputs available for disarming iSTAR Intrusion Zones.



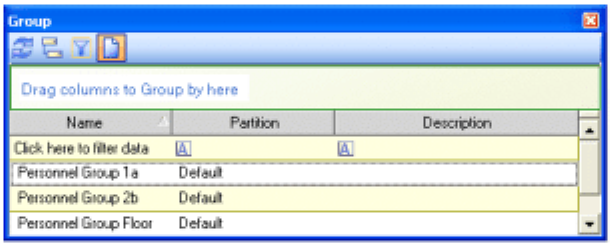
iSTAR Input

Drag columns to Group by here

Name	Partition	Description
Click here to filter data		
iSTAR Input10-ACM1-i	Default	
iSTAR Input11-ACM1-i	Default	
iSTAR Input12-ACM1-i	Default	
iSTAR Input13-ACM1-i	Default	
iSTAR Input14-ACM1-i	Default	
iSTAR Input16-ACM1-i	Default	
iSTAR Input1-ACM1-i5	Default	
iSTAR Input2-ACM1-i5	Default	
iSTAR Input3-ACM1-i5	Default	
iSTAR Input4-ACM1-i5	Default	
iSTAR Input5-ACM1-i5	Default	
iSTAR Input6-ACM1-i5	Default	
iSTAR Input7-ACM1-i5	Default	
iSTAR Input8-ACM1-i5	Default	
iSTAR Input9-ACM1-i5	Default	

6. Click an Input to select it. (The same Input can be used to both arm and disarm the zone, but it **cannot** be a Controlled Input.)
7. If required, click ... next to the **Personnel Group if Required** field.

   A selection list opens with the available Personnel Groups.



Name	Partition	Description
Click here to filter data	A	A
Personnel Group 1a	Default	
Personnel Group 2b	Default	
Personnel Group Floor	Default	

8. Select the Personnel Group to which the person must belong in order to disarm the Intrusion Zone.

NOTE Personnel who have the **Intrusion Zone Administrator** option selected on their record and have clearance to the door can always disarm the Intrusion Zone even if they are **not** in the selected Personnel Group. For information, see Configuring a Person to Arm/Disarm Intrusion Zones on Page 192.

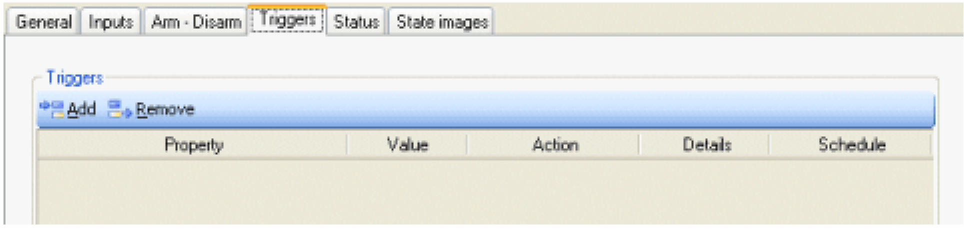
9. In the **Entrance Delay** field, click the up- and down-arrows to set the time in minutes and seconds that the person disarming the zone by the selected method has to enter and disarm before the zone violates. The range is from 00:00 to 20:30 (min:sec).

10. Click to select the **Allow Disarm While Violated** option or leave it clear.

iSTAR Intrusion Zone Triggers Tab

The **iSTAR Intrusion Zone** Triggers tab, shown in Figure 38 on Page 183, allows you to set up **Triggers**, configured procedures used by C•CURE 9000 to activate specific actions when a particular predefined condition occurs.

Figure 38: iSTAR Intrusion Zone Editor Triggers Tab



The tab contains one Action, **Activate Event**, that can be linked to a specific value of an Intrusion Zone-related state and to any panel or host Event configured in the system. Once the Intrusion Zone's state matches one of these values, the linked **Activate Event** action is triggered and the user-specified Event is set to an active state (if allowed by the Event, which should be armed at the time).

Typically you could use the activated Event to arm or disarm an Intrusion Zone, set off an alarm when an Intrusion Zone is in a Violated state, or schedule a nightly Arming check for a particular Intrusion Zone. For details about available Trigger properties, their corresponding values, the Event types, and Scheduling, see Table 42 on Page 184.

By creating new rows and selecting different values for each row, each value of the **Property** field can trigger its own Event. It is also possible to trigger two different Events for the same Intrusion Zone state value by creating two rows with the same value and then linking each row to its own Event.

You use the Triggers tab to accomplish the tasks listed below, needed to configure an iSTAR Intrusion Zone. The procedural steps for each task are detailed in the following subsections.

- Configuring Triggers for iSTAR Intrusion Zones on Page 184
- Deleting a Trigger from an iSTAR Intrusion Zone on Page 187

iSTAR Intrusion Zone Triggers Tab Definitions

The **iSTAR Intrusion Zone Triggers** tab has the buttons shown in Table 40 on Page 183 and the fields shown in Table 41 on Page 184.

Table 40: iSTAR Intrusion Zone Editor Triggers Tab Buttons

Button	Description
Add	Click this button create a new row in the **Triggers** table. You have to configure all the fields in the row and select an Event to complete the Add operation To add a new row after a specific existing row, click the row selector ▸ to select a row and then click **Add**.
Remove	Click this button to remove a selected row from the **Triggers** table. You have to click the row selector ▸ to select a row to remove. If **no** row is selected, this button is **not** available.

Table 41: iSTAR Intrusion Zone Editor - Triggers Tab Fields

Field	Description
Property*	Click in the **Property** field to display [...] and then click this button to display a dialog box with available Intrusion Zone properties. Double-click a Property to select it.
Value*	Click the down-arrow to select a value from the drop-down list. When the Intrusion Zone's **State** property matches this value, the event you specify in the **Event** field is activated.
Action	Click the down-arrow to select **Activate Event** (the only type available) from the drop-down list. This action will be executed when the value of the Intrusion Zone's **State** property matches that selected in the **Value** field.
Details	The name of the event configured for this row (read-only) is entered by the system once you make a selection in the **Event** field.
Event*	Click [...] in this field to select the event to be activated if the State for the current row on the grid has the specified value. NOTE: Switching rows in the grid updates this field with the user-selected event so that each row can have its own event to activate.
Schedule*	Click in the **Schedule** field to display [...] and then click this button to display a dialog box with available Schedules. Double-click a Schedule to select it.
*For detailed information about the relationships between the available properties, their corresponding values, the Event types, and Scheduling, see Table 42 on Page 184.	

Table 42: iSTAR Intrusion Zone Triggers Table Details

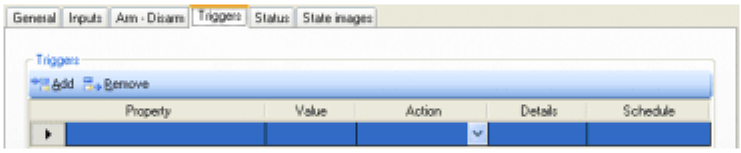
Property	Possible Values	Event Type	Schedule Type
Arm Check Status	Not Armed	Panel only	Must be scheduled Cannot be Always/Never
Mode Status	Armed/Disarmed	Panel Host	Always only Modifiable
Ready To Arm Status	Ready To Arm	Host only	Modifiable
	Not Ready To Arm	Panel Host	Always only Modifiable
Violation Status	Not Violated	Host only	Modifiable
	Violated	Panel Host	Always only Modifiable

Configuring Triggers for iSTAR Intrusion Zones

You can create as many triggers as you wish for any iSTAR Intrusion Zone.

To Configure Intrusion Zone Triggers

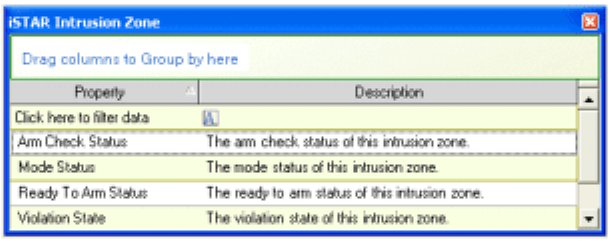
1. Create or modify an iSTAR Intrusion Zone. See:
   - Creating an iSTAR Intrusion Zone on Page 155
   - Modifying an iSTAR Intrusion Zone on Page 162
2. On the **iSTAR Intrusion Zone Editor**, click the **Triggers** tab to open.
3. Click **Add** to create a new trigger row, as shown in the following figure.



Property	Value	Action	Details	Schedule

4. Click in the **Property** field to display ... and click this button.

   A selection list opens with the properties available for iSTAR Intrusion Zones.



iSTAR Intrusion Zone

Drag columns to Group by here

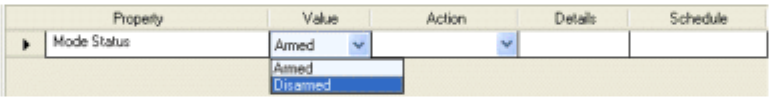
Property	Description
Click here to filter data	
Arm Check Status	The arm check status of this intrusion zone.
Mode Status	The mode status of this intrusion zone.
Ready To Arm Status	The ready to arm status of this intrusion zone.
Violation State	The violation state of this intrusion zone.

5. Click a property to add it to the row.

   Example:

   Mode Status

6. Click the down-arrow in the **Value** field to display a drop-down list of values for the property you selected.



Property	Value	Action	Details	Schedule
Mode Status	Armed			

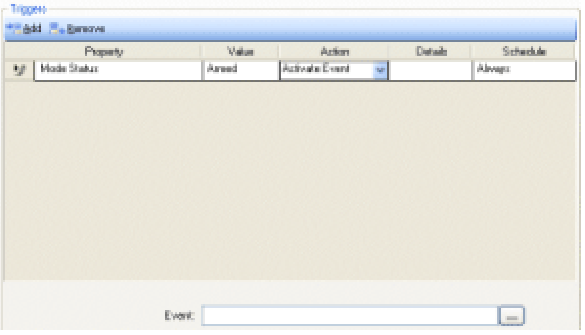
7. Click the **Value** you want to activate the event for this trigger to add it to the row.

   Example:

   Disarmed

8. Click the down-arrow in the **Action** field to display a drop-down list containing **Activate Event** as the only available action. Click **Activate Event** to add it to the row as the action that will be executed when the Intrusion Zone's state matches that selected in the **Value** field.

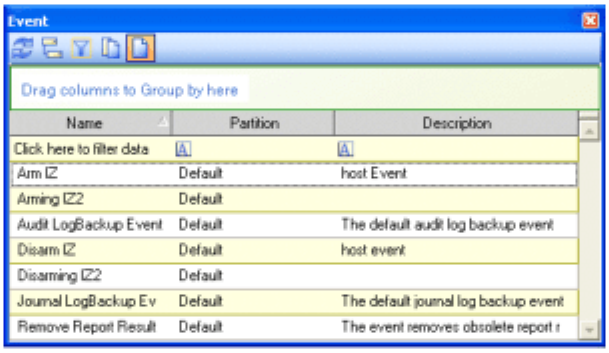
   The **Event** field displays on the bottom of the tab.



Property	Value	Action	Details	Schedule
Mode Status	Armed	Activate Event		Always

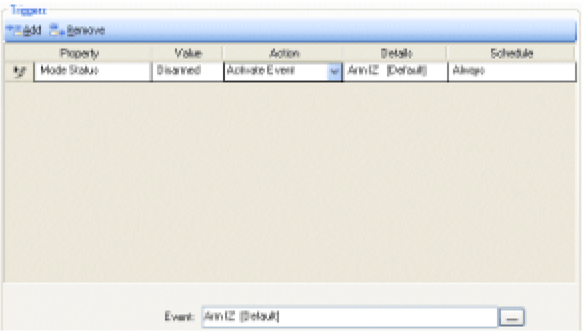
Event:

9. Click ... in the **Event** field to display a selection list of all events currently configured in the C•CURE 9000 system, and then click an Event to select it.



Name	Partition	Description
Click here to filter data	A	A
Arm IZ	Default	host Event
Arming IZ2	Default	
Audit LogBackup Event	Default	The default audit log backup event
Disarm IZ	Default	host event
Disarming IZ2	Default	
Journal LogBackup Ev	Default	The default journal log backup event
Remove Report Result	Default	The event removes obsolete report r

The system enters the name of the Event you select in the **Details** field for the row when you click anywhere outside the **Event** field. This event will be activated whenever the **State** for the current row on the grid matches the value specified in that row.

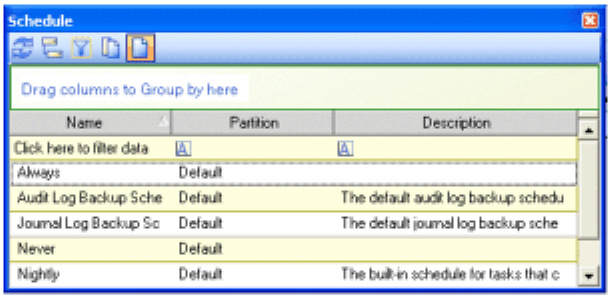


Property	Value	Action	Details	Schedule
Mode Status	Disarmed	Activate Event	Arm IZ (Default)	Always

Event: Arm IZ (Default)

The **Schedule** field contains the default entry **Always**, which is the only type valid for Panel Events. You **can** select a schedule for a Host Event and **must** select a schedule (other than **Always/Never**) for the Arm Check Status property (even though it is a Panel Event).

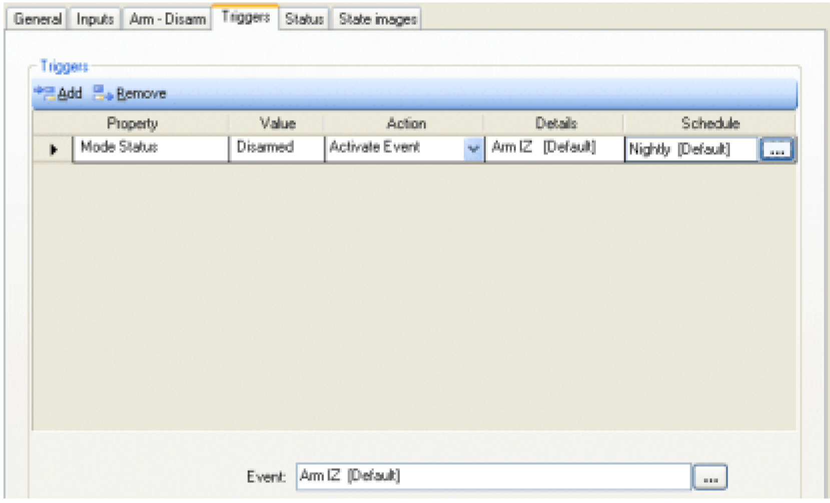
10. Click ... in the **Schedule** field to display a selection list of schedules configured in the C•CURE 9000 system.



Name	Partition	Description
Click here to filter data	A	A
Always	Default	
Audit Log Backup Sche	Default	The default audit log backup schedu
Journal Log Backup Sc	Default	The default journal log backup sche
Never	Default	
Nightly	Default	The built-in schedule for tasks that c

11. Click a Schedule to select it.

    The tab now appears as shown in the following example.



Property	Value	Action	Details	Schedule
Mode Status	Disarmed	Activate Event	Arm IZ [Default]	Nightly [Default]

Event: Arm IZ [Default]

12. To create more triggers for this iSTAR Intrusion Zone, repeat these steps for each trigger you want.

    Switching rows in the grid updates the **Event** field with the user-selected event so that each row can have its own event to activate.

Deleting a Trigger from an iSTAR Intrusion Zone

To Delete an iSTAR Intrusion Zone Trigger

1. On the **Triggers** tab, click a row to select it.
2. Click **Remove** to delete the trigger row.

iSTAR Intrusion Zone Groups Tab

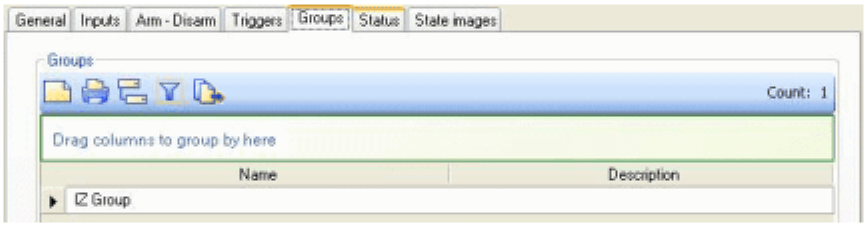
The iSTAR Intrusion Zone **Groups** tab, shown in Figure 39 on Page 188, lists the iSTAR Intrusion Zone Groups to which this Intrusion Zone belongs.

NOTE This tab does **not** display on the **iSTAR Intrusion Zone Editor** when you are configuring a new Intrusion Zone. It displays when you are editing an existing Intrusion Zone.

The Groups table on this tab is a Dynamic View that you can filter, group, print, and view in Card View, using the buttons described in Table 43 on Page 188.

You can select any of the Intrusion Zone Groups in the list and double-lick ▶ to edit it or right-click to display the Groups Context menu (described in the Groups chapter in the *C•CURE 9000 Software Configuration Guide*). You can also right-click in the **Name** or **Description** field of an Intrusion Zone Group row to display a standard edit menu.

Figure 39: iSTAR Intrusion Zone Editor Groups Tab



iSTAR Intrusion Zone Groups Tab Definitions

The **iSTAR Intrusion Zone Groups** tab has the buttons and fields shown in Table 43 on Page 188.

Table 43: iSTAR Intrusion Zone Editor Groups Tab Fields/Buttons

Fields/Buttons	Name	Description
▭	Card View	Click to display the list of iSTAR Intrusion Zone Groups in Card View.
🖨	Print	Click to print the list of iSTAR Intrusion Zone Groups.
▤	Group	Click to enable Grouping of the list. You can drag a column heading to the area labeled **Drag columns to group by here to** group the list by that heading.
▽	Filter	Click to display the filter bar. You can click in the filter bar to add filtering criteria to any column of the list. For more information about Filtering, see the Dynamic Views chapter in the *C•CURE 9000 Data Views Guide*.
Name		Name of the Group, up to 100 characters.
Description		Description of the Group.

iSTAR Intrusion Zone Status Tab

The iSTAR Intrusion Zone Status tab, shown in Figure 40 on Page 190, provides a read-only listing of critical information about the operational status of this iSTAR Intrusion Zone, including:

- Mode – displays the values: Armed, Disarmed, or Unknown
- Violated State – displays the values: Violated, Not Violated, or Unknown
- Ready To Arm State – displays the values: Ready to Arm, Not Ready to Arm, or Unknown
- First Violating Cause – displays a value indicating the initial cause of the Intrusion Zone being in a Violated State: Input X, for example
- Mode Changed Method Status– displays a value indicating why the Intrusion Zone's Mode changed: Host Command, Keypad Command, Card Swipe, or Unknown
- Time of Mode Changed Method – displays the date/time the Intrusion Zone's Mode changed

You can perform the following task from the Status tab:

- Viewing Intrusion Zone Status on the Status Tab on Page 189

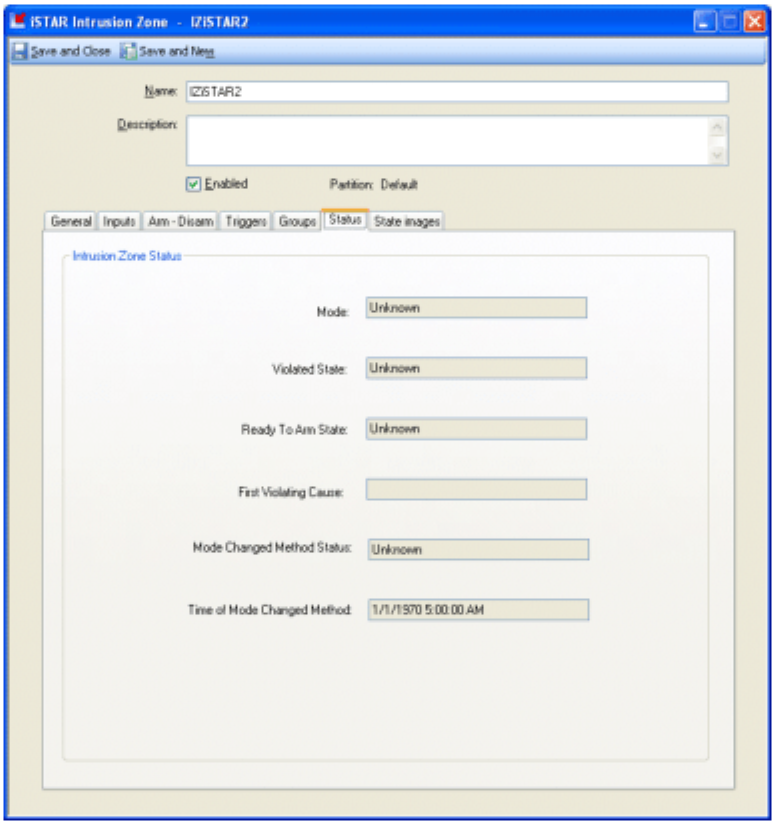
Viewing Intrusion Zone Status on the Status Tab

To View Status on the iSTAR Intrusion Zone Editor

1. In the Navigation Pane of the Administration Workstation, click the **Areas and Zones** pane button.
2. Click the **Areas and Zones** drop-down list and select **iSTAR Intrusion Zone**.
3. Click ➔ ▾ to open a Dynamic View showing a list of all existing iSTAR Intrusion Zone Objects.
4. Right-click the iSTAR Intrusion Zone whose status you want to view and click **Edit** from the context menu that appears.

   The **iSTAR Intrusion Zone Editor** opens with the **General** tab displayed.
5. Click the Status tab to open, as shown in Figure 40 on Page 190.

Figure 40: iSTAR Intrusion Zone Editor Status Tab



Name: IZiSTAR2

Description:

☑ Enabled

Partition: Default

Mode: Unknown

Violated State: Unknown

Ready To Arm State: Unknown

First Violating Cause:

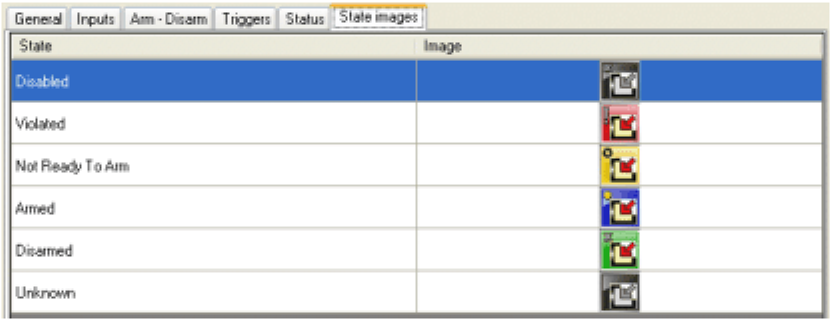
Mode Changed Method Status: Unknown

Time of Mode Changed Method: 1/1/1970 5:00:00 AM

iSTAR Intrusion Zone State Images Tab

The **iSTAR Intrusion Zone State Images** tab, shown in Figure 41 on Page 191 provides a means to change the default images used to indicate states for the iSTAR Intrusion Zone on the Monitoring Station. You can select other images to display for this Intrusion Zone or return to the default images, as described in State Images Tab Tasks on Page 191.

Figure 41: iSTAR Intrusion Zone Editor State Images Tab



State	Image
Disabled	⬛
Violated	🟥
Not Ready To Arm	🟨
Armed	🟦
Disarmed	🟩
Unknown	⬛

State Images Tab Tasks

You can change the image displayed for any Intrusion Zone state, or restore the default image.

To Change an Image

1. Double-click the default image in the tab to open a Windows file selection dialog box.
2. If necessary, navigate to find the new image.
3. Select the desired replacement image and click **Open**.

   The new image replaces the default image and displays in the **State Images** tab.

To Restore the Default Image

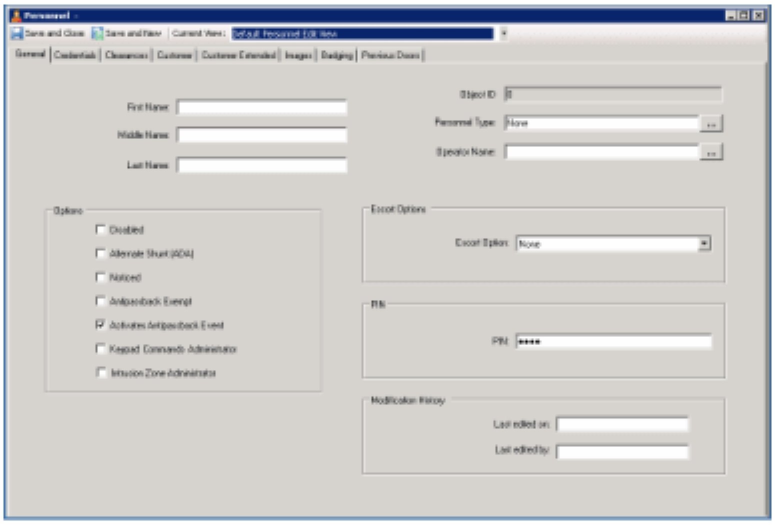
- Right-click the replacement image in the Intrusion Zone **State Images** tab and select **Restore Default**.

Configuring a Person to Arm/Disarm Intrusion Zones

You can configure a person to be able to Arm/Disarm Intrusion Zones using the Card swipe Arm/Disarm methods even if he or she is not in the Personnel Group configured for that Intrusion Zone.

You configure this on the **Personnel Editor General** tab, as shown in Figure 42 on Page 192.

Figure 42: Personnel Editor – General Tab



Current View: Default Personnel Edit View

First Name:

Middle Name:

Last Name:

Object ID: 0

Personnel Type: None

Operator Name:

☐ Disabled
☐ Alternate Shunt (ADA)
☐ Noticed
☐ Antipassback Exempt
☑ Activates Antipassback Event
☐ Keypad Commands Administrator
☐ Intrusion Zone Administrator

Escort Option: None

PIN: ••••

Last edited on:

Last edited by:

To Configure a Person to Arm/Disarm Intrusion Zones

1. In the Navigation Pane of the Administration Workstation, click the **Personnel** pane button.
2. Click the **Personnel** drop-down list and select **Personnel**.
3. Click **New** to create a new Personnel record.

   - or -

   Click to open a Dynamic View showing a list of all existing Personnel Objects, right-click the Personnel record you want to change, and click **Edit** from the context menu that appears.

   The **Personnel Editor** opens with the **General** Tab displayed.
4. In the **Options** box, click to select the **Intrusion Zone Administrator** option.

NOTE If this option is selected, this person can Arm/Disarm any Intrusion Zone using the Card swipe Arm/Disarm methods regardless of the Personnel Group configured for that Intrusion Zone.

If this option is **not** selected, this person can **only** use the Card swipe method to Arm/Disarm Intrusion Zones configured:

- For a Personnel Group in which he/she is included.
- With **no** Personnel Group required with the Card Swipe.

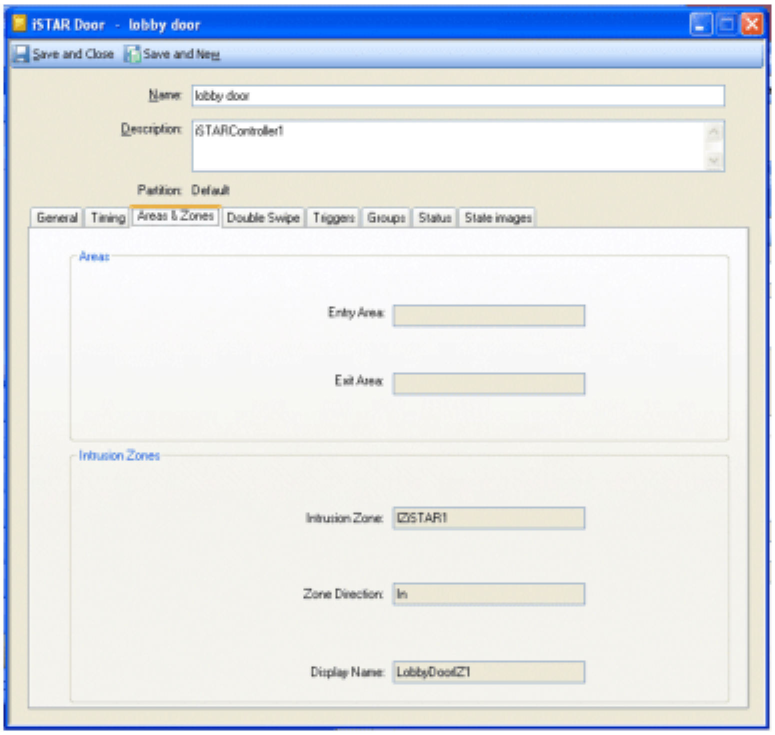
5. To save the Personnel record, click **Save and Close**.

Viewing Intrusion Zone Information on the Door Editor

A Door assigned to an iSTAR Intrusion Zone displays read-only assignment information on the **Door Editor** on the **Areas & Zones** tab, as shown in Figure 43 on Page 193.

NOTE If this Door is **not** assigned to an Intrusion Zone, the Intrusion Zones box is blank.

Figure 43: Door Editor — Areas & Zones Tab



Name: lobby door

Description: iSTARController1

Partition: Default

Entry Area:

Exit Area:

Intrusion Zone: IZiSTAR1

Zone Direction: In

Display Name: LobbyDoorIZ1

The **Areas & Zones** tab has the read-only fields shown in Table 44 on Page 193.

Table 44: Door Editor — Areas & Zones Tab Fields

Fields	Description
Intrusion Zone	Name of iSTAR Intrusion Zone this Door is assigned to.
Zone Direction	**In** indicates that this Door is assigned as an **Entrance Door** for the Intrusion Zone. **Out** indicates that this Door is assigned as an **Exit Door** for the Intrusion Zone.
Display Name	Displays the name you entered for this Door on the iSTAR Intrusion Zones Editor General tab.

To View a Door's Intrusion Zone Information

1. In the Navigation Pane of the Administration Workstation, click the **Hardware** pane button.
2. Click the **Hardware** drop-down list, select **iSTAR Door**, and click to open a Dynamic View showing a list of all existing iSTAR Doors.

   - or -

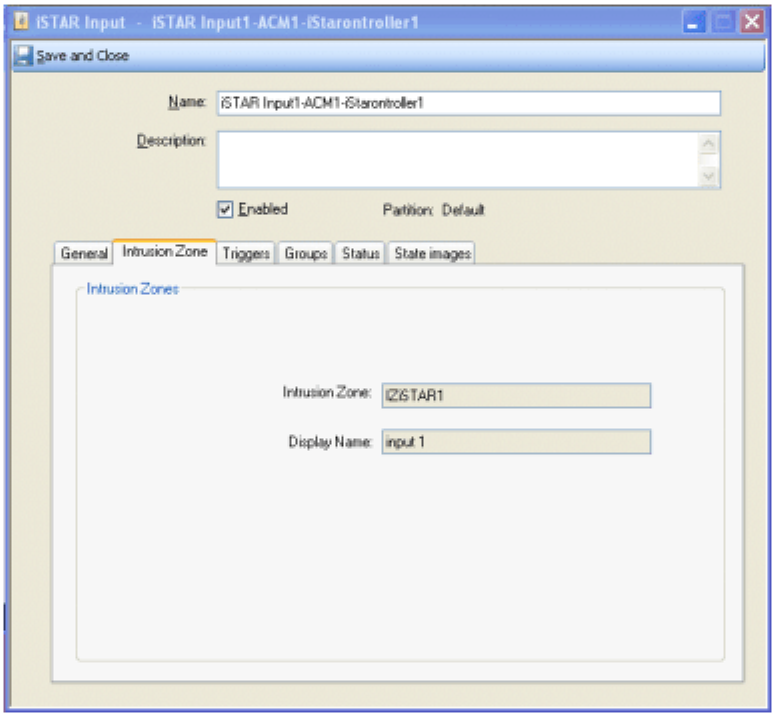
Expand the Hardware Tree.

3. In the Dynamic View list/Tree, select the iSTAR Door, right-click, and click **Edit** from the context menu that appears.
4. When the **iSTAR Door Editor** appears, click the **Areas & Zones** Tab.

Viewing Intrusion Zone Information on the Input Editor

An Input assigned as an iSTAR Intrusion Zone Controlled or Protected Input displays read-only assignment information on the **Intrusion Zone** tab of the **Input Editor**, as shown in Figure 44 on Page 195. This tab only displays when the Input is assigned to a zone. At the same time, the value in the Type field on the Input **General** tab changes from 'General' to 'Intrusion Zone'.

Figure 44: iSTAR Input Editor – Intrusion Zone Tab



iSTAR Input - iSTAR Input1-ACM1-iStarontroller1

Name: iSTAR Input1-ACM1-iStarontroller1

Description:

☑ Enabled

Partition: Default

Intrusion Zones

Intrusion Zone: IZiSTAR1

Display Name: input 1

The **Intrusion Zone** tab has the read-only fields shown in Table 45 on Page 195.

Table 45: Inputs Editor — Intrusion Zone Tab Fields

Fields	Description
Intrusion Zone	Name of iSTAR Intrusion Zone this Input is assigned to.
Display Name	Displays the name you entered for this Input on the iSTAR Intrusion Zones Editor Inputs tab in the **Controlled Inputs** table.

To View an Input's Intrusion Zone Information

1. In the Navigation Pane of the Administration Workstation, click the **Hardware** pane button.
2. Click the **Hardware** drop-down list, select **iSTAR Input**, and click ➡ ▾ to open a Dynamic View showing a list of all existing iSTAR Inputs.

   - or -

   Expand the Hardware Tree.

3. In the Dynamic View list/Tree, select the iSTAR Input, right-click, and click **Edit** from the context menu that appears.
4. When the **iSTAR Input Editor** appears, click the **Intrusion Zone** Tab.

3

Keypad Commands

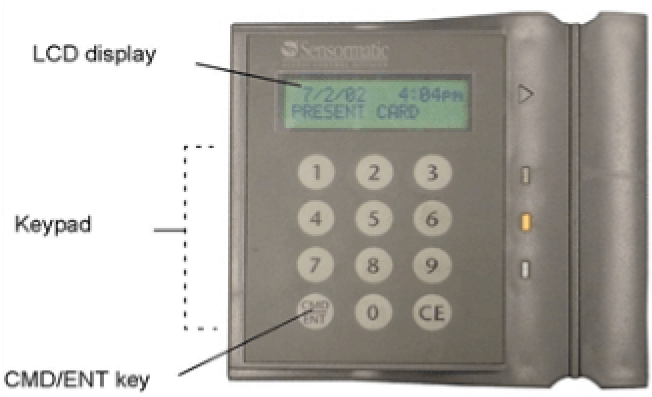
This chapter explains how to configure Keypad Commands.

In this chapter

Overview

You can configure Keypad Commands that authorized personnel can execute using the keypad on Readers (RMs) connected to iSTAR Controllers (see Figure 45 on Page 198).

Figure 45: Reader with Keypad



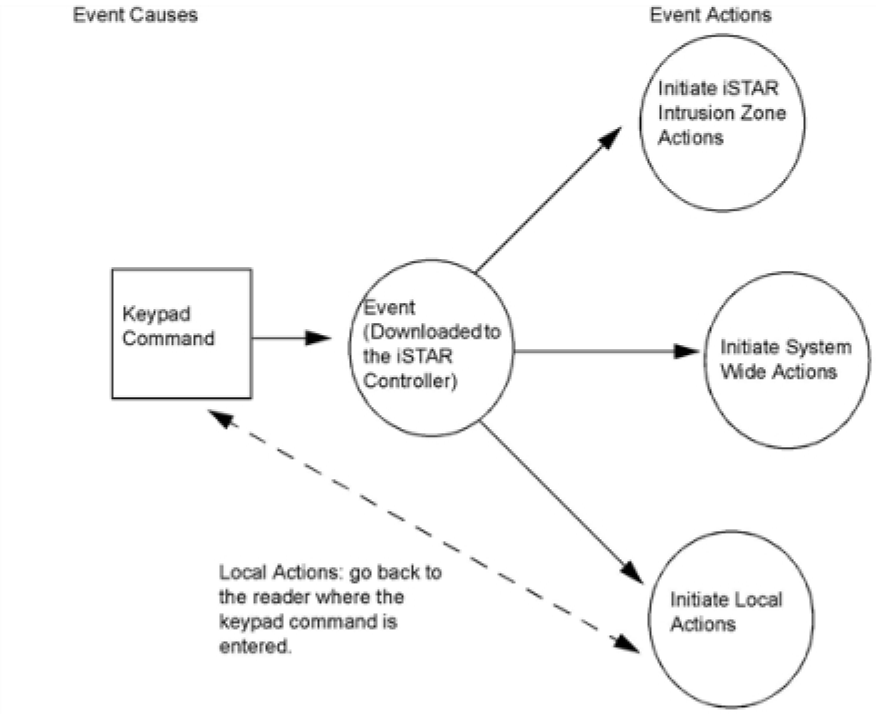
A Keypad Command is a unique (within an iSTAR Cluster) nine-digit number entered on the keypad (with optional prompting) that activates a specific Event.

Keypad Commands can activate Panel Events that initiate:

- Intrusion Zone Actions, such as arming, disarming, and toggling Intrusion Zones, as well as checking their status and the status of their Doors and Inputs. These Keypad Commands must be entered at Readers that are part of the Intrusion Zone.
- System-wide actions. These actions can control objects in the host and other clusters.
- Local target actions, such as locking/unlocking a door by entering a keypad command on its keypad. These actions operate on the security device that activated the event, the door that owns the reader with that keypad, rather than on a specific target.

Figure 46 on Page 199 illustrates the capabilities of keypad commands.

Figure 46: Keypad Commands and Associated Events


Event Causes
Event Actions
Keypad Command
Event (Downloaded to the iSTAR Controller)
Initiate iSTAR Intrusion Zone Actions
Initiate System Wide Actions
Initiate Local Actions
Local Actions: go back to the reader where the keypad command is entered.

Keypad Commands activate Events in a special way:

- The Event is activated with no end time, but when the activation is superseded, the Keypad Command disappears from the Event's cause list instead of remaining until another cause overrides it.
- These Keypad Command-activated Events 'live until overridden'. An Action is required to undo or override a Keypad Command Event.

The recommended procedure is to construct keypad commands in pairs; use one Keypad Command to activate an object, and another Keypad Command to deactivate the object.

The Keypad Command may be configured to require a card presentation and, optionally, a PIN to validate the command. The Keypad Command may also be limited to a specific personnel group's card numbers. Additionally, the Keypad Command may be limited to specific doors in the cluster, and specific readers may be configured to disallow the use of Keypad Commands.

Examples of Keypad Command Use

The following examples show security requirements that are met by creating keypad commands:

- The site, a multi-tenant office building, uses building security personnel to monitor tenants on all floors. To arm and disarm different intrusion zones, keypad commands initiate events that activate local actions.
  - The command **110** disarms any zone from a reader on a door that is part of the zone.
  - The command **120** arms any zone from a reader on an intrusion zone door.
- The site, a hospital, requires local door locking and unlocking for specific time periods to provide wheelchair access. In this case, Keypad Commands are created that initiate events with local door actions.
- The hospital staff enter the commands at readers outside the door.

- The Keypad Command **100**, named "Enter time 15", unlocks the door for 15 minutes (minimum activation time in Event configuration).
- The Keypad Command **200**, named "Enter time 30" unlocks the door for 30 minutes.
- The Keypad Command **300**, named "Enter time 00" locks the door.

How Keypad Commands Work

An Event activated by a Keypad Command, once activated, requires a separate action to override (deactivate) it.

The following sections describe the methods you can use to activate and deactivate Keypad Commands.

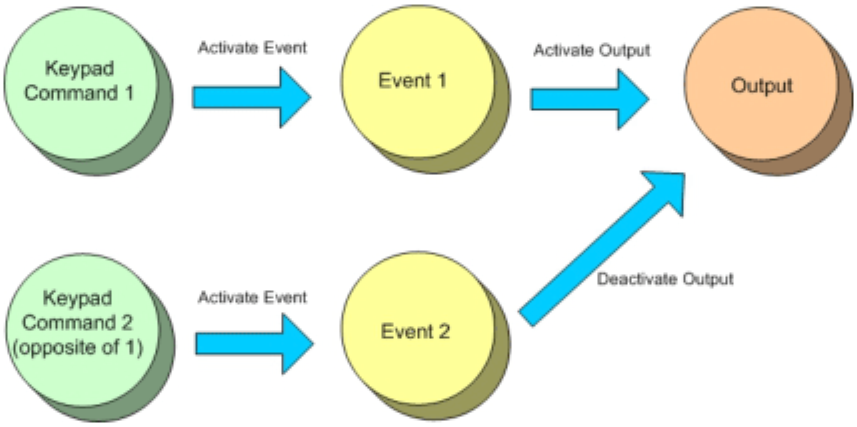
Method 1

Figure 47 on Page 200 demonstrates using two Keypad Commands to control an Output.

- Keypad Command 1 and Event 1 are used to activate the Output, while Keypad Command 2 and Event 2 are used to deactivate it.
- When the Event 2 Action asserts, it overrides the Action of Event 1, and Event 1 is overruled.

This method works well in situations when there are no other controls on the Output. However, this method leaves a deactivation on the Output at whatever priority level is set by Event 2. If Keypad Command 1 asserts again, it will override Event 2.

Figure 47: Method 1 - Controlling an Output with Two Keypad Commands



Method 2

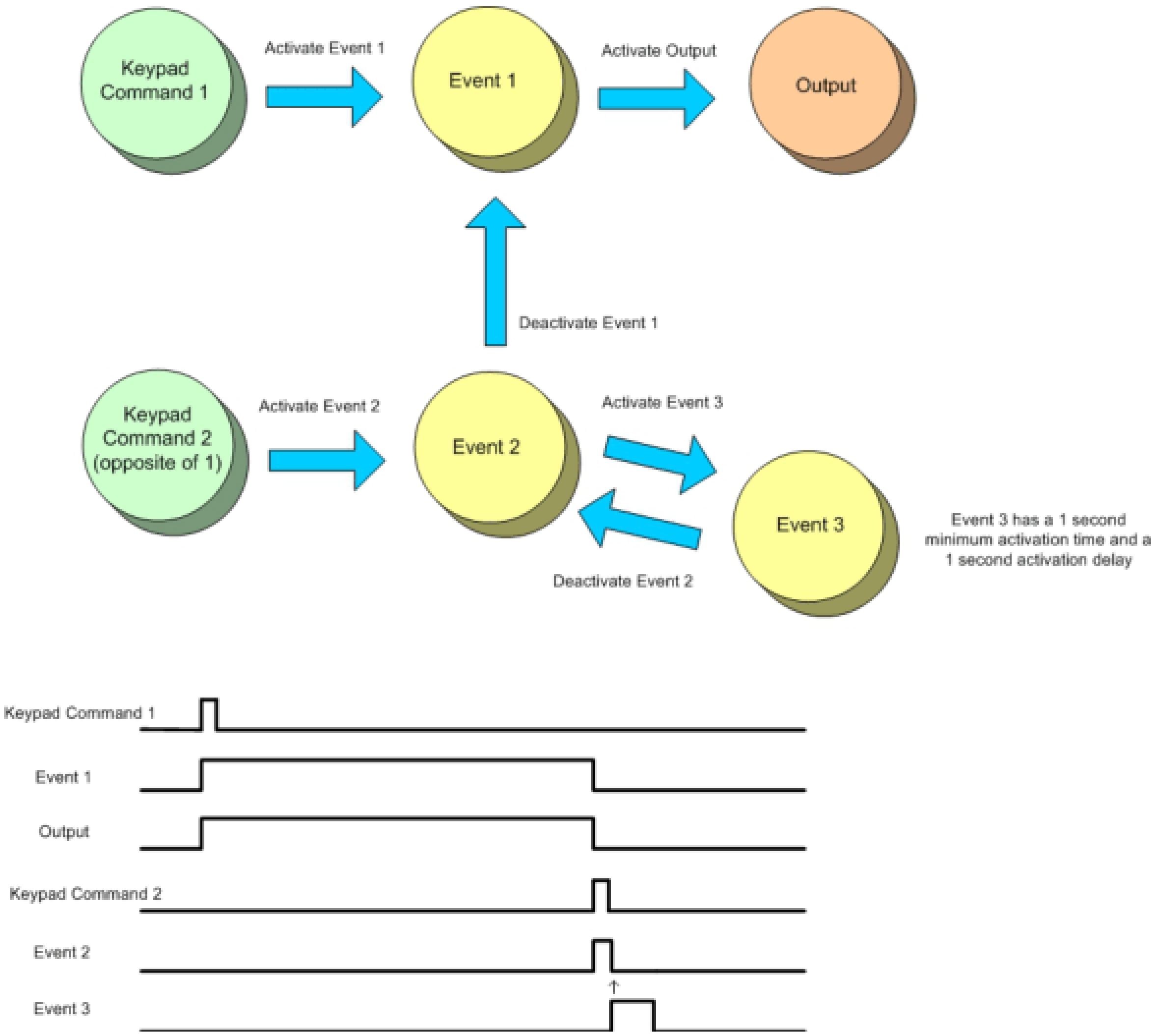
Figure 48 on Page 201 shows an alternate method that results in deactivation of all Keypad Command Events.

- Keypad Command 1 causes Event 1 and activates the Output.
- To reset the Output, Keypad Command 2 activates Event 2 which has the following two Actions:
  - One Action is to deactivate Event 1.
  - The second Action is to deactivate itself.

  Event 2 deactivates itself by activating Event 3, which has the Action of deactivating Event 2.

NOTE It is important that Event 3 have a minimum activation time of one second and an activation delay of one second.

Figure 48: Method 2 - Controlling an Output with Two Keypad Commands



Keypad Command Configuration Steps

Table 46 on Page 202 shows the C•CURE 9000 Editors and activities that create Keypad Commands.

Table 46: Creating Keypad Commands

Task	C•CURE9000 Editor	Configuration Notes	Additional Information
Define the Keypad Command format	Options & Tools>System Variables>iSTAR Driver Category	Defines the number of keypad characters in the Command field (required). Defines the number of keypad characters in the Prompt 1 and Prompt 2 fields (optional).	See Keypad Command Format on Page 205.
Configure and download a Keypad Event to an iSTAR Controller	Configuration>Event> New>Event Editor - or - Edit an exiting Event	Creates and downloads the event to be activated by the Keypad Command.	See the Events chapter in the *C•CURE 9000 Software Configuration Guide*.
Configure a Door Group	Configuration>Group> New>Group Editor - or - Edit an existing Door Group	Creates a Door Group to which the use of the Keypad Command can be limited.	See the Groups chapter in the *C•CURE 9000 Software Configuration Guide*.
Configure a Personnel Group (optional, depending on Validation Type)	Configuration>Group> New>Group Editor - or - Edit an existing Personnel Group	Creates a Personnel Group to whose members use of the Keypad Command can be limited.	See the Groups chapter in the *C•CURE 9000 Software Configuration Guide*.
Configure the Keypad Command	Areas and Zones>Keypad Command>New>Keypad Command Editor	Creates a Keypad Command and associates it with: • A Cluster. • The Event it activates. • The numerical sequence to execute the keypad command.	See Keypad Command Editor on Page 210.
Configure Reader(s)	From Hardware Pane> Hardware Tree, either • Create a new Reader for the iSTAR Controller - or - • Edit an existing Reader. For information, see the iSTAR Controller chapter in the *C•CURE 9000 Hardware Configuration Guide* Then, iSTAR Reader Editor> Keypad Tab	Allows one or more readers to accept keypad commands.	See Configuring Readers for Keypad Commands on Page 224.
Configure Personnel	Personnel>Personnel> New>Personnel Editor - or - Edit an existing Personnel Record	Enables a specific person **not necessarily** in the Keypad Command Personnel Group to execute the Keypad Command.	See Configuring a Person to Use Keypad Commands on Page 226.

Permissions Required to Configure Keypad Commands

A C•CURE 9000 operator would need the minimum permissions listed in Table 47 on Page 203 to be able to configure Keypad Commands:

Table 47: Permissions for Configuring Keypad Commands

Class	Permission
iSTAR Cluster	Read
iSTAR Controller	Read
ACM Board	Read
iSTAR Reader	Edit
Keypad Command	Edit
Personnel	Edit

Keypad Command Configuration Requirements

Keypad Commands must follow these guidelines and requirements:

- Keypad Command events must be downloaded to a Cluster.
- Local Keypad Commands for Intrusion Zones must be issued from a Reader that is part of a Door included in the Intrusion Zone (the local Keypad Command is applied to the Intrusion Zone that includes the Door. This allows a given local Keypad Command— for example, "Arm Local Intrusion Zone"—to be used in many Intrusion Zones). The associated Events for a given Intrusion Zone must be downloaded to a Controller in the Cluster that contains that Intrusion Zone.
- The Event Actions of most Keypad Commands can affect objects anywhere in the system. If the Event Actions affect objects outside the Cluster and the Cluster becomes disconnected from the host (a communications failure), the normal algorithms will be used on re-connection. If a momentary activity occurred during the communications failure, there will be no attempt to re-issue the activity. If an activation that is still true was missed during the communications failure, there will be an attempt to re-issue the activation.
- If the Keypad Command requires the swipe of a Card, Personnel must have clearance to a Door in order to issue a Keypad Command from that Door. This applies even if their Card configuration includes the Keypad Command Administrator option. It does **not** apply if the Keypad Command does **not** require card number.
- Keypad Commands can be entered from Doors that are locked, unlocked, or secure. This is done so a person can arm or disarm an Intrusion Zone from the outside Doors regardless of the Door state.
- For security reasons, if the iSTAR Controller does not recognize the first— the Command—portion of the Keypad Command (or if the Keypad Command is disabled), it will still ask for all parts configured for the Keypad Command, as well as for a Card presentation.

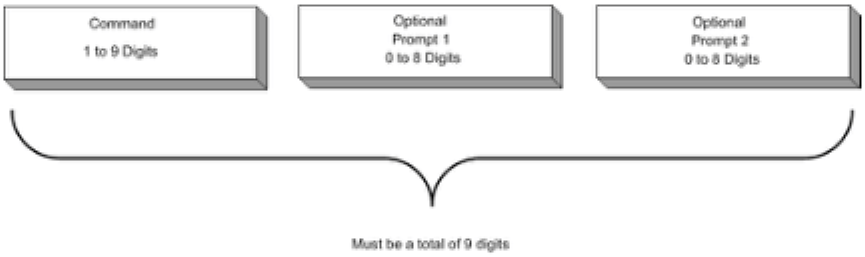
  If the Keypad Command is disabled, but is configured for a PIN, it will ask for a PIN. In addition, if the Keypad Command is recognized but the Card fails some test (Clearance, Lost, etc.) and the Keypad Command is configured for a PIN, the PIN is still requested.

  This is done to confuse someone who may be "trying" out the keypad to see if they can figure out the commands.

Keypad Command Format

Keypad Commands can be entered on the keypad as a single number or as a two- or three-part number. With two- or three-part Keypad Commands, the system helps the person entering the Keypad Command by prompting for the second and third parts.

Figure 49: Keypad Fields



Consequently, the first step in creating keypad commands is to define, system-wide, the command format. This involves the following:

1. Deciding whether the command format is to be one-part, two-part, or three-part. (The default is one-part with 9 digits.)
2. Defining the number of keypad characters in the Command Code (required).
3. Optionally, defining the number of keypad characters for Prompt 1.
4. Optionally, defining the number of keypad characters for Prompt 2.

You configure the Keypad Command format as described in Defining Keypad Command Formats on Page 207.

Format Requirements

Keypad Command formats must conform to the following guidelines:

- The combined value for the Command Code, Prompt 1 Code, and Prompt 2 Code can be any combination that adds up to 9 digits.

  Command Code is required and accepts a value of 1 to 9; Prompt 1 and Prompt 2 Codes are optional and accept a value from 0 to 8.
- The string for Prompt 1 is "ENTER ACCESS". This is a text only field with no internal significance.
- The string for Prompt 2 is "ENTER TARGET". This is a text only field with no internal significance.
- Keypad Command sequences and optional prompts must be unique.
- Personnel entering Command Code at keypads **must** bracket each code with the CMD/ENT key and must **not** use 0 (zero) as the first digit of the code.

  Example:

  CMD/ENT 222 CMD/ENT is correct;
  while CMD/ENT 022 CMD/ENT is incorrect.

> You should not modify the command formats after you use them to create commands. Modifications to the command format cause existing keypad commands to behave differently.

Example Formats

The following examples show keypad commands that use:

- Command Code only
- Command Code with Prompt 1
- Command Code with Prompt 1 and Prompt 2

Command Code Only

The Keypad Command in this example uses a Command Code format to arm and disarm an intrusion zone.

The format is configured as follows:

Command Code: 9

Prompt 1 Code: 0

Prompt 2 Code: 0

- To arm the intrusion zone, the security personnel press CMD/ENT 100 CMD/ENT.
- To disarm the intrusion zone, security personnel enter CMD/ENT 101 CMD/ENT.

C•CURE 9000 automatically pads the unused portion of the command field to conform to the nine-digit command code format:

000000100, 000000101

Security personnel need enter only the command portion of this field.

Command Code with Prompt 1

The Keypad Commands in this example arm and disarm Intrusion Zones on two floors. The Prompt 1 code expects security personnel to enter the code for the Intrusion Zone floor.

The format is configured as follows:

Command Code: 6

Prompt 1 Code: 3

Prompt 2 Code: 0

- To arm a zone, the security personnel enter CMD/ENT 200 CMD/ENT.
- When the reader displays the Prompt 1 message “ENTER ACCESS”, personnel enter **1** or **2**, the code indicating the first or the second floor.
- To disarm the zone, security personnel enter CMD/ENT 300 CMD/ENT.
- When the reader displays the Prompt 1 message “ENTER ACCESS”, personnel enter **1** or **2**, the code indicating the first or the second floor.

C•CURE 9000 automatically pads the unused portion of the command field and prompt fields to conform to the six-digit and three-digit requirements:

000200, 001 or 002

Security personnel need enter only the non-zero portions of the command

Command Code with Prompt 1 and Prompt 2

The Keypad Commands in this example turn lights on and off on two floors. The Prompt 1 and Prompt 2 code expect security personnel to enter the codes for the floor and light numbers.

The format is configured as follows:

Command Code: 3

Prompt 1 Code: 3

Prompt 2 Code: 3

- To toggle on/off, the security personnel enter CMD/ENT 1 CMD/ENT or CMD/ENT 2 CMD/ENT.
- When the reader displays the prompt 1 message "ENTER ACCESS", personnel enter **1** or **2**, the code indicating the first or the second floor.
- When the reader displays the prompt 2 message "ENTER TARGET", personnel enter the room number of the light.

C•CURE 9000 pads the unused portion of the command field and prompt fields to conform to the three-digit requirement:

001 or 002, 001 or 002, 056.

Security personnel need enter only the non-zero portions of the command.

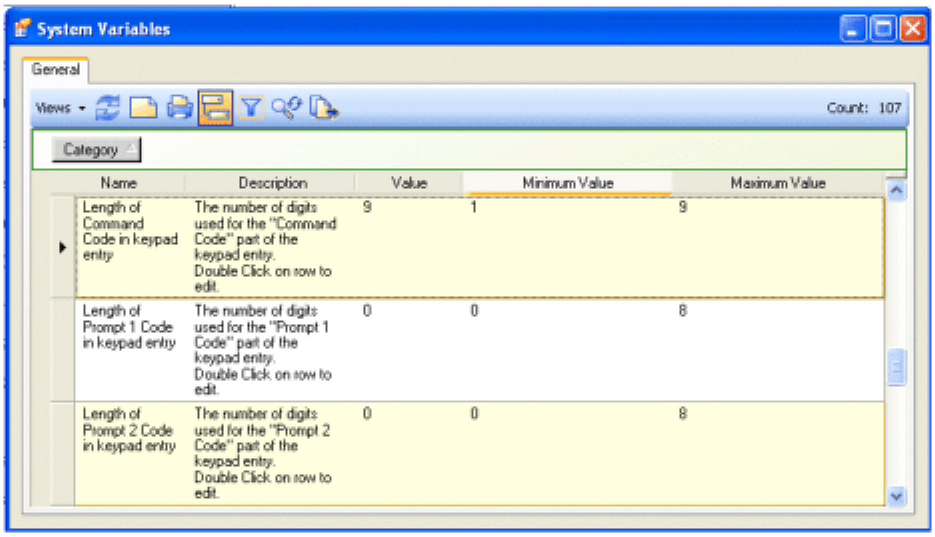
Defining Keypad Command Formats

To Define Keypad Command Formats

1. In the Administration Station, on the Options & Tools pane, select **System Variables**.
2. On the **General** tab, expand the **iSTAR Driver** category.
3. Scroll down to locate the "Maximum Length of Command Code in Keypad entry" system variable in the **Name** column.

   This is the first of the three Keypad Command Format system variables, as shown in Figure 50 on Page 208.

Figure 50: System Variables – Keypad Command Formats



Name	Description	Value	Minimum Value	Maximum Value
Length of Command Code in keypad entry	The number of digits used for the "Command Code" part of the keypad entry. Double Click on row to edit.	9	1	9
Length of Prompt 1 Code in keypad entry	The number of digits used for the "Prompt 1 Code" part of the keypad entry. Double Click on row to edit.	0	0	8
Length of Prompt 2 Code in keypad entry	The number of digits used for the "Prompt 2 Code" part of the keypad entry. Double Click on row to edit.	0	0	8

4. To edit the Command format:

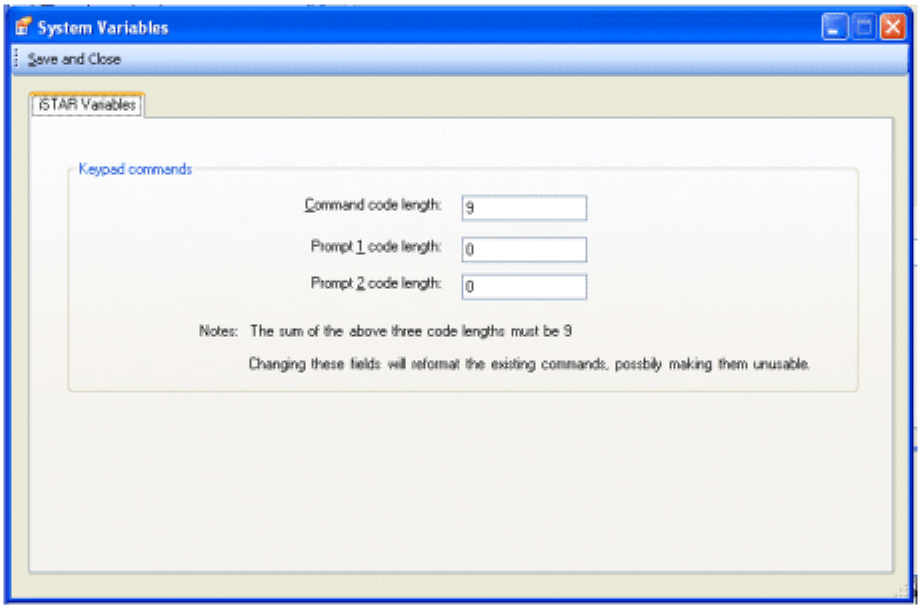
   Double-click in any one of these three Keypad Command System Variable rows.

   - or -

   Right-click in the row and then click **Edit** from the Context menu that appears.

   The **System Variables** Editor appears with the Keypad Commands on the **iSTAR Variables** tab, as shown in Figure 51 on Page 208.

Figure 51: System Variables Editor – Keypad Command Formats



Command code length: 9

Prompt 1 code length: 0

Prompt 2 code length: 0

Notes: The sum of the above three code lengths must be 9

Changing these fields will reformat the existing commands, possbily making them unusable.

5. Change the values in these fields according to the information given in this Keypad Command Format section on Page 205 thru Page 207 and in System Variable iSTAR Variables Tab Definitions on Page 209.

6. Click **Save and Close** when you are finished editing the formats.

System Variable iSTAR Variables Tab Definitions

The **iSTAR Variables** tab has the fields shown in Table 48 on Page 209.

Table 48: System Variables iSTAR Variables Tab Fields

Tab	Field	Description
Keypad Commands NOTE: The sum of the value of these three fields must equal 9. **Important** —If you change the values in the fields on this tab, keypad commands may not work. Check each keypad command to ensure that it is still usable.	Command code length	Enter the number of digits used for the "Command Code" part of the keypad entry. The valid range is 1 to 9, with a default value of 9. NOTE: The number you enter in this field controls the number of digits you can enter in the **Command Code** field on the **General** tab of the **Keypad Command Editor.**
	Prompt 1 code length	Enter the number of digits used for the Prompt 1 Code part of the keypad entry. The valid range is 1 to 8, with a default value of 0 (zero). NOTE: The number you enter in this field controls the number of digits you can enter in the Prompt 1 Code field on the **General** tab of the **Keypad Command Editor.** This field is unavailable if it has a value of 0 (zero).
	Prompt 2 code length	Enter the number of digits used for the Prompt 2 Code part of the keypad entry. The valid range is 1 to 8, with a default value of 0 (zero). NOTE: The number you enter in this field controls the number of digits you can enter in the Prompt 2 Code field on the **General** tab of the **Keypad Command Editor.** This field is unavailable if it has a value of 0 (zero).

Keypad Command Editor

The **Keypad Command Editor** in C•CURE 9000 lets you create and modify Keypad Command Objects that allow users to activate events through local keypads.

The **Keypad Command Editor** displays the following tabs for configuring Commands:

- Keypad Command General Tab on Page 211
- Keypad Command Permissions Tab on Page 213
- Keypad Command Groups Tab on Page 215 (when editing an existing Keypad Command)

To use the Keypad Command Editor, see Accessing the Keypad Command Editor on Page 210.

Accessing the Keypad Command Editor

You can access the **Keypad Command Editor** from the C•CURE 9000 **Areas and Zones** pane.

To Access the Keypad Command Editor

1. In the Navigation Pane of the Administration Workstation, click the **Areas and Zones** pane button.
2. Click the **Areas and Zones** drop-down list and select **Keypad Command**.
3. Click **New** to create a new Command.

   - or -

   Click ➡ ▾ to open a Dynamic View showing a list of all existing Keypad Command Objects, right-click the Keypad Command you want to change, and click **Edit** from the context menu that appears.

   The **Keypad Command Editor** opens.

The **Keypad Command Editor** has the buttons described in Table 49 on Page 210.

Table 49: Keypad Command Editor Buttons

Button	Description
Save and Close	Click this button when you have completed any changes to the Keypad Command and wish to save those changes. The Keypad Command closes.
Save and New	Click this button when you have completed any changes to the Keypad Command and wish to save those changes and also create a new Keypad Command. The Keypad Command you were editing is saved, and a new Keypad Command opens (either blank or including template information if you were using a template to create the new Keypad Command).
☒	Click this button when you want to close the **Keypad Command Editor** without saving your changes. A warning appears asking whether or not you want to save your changes before closing the editor. Click **Yes** to exit and save and **No** to exit and cancel your changes.

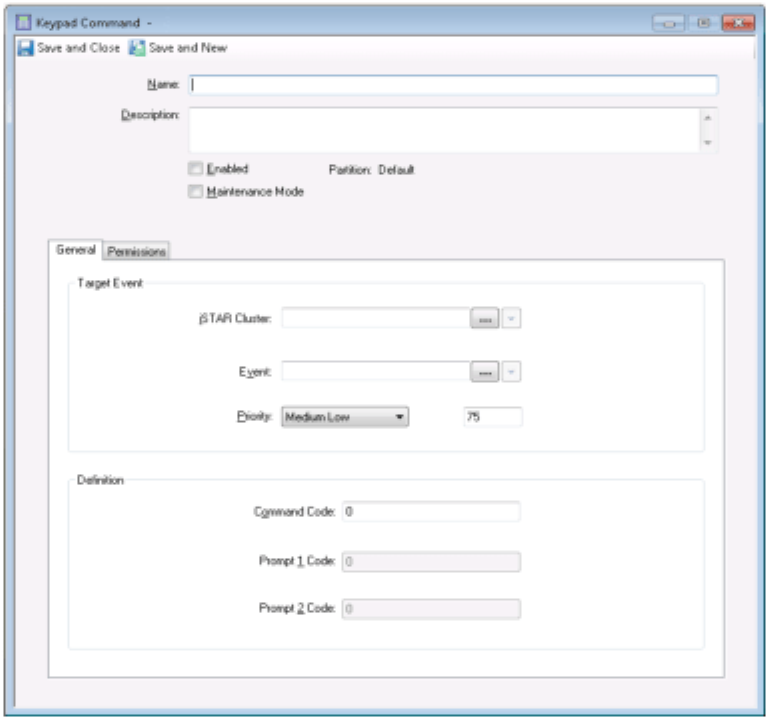
Keypad Command General Tab

The **Keypad Command General** tab, shown in Figure 52 on Page 211, lets you define the following for the Keypad Command:

- Home cluster
- Event which the command activates
- Priority of the Event
- Command Code and optional Prompt Codes

NOTE You can save a Keypad Command configuration without an iSTAR Cluster and an Event if you do not enable it. An existing Keypad Command becomes 'disabled' when it loses its Cluster and Event because the Event's Controller is either deleted or becomes 'unassigned.'

Figure 52: Keypad Command Editor General Tab



Name:

Description:

□ Enabled   Partition: Default

□ Maintenance Mode

iSTAR Cluster:

Event:

Priority: Medium Low   75

Command Code: 0

Prompt 1 Code: 0

Prompt 2 Code: 0

Keypad Command General Tab Definitions

The **Keypad Command Editor** and the **General** tab have the fields and buttons shown in Table 50 on Page 211.

Table 50: Keypad Command Editor - General Tab Fields

Fields/Buttons	Description
Name	Enter a unique name, up to 100 characters, to identify the Keypad Command.

Keypad Command Editor - General Tab Fields (continued)

Fields/Buttons	Description
Description	Enter a description of the Keypad Command, up to 255 characters.
Enabled	Select this check box to activate the Keypad Command.
Partition	A read-only field displaying the name of the Partition to which this Keypad Command belongs. (This field is visible only if the C•CURE 9000 system is partitioned.) NOTE: The Keypad Command belongs to the partition of the iSTAR Cluster selected in the Target Event box, **not** the Operator's New Object Partition. On the other hand, if the Keypad Command has no Cluster and no Event—is **not** enabled, when you save it, it belongs to the New Object Partition.
Maintenance Mode	Select this check box to put this Keypad Command into Maintenance Mode so whether or not Events, Status, and Activity related to this Keypad Command display on the Monitoring Station depends on the Operator's Privilege and the Application Layout assigned. For detailed information, see the Maintenance Mode chapter in the *C•CURE 9000 Hardware Configuration Guide*.
Target Event	
iSTAR Cluster	Select the home cluster for the command. (In a partitioned system, the iSTAR Cluster selection list is **not** limited by Partition, but includes all Clusters in the system.) NOTE: If you select the Event first, the system automatically enters the Cluster to which the Event's Controller belongs. This field is then unavailable.
Event	Select the Event to be activated by the Keypad command. (In a partitioned system, the Event selection list is **not** limited by Partition, but includes all panel Events in the system.) See the "Events" chapter in the *C•CURE 9000 Software Configuration Guide* for information about creating an event. NOTE: If an iSTAR Cluster is already selected, the available Events are related to that Cluster. If **no** Cluster is selected, all panel Events are available.
Priority	Indicates the priority level the system uses for sorting when displaying on the Monitoring Station and prioritizing actions associated with the event. The default priority is 75, Medium Low. Select a value from the drop-down list or type an integer from 0 to 200 to assign a priority to the Event. The lowest value is 0; the highest is 200.
Definition	
Command Code*	Defines the numbers to be pressed by personnel on the keypad for the command code (required).
Prompt 1 Code*	Defines the numbers to be pressed by personnel on the keypad for Prompt 1 (optional).
Prompt 2 Code*	Defines the numbers to be pressed by personnel on the keypad for Prompt 2 (optional).
*The total keypad command code must be unique for one cluster—the cluster of the iSTAR that owns the target event.	

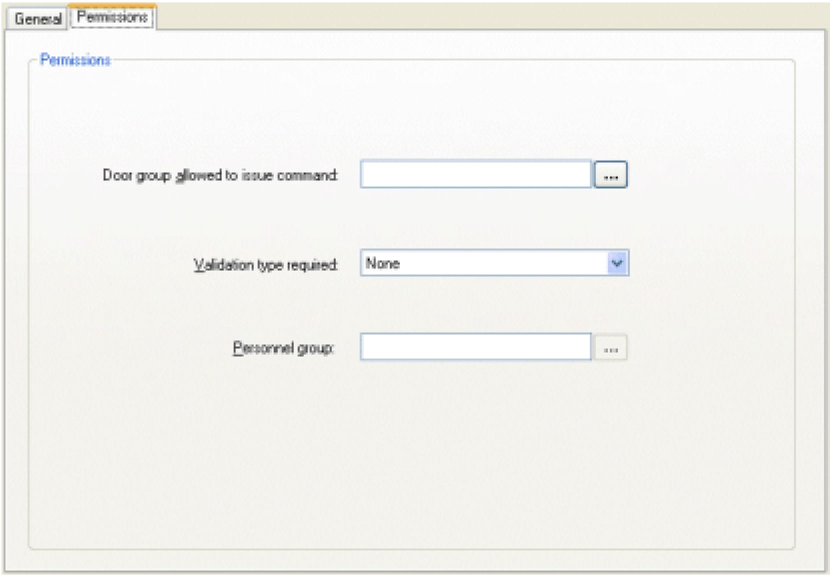
Keypad Command Permissions Tab

The **Keypad Command Permissions** tab, shown in Figure 53 on Page 213, lets you define the following for the Keypad Command:

- Doors at which the command will be available.
- Type of validation required once the keypad Command is entered.

Field for this tab are defined in Keypad Command Permissions Tab Definitions on Page 213.

Figure 53: Keypad Command Editor Permissions Tab



Door group allowed to issue command:

Validation type required: None

Personnel group:

Keypad Command Permissions Tab Definitions

The **Permissions** tab has the fields and buttons shown in Table 51 on Page 213.

Table 51: Keypad Command Editor - Permissions Tab Fields

Fields/Buttons	Description
Door group allowed to issue command	The Readers at the doors in the specified group can accept keypad commands. To specify a group, click ... and select a **Door Group** from the dialog box that appears. NOTE: Commands only function at doors within the home cluster.

Keypad Command Editor - Permissions Tab Fields (continued)

Fields/Buttons	Description
Validation type required	You can choose one of five validation modes from the this drop-down box. **None** – The Keypad Command does **not** require any extra validation. This is the **default**. **Credential Only** – The person **must** swipe a card with Clearance after entering the command. NOTE: Even Personnel with the **Keypad Commands Administrator** option selected (**Personnel General** tab) must have clearance to the door to validly use the command. **Credential and Personnel group** – The person **must** swipe a card with Clearance after entering the command, and must also belong to the Personnel group designated in the next field. NOTE: Personnel with the **Keypad Commands Administrator** option selected (**Personnel General** tab) who have clearance to the door do **not** have to be in the Personnel Group to validly use the command. **Credential and PIN** – The person **must** swipe a card with Clearance after entering the command, and in addition, must then enter a PIN. **Credential, Personnel Group and PIN** – All three of the preceding validation modes must be met by the person for the Keypad Command to be accepted.
Personnel group	NOTE: This field is available only if the Validation type selected in the preceding field specifies a Personnel Group. Click ... and select a **Personnel Group** from the dialog box that appears. NOTE: Personnel with the **Keypad Commands Administrator** option selected (**Personnel General** tab) can always activate all commands if they have clearance to the door.

Keypad Command Groups Tab

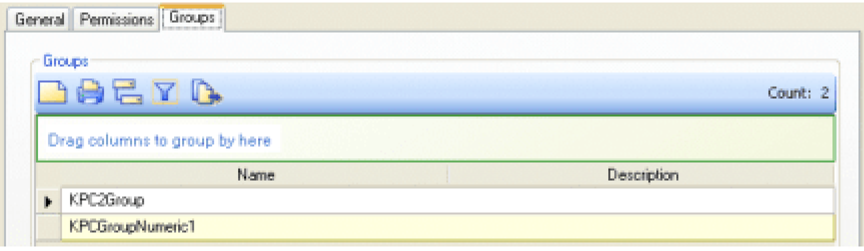
The Keypad Command **Groups** tab, shown in Figure 54 on Page 215, lists the Keypad Command Groups to which this Keypad Command belongs.

NOTE This tab does **not** display on the **Keypad Command Editor** when you are configuring a new Keypad Command. It displays when you are editing an existing Keypad Command.

The Groups table on this tab is a Dynamic View that you can filter, group, print, and view in Card View, using the buttons described in Keypad Command Editor Groups Tab Fields/Buttons on Page 215.

You can select any of the Keypad Command Groups in the list and double-click ▸ to edit it or right-click to display the Groups Context menu (described in the Groups chapter in the *C•CURE 9000 Software Configuration Guide*). You can also right-click in the **Name** or **Description** field of a Keypad Command Group row to display a standard edit menu.

Figure 54: Keypad Command Editor Groups Tab



Name	Description
KPC2Group	
KPCGroupNumeric1	

Keypad Command Groups Tab Definitions

The **Keypad Command Groups** tab has the buttons and fields shown in Table 52 on Page 215.

Table 52: Keypad Command Editor Groups Tab Fields/Buttons

Fields/Buttons	Name	Description
🗋	Card View	Click to display the list of Keypad Command Groups in Card View.
🖨	Print	Click to print the list of Keypad Command Groups.
▤	Group	Click to enable Grouping of the list. You can drag a column heading to the area labeled **Drag columns to group by here to** group the list by that heading.
▽	Filter	Click to display the filter bar. You can click in the filter bar to add filtering criteria to any column of the list. For more information about Filtering, see the Dynamic Views chapter in the *C•CURE 9000 Data Views Guide*.
Name		Name of the Group, up to 100 characters.
Description		Description of the Group.

Keypad Command Tasks

You can perform the following tasks using the Keypad Command Editor.

- Creating a Keypad Command on Page 216
- Creating a Keypad Command Template on Page 216
- Configuring a Keypad Command on Page 217
- Viewing a List of Keypad Commands on Page 220
- Modifying a Keypad Command on Page 222
- Deleting a Keypad Command on Page 222
- Setting a Property for a Keypad Command on Page 222
- Adding a Keypad Command to a Group on Page 223
- Configuring Readers for Keypad Commands on Page 224
- Configuring a Person to Use Keypad Commands on Page 226

Creating a Keypad Command

You can create a new Keypad Command using the **Keypad Command Editor**.

This procedure assumes that you have already defined the Keypad Command format for the system, configured the iSTAR Cluster and Controllers, configured a Keypad Command Event and downloaded it to an iSTAR Controller in the Cluster, and configured at least one Door Group—and if required by validation type, have also configured at least one Personnel Group.

To Create a Keypad Command

1. In the Navigation Pane of the Administration Workstation, click the **Areas and Zones** pane button.
2. Click the **Areas and Zones** drop-down list and select **Keypad Command**.
3. Click **New** to create a new Command. The **Keypad Command Editor** opens.
4. You can now configure the new Keypad Command.
5. To save your new Keypad Command, click **Save and Close**.

   - or -

   Alternatively, if you want to save the Keypad Command and then create a new one, click **Save and New**. The current Keypad Command is saved and closed, but the **Keypad Command Editor** remains open ready for a new Keypad Command.

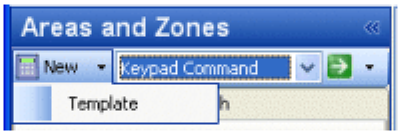
Creating a Keypad Command Template

You can create a new template for a Keypad Command. A Keypad Command template saves you time because you do not have to re-enter the same Command information again.

To Create a Keypad Command Template

1. In the **Navigation** Pane of the Administration Workstation, click the **Areas and Zones** pane button.

2. Click the **Areas and Zones** drop-down list and select **Keypad Command**.
3. Click the down-arrow on the **New** button, and click **Template**.



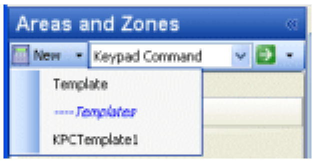
The **Keypad Command Editor** where you can configure the Command template opens.

4. Configure the template to meet your requirements. If you configure values for the **Priority** and **Validation type required** fields, these become part of the template; then when you subsequently create a new Keypad Command from that template, these values are already filled in.
5. In the **Name** field, enter the name you wish to use for the template.

   Example:

   KPCTemplate1
6. To save the template, click **Save and Close**.

   The template will be available as an option on the pull-down menu on the **New** button in the **Areas and Zones** pane.



Configuring a Keypad Command

This procedure assumes that you have already defined the Keypad Command format for the system, configured the iSTAR Cluster and Controllers, configured a Keypad Command Event and downloaded it to an iSTAR Controller in the Cluster, and configured at least one Door Group—and if required by validation type, have also configured at least one Personnel Group.

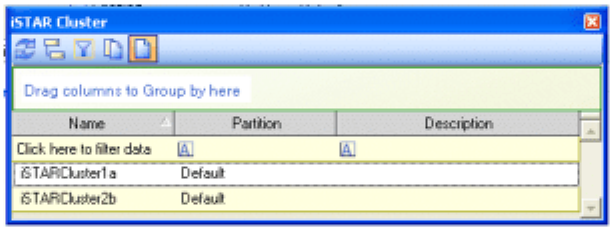
To Configure a Keypad Command

1. Create a new Keypad Command or modify an existing Keypad Command.

NOTE If you are modifying an existing Keypad Command, you **cannot** change the iSTAR Cluster field.

2. Type a **Name** and **Description** for the Keypad Command that sufficiently identifies this Keypad Command and its purpose.
3. In the **Target Event** box on the **General** tab, enter information as follows:

   a. In the **iSTAR Cluster** field, click ... and then select the home Cluster for the Keypad Command's Event from the Selection list that appears.



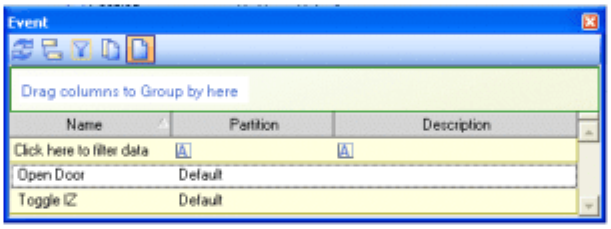
iSTAR Cluster

Drag columns to Group by here

Name	Partition	Description
Click here to filter data	A	A
iSTARCluster1a	Default	
iSTARCluster2b	Default	

NOTE If you select the Event first, the system automatically enters the Cluster to which the Event's Controller belongs.

b. In the **Event** field, click ... and then select the Event to be activated by the Keypad Command from the Selection list that appears.



Event

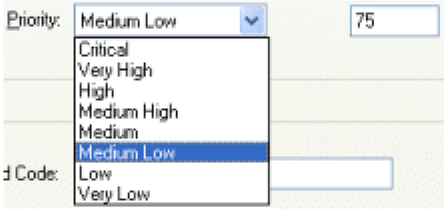
Drag columns to Group by here

Name	Partition	Description
Click here to filter data	A	A
Open Door	Default	
Toggle IZ	Default	

NOTE If an iSTAR Cluster is already selected, the available Events are related to that Cluster. If **no** Cluster is selected, all panel Events are available.

c. To change the Priority level assigned to the Keypad Command's Event action from the **Medium Low** 75 default,

Click the **Priority** down-arrow to select a new value.



Priority: Medium Low 75

- or -

Type an integer from 0 (zero) to 200 in the related numeric field.

4. In the **Definition** box on the **General** tab, configure the Keypad Command Code as follows:

a. In the **Command Code** field, enter the numbers that personnel will enter on the Keypad to activate the Command.

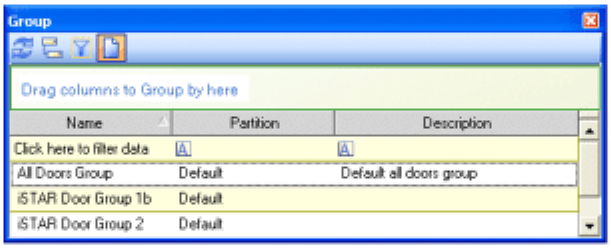
b. If the Keypad Command format defined for the system includes the optional Prompt 1 Code or both Prompt 1 and Prompt 2 Codes, the field(s) will be available for you to type the numbers for personnel to enter on the Keypad.

NOTE Make sure that the total Keypad Command Code is **unique** for one cluster—the cluster of the iSTAR that owns the target Event.

For detailed formatting information, see Keypad Command Format on Page 205.

5. Click the **Permissions** tab. The fields on this tab allow you to control the access to Keypad Commands.

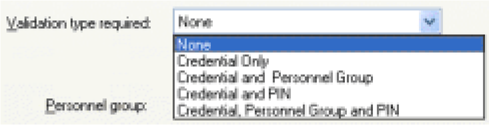
a. In the **Door group allowed to issue command** field, click [...] and then select the Door Group from the Selection list that appears. (This list only includes the "All Doors Group" and iSTAR Door Groups.)



Name	Partition	Description
Click here to filter data	A	A
All Doors Group	Default	Default all doors group
iSTAR Door Group 1b	Default	
iSTAR Door Group 2	Default	

Keypad Commands will be allowed at those Doors in the selected group that are within the Cluster selected for the Keypad Command on the **General** tab.

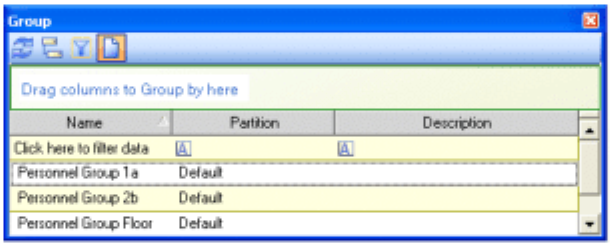
b. To specify additional validations for this Keypad Command when it is entered on a keypad (the default is **None**), click the down-arrow in the **Validation type required** field and select an option from the drop-down list.


Validation type required: None

None
Credential Only
Credential and Personnel Group
Credential and PIN
Credential, Personnel Group and PIN
Personnel group:

If you select either **Clearance and Personnel Group** or **Clearance, Personnel Group and PIN**, the **Personnel group** field becomes available. You must then select the group whose members will be allowed to use this Keypad Command.

c. If required, in the **Personnel group** field, click [...] and then select a Personnel Group from the Selection list that appears.



Name	Partition	Description
Click here to filter data	A	A
Personnel Group 1a	Default	
Personnel Group 2b	Default	
Personnel Group Floor	Default	

NOTE Personnel who have the **Keypad Command Administrator** option selected on their record can issue the Keypad Command even if they are **not** in the selected Personnel Group. For information, see Configuring a Person to Use Keypad Commands on Page 226.

6. Enable the Keypad Command by selecting the **Enabled** check box on the top of the Editor.

7. To save the configured Keypad Command, click **Save and Close**.

   - or -

   Alternatively, if you want to save the Keypad Command and then create a new one, click **Save and New**. The current Keypad Command is saved and closed, but the **Keypad Command Editor** remains open ready for a new Keypad Command.

8. You can optionally configure specific Readers to allow the entry of Keypad Commands, disallow them, or allow them during certain time periods. For configuration information, see Configuring Readers for Keypad Commands on Page 224.

9. As mentioned in the note above, you can optionally configure certain Personnel as Keypad Command Administrators, which allows them to use Keypad Commands without being in a designated Personnel Group. For configuration information, see Configuring a Person to Use Keypad Commands on Page 226.

Viewing a List of Keypad Commands

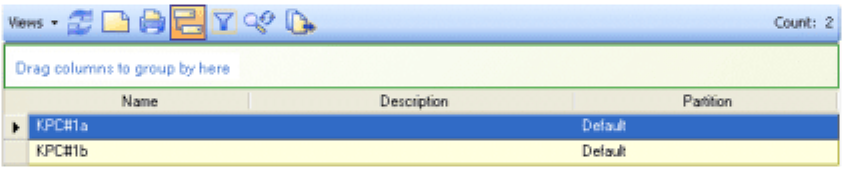
You can display a list of the Keypad Commands you have created by opening a Dynamic View of Keypad Commands.

NOTE The information in Dynamic Views is dynamically updated.

To View a List of Keypad Commands

1. In the **Navigation** Pane of the Administration Workstation, click **Areas and Zones** to open the **Areas and Zones** pane.
2. Select **Keypad Command** from the **Areas and Zones** drop-down list.
3. Click ➡ ▾ to open a Dynamic View listing all Keypad Command Objects, as shown in Figure 55 on Page 220. (You can also click the down-arrow of this button to either view the list in the current tabbed view or open a new tabbed view).

Figure 55: Keypad Commands List



Name	Description	Partition
KPC#1a		Default
KPC#1b		Default

You can sort, filter, and group items in the list. You can right-click a Keypad Command in the list to open the Keypad Command Context menu and perform any of the functions on that menu.

For more information on using Dynamic Views, see the Dynamic Views chapter in the *C•CURE 9000 Data Views Guide*.

Keypad Command List Context Menu

The context menu that opens when you right-click a Keypad Command in the Keypad Command Dynamic View includes the selections described in Table 53 on Page 221.

Table 53: Keypad Command List Right-Click Context Menu Options

Menu Selection	Description
Edit	Click this menu selection to edit the selected Keypad Command. The **Keypad Command Editor** opens. You can rename the Keypad Command, change the description and any other attributes with the exception of the iSTAR Cluster.
Delete	Click this menu selection to delete the selected Keypad Command. A prompt appears asking you to confirm that you want to delete the Keypad Command. Click **Yes** to delete the Keypad Command or **No** to cancel the deletion.
Set property	Click this menu selection to change the value of the selected properties in the selected Keypad Command(s). A dialog box appears asking you to select a property to change. Click ... to open a selection list and click the property you wish to change. You can then change the value of the following properties: • **Description** – You can change the textual description of the Keypad Command(s) by selecting this property and typing in a new value. • **Enabled** – You can determine whether or not the Keypad Command(s) are activated on the system by selecting this property and selecting/clearing the **Value** check box. • **Priority** – You can change the priority level for the Keypad Command(s) by selecting this property and clicking the up/down arrows next to the **Value** field.
Add to Group	You can add one or more selected Keypad Commands to a Group of Keypad Commands. When you click this menu choice, a dialog box appears for you to select the Group to which to add the Keypad Command. When you click a Group of Keypad Commands in the list, the selected Keypad Command is added to the Group.
Export selection	Click this menu selection to Open an Export...to XML or CSV file dialog box to export one or more of the selected Keypad Command records to either an XML or a CSV file. This allows you to quickly and easily create XML/CSV reports on the selected data. NOTE: Although XML is the initial default file type, once you choose a type in the **Save as type** field, whether XML or CSV, that becomes the default the next time this dialog box opens. • When you export to an XML file, all available data for the selected object(s), whether displayed in the Dynamic View or not—as well as all the child objects of the selected record(s), is exported. • When you export to a CSV file, only data in the columns displaying in the Dynamic View is exported, and in the order displayed. This allows you to both select and arrange data fields for your report. In addition, exporting to a CSV file allows you to view the exported data in an Excel spreadsheet and further manipulate it for your use. For more information, see the Dynamic Views chapter in the *C•CURE 9000 Data Views Guide*. NOTE: When you click **Export Selection**, you are running the export on the client computer. Consequently, the system does not use the Default Export Directory Path—which is on the server. It opens a directory on the client, reverting to the last directory used. You can navigate to the default export server directory, if you wish. Or to avoid confusion or use the same destination folder for both client and server computers, you can use UNC (Universal Naming Convention) paths, for example: \\Computer Name\Program Files\Software House\SWHouse\SWHSystem\Export.
Find in Audit Log	Click this menu selection to Open a **Query Parameters** dialog box in which you can enter prompts and/or modify the Query criteria to search for entries in the Audit Log that reference the selected Keypad Command. When found the results display in a separate Dynamic View.
Find in Journal	Click this menu selection to Open a **Query Parameters** dialog box in which you can enter prompts and/or modify the Query criteria to search for entries in the Journal that reference the selected Keypad Command. When found the results display in a separate Dynamic View.
Turn Maintenance Mode On	Click this menu selection to put this Keypad Command into Maintenance Mode. For detailed information, see the Maintenance Mode chapter in the *C•CURE 9000 Hardware Configuration Guide*.

Modifying a Keypad Command

You can modify an existing Keypad Command by editing it using the **Keypad Command Editor**.

To Modify a Keypad Command

1. In the **Navigation** Pane of the Administration Workstation, click **Areas and Zones** to open the **Areas and Zones** pane.
2. Select **Keypad Command** from the **Areas and Zones** drop-down list.
3. Click ➔ ▾ to open a Dynamic View showing all Keypad Command Objects.
4. Right-click the Keypad Command in the list that you want to change and select **Edit** from the context menu that appears.

   - or -

   Double-click the Keypad Command you want to change.

   The **Keypad Command Editor** opens for you to edit the Keypad Command making changes as you wish in the fields on the top of the editor, and on the **General** and **Permissions** tabs (with the exception of the iSTAR Cluster).
5. To save the modified Keypad Command, click **Save and Close**.

   - or -

   Alternatively, if you want to save the Keypad Command and then create a new one, click **Save and New**. The current Keypad Command is saved and closed, but the **Keypad Command Editor** remains open ready for a new Keypad Command.

Deleting a Keypad Command

You can delete a Keypad Command.

To Delete a Keypad Command

1. In the **Navigation** Pane of the Administration Workstation, click **Areas and Zones** to open the **Areas and Zones** pane.
2. Select **Keypad Command** from the **Areas and Zones** drop-down list.
3. Click ➔ ▾ to open a Dynamic View showing all Keypad Command Objects.
4. Right-click the Keypad Command in the list that you want to delete and select **Delete** from the context menu that appears.
5. Click **Yes** on the "Are you sure you want to delete the selected Keypad Command?" message box.

Setting a Property for a Keypad Command

You can use **Set Property** to quickly set a property for a Keypad Command without opening the **Keypad Command Editor**. You use Set Property for mass updates.

To Set a Property for Keypad Commands

1. In the **Navigation** Pane of the Administration Workstation, click **Areas and Zones** to open the **Areas and Zones** pane.
2. Select **Keypad Command** from the **Areas and Zones** drop-down list.
3. Click ➔▾ to open a Dynamic View showing all Keypad Command Objects.
4. Right-click the Keypad Command in the list for which you want to set the property and select **Set Property** from the context menu.
5. Specify the property for the Keypad Command. Click the drop-down button to see a list of properties.
6. Enter the value for the property and click **OK**.
7. Click **OK** on the **Setting Properties of Keypad Command** message box.

Adding a Keypad Command to a Group

You can use **Add To Group** to add the Keypad Command Object to a Group.

To Add Keypad Commands To a Group

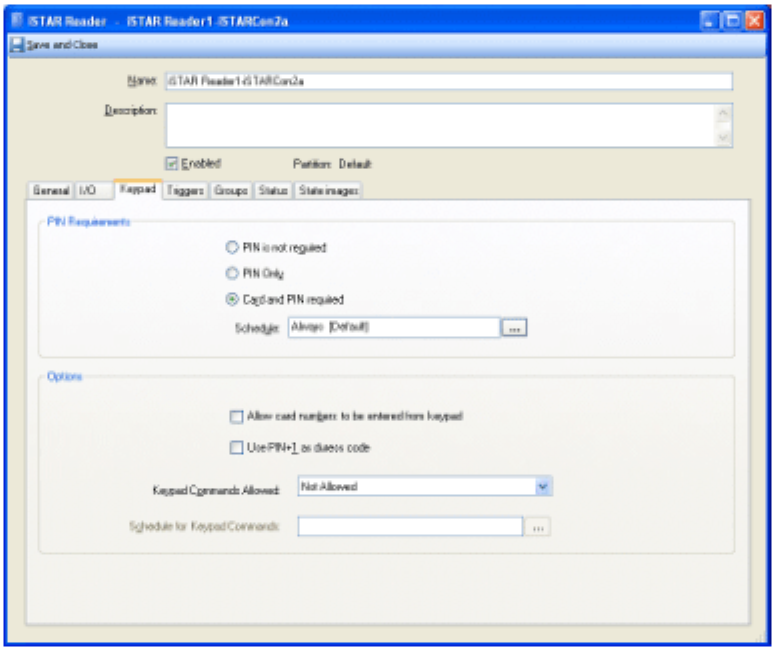
1. Make sure that the Group is already configured for the Keypad Command to be added to it.
2. In the **Navigation** Pane of the Administration Workstation, click **Areas and Zones** to open the **Areas and Zones** pane.
3. Select **Keypad Command** from the **Areas and Zones** drop-down list.
4. Click ➔▾ to open a Dynamic View showing all Keypad Command Objects.
5. Right-click the **Keypad Command** in the list that you want to add to a Group and select **Add To Group** from the context menu.
6. When the **Group** list displays, select the Group you want to add the Keypad Command to.

Configuring Readers for Keypad Commands

You can configure a Reader to allow/disallow the use of Keypad Commands as the default at that Reader. You can also specify that Keypad Commands can only be used at the Reader during particular times.

You configure these properties on the **Keypad** Tab of the **iSTAR Reader Editor**, as shown in Figure 56 on Page 224.

Figure 56: iSTAR Reader Keypad Tab



Name: iSTAR Reader1-iSTARCon2a

Description:

☑ Enabled

Partition: Default

○ PIN is not required

○ PIN Only

● Card and PIN required

Schedule: Always (Default)

□ Allow card numbers to be entered from keypad

□ Use PIN+1 as duress code

Keypad Commands Allowed: Not Allowed

Schedule for Keypad Commands:

NOTE You can also manually **enable/disable** the use of Keypad Commands at selected Readers for a specified time: in the Administration application from either the Readers Dynamic View or Hardware Tree or in the Monitoring Station from the Status List for Readers. For information, see Enabling/Disabling Keypad Commands at Readers on Page 227.

To Configure Keypad Command Use for an iSTAR Reader

1. In the Navigation Pane of the Administration Workstation, click the **Hardware** pane button.

2. Click the **Hardware** drop-down list, select **iSTAR Reader**, and click to open a Dynamic View showing a list of all existing iSTAR Readers.

   - or -

   Expand the Hardware Tree.

3. In the Dynamic View list/Tree, select the iSTAR Reader for which you want to set the use of Keypad Commands, right-click, and click **Edit** from the context menu that appears.

4. When the **iSTAR Reader Editor** appears, click to open the **Keypad** Tab, shown in Figure 56 on Page 224.

5. In the **Options** box, click the down-arrow in the **Keypad Commands Allowed** field and select **Not Allowed**, **Always Allowed**, or **Allowed during specified schedule** from the drop-down list. (The default is **Not Allowed**.)

If you select **Allowed during specified schedule**, the **Schedule for Keypad Commands** field becomes available. (The default is **Always**.)

a. Click ... to open a Schedule selection list.

b. Click to select the desired Schedule.

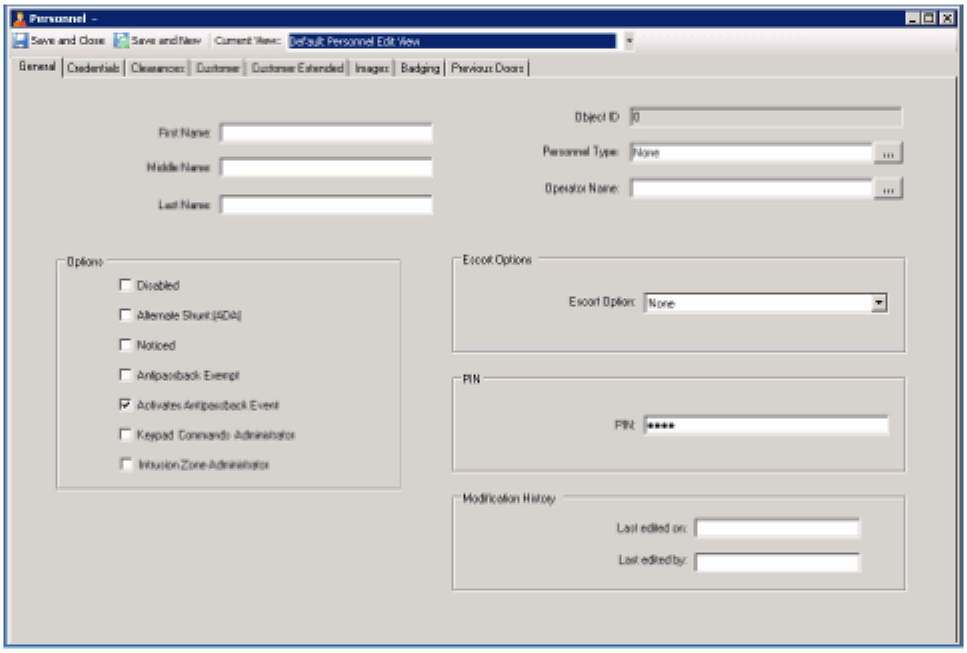
6. To save these Reader Keypad Command properties, click **Save and Close**.

Configuring a Person to Use Keypad Commands

You can configure a person to be able to use Keypad Commands even if he or she is not in a Personnel Group granted the Keypad Command permission.

You configure this on the **Personnel Editor General** tab, as shown in Figure 57 on Page 226.

Figure 57: Personnel Editor – General Tab



Current View: Default Personnel Edit View

First Name:

Middle Name:

Last Name:

Object ID: 0

Personnel Type: None

Operator Name:

Options

- ☐ Disabled
- ☐ Alternate Shunt (ADA)
- ☐ Noticed
- ☐ Antipassback Exempt
- ☑ Activates Antipassback Event
- ☐ Keypad Commands Administrator
- ☐ Intrusion Zone Administrator

Escort Options

Escort Option: None

PIN

PIN: ****

Modification History

Last edited on:

Last edited by:

To Configure a Person to Use Keypad Commands

1. In the Navigation Pane of the Administration Workstation, click the **Personnel** pane button.
2. Click the **Personnel** drop-down list and select **Personnel**.
3. Click **New** to create a new Personnel record.

   - or -

   Click to open a Dynamic View showing a list of all existing Personnel Objects, right-click the Personnel record you want to change, and click **Edit** from the context menu that appears.

   The **Personnel Editor** opens with the **General** Tab displayed.
4. In the **Options** box, click to select the **Keypad Commands Administrator** option.

NOTE If this option is selected, this person can use any Keypad Commands regardless of the Personnel Group the command is validated for.

If this option is **not** selected, this person can **only** use Keypad Commands configured:

- For a Personnel Group in which he/she is included.
- Without any types of validation.

5. To save the Personnel record, click **Save and Close**.

Enabling/Disabling Keypad Commands at Readers

You can manually enable/disable Keypad Commands at one or more selected Readers whether or not Keypad Commands are allowed at the Reader by default. You can also view a Reader's Keypad Command Cause to see both the default/current Keypad Command state and enable/disable from there. You can perform these actions in several different places:

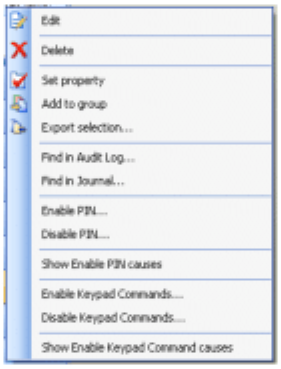
- Administration application
  - Reader Dynamic View
  - Hardware Tree – Reader Object
- Monitoring Station
  - Reader Status List

To View the Reader Keypad Command Cause List

1. In the Navigation Pane of the Administration Workstation, click the **Hardware** pane button.
2. Click the **Hardware** drop-down list, select **iSTAR Reader**, and click ➡ ▾ to open a Dynamic View showing a list of all existing iSTAR Readers.

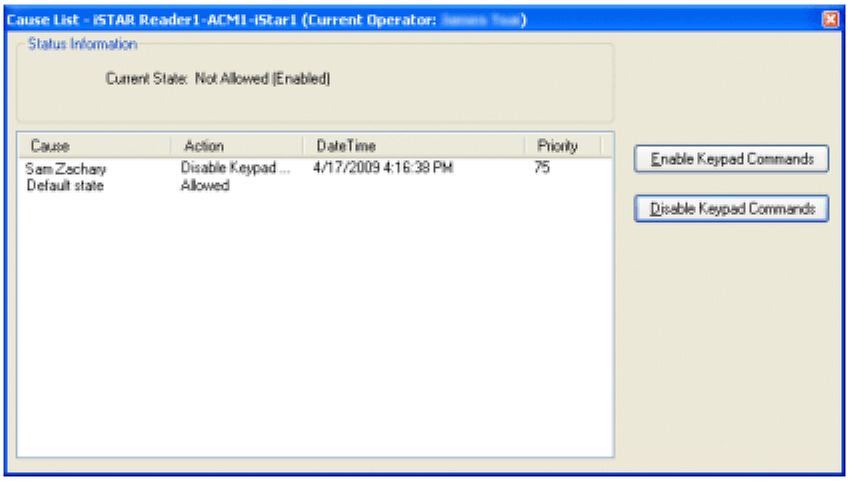
   - or -

   Expand the Hardware Tree.
3. In the Dynamic View list or in the Tree, select the iSTAR Reader whose Keypad Command Cause List you want to view and right-click to display the context menu.



4. Click **Show Enable Keypad Command Causes** to open the Cause List dialog box shown in the example in Figure 58 on Page 228.

Figure 58: Reader Keypad Command Cause List Example



Cause List - iSTAR Reader1-ACM1-iStar1 (Current Operator: [redacted])

Status Information

Current State: Not Allowed (Enabled)

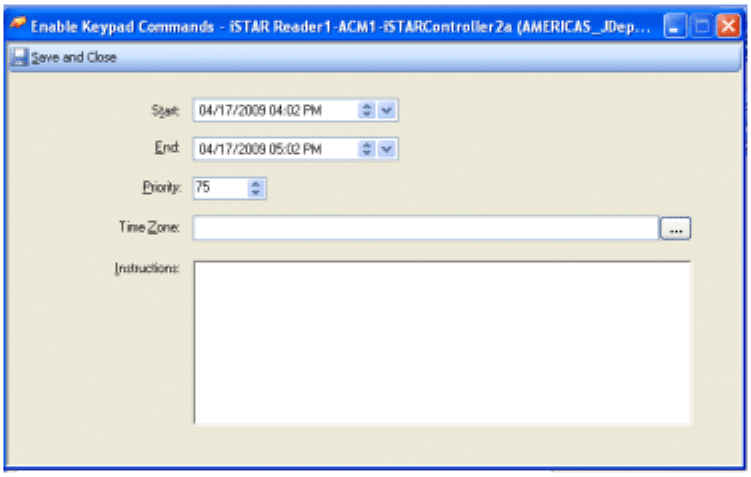
Cause	Action	DateTime	Priority
Sam Zachary	Disable Keypad ...	4/17/2009 4:16:38 PM	75
Default state	Allowed		

The Status Information on the top indicates that this Reader is currently enabled while Keypad Commands are currently **not** allowed at this reader. Since as shown in the Cause list the Keypad Command default state at this Reader is **Allowed**, its current state is the result of the **Disable Keypad Command** Manual Action at 4:16:38 PM on 4/17/2009 with a Priority of **75**.

5. If you want to Enable or Disable Keypad Commands at this Reader, click the **Enable Keypad Commands** or **Disable Keypad Commands** button.

   A Manual Action dialog box such as that shown in the example in Figure 59 on Page 228 displays.

Figure 59: Enable Keypad Commands for Reader Manual Action Dialog Box



Enable Keypad Commands - iSTAR Reader1-ACM1-iSTARController2a (AMERICAS_JDep...

Start: 04/17/2009 04:02 PM

End: 04/17/2009 05:02 PM

Priority: 75

Time Zone:

Instructions:

6. Enter Start and End date/times and a Priority for the Action, as well as the Time Zone and if necessary, any instructions.

7. Click **Save and Close**.

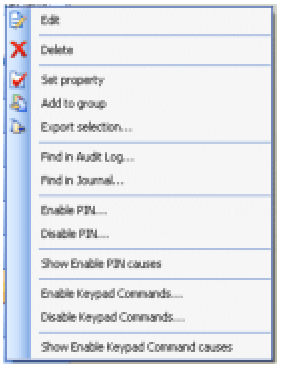
To Manually Enable/Disable Keypad Commands

1. In the Navigation Pane of the Administration Workstation, click the **Hardware** pane button.
2. Click the **Hardware** drop-down list, select **iSTAR Reader**, and click ➡ ▾ to open a Dynamic View showing a list of all existing iSTAR Readers.

   - or -

   Expand the Hardware Tree.
3. In the Dynamic View list or in the Tree, select the iSTAR Reader at which you want to enable/disable Keypad Commands.

NOTE In the Dynamic View list, you can select multiple Readers at the same time.



4. Click **Enable Keypad Commands/Disable Keypad Commands**.

   A Manual Action dialog box such as that shown in the example in Figure 59 on Page 228 displays.
5. Enter Start and End date/times and a Priority for the Action, as well as the Time Zone and if necessary, any instructions.
6. Click **Save and Close** to save your changes.

Index