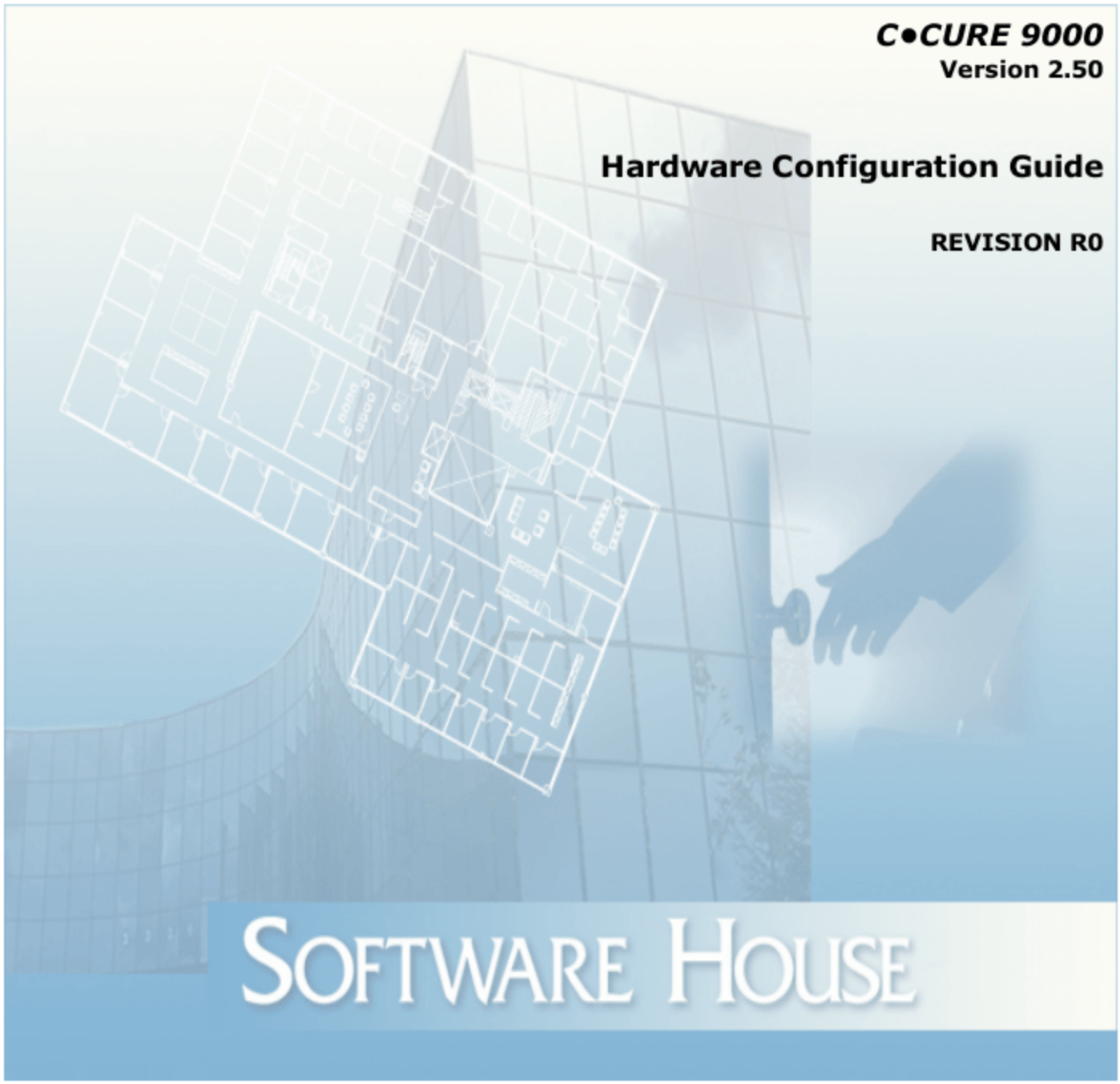
SOFTWARE HOUSE

From Tyco Security Products



UM-130 R0

C•CURE 9000 version: 2.50
Document Number: UM-130
Revision: R0
Release Date: December 2015

Table of Contents

Preface

This *C•CURE 9000 Hardware Configuration Guide* is designed for new and experienced security system users. The manual describes the various hardware objects in the C•CURE 9000 application program and presents procedures for configuring and using them.

The manual assumes that you have already installed C•CURE 9000 and have familiarized yourself with the basic C•CURE 9000 information provided in the *C•CURE 9000 Getting Started Guide*.

In this preface

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.

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]	

1

The Hardware Pane

This chapter explains how to use the C•CURE 9000 Hardware pane to configure and manage the hardware components that are connected to the C•CURE 9000 server.

In this chapter

Using the Hardware Pane

The Hardware pane displays a tree structure that shows how you have configured the hardware on the C•CURE 9000 system. For example, the hardware tree shows you which readers, inputs, and outputs are configured for each controller.

You can use the Hardware Tree to navigate to hardware components you want to view or edit, or to create new hardware components, such as a reader you want to add to a controller.

The Hardware Tree displays, by default, folders for Digital Certificates, Floors, Reader LCD Message Sets, and a Hardware Folder called **Company Name**.

The folder called **Company Name** is the default container for apC Comm Ports and the Controllers, Readers, Doors, Elevators, Inputs, and Outputs.

This folder is re-namable so that you can customize the C•CURE 9000 Hardware Tree to your site's needs.

You can create additional Hardware Folders as needed.

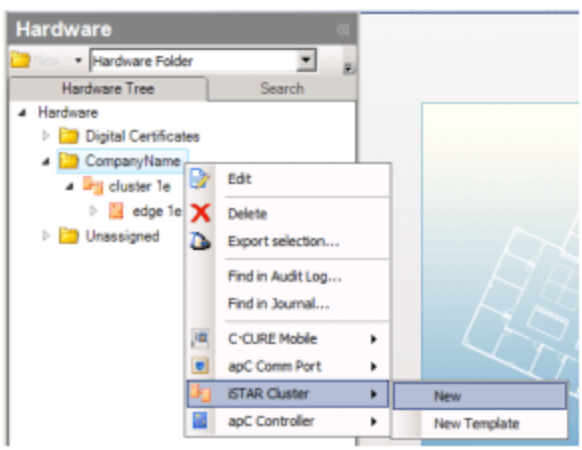
You can click on the ⊟ to the left of a folder or object to expand the tree.

When you select a folder or object in the tree, you can right-click to display a context menu that shows the objects you can create under the selected folder or object.

Example:

If you right-click on the **Company Name** folder, the context menu shows that you can create a wide variety of Hardware Tree objects in this folder.

Figure 1: Hardware Tree Context Menu



The following topics provide more information about using the Hardware pane.

- Partitions on Page 21
- Hardware Tree on Page 22
- Hardware Tree Objects on Page 22
- Hardware Tree Tasks on Page 23

Partitions

If you partition the C•CURE 9000, a new Hardware folder is created for each Partition you create, and given the same name as the Partition.

You can also create additional Hardware folders to contain hardware devices if you need to separately group hardware to reflect, for example, a multi-tenant building, a campus, or a multi-site company.

You can use Partitioning and Privileges to control Operator access to each tenant's hardware folder(s) if you don't want one tenant to be able to view another tenant's security access hardware and personnel.

The **New Object Partition** setting in the Administration Workstation determines the Partition in which an Operator can create objects, in addition to Hardware Tree objects such as Floors that reside at the root of the Hardware Tree. You can use the Privilege Editor to grant or deny an Operator access to a Partition, which affects whether they can view or create objects in that Partition.

For example, you could create a privilege that has no access to the Partition (and Hardware folder) called Company A, but with full access to Company B, and assign it to Operators from Company B, so that they can view their configuration but not the configuration for Company A. See the *C•CURE 9000 Software Configuration Guide* for more information about the Privilege Editor.

You can also drag and drop objects to move them in the Hardware Tree. For example, you can move C•CURE Mobile objects from one Hardware folder to another. See Using Drag and Drop in the Hardware Tree on Page 27 for more information.

Hardware Tree

The Hardware pane displays a tree structure that shows how you have configured the hardware on the C•CURE 9000 system. For example, the hardware tree shows you which readers, inputs, and outputs are configured for each controller.

You can use the Hardware Tree to navigate to hardware components you want to view or edit, or to create new hardware components, such as a reader you want to add to a controller.

The Hardware Tree displays, by default, folders for Floors, Digital Certificates, and a Hardware Folder called **Company Name**.

The folder called **Company Name** is the container for your Comm Ports, Controllers, Readers, Doors, Elevators, Inputs, and Outputs.

This folder is re-namable so that you can customize the C•CURE 9000 Hardware Tree to your site's needs.

You can click on the ⊞ to the left of a folder or object to expand the tree.

When you select a folder or object in the tree, you can right-click to display a context menu that shows the objects you can create under the selected folder or object. For example, if you right-click on the **Company Name** folder, the context menu shows that you can create a wide variety of Hardware Tree objects in this folder.

If you Partition your C•CURE 9000, a new Hardware folder is created for each Partition you create. This hardware folder is given the same name as the Partition.

You can also create additional Hardware folders to contain hardware devices if you need to separately group hardware to reflect, for example, a multi-tenant building, a campus, or a multi-site company.

You can use Partitioning and Privileges to control Operator access to each tenant's hardware folder(s) if you don't want one tenant to be able to view another tenant's security access hardware and personnel.

For example, you could create a privilege that has no access to the Partition (and Hardware folder) called Company A, but with full access to Company B, so that Operators from Company B can view their configuration but not the configuration for Company A.

You can also drag and drop objects to move them in the Hardware Tree. For example, you can move C•CURE Mobile objects from one Hardware folder to another. See Using Drag and Drop in the Hardware Tree on Page 27 for more information.

Hardware Tree Objects

Table 1 on Page 23 shows the types of objects (and objects that reside under them as child objects) in the Hardware Tree.

Table 1: Hardware Tree Objects

Object	Description
Hardware Folder	See Hardware Folders on Page 31.
Digital Certificate	These objects reside in the Hardware Tree but they are created using **Encryption Options** from the Options & Tools pane. See the *C•CURE 9000 System Maintenance Guide* for more information.
Floor	See Floors Overview on Page 396.
Reader LCD Message Set	See Reader LCD Message Set Overview on Page 382
apC Comm Port	See apC Comm Port Editor on Page 310.
CCURE Mobile device	These objects reside in the Hardware Tree but they are documented in the *C•CURE Mobile Handheld Reader User Guide*. NOTE: C•CURE Mobile cannot be used in UL applications.
iSTAR Cluster	See Configuring iSTAR Clusters on Page 87.
apC Controller	See apC Panel Overview on Page 296.

Hardware Tree Tasks

Creating a New Object in the Hardware Tree

Most objects in the Hardware Tree support a right-click Context Menu that shows you the actions you can perform on that object.

The right-click Context Menu for an object has selections for objects that you can create under that object.

For example, if you want to create an iSTAR Cluster in a Hardware Folder, right-click on the Hardware Folder and select iSTAR Cluster from the menu.

To Create a New Object in the Hardware Tree

1. Select the Folder or Object that will contain the object you want to create.
2. Right-click on the object and you should see in the Context menu a list of the objects that you can create.
3. Select the object you wish to create and select **New** from the menu.
4. The Editor for the object opens and you can configure the object.

Deleting an Object in the Hardware Tree

You can delete objects from the Hardware Tree if they are no longer needed. If you delete an object that has a child object (such as a Door or Reader) below it, those objects are also deleted.

To Delete an Object in the Hardware Tree

1. Select the Folder or Object that you wish to delete.
2. Right-click on the object and select **Delete**.
3. A confirmation dialog box appears to confirm that you want to delete the object. Click **Yes** to delete the object, or **No** to cancel the deletion.
4. A dialog box appears to confirm the deletion. You can click:
   - **OK** to close the dialog box.
   - **Print** to print the deletion message.
   - **Email** to send the deletion message to the email address you have configured in the Customer Support section of the C•CURE 9000 System Variables.

Viewing a List of Hardware Tree Objects

You can view a list of any type of Hardware Tree object.

To View a List of Hardware Tree Objects

1. Click the **Hardware** button in the Navigation Pane to open the Hardware Tree.
2. Use the drop-down list in the Hardware pane to select the object type that you want to list.
3. Click  and a Dynamic View listing the object type appears in the content area.
4. You can filter, sort, group, and add columns to the list. See the *C•CURE 9000 Data Views User Guide* chapter on Dynamic Views for more information.

The Dynamic View for an object type includes a column that displays the Time Zone in which the object resides. This can be useful in determining when an Event or Trigger is activated for an object in a different Time Zone than the C•CURE 90000 Server.

If you right-click a row in the Dynamic View, a context menu is displayed. This menu contains a number of standard selections, as well as selections that are specific for different object types. See **Using the Object List Context Menu** in the *C•CURE 9000 Getting Started Guide* for more information about the object context menu.

The context menu for iSTAR, apC, ASSA ABLOY, Connected Program readers allows you to select one or more readers and Add or Remove Cards formats. See Add or Remove Reader Card Formats on Page 25 for more information.

Add or Remove Reader Card Formats

The context menu for for iSTAR, apC, ASSA ABLOY, and Connected Program readers allows you to select one or more readers and add or remove Cards formats. For iSTAR, the APERIO, Schlage Wireless, Direct Connect Wiegand, and RM readers offer this selection.

The context menu actions are equivalent to opening each of the selected readers and adding/removing the card format from each reader.

The limits for card formats allowed for apC (8 per reader) and iSTAR (10 per reader) are enforced when using these menu actions.

If the selected Card Formats cannot be added or removed from the selected readers, the confirmation dialog box for the Add/Remove displays "Already has card format" or or "Nothing to remove...". Errors that occur are shown in the confirmation dialog box as well.

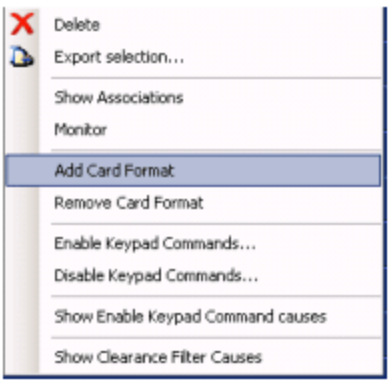
To Add or Remove Card Formats from a Reader via a Dynamic View

1. From the Hardware pane, use the drop-down menu to select the type of Reader you want to display in a dynamic View, and click  .

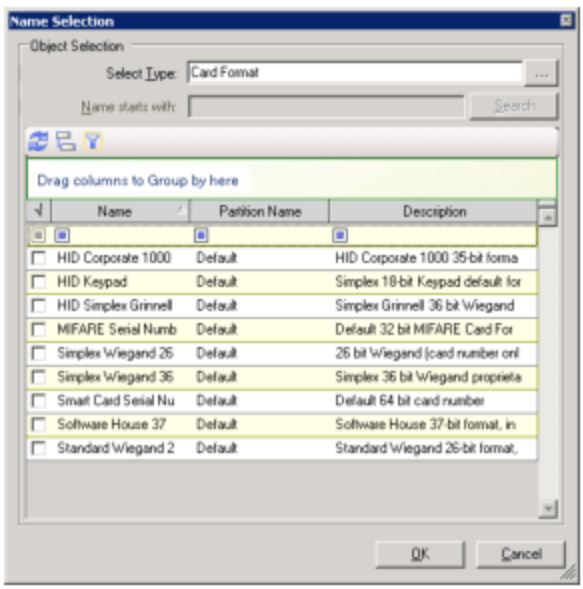
   Example:

   If you select iSTAR Reader, the Dynamic View displays multiple types of iSTAR Reader. If you select iSTAR Aperio Reader, only that type of reader is displayed.

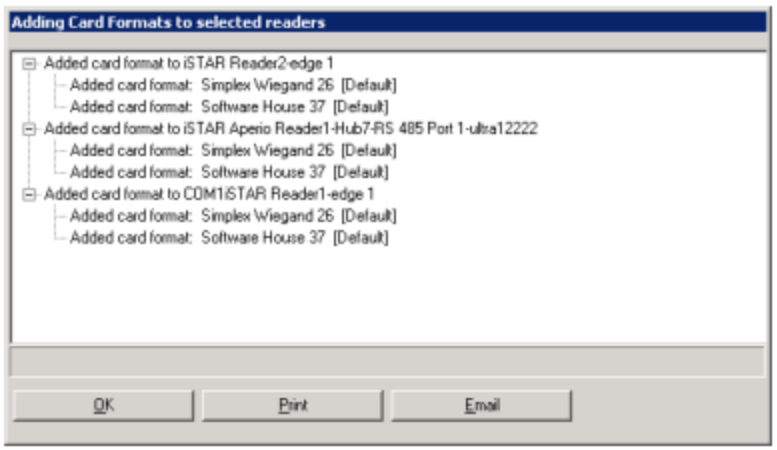
2. Select one or more readers from the list (you can use multiple selection keystrokes such as **CTRL+Left-click** and **SHIFT+Left-click** to select more than one reader).
3. Right-click the selected readers to display the context menu.



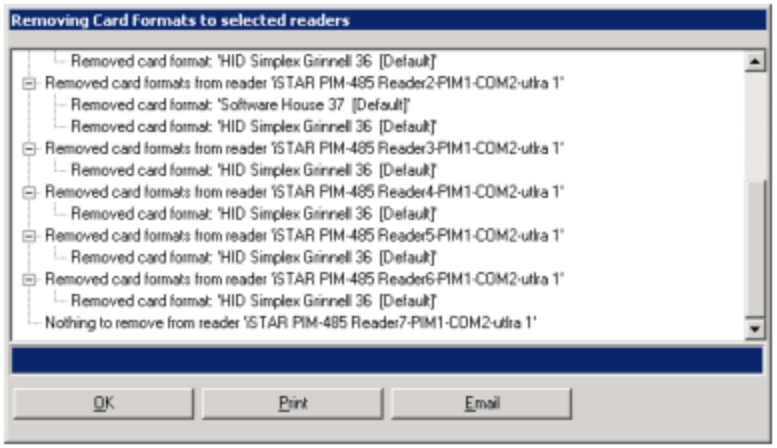
4. Select **Add Card Format** or **Remove Card Format** from the menu.
5. The Card Format Name Selection dialog box appears. Select (☑) each Card Format that you want to add or remove from the readers, then click **OK**.



6. If you added readers, a confirmation dialog box appears, showing the formats added:



7. If you removed readers, a confirmation dialog box appears, show the formats removed:



8. Click **OK** to complete the Add/Remove.

Using Drag and Drop in the Hardware Tree

You can drag and drop objects to move them in the Hardware Tree, within certain restrictions.

- You cannot move Root level objects such as Folders and Floors.
- You cannot move objects in Hardware Folders to the Root level.
- You cannot move objects that are Folders, such as a folder named C•CURE Mobile (but you can move their contents to another C•CURE Mobile folder).
- You cannot move child objects of one Controller to another Controller.

NOTE Some objects cannot be moved to another partition via drag and drop. For example, you cannot move an iSTAR Controller to a different Partition via drag and drop, nor can you move a non-partitionable object. Also, you cannot move an iSTAR Cluster to a different Partition if the Cluster is Enabled.

To determine if you can drag and drop an object, click on the object and then drag to the right with the mouse. If the  cursor appears, you can drag and drop the object. If you try to drop the object in an invalid location, the object instead remains in its original location. For example, if you tried to drop an apC Comm Port in an iSTAR Cluster, the object is not be moved, and an error message "Invalid Hardware Folder" appears.

To Drag and Drop an Object in the Hardware Tree

1. Click the **Hardware** button in the Navigation Pane to open the Hardware Tree.
2. Click on an object to select it (the object will be highlighted when selected).
3. Drag to the right with the mouse. The drag and drop cursor  appears. (If it does not appear, you cannot drag and drop the object.)
4. Drag the object to the location you want and release the mouse button. If you have chosen a valid location for the object, it then appears in the new location.

   Example

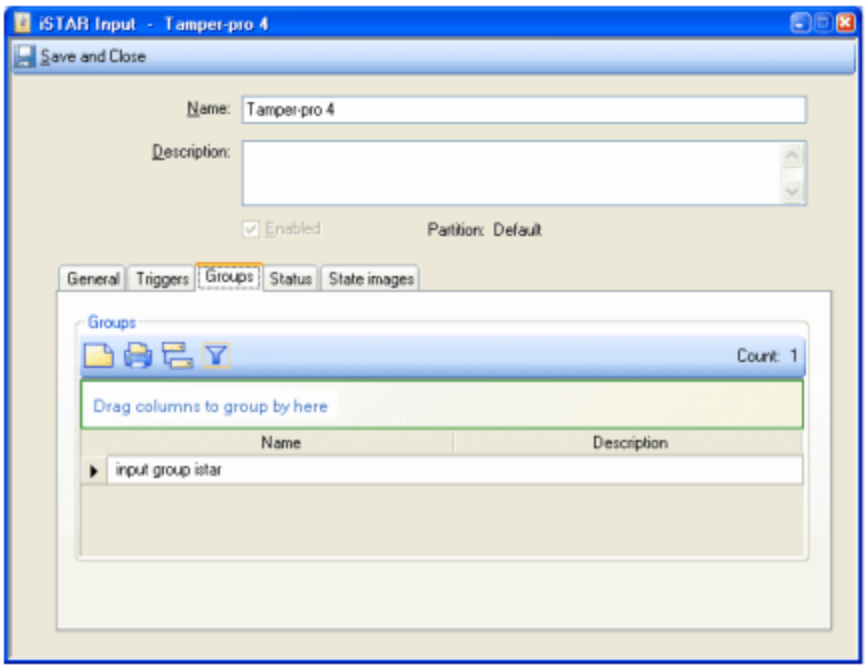
   If you drag an apC Controller to a different Hardware Folder, the apC and all its child objects are moved to that Hardware Folder.

Groups Tab for Hardware Devices

The Groups tab for a Hardware device lists all of the Groups to which the Hardware device currently being edited belongs. The Groups in the list are lists of Hardware devices of the same type (such as Inputs, Readers, and so on).

Figure 2 on Page 28 shows the Groups tab for an iSTAR Input, which is typical for a Hardware device.

Figure 2: Typical iSTAR Group Tab



Hardware Groups Tab Definitions on Page 29 provides definitions for the fields and buttons on an iSTAR Device Group tab.

Editing a Hardware Device Group

You can edit any of the Groups in the list on the Groups tab by double-clicking on the Group's name in the list of Groups.

Adding a Hardware Device to a Group

To add a Hardware device to a Group, you need to either:

- Edit the Group by opening the Configuration pane and using the Group Editor.

  or

- Display a list of devices of that type and use the context menu **Add to Group** selection. You cannot add the Hardware device to a Group from the Groups tab (the device is already a member of every Group that is listed here).

  See Add a Hardware Device to Group from a Dynamic View on Page 409 for more information.

Hardware Groups Tab Definitions

Table 2 on Page 29 provides definitions of the fields and buttons on the Groups tab for a Hardware pane device.

Table 2: Groups Tab Definitions

Field/Button	Icon	Description
Card View		Displays the list of Groups in Card View.
Print		Prints the list of 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. See the *C•CURE 9000 Data Views Guide* for more information about filtering a Dynamic View list.
Row Selector		Click to select a row in the table.
Count		This field displays the number of Groups in the list.
Name		This column lists the names of the Groups of which this device is a member.
Description		This column lists the descriptions of the Groups of which this device is a member.

Add a Hardware Device to Group from a Dynamic View

When you select a Hardware device from a Dynamic View and then right-click for the context menu, **Add to group** appears as a menu selection. This function enables you to add the object(s) to a Group. More more information about the Group function see Groups Tab for Hardware Devices on Page 28.

To Add a Hardware Device To a Group

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the Hardware pane.
2. Select a Hardware device from the Hardware pane drop-down list.
3. Click  to open a **Dynamic View** showing all objects of that type.
4. Right-click on the object that you want to add to a Group and select **Add To Group**. A list of Groups is displayed.
5. Select the Group from the list, and the object is added to that group.
6. Click **OK** to confirm your choice.

Refreshing the Hardware Tree

To make sure that all the folders and objects in the Hardware Tree are accurately displayed on the screen, you can Refresh the Hardware Tree.

To Refresh the Hardware Tree

1. Click the **Hardware** button in the Navigation Pane to open the Hardware Tree.
2. Right-click on **Hardware** and select **Refresh Tree** from the context menu. The Hardware Tree is updated.

Hardware Folders

You can create additional Hardware Folders if you need to organize the Controllers and access hardware into separate folders.

When you create a new Partition, a new Hardware Folder is automatically created to contain objects that reside in that Partition.

A Hardware Folder pane displays a tree structure that shows how you have configured the hardware on the C•CURE 9000 system. For example, the hardware tree shows you which readers, inputs, and outputs are configured for each controller.

You can use the Hardware Tree to navigate to hardware components you want to view or edit, or to create new hardware components, such as a reader you want to add to a controller.

The following topics provide more information about Hardware folders.

- Controllers and Dependent Objects on Page 31
- Creating a New Hardware Folder on Page 32
- Creating and Using a New Hardware Folder Template on Page 32
- Renaming a Hardware Folder on Page 33

Controllers and Dependent Objects

Dependent (child) objects that are managed under iSTAR and apC controllers include inputs, outputs, readers, boards, elevators, floors and doors. Controllers are parent objects to these and are created first. The parent objects are created within the company name folder in the hardware tree and must be created before the child objects in their respective classes, such as apC and iSTAR.

For iSTAR controllers, a cluster object encompasses a system of one or more iSTAR controllers, determining communications between individual controllers. To configure an iSTAR controller in the C• CURE 9000 system, you must first create a cluster. Each cluster is configured as either Non-encrypted (iSTAR Classic/Pro and Ultra) or Encrypted (iSTAR eX/Edge and Ultra) controllers. The cluster must have a controller that is the primary communication path to the host and may have an optional secondary communication path. The secondary communication path can be set to the same controller as the primary path.

In the instance of apC controllers, a communications port must be set up before these controllers and their dependent objects can be configured.

Elevators are similar to doors, but have many exit points which are determined by the floor objects. Floors are created independently but are added into the system through the selection of elevator buttons. Elevators also require readers, inputs, and outputs. The inputs are used to determine at which floor the cardholder exited and the outputs are used to control the elevator buttons.

NOTE Elevators (configured on iSTAR or apC controllers) have not been evaluated by UL.

Doors which are configured as part of an apC or iSTAR controller have properties that are unique to each controller, whereas a Door object is a base class that recognizes only those properties which are common to all controllers. Accordingly, door objects are created last because each door object requires the controller-specific dependent objects to

exist for the door. Doors typically require readers, inputs and outputs. The inputs are used for door state monitors and exit devices. The outputs are used for locks and automatic door openers.

Example:

C•CURE 9000 dependent object hierarchy examples:

- iSTAR Cluster>iSTAR Controller>Readers, Inputs, Outputs> iSTAR Doors
- apC Comm Port>apC Controller>Readers, Inputs, Outputs>apC Doors

Creating a New Hardware Folder

Perform the following steps to create a new Hardware Folder.

To Create a New Hardware Folder

1. Click the **Hardware** button in the Navigation Pane to open the Hardware Tree.
2. Right-click on **Hardware** in the tree and select **Hardware Folder>New** from the context menu. The Hardware Folder dialog box opens.
3. Type the name for the new folder into the **Name** field.
4. Optionally type a description for the new folder into the **Description** field.
5. Click **Save and Close** to save the new folder.
6. Right-click on **Hardware** and select **Refresh Tree** from the context menu. The Hardware Tree is updated to display the new folder.

Creating and Using a New Hardware Folder Template

You can create a Hardware Folder Template that you can use as a basis for creating additional Hardware Folders.

In a template, you can fill in field values that will have the same values for all Hardware Folders, and then use the template when you are creating new Hardware Folders.

To Create a New Hardware Folder Template

1. Click the **Hardware** button in the Navigation Pane to open the Hardware Tree.
2. Right-click on **Hardware** in the tree and select **Hardware Folder>New Template** from the context menu. The Hardware Folder dialog box opens.
3. Type the name for the new folder into the **Name** field.
4. Optionally type a description for the new folder into the **Description** field.
5. Click **Save and Close** to save the new folder template.

To Use a Hardware Folder Template to Create New Hardware Folders

1. Click the **Hardware** button in the Navigation Pane to open the Hardware Tree.

2. Right-click on **Hardware** in the tree and select **Hardware Folder** from the context menu. The next level menu appears listing the Hardware Folder Templates you have previously created under the *---- Templates* category.
3. Click on the name of the Hardware Folder Template you wish to use as the basis for the new Hardware Folder.
4. Type the name for the new folder into the **Name** field.
5. Optionally type a description for the new folder into the **Description** field.
6. Click **Save and Close** to save the new folder.
7. Right-click on **Hardware** and select **Refresh Tree** from the context menu. The Hardware Tree is updated to display the new folder.

Renaming a Hardware Folder

You can rename a Hardware Folder to customize it to your site's needs. Typically, you will want to rename the default folder, **Company Name**, with a more suitable name.

To Rename a Hardware Folder

1. Click the **Hardware** button in the Navigation Pane to open the Hardware Tree.
2. Right-click on the folder that you want to rename, and select **Edit** from the context menu. The Hardware Folder Editor dialog box opens.
3. Type the new name for the folder into the **Name** field.
4. Optionally type a description for the folder into the **Description** field.
5. Click **Save and Close** to save the renamed folder.

Templates

The C•CURE 9000 Hardware pane supports the concept of Templates for almost all objects in the Hardware Tree. A Template is a re-usable object you can create and configure with settings that you would like to use when creating other objects. For example, if all of the iSTAR Readers are the same reader type, using the same card format, you could create a Reader Template that contained those settings, and apply that Template to any iSTAR Reader object that you create, to make Reader configuration faster and more consistent. The Template objects you create do not appear in the Hardware Tree, but they are available to be applied when you create an object of the same type as the Template.

The following topics provide more information about using the Hardware Templates.

Creating a Template

To create a new Template for an object, it is necessary to create an instance of the parent object for the object so that the object type for the Template appears in the Hardware Tree. For example, to create a Template for the iSTAR eX Controller object type, you need to create an iSTAR Cluster that can contain iSTAR eX Controllers first, then create the iSTAR eX Controller Template.

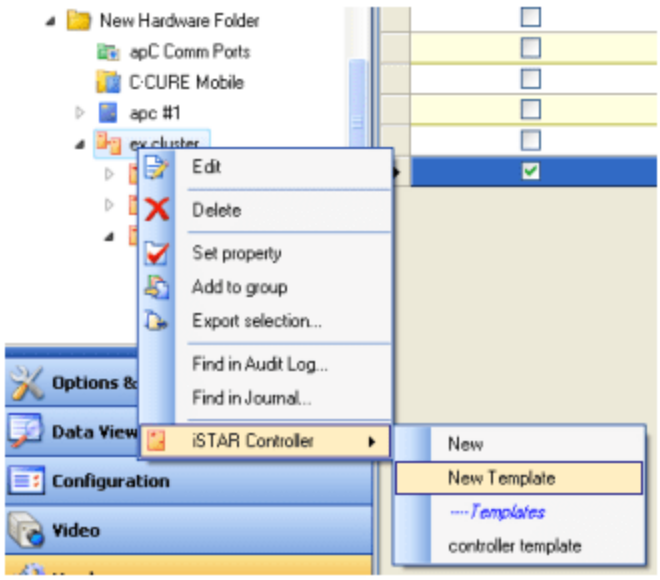
To Create a Template

1. In the Navigation pane of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Navigate to the Hardware folder that contains the object type for which you want to create a new Template.

   Example:

   If you want to create a Template for an iSTAR eX Controller, navigate to a folder that contains an iSTAR Cluster for iSTAR eX Controllers.
3. Select the parent object type (in this case, iSTAR Cluster) and right-click to display the context menu.
4. Select the object type for the Template from the context menu, then select **New Template**. See the example in Figure 3 on Page 35.

Figure 3: Creating a New Controller Template



5. The editor for the object opens the new Template.
6. Configure any settings you want to include in the Template.
7. To save the new Template, click **Save and Close**.

The new template appears under ---- *Templates* in that object type's context menu drop-down list in the Hardware tree. For example, in Figure 3 on Page 35, an iSTAR Controller Template named **controller template** appears in the context menu.

Editing a Template

If you have created a Template and need to make changes to it, you need to locate the Template to edit it. Because you cannot view Templates in the Hardware Tree, and most default Dynamic Views do not list Templates, you may need to create a new Dynamic View that shows the Templates you have created.

This section will use Inputs as an example, and show you how to create a Dynamic View that lists the Input Templates along with the Controller Inputs.

Note that you can create a Dynamic View that shows only apC Inputs or iSTAR Inputs by choosing that object type, or you can create a View that lists all Input (or Door or Reader) objects, then filter that view to show only the Inputs (or Doors or Readers) of a particular type.

To View Templates in a Dynamic View

1. Navigate to Data Views and choose **Dynamic View** from the Data Views drop-down list.
2. Click **New**. The Dynamic View editor opens.
3. Type a name for your Dynamic View in the **Name** field. Include 'with Templates' in the name of the Dynamic View so that you can find the view again easily.

Example:

Inputs Dynamic View (with Templates)

4. Type a description of the view in the **Description** field.
5. Click [...] in the **View Type** field. A dialog box appears listing the object types you can choose for your Dynamic View.
6. Click on 'Click here to filter data' and type the first letter of the name of the object type for which you wish to create a Dynamic View. The list of object types is filtered to show only the types that begin with that letter.

   Example:

   To create a list of Inputs, type 'i' then click on **Input**.
7. Click **Add** to add a column to the Dynamic View.
8. Click [...] in **Column Property**, then click **Name** to add the Name Property to display in the column.
9. Click **Add** to add a column to the Dynamic View.
10. Click [...] in **Column Property**, then click **Template** to add the Template Property to display in the column.
11. You can click **Add** again to add more columns as needed.
12. Click **Save and Close** to save the Dynamic View.
13. In the Data Views pane, click [▾] to display a list of your Dynamic Views.
14. Double-click on the Dynamic View you just created. When it appears, it will list all of the objects of the object type you specified, and the Template column identifies which objects are Templates.
15. Find the Template you wish to edit, and double-click it to open the editor to edit the Template.
16. When you have completed making changes to the Template, click **Save and Close** to save your changes.

Creating an Object from a Template

You can create objects such as Controllers, Doors, and Elevators from Templates.

To Create an Object from a Template

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Navigate to the Hardware folder that contains the parent object in which you want to create the new object from a Template.
3. Select the parent object and right-click to display the context menu.
4. Select the object type and click the Template you want to use from the context menu.

   Example:

   In Figure 3 on Page 35, you could select **controller template** to create an iSTAR Controller from a Template.
5. The Editor for the object opens so that you can edit the new object. The settings from your Template are already configured.
6. Configure any additional settings.

7. To save the new object, click **Save and Close**.

Using Templates for Controller Inputs, Outputs, and Readers

You can use Templates as the basis for objects that you create while configuring Controllers in C•CURE 9000. For example, if you are configuring an iSTAR Controller that has an I/8 board, you can create an Input template and use that template as the basis for one or more iSTAR Inputs on that I/8 board.

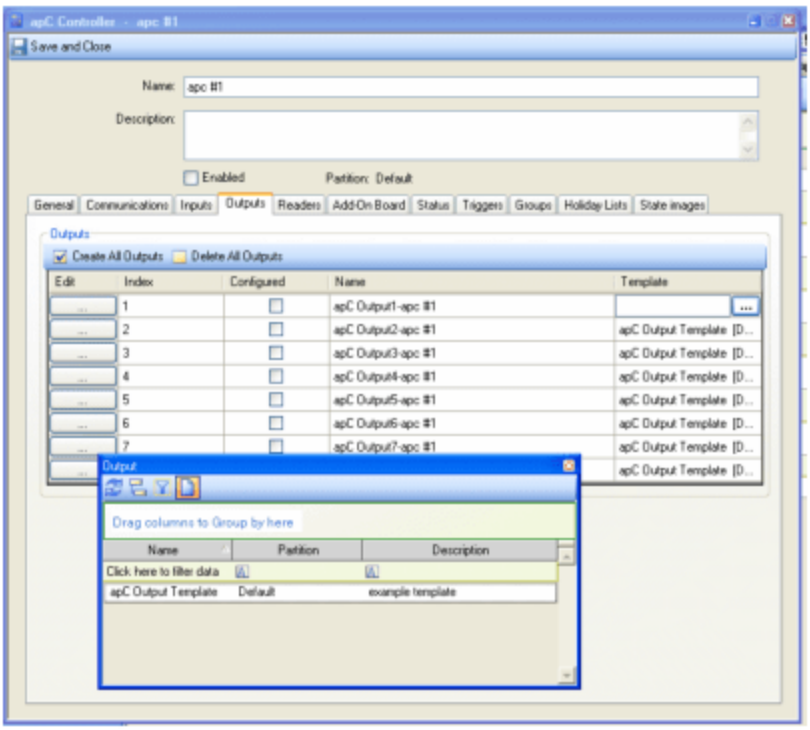
Typically, you create these objects from a tab within the Controller editor. The tab where you create such an object contains a table that includes a Template column for you to identify a Template to use as a basis for the objects you create.

Example:

The apC Controller editor has tabs for Inputs, Outputs, and Readers. On each of these tabs, there is a **Template** column that lets you select a Template to use for creating new objects.

Figure 4 on Page 37 shows an example of an apC Outputs tab with an apC Template selected in the **Template** column.

Figure 4: apC Outputs Template



By default, when you select a Template for one object in the list, the same Template is added as the basis for each object. You can use more than one Template by configuring the objects for which you want to use one Template, then choosing one or more different Templates for the remaining objects.

To Use Templates for Controller Inputs, Outputs, or Readers

1. From the Hardware pane, open the Controller Editor for the Controller you want to configure.

2. Click the tab in the Controller Editor for the objects you want to configure.

   Example:

   In the apC Editor, click the Outputs tab to configure Outputs on this apC.

3. To specify a Template for an object you want to configure, click in the **Template** column of an object that is not yet configured (**Configured** column value is ☐).
4. Click ... to select a Template. A dialog box opens listing the available Templates. See Figure 4 on Page 37 for an example.
5. Click on a Template in the list to select it. That Template is added to every object in the table that is not already configured.
6. Select the Configured column ☑ for each object you want to configure with the selected Template.
7. If you want to select a different Template for any of the remaining objects in the table that you have not yet configured (Configured column value is ☐):
   a. Click in the **Template** column of that object, then click ... to select a Template. A dialog box opens listing the available Templates.
   b. Click on a Template in the list to select it. That Template is added to every object in the table that is not already configured.
   c. Select the **Configured** column ☑ for each object you want to configure with the selected Template.
8. Repeat Step 7 for any additional objects for which you want to choose a different Template.
9. To edit any of the objects, click ... in the **Edit** column for that object. The editor for that object opens. The fields that were configured in the Template are already configured in the object you are editing.
10. When you have completed configuring an object from the Template, click **Save and Close** in the object editor to save the object.
11. Click **Save and Close** in the Controller editor to save the your changes to the Controller.

Deleting a Template

You can delete a template that you have created by using the right-click context menu in a Dynamic View.

To Delete a Template

1. In the Navigation pane, select the type of object you want to delete from the drop-down list. (For example, in the Hardware pane, choose apC Comm Port from the drop-down list.)
2. Click the Search pane.
3. Select the **Template** check box
4. Click ... to display a list of the objects that includes the Templates you have defined.
5. Select the Template(s) from the list that you wish to delete.
6. Right-click on a selected Template to bring up the context menu for the object.
7. Select **Delete** from the menu to delete the Template.

Viewing a List of Templates

You can include Templates in a list of objects of a type.

Typically the Dynamic View for an object type does not include Template objects. You can use the Template check box to cause the Dynamic View to list all the Templates you have created.

To View a List of Templates

1. In the Navigation pane, select the type of object you wish to view from the drop-down list. (For example, in the Hardware pane, choose apC Comm Port from the drop-down list.)
2. Click the Search pane.
3. Select the **Template** check box
4. Click ... to display a list of the objects that includes the Templates you have defined.

Copying, Pasting, and Renaming Clusters and Controllers

The C•CURE 9000 supports the ability to duplicate an existing configured iSTAR Cluster with all of its included Security Objects - Controllers, Boards, Inputs, Outputs, Readers, Doors, Elevators, Triggers (plus associated Events).

- The **Copy & Paste** context menu selection can be used to make a duplicate of a Cluster and its Child Objects on the same partition on the same system.
- The **Copy To** context menu selection can be used to make a duplicate of a Cluster and its Child Objects on a different partition on the same system, using Paste From.
- With a flash drive or other portable memory device or shared drive, the **Copy To** and **Paste From** context menu selections can be used to duplicate the Cluster and Children on another system.
- The **Rename** context menu selection is used to give these duplicated Objects new names.
- If you are extensively using the **Copy & Paste** and **Rename** features, it is good practice to establish a naming convention for the site and then rename based on that convention.

Example:

Create the new Clusters and Controllers with -Bldg appended to all of the objects. While Copying and Pasting you can use **Search and Replace** to change **-BLDG-Copy-datetime** to **-BLDG-A**. See Using Search and Replace on Page 43.

NOTE The Export and Import of Clusters does not include all the doors, elevators and events (configured via triggers). **Copy & Paste** includes all of those objects.

When an iSTAR Cluster is selected and **Copy & Paste** is used, the following objects that belong to that cluster are copied and pasted:

- All configured Controllers plus the following components of each Controller:
  - Boards (all the boards including GCM, ACMs, Aperio Hubs or Schlage PIMs, etc.)
  - Inputs (including I/8s, I/8-CSIs)
  - Outputs (including R/8s)
  - Readers (all types)
  - Doors
  - Elevators
  - Triggers, including their associated Events and actions

When an iSTAR Controller is selected and **Copy & Paste** is used, the following objects that belong to that Controller are copied and pasted:

- Boards (all the boards including GCM, ACMs, Aperio Hubs or Schlage PIMs, etc.)
- Inputs (including I/8s, I/8-CSIs)
- Outputs (including R/8s)
- Readers (all types)
- Doors
- Elevators
- Triggers, including their associated Events and actions

Privileges

To use the **Copy & Paste**, **Copy To**, **Copy From** and **Rename** features, you must be an Administrator or an operator that has a Privilege with those Permissions granted for **iSTAR Controller** and **iSTAR Cluster**.

The **iSTAR Controller** and **iSTAR Cluster** Privilege Permission features are located in the **Privileges** dialog box **Defaults** tab. Click on the **Hardware>Controllers>iSTAR**. Locate the **iSTAR Controller** and **iSTAR Cluster** for the Permissions for the Privilege.

See the *C•CURE 9000 Software Configuration Guide* 'Privileges' chapter for more information.

Important Copy and Paste Process Information

- All the child objects that are copied and pasted follow the same naming convention (i.e., **Copy [date-time]** will be appended to their original names.)
- If copying and pasting on the same system, the objects are pasted in the same partition as the source objects. If you are pasting on another system, the pasted objects will have the same partition as the object or folder on which user right-clicked and selected **Paste From**.
- All the export files are .xml files.
- During import, the secondary objects must exist on the destination system. If not, then the import of object that refers to secondary object will be aborted. For example, Event A is configured to activate Event B. Here Event B is the secondary object and it must already exist otherwise the import will be aborted.
- **Copy & Paste** copies all triggers assigned to the object, including the events and event actions, but not all of the event action targets, such as a sound object.
- When copying a panel which has panel events associated with it, the panel events are copied but not assigned to the panel. The panel must be assigned manually after the copy is complete and host events must be reconfigured.

Copy & Paste Tasks

When you copy a Controller, or a Controller in a Cluster, the MAC address is also copied. The copied Controller MAC address must be changed to a unique MAC address before the unit can be enabled.

You can perform the following tasks using **Copy & Paste**:

- Copying and Pasting on the Same System on Page 41
- Copying to a Mapped Drive or Another System Using a Flash Drive on Page 45
- Copying and Pasting from Partition to Partition on Page 49

NOTE The same procedures can be used to copy and paste individual Controller configurations.

Copying and Pasting on the Same System

The following procedure is used to create a copy of the following:

- A Cluster, plus all the objects within that Cluster with the same names as the existing ones with **-Copy [date-time]** appended to their names.
- A Controller with **-Copy [date-time]** appended to its name, plus all the objects within that Controller.

Example:

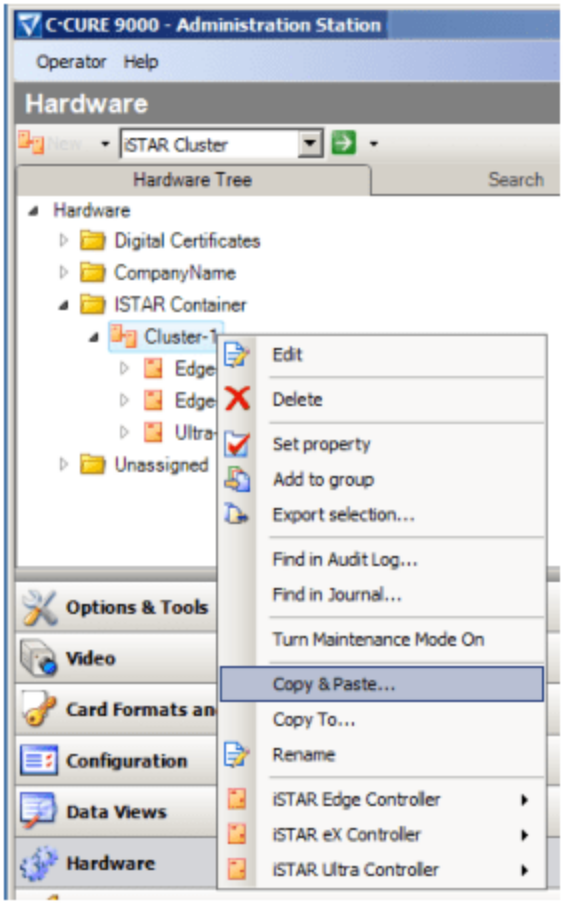
For a Cluster named Cluster5, the new cluster's name will be Cluster5-Copy [date-time], and if the Cluster has a Controller named Controller7, the new name will be Controller7-Copy [date-time].

For a Controller named Controller6, the new name will be Controller6-Copy [date-time].

To Create a Copy of an Existing Cluster or Controller on the Same System

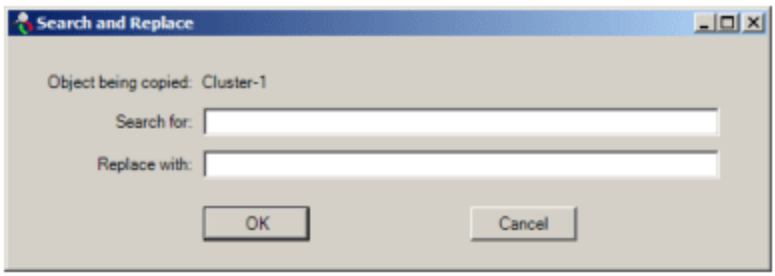
1. Right-click on an existing Cluster, or Controller, in the Hardware tree and select **Copy & Paste** from the context menu. Figure 5 on Page 42 shows selecting to copy and paste a Cluster.

Figure 5: Copy & Paste Context Menu Selection



The **Search and Replace** dialog box, as shown in Figure 6 on Page 43, appears.

Figure 6: Search and Replace Dialog Box



Using Search and Replace

Prior to the paste operation, the system provides the ability to replace a particular string in the names of objects being copied in the objects being pasted. Normally, the pasted objects will have the string **-Copy [date-time]** appended to the names. The **Search and Replace** dialog box allows you to replace the name.

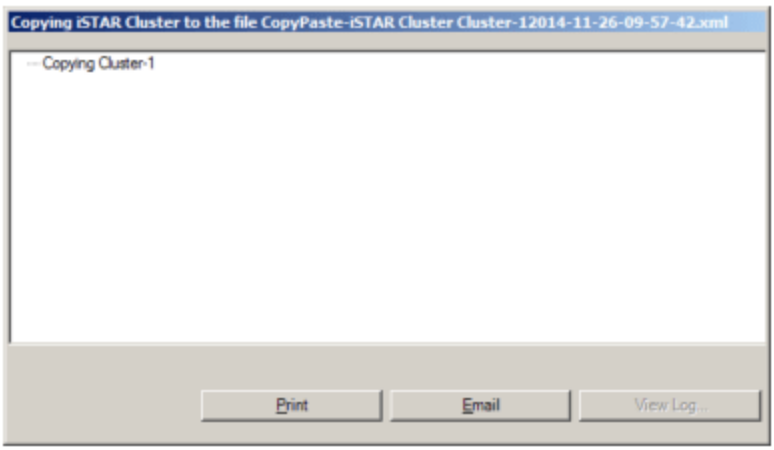
- Any string can be entered in the **Search for** field, and the string that it will replace in the **Replace with** field.
- Objects in conflict will have **-Copy [date-time]** appended to their names
- Partial matches are considered. For example, if **Door** is entered in the search field and **Dr** in the replace field with an object named **FrontDoorReader** then it is renamed as **FrontDrReader**. Selecting the **Cancel** button will abort the Paste operation.
- If both the **Search for** and **Replace with** fields are left blank, the object names are appended with **-Copy [date-time]**.
- Both **Search for** and **Replace with** fields must have a string entered or both fields must be blank. Leaving one field blank is not allowed by the C•CURE 9000 software.

NOTE If the **Copy & Paste** operation is stopped before it completes, the entire operation is canceled.

2. Click **OK**. If you selected to search and replace, the system searches for the string and performs the replace while copying the Cluster or Controller.

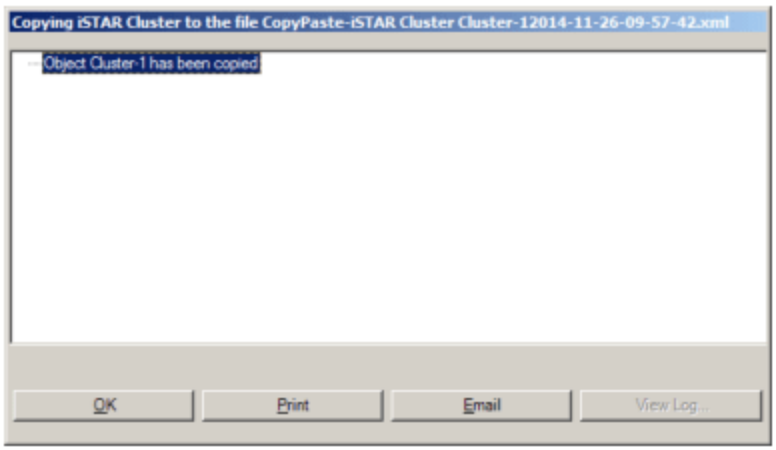
   The **Copying Status** Window, shown in Figure 7 on Page 44, appears. The time required depends on the complexity of the Cluster or Controller. The time is 10 to 60 seconds for most Clusters.

Figure 7: Copying Status Window



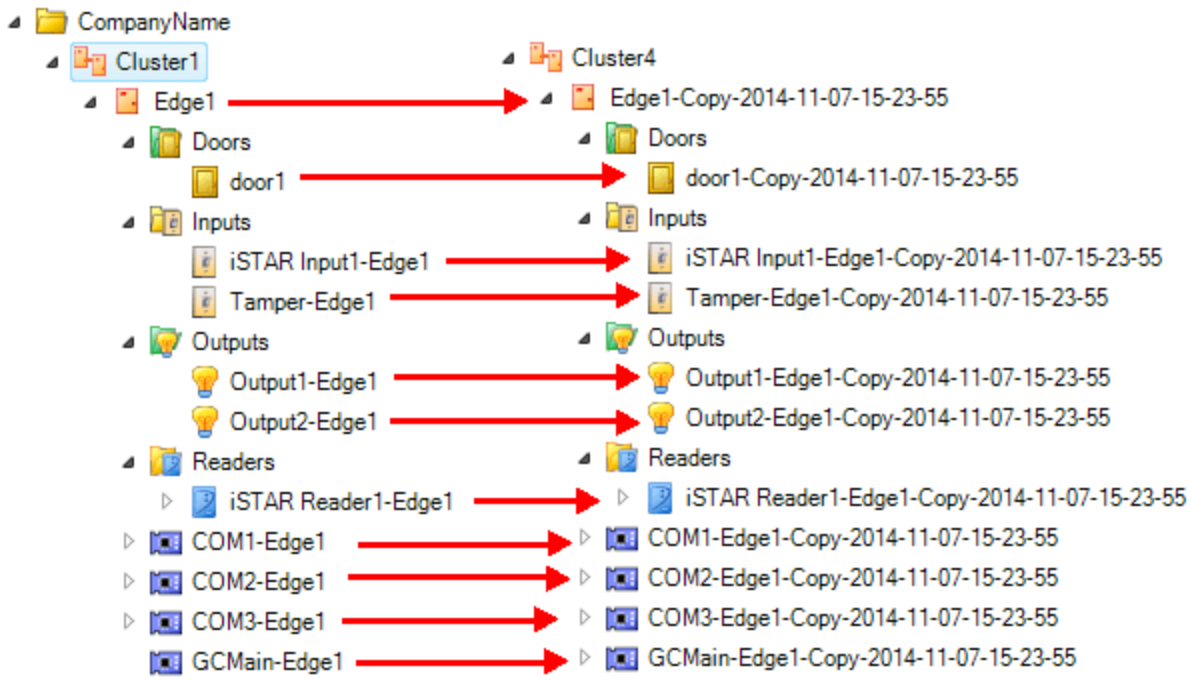
3. Click **OK** when the object is displayed as copied, as shown in Copying Status Window on Page 44.

Figure 8: Copying Status Window - Complete



When the copy is complete, shown side-by-side in Figure 9 on Page 45, all Readers, Inputs, Outputs, Doors, etc. have **-Copy [date-time]** appended to their names.

Figure 9: Hardware Tree - Copy Complete

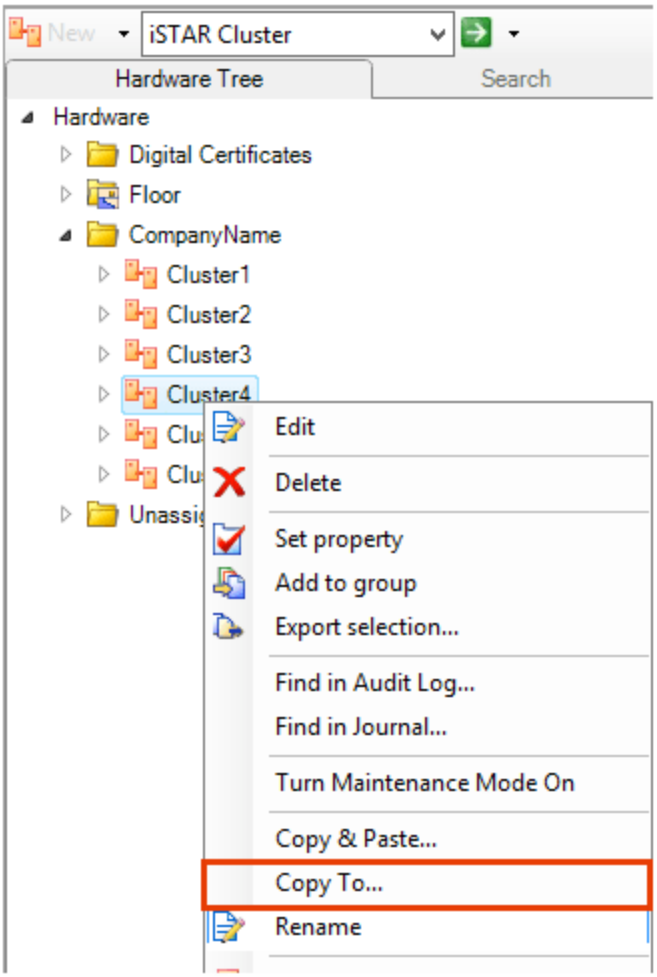


Copying to a Mapped Drive or Another System Using a Flash Drive

To Copy a Cluster or a Controller to a Mapped Drive or Another System

1. Right-click on the Cluster and select **Copy to**.

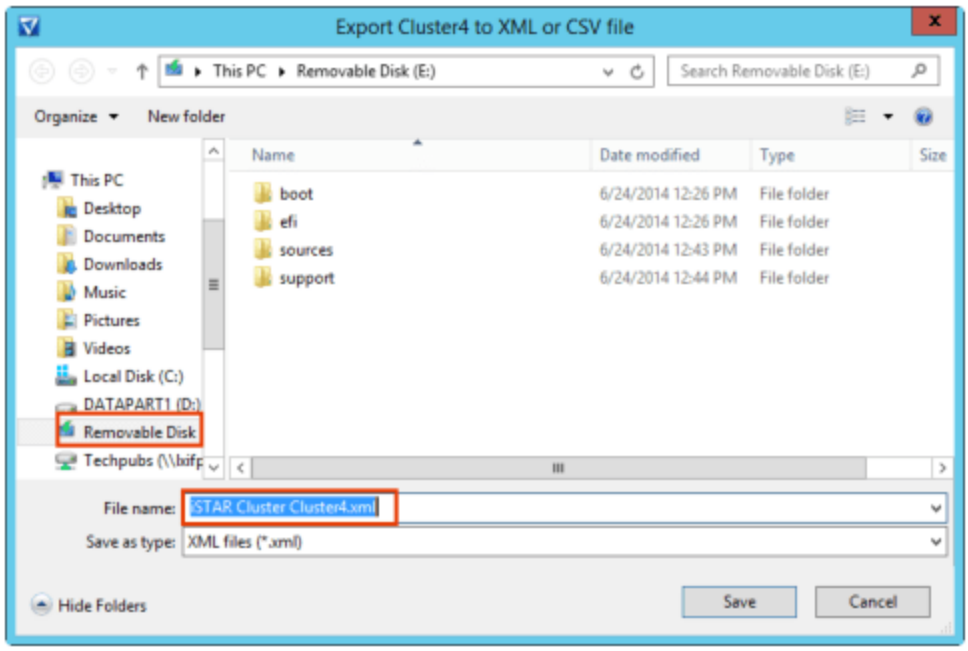
Figure 10: Copy To Menu Selection



The Export Window, shown in Figure 11 on Page 47, opens.

2. Select the Flash Drive (or the mapped drive), and edit the **File name** if desired.

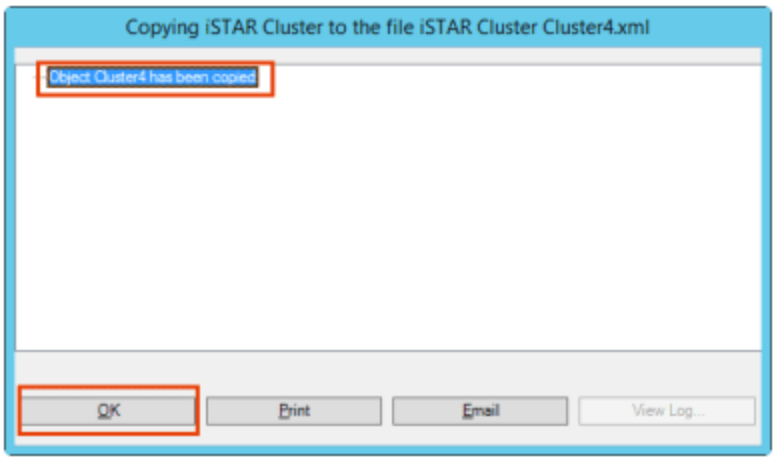
Figure 11: Copy to Flash Drive



3. Click **Save**.

   The **Copy To Status** Window, shown in Figure 12 on Page 47, appears.

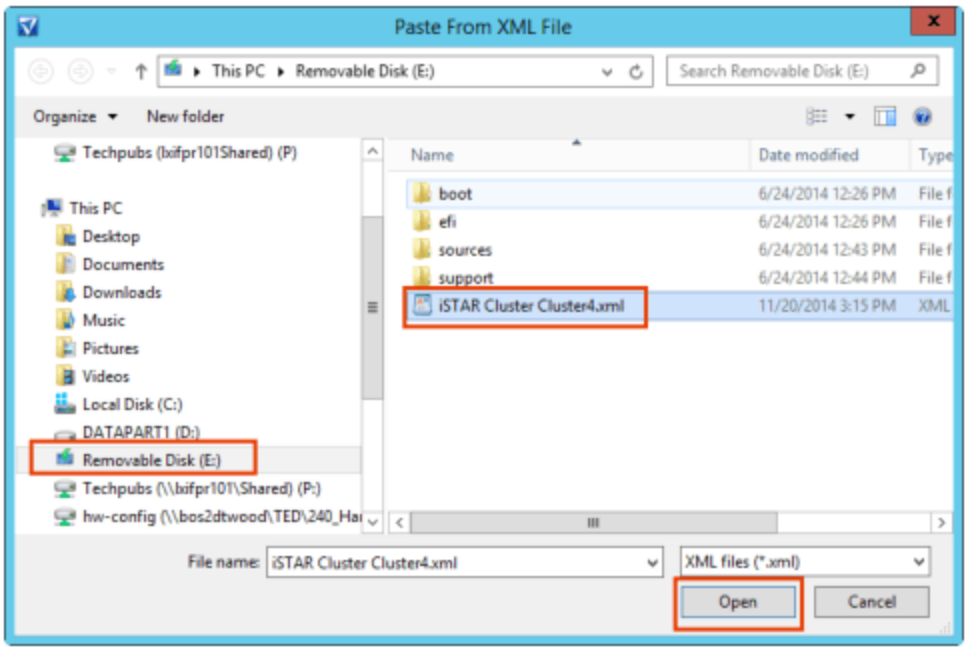
Figure 12: Copy To Status Window



4. Click **OK** when the object is displayed as copied.
5. Insert the Flash drive into the system where you want to copy the objects. Or, browse to the mapped drive on the system.

   In this example, a **simulated** hardware folder is representing the other system.
6. Right-click on the target folder in the new system's **Hardware** tree and select **iSTAR Cluster>Paste From**.
7. Select the Flash Drive (or the mapped drive), the **.xml** file, and click **Open** as shown in Figure 13 on Page 48Figure 13 on Page 48

Figure 13: Paste From Window

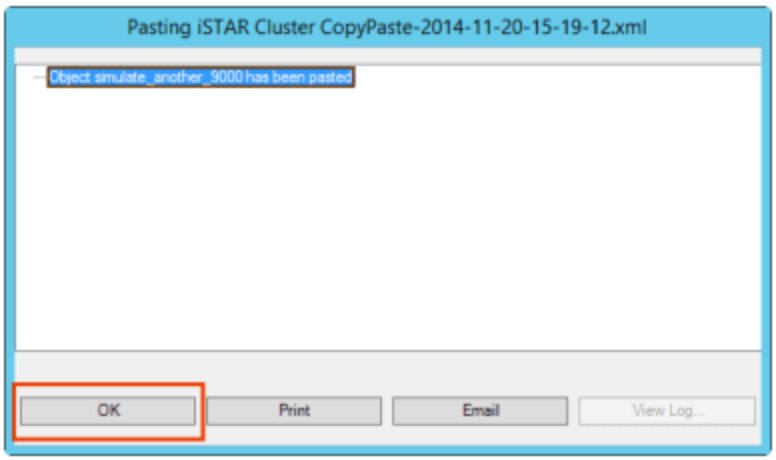


The **Search and Replace** dialog box appears. For information about Search and Replace, see Using Search and Replace on Page 43

8. Click **OK** in the **Search and Replace** dialog box. If you selected to search and replace, the system searches for the string and performs the replace while copying the objects.

   The **Pasting Status** Window, shown in Figure 14 on Page 48, appears.

Figure 14: Pasting Status Window



9. Click **OK** in the Pasting Status Window when the object is displayed as pasted.

   The copied Cluster appears under the simulated folder in the **Hardware** tree on the system.

Copying and Pasting from Partition to Partition

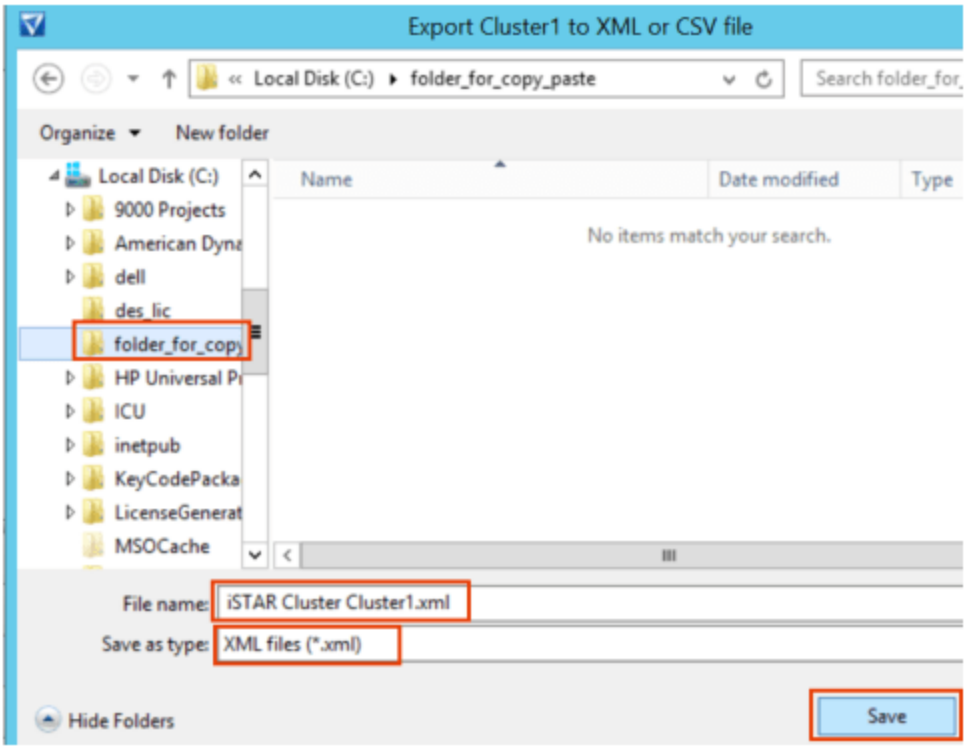
To Copy and Paste for a Partition to a Partition

1. Right-click on the Cluster or Controller and select **Copy To**.

   The **Export** Window appears.

2. Select a folder on the system to save the .xml file, and click **Save**, as shown in Figure 15 on Page 49.

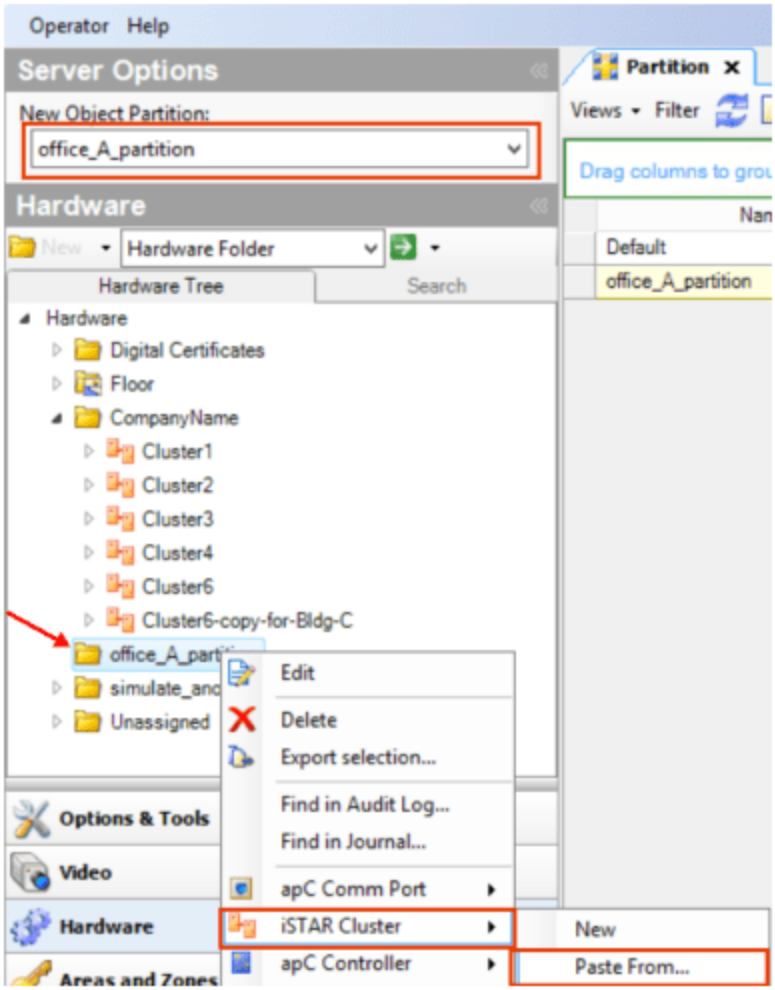
Figure 15: Export Window



3. Select the other partition where you want to copy the object.

4. Right-click on the **Hardware** folder in the partition and select **iSTAR Cluster>Paste from**, as shown in Figure 16 on Page 50Figure 16 on Page 50

Figure 16: Partition Selection



The **Paste From** Window appears.

5. Browse to the .xml file you saved on the system.
6. Select the .xml file and click **Open**.

   The **Search and Replace** dialog box appears. For information about **Search and Replace**, see Using Search and Replace on Page 43
7. Click **OK** in the **Search and Replace** dialog box. If you selected to search and replace, the system searches for the string and performs the replace while copying the objects.

   The Pasting Status Window appears.
8. Click **OK** in the **Pasting Status** Window when the object is displayed as pasted.

   The copied object appears in the Partition.

Renaming Clusters and Controllers

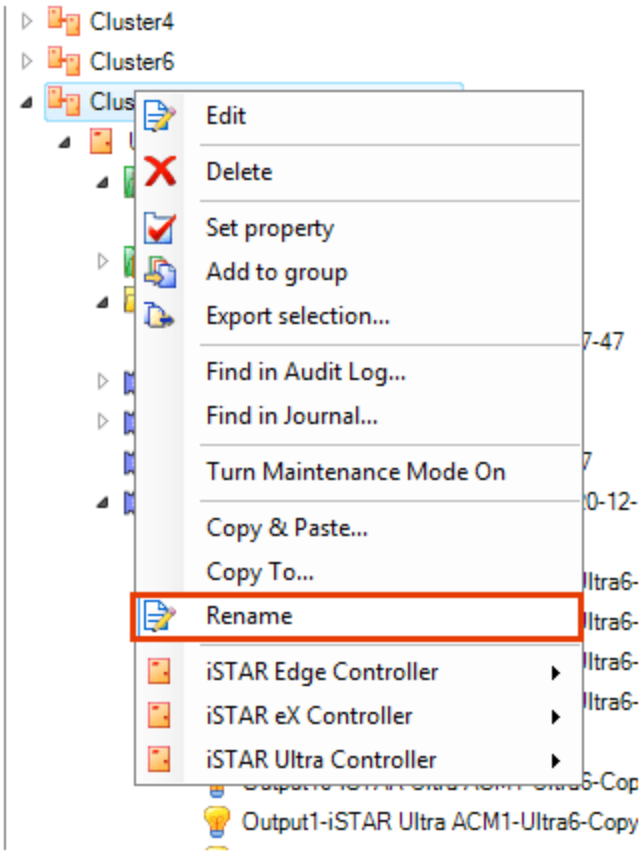
If you did not use the **Search and Replace** option in the **Copy & Paste** procedure, you can use the **Rename** selection on the Context menu.

The following procedure renames **-Copy [date-time]** that was appended to the end of a Cluster and its objects during **Copy & Paste** to **-Bldg-C**.

To Rename Clusters and Controllers

1. Right-click on the object and select **Rename**, as shown in Figure 1 on Page 51.

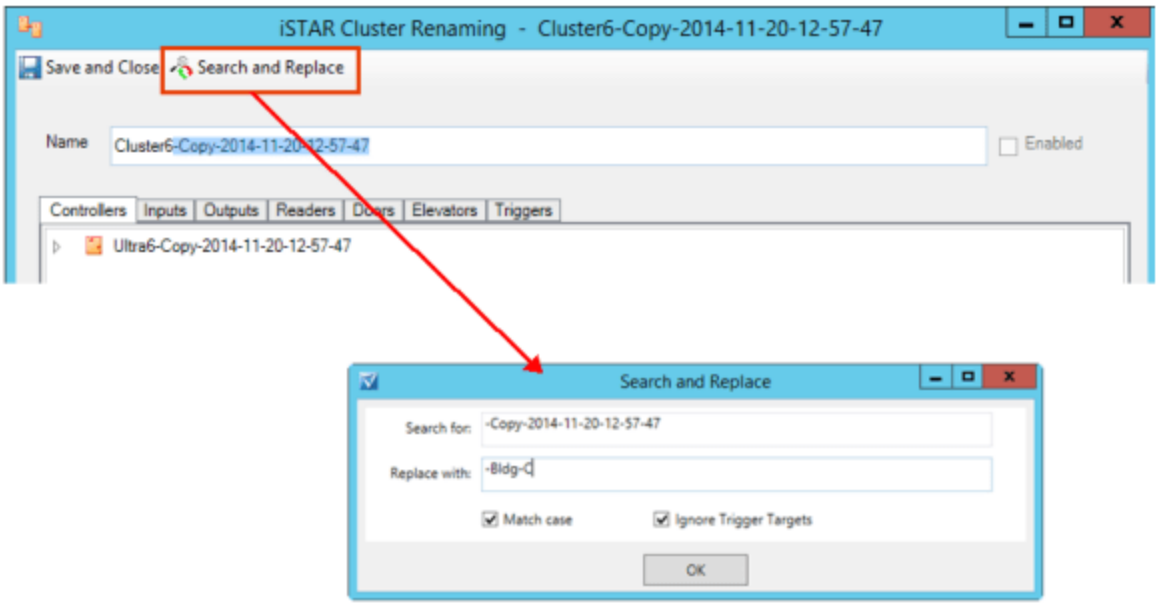
Figure 1: Rename Cluster



The **Renaming** dialog box appears.

2. Click **Search and Replace** to open the **Search and Replace** dialog box, as shown in Figure 2 on Page 52.

Figure 2: Cluster Renaming



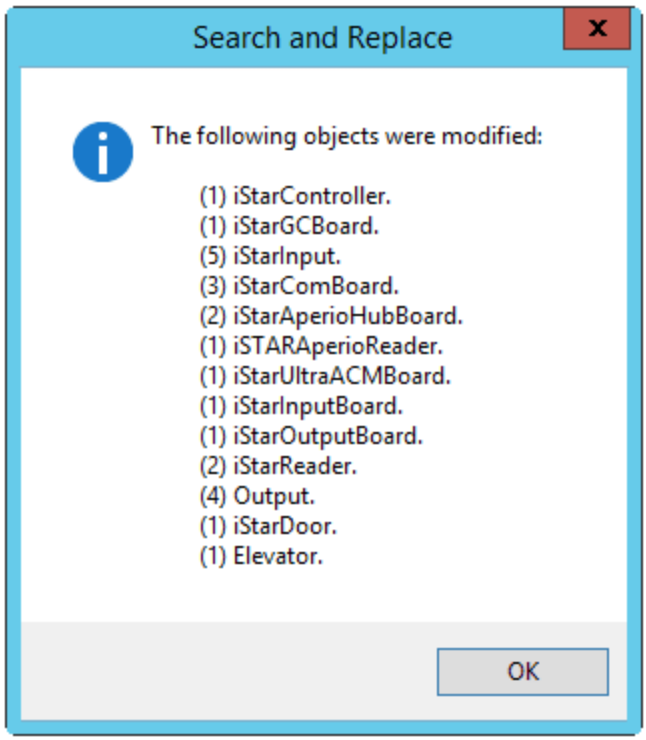
3. Enter the new name in the **Replace with** field (in this example it's **-Bldg-C**).
4. Optional selections
   - Click on the **Match case** check box to match the case entered.
   - Click in the **Ignore Trigger Targets** check box to ignore Trigger target events.

Use caution if renaming original Events. The Events may be linked to other objects. Use the **Show Association** feature to determine if they are. See the *C•CURE 9000 Getting Started Guide* for information about using Show Association.

5. Click **OK**.

   An informational dialog box appears displaying all the objects that were modified with the new name.

Figure 3: Rename Results



6. Click **OK**.
7. Verify that the rename changes are complete. Click on the tabs in Renaming dialog box.

NOTE Because **Ignore Trigger Targets** was selected in the **Search and Replace** dialog box, the original Trigger Target Events were not renamed, but another copy of the Events exist with the **-Copy [date-time]** appended to the end.

Rename Results

The next series of graphics illustrate the effect of the Rename operation.

Figure 4: Controller Tab and Input Tab

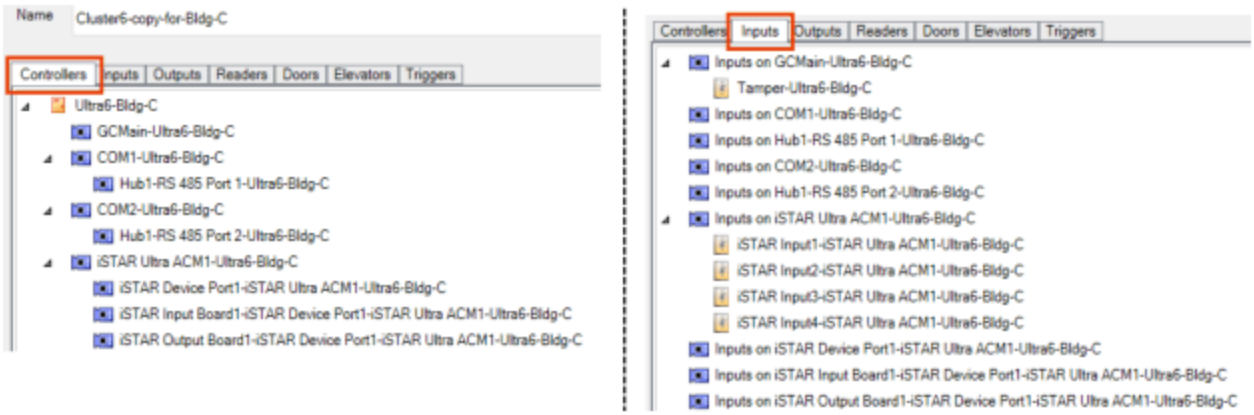


Figure 5: Outputs Tab and Readers Tab

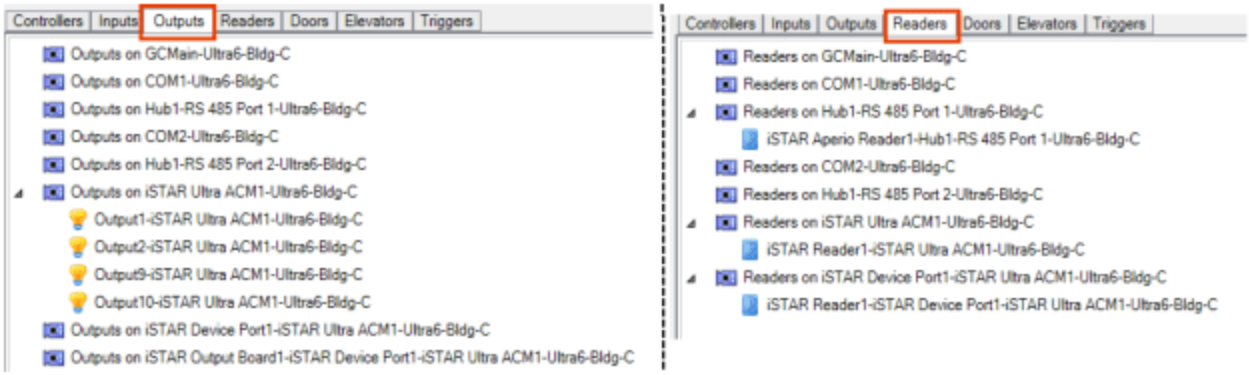


Figure 6: Doors Tab and Elevators Tab

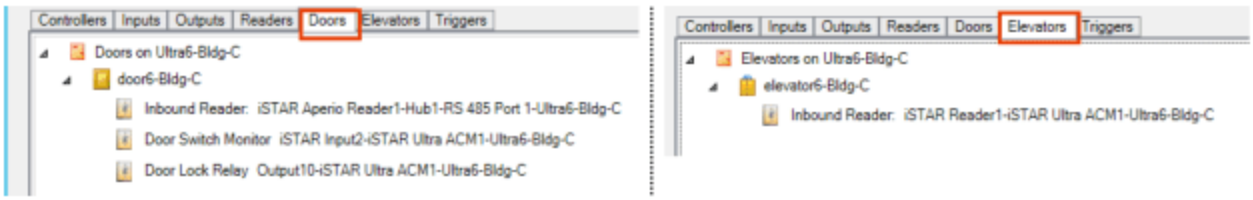


Figure 7: Triggers Tab

Trigger Target Events

Notice that the original Trigger Target Events were not renamed, but another copy of the Events exists with the [**-Copy-date-time**] stamp. The date-time stamped ones can be further renamed and used as desired.

Use caution if renaming original Events. The Events may be linked to other objects. Use the **Show Association** feature to determine if they are. See the *C•CURE 9000 Getting Started Guide* for information about using Show Association.

Figure 8: Trigger Targets

Battery Low Journal Trigger Event	The default Battery Low Journal Trigger event	Inactive	Armed
Intrusion Zone Error Journal Trigger Event	The default Intrusion Zone Error Journal Trigger event	Inactive	Armed
Tamper		Inactive	Armed
Door_Held		Inactive	Armed
Door_forced		Inactive	Armed
controller_inactive		Inactive	Armed
controller_inactive-Copy-2014-11-20-12-57-47		Inactive	Armed
Door_forced-Copy-2014-11-20-12-57-47		Inactive	Armed
Door_Held-Copy-2014-11-20-12-57-47		Inactive	Armed

2

Maintenance Mode

This chapter describes how to configure and use Maintenance Mode.

In this chapter:

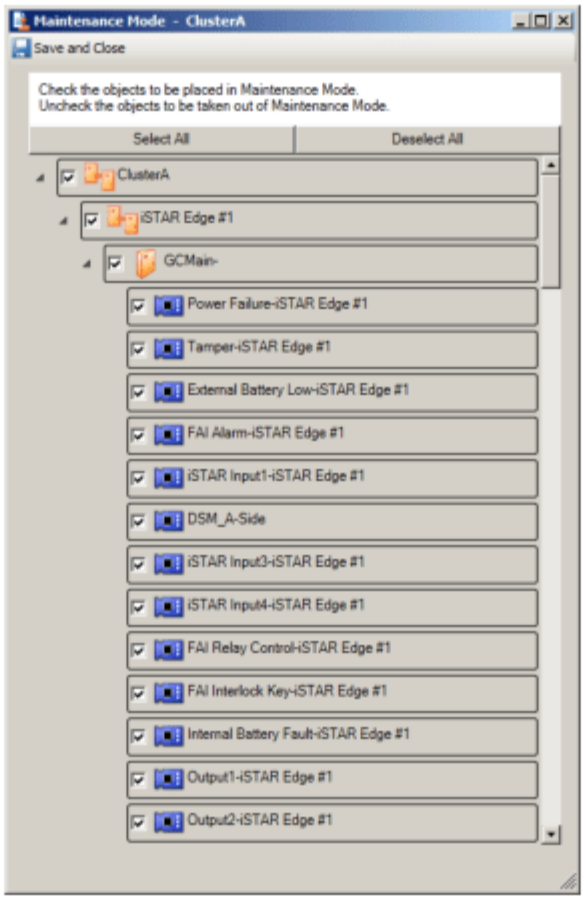
Maintenance Mode Dialog Box

The Maintenance Mode dialog box, shown in Figure 1 on Page 58, opens when Maintenance Mode is selected or deselected.

See the following for more information:

- Maintenance Mode Overview on Page 59
- Maintenance Mode Objects Supported on Page 60
- Maintenance Mode Configuration Tasks on Page 61

Figure 1: Maintenance Mode Dialog Box (Cluster)



Maintenance Mode Overview

Maintenance Mode is used to limit information about an object displayed on the Monitoring Station. Maintenance Mode only affects what is reported at the Monitoring Station.

Some examples for using Maintenance Mode:

- To Not display information about:
  - Parts of the system being installed by an integrator
  - Hardware being serviced, requiring maintenance, or being tested.
- To only monitor information about hardware being serviced, requiring maintenance, or being tested.
- To view information about all objects, including those tagged Maintenance Mode.

Placing an object into Maintenance Mode does not prevent actions from occurring. For example, if an event assigned to an intrusion zone in Maintenance Mode activates an output that turns on the building-wide evacuation alarm, the activation of the output will still occur.

Arming and disarming of inputs and events do not affect what is reported when the object is activated. In other words, arming of an event by an event assigned to a Maintenance Mode intrusion zone will be reported as activity.

Maintenance Mode is only reported in Journal messages when an object is tagged Maintenance Mode. When the object is taken out of Maintenance Mode it is not reported in a Journal message.

Operator Privilege and Application Layout Filtering assignments determine whether or not an object in Maintenance Mode is viewable as being in Maintenance Mode on the Monitoring Station. Only Monitoring Station operators with the correct privilege and Application Layout Filtering can view objects in Maintenance Mode.

See the following for more information:

- Maintenance Mode Objects Supported on Page 60
- Maintenance Mode Configuration Tasks on Page 61

Maintenance Mode Objects Supported

The following objects are supported in Maintenance Mode:

- apC Comm Ports
- apC Controllers
- apC Add-On Boards
- apC I32 Input Boards
- apC I8 Input Boards
- apC R48 Output Boards
- apC R8 Output Boards
- apC Inputs
- apC Readers
- apC Doors
- Areas
- C-CURE Mobile
- Elevators
- Events
- Floors
- Intrusion Zones
- Keypad Commands
- iSTAR Clusters
- iSTAR Controllers
- iSTAR Doors
- iSTAR Inputs
- iSTAR Readers
- iSTAR Aperio Hub
- iSTAR Aperio Readers
- iSTAR Aperio Doors
- iSTAR Comm Ports
- iSTAR PIM-485 Readers
- iSTAR Schlage Readers
- iSTAR Schlage Doors
- iSTAR Device Ports
- iSTAR ACM Boards
- iSTAR GCM Boards
- iSTAR Input Boards
- iSTAR Output Boards
- iSTAR Ultra ACMs
- Outputs
- Star Coupler Ministar
- Star Coupler Star
- Star Coupler WPSC

Maintenance Mode Configuration Tasks

Operator privileges and application layout assignments must be configured to use, view, or filter objects in maintenance mode.

The following tasks are described:

Configuring Privileges to Turn Maintenance Mode On and Off

Only operators who have the **Turn Maintenance Mode On** and/or **Turn Maintenance Mode Off** privilege assigned to them can put an object into Maintenance Mode and take an object out of Maintenance Mode.

The following procedure describes how to configure the privilege to include Maintenance Mode.

To Configure the Privilege

1. Click the **Configuration** pane.
2. Select **Privilege** from the **Configuration** drop-down menu to open the Privileges dialog box.
3. Click the **Defaults** tab.
4. Under **Classes**, click an object to view the permissions for that object.
5. Scroll down to locate **Turn Maintenance Mode On** and **Turn Maintenance Mode Off.**
6. Click in the **Grant** column next to **Turn Maintenance Mode On** and/or **Turn Maintenance Mode Off** to enable the permission(s) for this Privilege configuration.
7. See the *C•CURE 9000 Software Configuration Guide* for complete Privilege configuration information.
8. Click **Save and Close** when done with the configuration.

Configuring the Application Layout for Maintenance Mode Filtering

Application layouts can be configured to allow operators to filter objects in Maintenance Mode in the Monitoring Station and the Administration application Dynamic Views.

The following procedure describes how to configure the application layout to allow Maintenance Mode filtering. The Operator must have the correct privileges to use filtering. See Configuring Privileges to Turn Maintenance Mode On and Off on Page 61.

See the *C•CURE 9000 Data Views Guide* for more information about configuring the application layout.

To Configure Maintenance Mode Filtering in the Application Layout

1. Click the **Data Views** pane.
2. Select **Application Layout** from the **Data Views** drop-down menu.
3. Edit or add an Application Layout.
4. Click the **Filtering** tab.
5. See the *C•CURE 9000 Data Views Guide* "Application Layout chapter" for information about the Filtering tab fields.
6. Click **Save and Close** when done with the configuration.

Turning Maintenance Mode On and Off

NOTE To use Maintenance Mode, operators must have the correct privilege permissions assigned to them. See Configuring Privileges to Turn Maintenance Mode On and Off on Page 61

There are several ways to turn Maintenance Mode on and off:

- Right-click on an object in the object tree and select **Turn Maintenance Mode On** or **Turn Maintenance Mode Off**.
- Right-click on an object in the Dynamic View and select **Turn Maintenance Mode On** or **Turn Maintenance Mode Off**.
- Click in the Maintenance Mode column check box in the Dynamic View.

- Open the object editor and select the **Maintenance Mode** check box. Deselect the check box to turn it off.

iSTAR Cluster

To Put a Cluster Into Maintenance Mode

1. Click the **Hardware** pane.
2. Locate the Cluster in the Hardware tree, or in the Dynamic View.
3. Right-click on the Cluster name and select **Turn Maintenance Mode On** to open the Maintenance Mode dialog box.
4. The Maintenance Mode dialog box opens with the Cluster and all of its components/objects selected.
5. Click **Save and Close**.

To Take a Cluster Out of Maintenance Mode

1. Click the **Hardware** pane.
2. In the **Hardware** tree, or in the Dynamic View, right-click on the Cluster and select **Turn Maintenance Mode Off** to open the Maintenance Mode dialog box.
3. Click **Deselect All**.
4. Click **Save and Close**.

To Add an iSTAR to a Cluster in Maintenance Mode

1. Right-click on the Cluster name and select **Turn Maintenance Mode Off** to open the Maintenance Mode dialog box.
2. Select the check box next to the iSTAR name.
3. Click **Save and Close**.

iSTAR Controller or apC Controller

To Put iSTAR or apC Components/Objects into Maintenance Mode

1. Click the **Hardware** pane.
2. Locate the controller in the Hardware tree or in the Dynamic View.
3. Right-click on the iSTAR or apC, controller and select **Turn Maintenance Mode On** to open the Maintenance Mode dialog box.
4. Click the iSTAR or apC, controller name, or click **Select All** to select all components and objects belonging to the controller. Or, click on the separate components and/objects that you want to put into Maintenance Mode.
5. Click **Save and Close**.

Taking an iSTAR or apC Controller Out of Maintenance Mode.

To Take an iSTAR or apC Components/Objects Out of Maintenance Mode

1. Click the **Hardware** pane.
2. In the **Hardware** tree, click on the Cluster where the iSTAR, or apC, controller belongs.
3. Right-click on the controller and select **Turn Maintenance Mode Off** to open the Maintenance Mode dialog box.
4. Deselect the controller, components and/or objects.
5. Click **Save and Close**.

Putting Objects (Doors, Readers, Events, Elevators, etc.) into Maintenance Mode

To Put Objects into Maintenance Mode

1. Click the **Hardware** pane.
2. Locate the object, right-click on it and select **Turn Maintenance Mode On**.

   To turn off Maintenance Mode, right-click on the object and select **Turn Maintenance Mode Off**.

Viewing Maintenance Mode Objects in the Dynamic View

The Dynamic View can be customized to display objects that are in Maintenance Mode. See the *C•CURE 9000 Data Views User Guide* for information about adding the Maintenance Mode column to the Dynamic View.

Filtering Partitions and Maintenance Mode Objects in the Dynamic View

Application Layout Filtering configuration allows Operators to filter a Dynamic View to show only selected partitions and/or to view objects that are in Maintenance Mode in the Administration application and in the Monitoring Station. Only Operators with the correct privilege and Application Layout assigned to them are allowed to use filtering.

See Configuring Privileges to Turn Maintenance Mode On and Off on Page 61 and Configuring the Application Layout for Maintenance Mode Filtering on Page 62

3

Configuring Dialup

This chapter explains how to configure dial up for use with the iSTAR Pro and the iSTAR Ultra SE (Pro Mode only).

In this chapter

iSTAR Dialup

Dialup enables you to connect the C•CURE 9000 to the iSTAR Pro (with a 56K PCMCIA modem card) and iSTAR Ultra SE (in Pro Mode with a USB-based modem card) controllers at remote locations using modems and standard telephone lines.

The C•CURE host and iSTAR phone line/modem connection is based primarily on Windows standard telephony communications and Routing and Remote Access Service (RRAS).

- The lowest level of the communications, which deals with modem states, is handled by the Microsoft Windows Telephony Application Programming Interface (TAPI). TAPI supports the use of any type of standard modem on the host.
- The higher level of the communications, which deals with the transmission of C•CURE relevant data, is handled by Microsoft RRAS. RRAS treats dial-up connections as if they were network connections. Consequently, the C•CURE host views the connection established between the iSTAR and itself via a phone line and modem as any other network connection.
- Serial port-based dialup modems and USB port based modems are supported.

Dialup Limitations

- Dialup is only supported on Windows Server 2008 R2, 2012, and 2012 R2.
- Dialup is not supported in configurations using redundancy.
- Dialup can be used only as the primary connection method **or** the secondary communication method, not as both.

  Example:

  – Dialup is used as the primary communication method and there is no secondary communication method.

  – TCP/IP is used as the primary communication method and Dialup is used as the secondary communication method.
- A cluster used for dialup can only contain one iSTAR controller.
- Fast Personnel download is not supported.
- Dialup is not supported on a separate RRAS server.

iSTAR Dialup Configuration Sequence

NOTE The configuration information in this section only applies to the C•CURE 9000, and assumes that you completed the operating system setup as described in the *Operating System Setup for Dialup Guide*. This guide is located in the C•CURE 9000 Installation DVD English\Manuals folder.

The dialup configuration sequence is described in Table 3 on Page 69.

Table 3: iSTAR Dialup Configuration Sequence

Step	Task	See...
1	Configure the Comm ports to which the host modems are attached in C•CURE 9000 using the iSTAR Comm Port Editor.	Configuring the iSTAR Comm Port on Page 70
2	Configure the host modems in C•CURE 9000 using the Host Modem editor.	Configuring the Host Modem on Page 73
3	Create an iSTAR Cluster. Click the **Dialup** tab to configure dialup settings.	Creating a Cluster for Dialup on Page 76
4	Configure the iSTAR controller.	iSTAR Pro Controller Editor on Page 137
5	1. Open the iSTAR Cluster you created in Step 3. 2. Click the **Communications** tab. 3. Add the controller you configured in Step 4. 4. Configure the communication with the host.	Configuring iSTAR Clusters on Page 87
6	Configure/Grant Privileges for the iSTAR Controller dialup permissions using the Privilege editor.	*C•CURE 9000 Software Configuration Guide*
7	Configure Events to download to the controller and select the dial up conditions using the Event editor. Select the Dialup settings from the Event Editor General tab.	*C•CURE 9000 Software Configuration Guide*
8	Configure the System Variables **Dialup** settings (dial-up user name, password, domain, grace seconds, cycle seconds) to use RRAS.	*C•CURE 9000 System Maintenance Guide*

Configuring the iSTAR Comm Port

Use the iSTAR Comm Port dialog box, shown in Figure 17 on Page 70, to communicate with a serial port connection.

See Table 4 on Page 70 for descriptions of the fields on the Comm Port editor General Tab.

NOTE

- The iSTAR Comm Port only supports a serial port.
- Triggers are not supported.

Figure 17: iSTAR Comm Port Editor Dialog Box

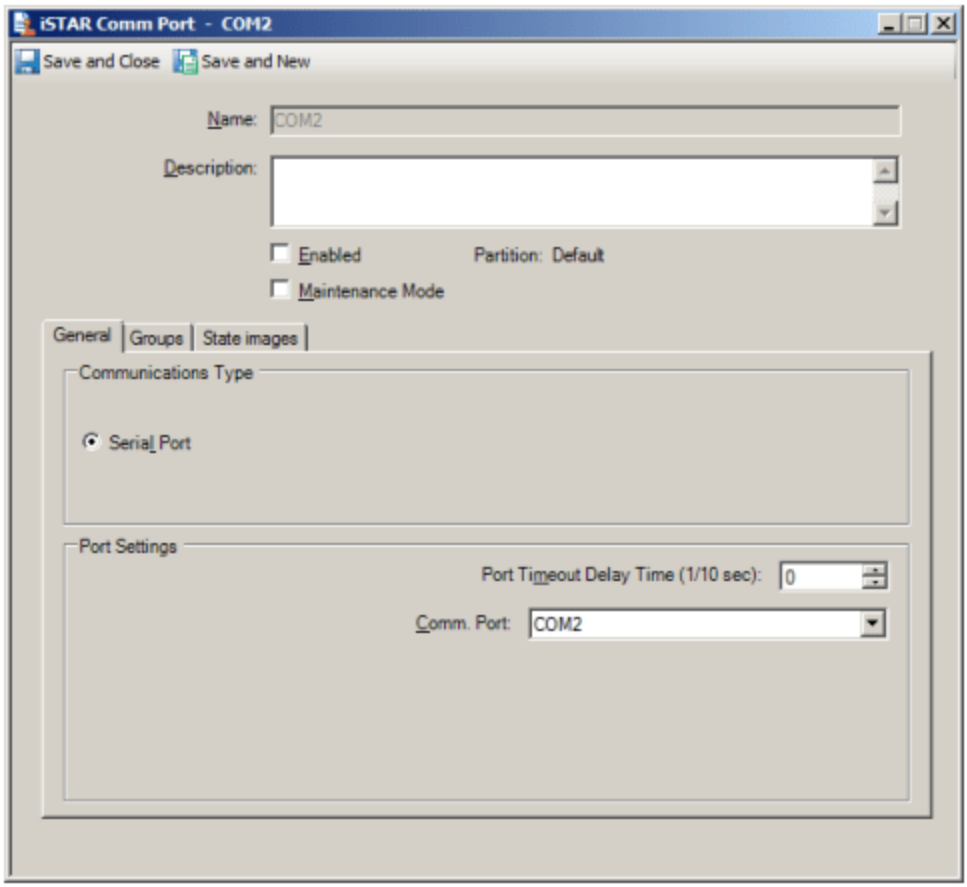


Table 4: iSTAR Comm Port Field Definitions

Field	Description
Name	The Name field will reflect the Comm Port you select.
Description	Enter a textual comment about the controller, such as its location or purpose. This text is for information only.

iSTAR Comm Port Field Definitions (continued)

Field	Description
Enabled	This setting determines whether or not the iSTAR Comm Port is able to provide communication between the iSTAR Controller and the C•CURE 9000 Server. Select **Enabled** to set the Comm Port online. To take the Comm Port offline, clear the **Enabled** selection. If the iSTAR Comm Port is currently in use by iSTAR controllers, you must disable all the controllers before you attempt to take the Comm Port offline. If any iSTAR controllers are enabled when you attempt to take the iSTAR Comm Port offline, an error message is displayed - "Port cannot be disabled with enabled controllers. Please disable controllers first. When the controllers are re-enabled they will do a full personnel download." The message explains that when you re-enable the iSTAR Comm Port and then re-enable the iSTAR controllers, each controller will perform a full personnel download. NOTE: Fast Personnel Download is not supported.
Maintenance Mode	Click to put the iSTAR Comm Port into Maintenance Mode. See Chapter 2: Maintenance Mode for more information.
Partition	This read-only field identifies the Partition.
Communications Type	
Serial Port	Selected by default.
Port Settings	
Port Timeout Delay Time (1/10 sec)	The **Port Timeout Delay Time** is the extra interval that the host waits for a response from the iSTAR panel after sending a message to the panel. If the host does not receive a response in the specified time, the host re-transmits the message or declares a communications failure. This field allows you to set the timeout delay for all panels that use a specific port. Software House recommends that you set this period to 20 (2 seconds). However, if you require additional delay time because iSTAR controllers run on a Digiboard, Equinox board, or over a network, you may need to increase this value. Keep this value as small as possible, or system performance may be affected. If your panel goes into communications failure often, try setting this value between 30 (3 seconds) and 50 (5 seconds). Range: 0 through 99. Default: 0.
Comm Port	Select the Communications Serial Port from the drop-down list. The Name field will reflect the port number that you select. The range is COM1 to COM256.

To Configure the iSTAR Comm Port

1. Open the C•CURE 9000 Administration **Hardware Pane**, select the Hardware Folder in which you want the iSTAR Comm Port to reside.
2. Right-click the folder to display the context menu, click **iSTAR Comm Port** and, then click **New**. The **iSTAR Comm Port** editor appears.

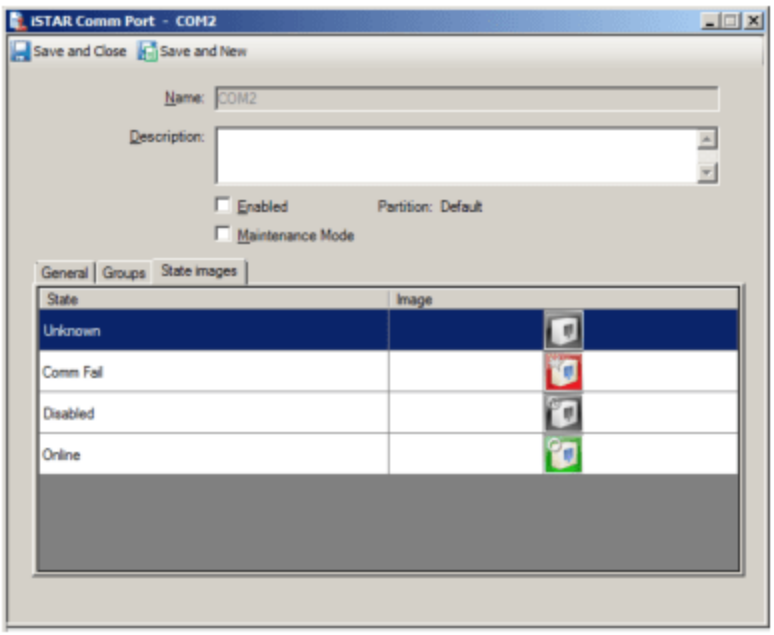
   You may also choose **New Template**. For further information about creating Templates, see Creating a Template on Page 34.
3. Enter a unique Host Communications Port name in the **Name** field (required).
4. Enter a textual description of the Comm Port (optional) in the **Description** field.

5. You can set a **Port Timeout Delay Time** in tenths of a second units by entering it in the field or by using the up/down arrows.
6. Select the **Comm Port** from the drop-down list.
7. Select the **Enabled** check box to put the Comm Port online after you have completed the configuration procedure.
8. Click **Save and Close**.
9. Go to Configuring the Host Modem on Page 73.

iSTAR Comm Port State Images Tab

The **State images** tab, shown in Figure 1 on Page 72, provides a means to change the default images used to indicate communication port states. These images appear on the Monitoring Station and change according to the state of the object that they represent.

Figure 1: iSTAR Comm Port State Images Tab



To Change a State Image

1. Double-click the existing image. A Windows Open dialog box appears allowing you to browse for a folder in which you have placed replacement images.
2. When you locate the replacement image, select it and click **Open** to add it to the image listing.
3. If you are done editing the iSTAR Comm Port, click **Save and Close** to save the Comm Port's configuration. Alternatively, if you want to save the Comm Port and create a new one, click **Save and New**. The Comm Port Editor remains open to allow you to create a new Comm Port.

To Restore to the Default Image

- Right-click on the new image and select **Restore Default**.

Configuring the Host Modem

The Host Modem dialog box, shown in Figure 18 on Page 73, lets you specify the communication port, the dialing direction, and the phone numbers the iSTAR Pro/SE Pro Mode can use.

NOTE Hyphens, parentheses, and spaces are not allowed in phone numbers.

The Host Modem dialog box definitions are described in Table 5 on Page 73.

Figure 18: Host Modem Dialog Box

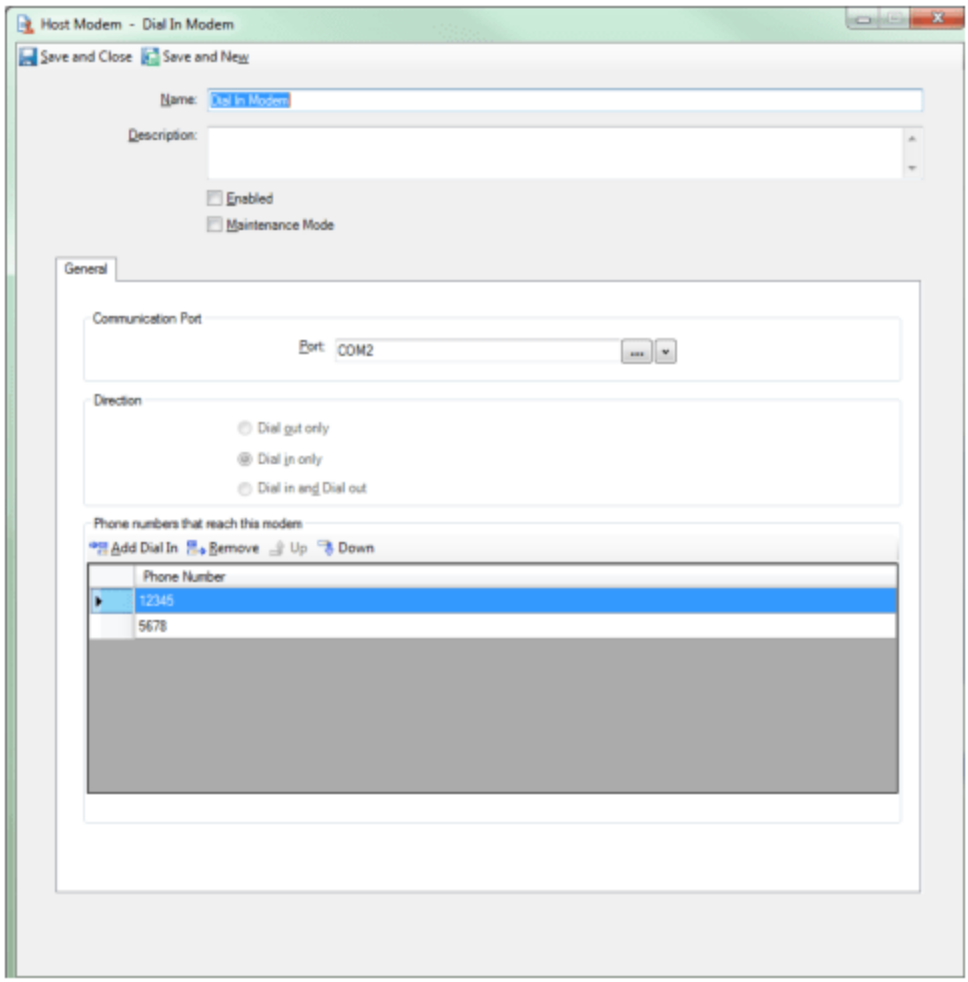


Table 5: Host Modem Dialog Box Definitions

Field	Description
Name	Enter a unique name for the host modem configuration.
Description	A textual comment for information only.
Enabled	Select **Enabled** to set the host modem online. To take the host modem offline, clear the **Enabled** selection.

Table 5: Host Modem Dialog Box Definitions (continued)

Field	Description
Maintenance Mode	Click to put the iSTAR Comm Port into Maintenance Mode. See Chapter 2: Maintenance Mode for more information.
Partition	This read-only field identifies the Partition in which this Controller resides.
Communication Port	Click ... to open the **Name Selection** dialog to select the iSTAR Comm Port. NOTE: The iSTAR communication ports must already be configured. See Configuring the iSTAR Comm Port on Page 70
Direction	**Dial out only** Select this option to specify that this modem is used only for dialing out to panels/controllers **Dial in only** Select this option to specify that this modem is used only for dialing into the host. **Dial in and Dial out** Select this option to specify that this modem is used for both incoming and outgoing calls.
Phone numbers that reach this modem	Displays the list of phone numbers that reach this host modem. Use the buttons to the right of the list to modify the numbers in the list. • The phone number can be up to 35 characters long. • Hyphens, parentheses, and spaces are not allowed in phone numbers. • If **Dial out only** is selected in the Direction box, this box and the **Add Dial In**, and **Remove** buttons are unavailable.

To Configure Modems for the Host

1. Ensure that the iSTAR communication ports are configured. See Configuring the iSTAR Comm Port on Page 70.
2. Open the C•CURE 9000 Administration **Hardware** Pane, select the Hardware Folder in which you want the iSTAR modem configuration to reside.
3. Right-click the folder to display the context menu, click **Host Modem**, and then click **New**.

   The Host Modem dialog box, shown in Figure 18 on Page 73, appears.
4. Enter a unique Host Modem name in the **Name** field (required).
5. Enter a textual description (optional) of the Host Modem configuration in the **Description** field.
6. Click ... in the **Port** field to open the **Name selection** dialog box and click the iSTAR Comm Port you want to use.
7. Select the dial Direction: **Dial out only**, **Dial in only**, or **Dial in and Dial out**.
8. In the **Phone numbers that reach this modem** box:
   a. Click **Add Dial In** to add a new row.
   b. Click in the new row and enter a phone number.
   c. Repeat step a and step b for each phone number you want to add.

9. Click **Enabled** to put the Host Modem online.
10. Optional. Click on the **State Images** tab to change the default images used to indicate communication port states on the Monitoring Station.
11. Click **Save and Close**.
12. Go to Creating a Cluster for Dialup on Page 76.

Creating a Cluster for Dialup

This section describes how to create a cluster to use dial-up on the iSTAR Pro or Ultra SE Pro Mode controller.

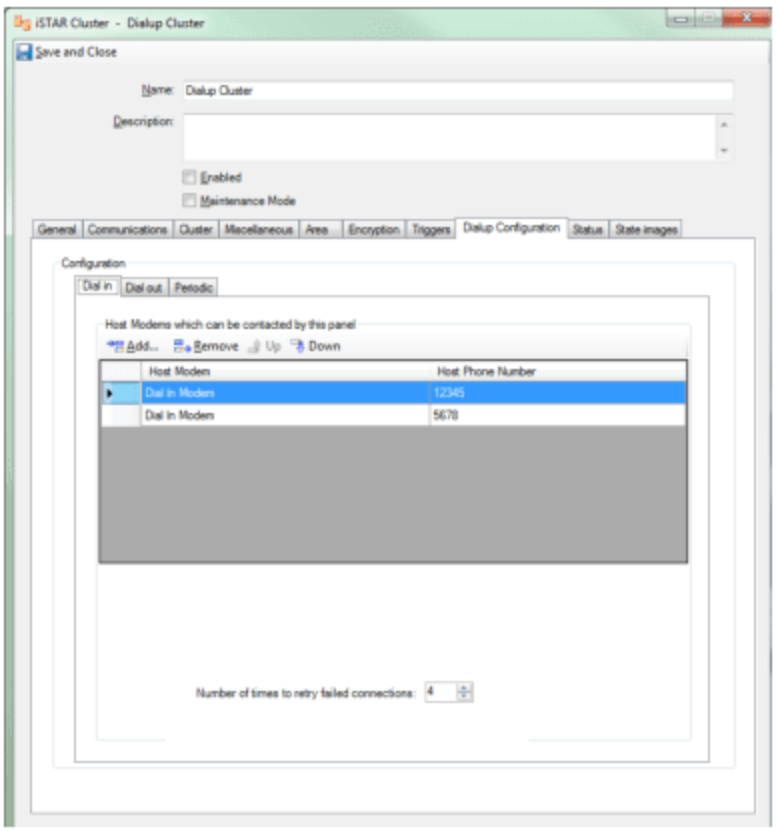
The **Dialup Configuration** tab in the **iSTAR Cluster** Editor dialog box, shown in Figure 2 on Page 76, lets you select pre-configured host modems and specify other dial-up configurations.

This tab is only available for unencrypted clusters and for use with the iSTAR Pro or iSTAR Ultra SE in Pro Mode.

NOTE

- You can only have one controller in a cluster that uses dialup.
- To enable a cluster, a dial-in and a dial-out phone number must be configured.
- Alternate master is not supported.

Figure 2: iSTAR Cluster Dialup Configuration Tab



There are three tabs under Configuration:

- **Dial In** lets you select host modems that the controller can call when dialing the host.
- **Dial Out** lets you select host modems that the controller can use to dial out.
- **Periodic** lets you specify a controller to periodically upload activity to the host, receive download configuration changes, and cardholder information from the host at that time.

Table 1: iSTAR Cluster Dialup Configuration Tab Definitions

Field	Description
Dial In Tab	
Host Modem/Host Phone Number	Click to **Add** to open the **Name Selection** dialog box host to select the host modems and host phone numbers that the host can use to contact this controller. • The host calls the modems in the order that they are listed. • A modem/phone combination can be listed more than once, but you cannot enter more than 8 modem/phone combinations.
Number of times to try connections	Specify the number of times the controller dials each telephone number in the list when the controller cannot contact the host. **Example:** If 2 is entered in this field, the controller dials each telephone number in the list two times. If the requisite connection attempts with all the phone numbers in the list fail, the controller is considered to be in Comm fail.The system will use the **Retry interval during communication failure** value to set the timing of communication attempts. Default: 2 Range: 0-99
Dial Out Tab	
Host Modems/ Remote Phone Number	Click **Add** to add host modems and remote phone numbers that the host can use to dial out. • The host calls the modems in the order that they are listed. • A modem/phone combination can be listed more than once, but you cannot enter more than 8 modem/phone combinations.
Automatically initiate connection when configuration changes after hh:mm	Specify the time to automatically download configuration changes to the dial-up controller. Then, click on the check box to enable the download time. **Example:** Cardholder additions and deletions. NOTE: - Leaving this unselected means that configuration changes will not be downloaded until the next normal connection with the controller. - Selected with a time of 00.00 indicates immediate download. - Changes to the controller, such as change to an object's name or description, do not cause a download to the controller. Range: 0 to 23 hours 59 minutes.
Periodic Tab NOTE: To make changes to the Periodic tab you must uncheck **Enabled**, click **Save and Close** and then reopen the Cluster editor.	
Redial interval during communications failure	Specify the interval of time the host waits to redial the controller when there is a communication failure. Enter the time in hh:mm format. • Default: 30 minutes. • Range: 0 minutes to 24 hours 59 minutes.

Table 1: iSTAR Cluster Dialup Configuration Tab Definitions (continued)

Field	Description
Schedule	Click ... to open the **Name Selection** dialog box to select a non-recurring schedule for periodic dialing, and downloading configuration changes and cardholder information. NOTE: If the predefined '**Always**' schedule is selected, the controller will only use the time interval specified by **Dial interval outside of schedule**.The **Dial interval during schedule** setting will be ignored.
Dial interval during schedule	Specify the frequency that the host dials the controller when the time specification is in effect. • Enter the time in hh:mm format. • Range: 0 to 24:00 hours.
Dial interval outside schedule	Specify the frequency that the host dials the controller when the time specification is not in effect. • Enter the time in hh:mm format. • Range: 0 to 24:00 hours.

To Configure a Cluster for Dialup

1. Click on the **Dialup Configuration** tab in the iSTAR Cluster Editor dialog box.
2. See Table 1 on Page 77 for **Dial In**, **Dial Out**, and **Periodic** tab configuration information.
3. Click **Save and Close** when done.
4. Go to iSTAR Pro Controller Editor on Page 137 to configure the controller.

4

Configuring C•CURE iSTAR Clusters

This chapter explains how to configure iSTAR Clusters in the C•CURE 9000 system.

In this chapter

Cluster Communications Overview

iSTAR controllers are organized for network communications into user-defined, logical groups called *Clusters*. Clusters contain one or more iSTAR controllers. A C•CURE 9000 server (host) can be connected to multiple iSTAR clusters. An iSTAR Controller must belong to a Cluster.

NOTE A Cluster can have a maximum of 16 controllers.

Cluster Configuration and Distributed Management

One or more controllers can be configured for communications purposes into user-defined groups called **Clusters**. Clusters have a primary communication path to the host that use **Masters** to control communications among cluster members and the host over the network. Clusters also support a backup communications path, the secondary communications path. The cluster can use the secondary path to communicate with the host when a communications failure occurs on the primary path. Secondary paths can only exist on the Master.

NOTE The Alternate Master capability cannot be configured in newly-created iSTAR clusters in version 2.20 or later.

iSTAR Clusters that already have an Alternate Master, when upgraded to version 2.20 or later, retain the Alternate Master, but if the cluster is edited and the Alternate Master is removed, this change will permanently remove the ability to configure an Alternate Master for this cluster.

See the iSTAR Cluster Communications Tab on Page 95 for more information.

NOTE Secondary communications paths have not been evaluated by UL.

Communications among iSTAR controllers provide distributed functionality at the controller level that is not typically available on security management systems.

A cluster can only contain controllers that support compatible methods of encryption (or do not use encryption).

- You can create a Non-Encrypted Cluster containing iSTAR Classic, iSTAR Pro, or iSTAR Ultra Controllers.
- You can create an Encrypted Cluster containing iSTAR eX, iSTAR Edge, or iSTAR Ultra Controllers.

NOTE

Previously, clusters were categorized by **Controller Type** rather than **Encryption Setting**. The composition of clusters and the models of controllers they contain has not changed. When C•CURE 9000 is upgraded, cluster types are changed to reflect **Encryption Settings**, but existing controllers remain in the same clusters.

This change has the following additional effects:

- Existing Reports: ControllerType field is ignored.
- Existing Queries: If ControllerType is included, the query cannot run until the Query is edited and ControllerType is removed.
- Dynamic Views: ControllerType is replaced by EncryptionSetting.
- Existing Imports: ControllerType is marked as an Import Only property and used to set the Encryption Setting value.

Master controllers use the primary or secondary communications path to communicate with the C•CURE System host. Establishing and maintaining a connection with the host involves the following administrative actions through the use of iSTAR Clusters:

- Establishing connections via the primary communications path. You set up a primary communications path for a cluster when configuring controllers and clusters.
- Downloading cardholder and configuration information from the host to the controller.
- Maintaining communications via the primary communications path. If a communications failure occurs on the primary communications path, controllers can re-establish communications via a secondary communications path.

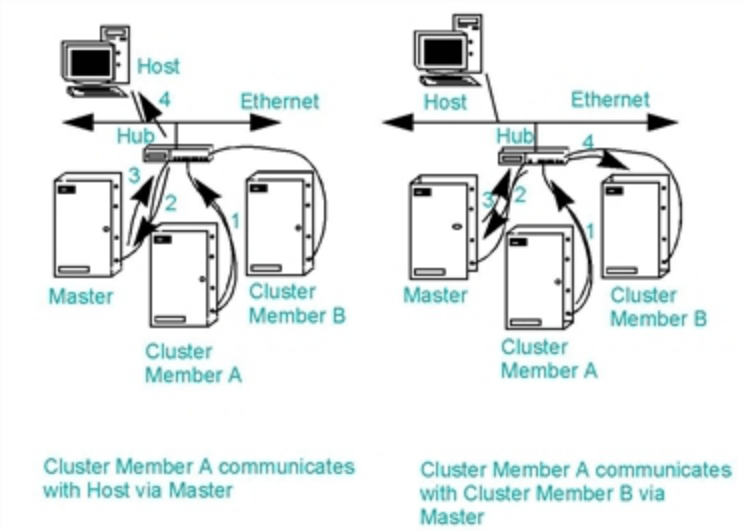
Networked iSTAR Controllers (Clusters)

Controllers are organized for network communications into user-defined or logical groups called **Clusters**. This section describes the key elements of clusters.

Master and Cluster Members

Each cluster has one controller that serves as the **Master** with all other controllers in the cluster acting as **Cluster Members**. The master manages all communications between the cluster and a host computer. Cluster members can communicate with each other via the master, over an Ethernet network. Cluster members cannot communicate with each other directly. Figure 19 on Page 82 (left) shows how Cluster Member A communicates with the host via the master. The figure (right) shows how Cluster Member A communicates with Cluster Member B via the master.

Figure 19: Cluster Members



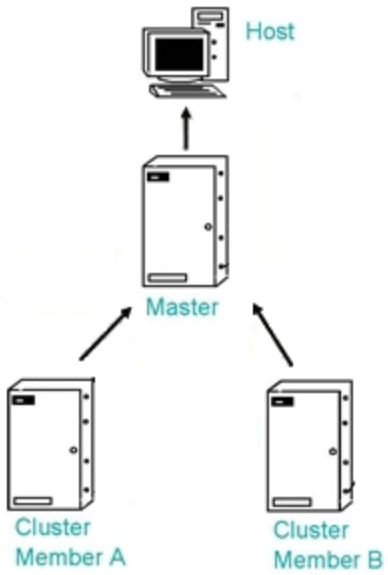
The Primary Communications Path

The **Primary Communications Path** is the first communications path that master controllers use to establish communications with the host. Controllers communicate with the host directly. The **Connection type** is TCP/IP over Ethernet.

The **Master** is the one controller in a cluster that is responsible for passing messages between the host and cluster members. Cluster members do not communicate with the host directly; they communicate with the host through the master. Connections are established in the following bottom-to-top order:

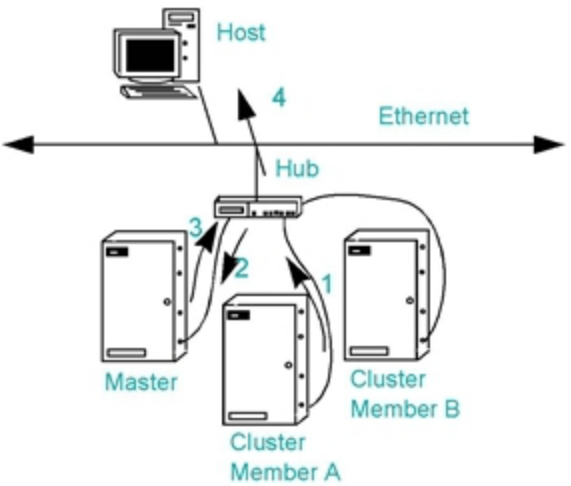
- The **Master** is responsible for establishing a connection with the host. The host does not establish a connection with the master.
- **Cluster Members** are responsible for establishing connections with the master. The master never tries to establish a connection with a cluster member, as shown in Figure 20 on Page 83.

Figure 20: Cluster Communication Path



The **Connection type** is how the master connects to the host: TCP/IP over Ethernet. Cluster members are connected to the master via Ethernet only. Figure 21 on Page 83 shows the Primary Communications Path for Cluster Member A. The master/host connection type is TCP/IP over Ethernet.

Figure 21: Primary Communications Path



Primary Communications Path for Cluster Member A

Establishing Connections Via the Primary Communications Path

The primary communications path is comprised of the following connections:

- The master connects directly to the host using a network connection.
- Cluster members connect to the master using a network connection. After connections are established, the master manages cluster communications by passing messages between cluster members and the host.

Connections are established in a bottom-to-top order. Thus, clusters members are responsible for establishing connections with the master, and the master is responsible for establishing a connection with the host.

Setting Up the Primary Communications Path

Before controllers can establish any connections, you must configure the cluster's primary communications path by performing the following tasks:

- Use the C•CURE 9000 Administration Application to first configure the cluster and then the iSTAR Controllers. See Configuring iSTAR Clusters on Page 87 and Configuration Overview for iSTAR Controllers on Page 119 for information.
- Use the iSTAR Configuration Utility (ICU) to manually configure the master. After you configure the master, it reboots and then establishes a connection with the C•CURE 9000 Server. The server downloads cardholder and configuration information to the master.

  After downloading information from the host, the master auto-configures its cluster members. Cluster members then reboot and establish connections with the master.

Downloading Cardholder and Configuration Information

The following information is downloaded to the master and its cluster members from the host:

- Cardholder data for personnel with clearances on the controller.
- Configuration information for inputs, outputs, and readers on the controller.
- Events that are controlled by the controller.
- Cluster information that the controller uses to communicate with other cluster members.

NOTE The C•CURE 9000 Server downloads cardholder and configuration information to the controller under the following conditions:

- Initial configuration
- Each time the controller is powered on
- Each time the cluster is taken offline/online

Changes to personnel, clearances, inputs, outputs, readers, and events are immediately downloaded.

Maintaining Communications

Although a communications link may be open between two devices, long periods of time can exist when devices do not communicate because of low system activity. In the absence of this type of communications, devices send "keep-alive" messages, called **Connection Verification** messages, to verify that connections are alive.

Example:

The master and host send these messages to each other to confirm that the connection between them is open. If the host does not receive a connection verification message from the master in a specified amount of time, the host closes the communications link with the master and waits for a connection attempt from the cluster. When the master does not receive a connection verification message from the host in the specified amount of time, it also declares a communications failure for the primary communications path and then notifies its cluster

members of the communications failure. At this time, cluster communications revert to the secondary communications path.

Use the **Communications** and **Cluster** tabs in the C•CURE 9000 Administration Application, iSTAR Cluster dialog box, to configure connection verification messages for the master, host and cluster members. See Configuring iSTAR Clusters on Page 87 for more information.

Establishing a Secondary Communications Path

If a communications failure occurs on the primary communications path, communications can be re-established via the cluster's secondary communications path. The secondary communications path must be a second connection between the master and the host. The network connection must be one that is not already being used as the primary path.

While communicating via the secondary path, the cluster attempts to re-establish communications with the host on the primary communications path. When a connection is re-established on the primary path, communications revert to the primary path and the communications link on the secondary path is closed.

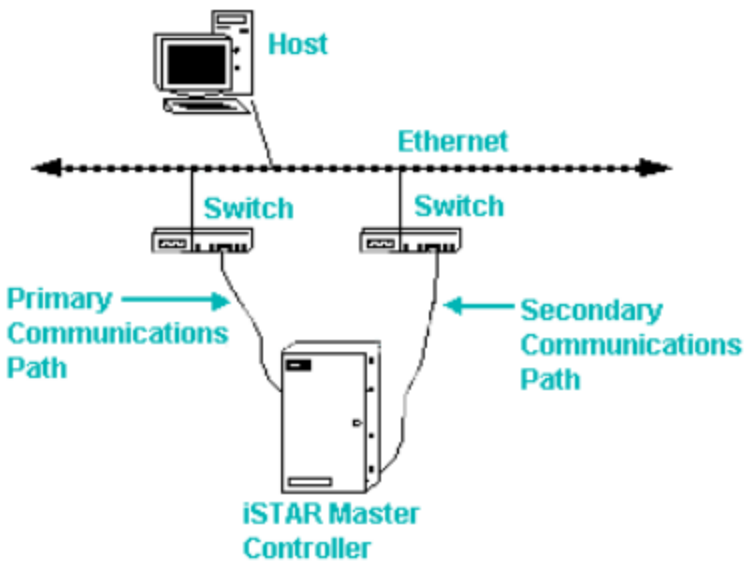
Use the **Communications** tab in the **Cluster** dialog box in the C•CURE 9000 Administration Application to configure the secondary communications path (see iSTAR Cluster Communications Tab on Page 95).

The Secondary Communications Path

A **Secondary Communications Path** is the host communications path that is used by a controller if a communications failure occurs on the primary communications path. The secondary path is activated by the iSTAR Controller's dual network capability.

Figure 22 on Page 85 shows an example of a secondary communications path on the host using an Ethernet connection and a secondary communications path on another network card, using an Ethernet connection.

Figure 22: Primary and Secondary Communications Path to Host



Distributed Cluster Management

Cluster communications allow iSTAR controllers to share information and control actions throughout a cluster without host intervention. **Distributed Cluster Management** is the distribution of system functionality from the host to cluster members.

Distributed cluster management lets a controller perform many actions locally and share information with other cluster members even when the controller is not communicating with the host, during a communications failure for example.

NOTE Cluster members communicate with each other through the master. Although a communications failure with the host may not affect cluster communications, a communications failure with the master can cause communications problems in the cluster.

Unassigned Folder

The Unassigned folder is a repository for iSTAR controllers that have been configured for an iSTAR cluster, in an existing partition, but which have been removed from the iSTAR cluster, or the cluster has been deleted. Such controllers will be listed under the Unassigned folder until they are reassigned to another iSTAR cluster or deleted.

Configuring iSTAR Clusters

Before you can create and configure iSTAR Controllers, you must create an iSTAR Cluster. The Cluster dialog box lets you configure clusters by performing the following tasks:

- Add controllers to the cluster.
- Configure a primary communications path for the cluster.
- Configure a secondary communications path for the cluster.
- Configure communications between cluster members and the master.
- Configure the number of unacknowledged messages for controllers.
- Set Triggers for the cluster.
- Evaluate cluster status.
- Change state images that appear on the Monitoring Station.

Figure 23: Hardware Pane - Creation of an iSTAR Cluster

Creating an iSTAR Cluster

You can create an iSTAR Cluster in a Hardware Folder in the Hardware tree. You can either select a folder, then pick iSTAR Cluster from the Hardware tree drop-down list, or right-click on the folder and select iSTAR Cluster from the context menu.

To Create an iSTAR Cluster

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Expand the Hardware tree and select the folder where you want to create the iSTAR Cluster.
3. Right-click on the folder and select **iSTAR Cluster>New** to create a cluster for one or more iSTAR controllers. The iSTAR Cluster Editor dialog box opens, as shown in Figure 26 on Page 92.

   See iSTAR Cluster Editor on Page 91 for instructions on configuring the Cluster.
4. Enter a **Name** (required) and **Description** (optional).
5. Select an **Encryption Setting**:
   - **Encrypted** for a Cluster that will contain iSTAR eX, iSTAR Edge, or iSTAR Ultra controllers that will use an iSTAR encryption method.
   - **Non-Encrypted** for a Cluster that will contain iSTAR Pro, iSTAR Classic, or iSTAR Ultra controllers that will not use an iSTAR encryption method.

   NOTE This field becomes Read-only once you add iSTAR controllers to the Cluster and save it, because changing this setting while there are controllers in the cluster would cause problems.

   If you need to change this setting, you must remove all controllers from the Cluster, change the Encryption Settings on the Cluster Encryption tab (see iSTAR Cluster Encryption Tab on Page 105), then add controllers of the appropriate type.
6. Click **Save and Close** to save the Cluster. The new iSTAR Cluster icon displays in the tree, one level below the folder that you selected.

Creating and Using an iSTAR Cluster Template

You can create an iSTAR Cluster Template that you can use as the basis for creating new iSTAR Clusters with specific settings that you choose when creating the Template.

Example

If you want all of your iSTAR Clusters to use 60 seconds instead of the default 10 seconds for the Connection to Host Interval, you can create an iSTAR Cluster Template with Connection to Host Interval set to 60 seconds, and every iSTAR Cluster you create from this Template will inherit that setting.

To Create an iSTAR Cluster Template

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Expand the Hardware tree and a hardware folder.
3. Right-click on the folder and select **iSTAR Cluster>New Template** from the context menu (see Figure 24 on Page 89).

Figure 24: New Cluster Template from Hardware Folder Context Menu

Alternatively, select **iSTAR Cluster** in the Hardware pane drop-down list, click the down-arrow next to the **New** button, then select **iSTAR Cluster>New Template** from the menu.

The iSTAR Cluster Editor opens a new Template that you can configure and save.

4. Enter a unique name for the Template in the **Name** field (required) and type a textual description for the Template in the **Description** field (optional).

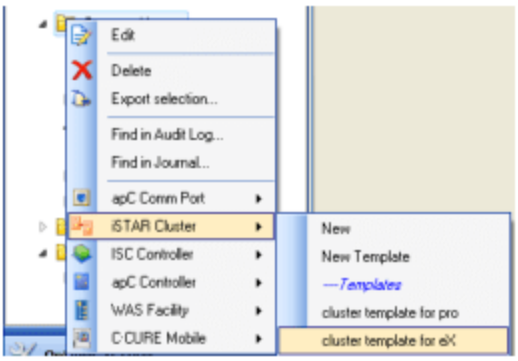
5. Select the **Encryption Setting** for the Cluster Template. Only controllers of the types supported by this setting can subsequently be added to Clusters created from this Template. (This field becomes read-only after you save the Cluster Template).
6. Navigate to the Communications, Cluster, Miscellaneous, Encryption, Triggers, and State Images tabs and configure any settings that you would like to be included in your Template. See iSTAR Cluster Editor on Page 91 for more information about the iSTAR Cluster Editor tabs.
7. Click **Save and Close**. The Cluster Template is saved with your settings. You can now use the Template as the basis of new iSTAR Clusters you subsequently create.

NOTE A Cluster Template is not saved inside of a Hardware folder, and it is not visible in the Hardware tree. To edit a Cluster Template, select **iSTAR Cluster** from the Hardware drop-down list and click to display a Dynamic View listing all iSTAR Clusters, including Cluster Templates. Double-click on a Cluster Template in the Dynamic View to edit it.

To Create an iSTAR Cluster from a Template

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Expand the Hardware tree and a hardware folder.
3. Right-click on the folder and select **iSTAR Cluster>New** from the context menu (see Figure 25 on Page 90).

Figure 25: New iSTAR Cluster from a Template



The iSTAR Cluster Editor and you can edit the new Cluster.

4. Enter a unique name for the Cluster in the **Name** field (required) and type a textual description for the Cluster in the **Description** field (optional).
5. Select the **Encryption Setting** for the Cluster Template. Only controllers of the types supported by this setting can subsequently be added to Clusters created from this Template. (This field becomes read-only after you save the Cluster Template).
6. Navigate to the Communications, Cluster, Miscellaneous, Encryption, Triggers, and State Images tabs and configure any settings that you would like to be included in your Cluster. See iSTAR Cluster Editor on Page 91 for more information about the iSTAR Cluster Editor tabs.
7. Click **Save and Close**. The iSTAR Cluster is saved with your settings.

iSTAR Cluster Editor

The iSTAR Cluster Editor is used to configure iSTAR Clusters for your C•CURE 9000 system. All iSTAR Controllers must be contained in an iSTAR Cluster in order to communicate with a C•CURE 9000 Server. You need to create at least one iSTAR Cluster before you can create any iSTAR Controllers.

iSTAR Cluster Editor Tabs

The iSTAR Cluster Editor includes the following tabs:

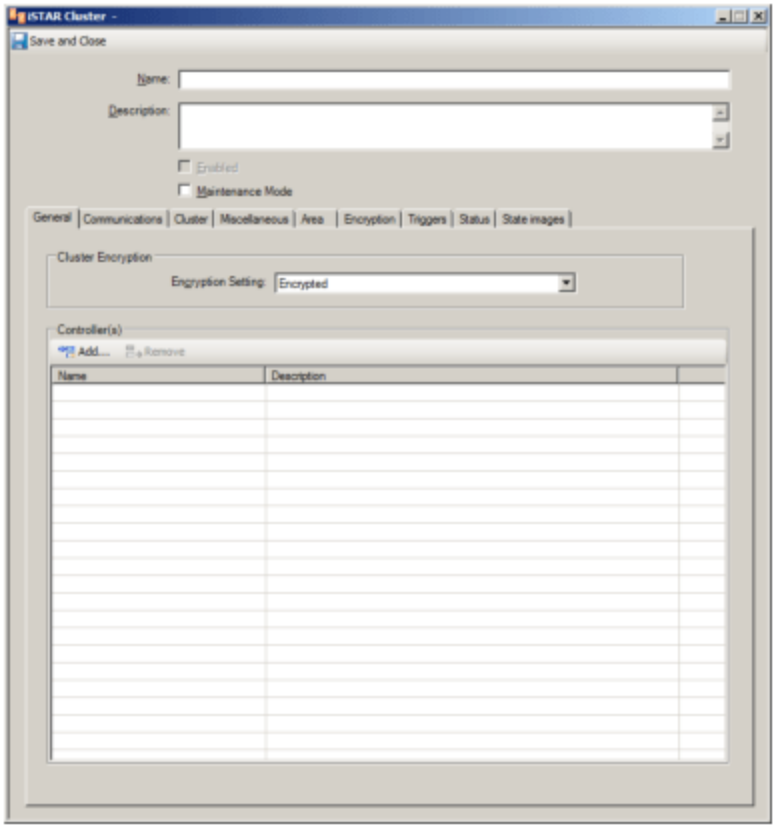
Accessing the iSTAR Cluster Editor

Perform the following steps to access the iSTAR Cluster Editor.

To Access the iSTAR Cluster Editor

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane (see Figure 23 on Page 87).
2. Expand the Hardware tree and select the Cluster that you want to configure.
3. Right- click and select **iSTAR Cluster>Edit** to open the selected Cluster in the iSTAR Cluster Editor (see Figure 26 on Page 92).

Figure 26: iSTAR Cluster Editor



iSTAR Cluster General Tab

The iSTAR Cluster General Tab provides an interface to manage controllers that you have configured for a cluster. From the General tab, you can add or remove iSTAR Controllers from a Cluster. An example of an iSTAR Cluster General tab is shown in Figure 26 on Page 92.

See iSTAR Cluster General Tab Definitions on Page 94 for definitions of the fields and buttons on the iSTAR Cluster.

iSTAR Cluster General Tab Tasks

You can perform the following tasks from the iSTAR Cluster General Tab.

- Adding a Controller to a Cluster on Page 93.
- Removing a Controller from a Cluster on Page 93.

Adding a Controller to a Cluster

To Add a Controller to a Cluster

1. Open the iSTAR Cluster editor for the Cluster to which you wish to add a Controller. See To Access the iSTAR Cluster Editor on Page 91.
2. Click **Add**.

   The iSTAR Controller selection dialog box opens. This dialog box lists all iSTAR Controllers that can be added to this Cluster. Only iSTAR Controllers with the same Encryption Setting as the Cluster (Encrypted or Non-encrypted) that are currently Unassigned (not currently attached to an iSTAR Cluster) appear in this dialog box.
3. Select one or more iSTAR Controllers from the dialog box. You can use multiple selection keystrokes such as **CTRL+Left-click** and **SHIFT+Left-click** to select more than one Controller.
4. Click **OK** to add the selected iSTAR Controllers to the list of Controllers in the iSTAR Cluster.
5. Click **Save and Close** to save your changes.

Removing a Controller from a Cluster

You can remove iSTAR Controllers from an iSTAR Cluster using the iSTAR Cluster General tab. Once you remove a Controller from an iSTAR cluster, the Controller is moved to the **Unassigned** folder and can subsequently be added to a different iSTAR Cluster with the same Encryption Setting.

To Remove a Controller from a Cluster

1. Open the iSTAR Cluster Editor for the Cluster to which you wish to add a Controller. See To Access the iSTAR Cluster Editor on Page 91.
2. From the Controller(s) list on the General tab, select one or more iSTAR Controllers you wish to remove from the Cluster. You can use multiple selection keystrokes such as **CTRL+Left-click** and **SHIFT+Left-click** to select more than one Controller.

   If the Cluster is **Enabled**, you cannot remove a Controller that is selected on the Communications tab as either the controller having primary communications with the host (C•CURE 9000 Server) or the controller having

secondary communications with the host. The **Remove** button becomes unavailable if you select such a controller.

3. Click **Remove**. The Controllers you selected are deleted from the Controller(s) list of this Cluster.
4. Click **Save and Close** to save your changes. The Controllers you removed from this Cluster now appear in the **Unassigned** folder in the Hardware tree, and can be re-assigned to another Cluster with the same Encryption Setting.

iSTAR Cluster General Tab Definitions

The iSTAR Cluster General tab includes the fields and buttons described in Table 6 on Page 94.

Table 6: iSTAR Cluster General Tab Definitions

Field/Button	Description
Name	Enter a name (up to 100 characters long) of the iSTAR Cluster that you are configuring.
Description	Type a description of the iSTAR Cluster that you are configuring.
Enabled	Enabled is grayed out until: 1. The controller's are configured. See Chapter 5, Configuring C•CURE iSTAR Controllers 2. A **Controller having primary communications with host** is selected on the **iSTAR Cluster Communications tab**. 3. Click **Enabled** to put the cluster online.
Maintenance Mode	Click to put the Cluster or iSTARs and/or their components into Maintenance Mode. See Chapter 2: Maintenance Mode for more information.
Partition	This read-only field identifies the Partition in which this iSTAR Cluster resides. Select the **Encryption Setting** for the Cluster Template. Only controllers of the types supported by this setting can subsequently be added to Clusters created from this Template. (This field becomes read-only after you save the Cluster Template). you want to change the Partition of a Cluster, see Using Drag and Drop in the Hardware Tree on Page 27.
Encryption Setting	A read-only field displaying the Encryption Setting for the Cluster.
Controllers	
Add	To add an iSTAR Controller to your Cluster, click **Add** to display the iSTAR Controller selection dialog box. Select one or more controllers and click **OK** to add it to the iSTAR Cluster.
Remove	To remove an iSTAR Controller from your Cluster, select the iSTAR Controller you want to remove in the list, then click **Remove**.
Name column	Displays the name of the controller.
Description column	Displays the description text for the controller.

iSTAR Cluster Communications Tab

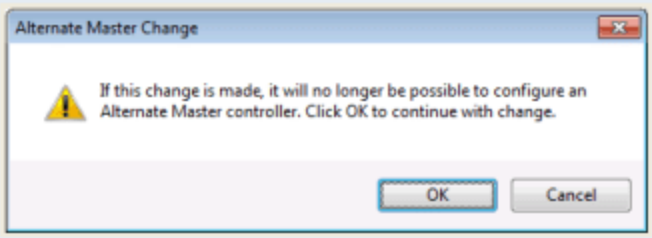
The **Communications** tab in the **iSTAR Cluster** dialog box lets you configure communications from the Controllers in a cluster to the C•CURE 9000 Server (Host). Primary and Secondary communications can be configured for an iSTAR controller that has two Onboard Ethernet Adapters. When one adapter is chosen as primary, the other can become the secondary.

If you are using iSTAR Pro dialup, the cluster must be configured for dialup communication.

NOTE

For a cluster that existed prior to version 2.20, you can have one controller configured for the Primary communications path as a Master controller, and a second, different, controller configured for the Secondary communications path as an Alternate Master.

However, if you remove the Alternate Master from the cluster, you will no longer be able to configure an Alternate Master for the cluster. A message box appears when you change **Controller having secondary communications with host** to None, informing you that the change will remove the Alternate Master.



For a new cluster created in version 2.20 or later, you cannot configure an Alternate Master. If you configure both a Primary and Secondary communications path, you must use the same controller, which must have two onboard Ethernet Adapters.

NOTE

Dialup can be used only as the primary connection method or the secondary communication method, not as both.

Example:

- Dialup is used as the primary communication method and there is no secondary communication method.
- TCP/IP is used as the primary communication method and Dialup is used as the secondary communication method.

Communications tab definitions are listed in Table 7 on Page 97.

Number of Failed Attempts Before Connection Fails on Page 98 explains how to configure the cluster's controllers to attempt to connect to the cluster, and resolve communications failures.

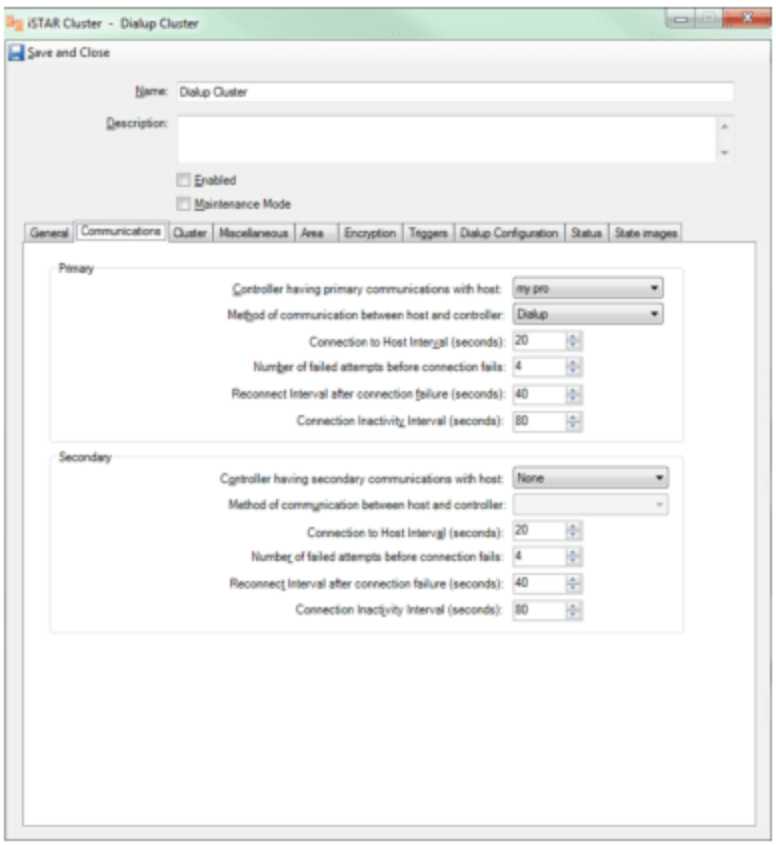
NOTE

Secondary communications paths have not been evaluated by UL.

To Configure the iSTAR Cluster - Communications Tab

1. From the **iSTAR Controller** dialog box, click the **Communications** tab. The **Communications** tab opens, shown in Figure 27 on Page 96.

Figure 27: iSTAR Cluster Communications Tab



2. **Controllers having primary/secondary communication with host** allows you to select the controller in the cluster that has **primary** or **secondary** communications with the host (C•CURE 9000 server). Choose a controller using the drop-down selection.
3. **Method of communication between host and controller** allows a selection of the communication type designated for the iSTAR controller that communicates with the host. Choose the connection type of **Onboard Ethernet** or **Dialup** (iSTAR Pro or iSTAR Ultra Pro Mode only) using the drop-down selection.
4. In the **Connection to Host Interval** entry field, specify the number of seconds that a controller waits between attempts to connect to the host.

   UL requires a maximum of 200 seconds supervision on the Communications link between the protected premise equipment and the central station.
5. In the **Number of failed attempts before connection fails** field, specify the number of attempts that a controller makes to first connect to the host before the controller is declared to be in communications failure. See Number of Failed Attempts Before Connection Fails on Page 98 for more information.
6. In the **Reconnect Interval after connection failure** field, specify the number of seconds that controllers wait between attempts to re-connect to the host. This field sets the rate at which controllers attempt to reconnect or

connect to the host after a communications failure occurs between the host and the controller. The default interval is 40 seconds. The maximum value is 9999 seconds and the minimum is 1 second.

7. In the **Connection Inactivity Interval** field, specify the number of seconds that a controller waits between attempts to connect to the host. The default interval is 80 seconds. The possible values are between 15 and 80 seconds.
8. Navigate to the iSTAR Cluster - Cluster Tab on Page 99 or click **Save and Close** to save the cluster and begin configuring iSTAR Controllers.

Table 7: iSTAR Cluster Communications Tab Definitions

Field	Description
Controllers having primary or secondary communication with host	This field allows you to select the controller that has primary or secondary communications with the host. Choose a controller using the drop-down selection.
Method of communication between host and controller	This field allows you to select the communication type designated for the iSTAR controllers, **PCMCIA Ethernet, Onboard Ethernet** or **Dialup** (iSTAR Pro/iSTAR Ultra SE Pro Mode only).
Connection to Host Interval [seconds]	Specify the number of seconds that a controller waits between attempts to connect to the host. Use the **Number of failed attempts before connection fails** field in the **Communications tab** to specify the number of connection attempts a controller makes before a communications failure is declared for the controller. The maximum value is 9999 seconds and the minimum is 1 second. The default value is 20 seconds.
Number of failed attempts before connection fails	Specify the number of attempts that a controller makes to first connect to the host before the controller is declared to be in communications failure. See Number of Failed Attempts Before Connection Fails on Page 98. The default value is 4 attempts.
Reconnect Interval after connection failure [seconds]	Specify the number of seconds that controllers wait between attempts to re-connect to the host. This field sets the rate at which controllers attempt to reconnect or connect to the host after a communications failure occurs between the host and the controller. The default interval is 40 seconds. The maximum value is 9999 seconds and the minimum is 1 second.
Connection Inactivity Interval [seconds]	Specify the number of seconds that a controller waits between attempts to connect to the host. The default interval is 80 seconds. The possible values are between 15 and 80 seconds.

Number of Failed Attempts Before Connection Fails

The **Number of failed attempts before connection fails** field in the **Communications tab** specifies the number of connection attempts a controller makes before a communications failure is declared for the controller. The default is 4 attempts. The maximum is 99 attempts and the minimum is 1 attempt.

If a connection is established, the controller and host use connection verification messages to maintain the connection.

If a connection is not made in the specified number of attempts, a communications failure is declared for the controller, and the following connections are attempted:

- If the secondary communications path uses an alternate host, the controller attempts to connect to the alternate host, which passes the controller's messages to the host. At the same time, the controller tries to re-establish a connection with the host at the rate specified in the **Reconnect Interval after connection failure** field.
- If the secondary communications path does not use an alternate host, the controller attempts to connect to the host forever, or until a connection is established. The controller attempts to connect to the host at the rate specified in the **Reconnect Interval after connection failure** field.
- The controller broadcasts a request across its subnet for the host's IP Address. The host responds to the request. If the host does not respond in a set amount of time and the iSTAR Configuration Utility is configured for auto-response, the utility responds to the controller. See the ***iSTAR eX Installation and Configuration Guide*** for information.

If a communications failure occurs, the following connections are attempted simultaneously:

- If the secondary communications path uses an alternate host, the controller attempts to connect to the alternate host, which passes the controller's messages to the host. At the same time, the controller tries to re-establish a connection with the host at the rate specified in the **Reconnect Interval after connection failure** field.
- If the secondary communications path does not use an alternate host, the controller attempts to re-connect to the host forever or until a connection is established. The controller attempts to reconnect to the host at the rate specified in the **After connection failure, controller attempts to reconnect every XX seconds** field.
- The controller broadcasts a request across its subnet for the host's IP Address. The host responds to the request. If the host does not respond in a set amount of time and the iSTAR Configuration Utility is configured for auto-response, the utility can respond to the controller. See the ***iSTAR eX Installation and Configuration Guide*** for information. If a connection is established, the controller and host use connection verification messages to maintain the connection. The default is 4 attempts. The maximum is 99 attempts and the minimum is 1 attempt.

iSTAR Cluster - Cluster Tab

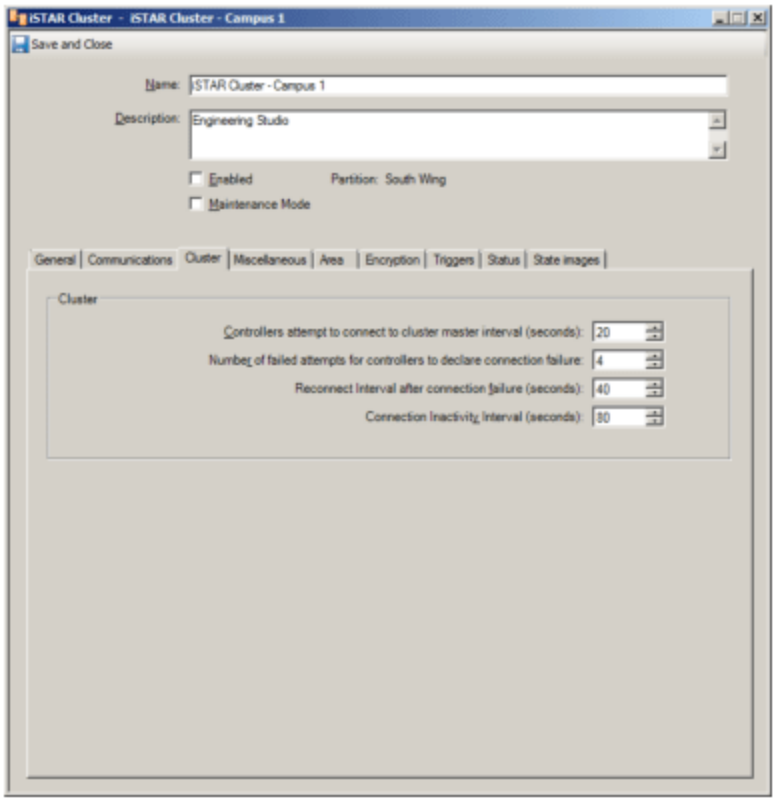
The Cluster tab regulates the connection and reconnection intervals between the primary iSTAR Controller and those controllers which are cluster members.

NOTE The Cluster tab has not been evaluated by UL.

To Configure the iSTAR Cluster - Cluster Tab

1. From the **iSTAR Controller** dialog box, click the **Cluster** tab. The **Cluster** tab opens, shown in Figure 28 on Page 99.
2. Specify the number of seconds that the primary controller attempts to connect with the host server in the **Controllers attempt to connect to cluster master interval** entry field. The range is from 1 to 9999 seconds; the default value is 20 seconds.

Figure 28: iSTAR Cluster Cluster Tab



3. Enter the number of instances after which the primary controller transmits a connection failure in the **Number of failed attempts for controllers to declare a connection failure** entry field. The range is from 1 to 99; the default value is 4.
4. Specify the number of seconds after which the primary controller attempts to reconnect after a connection failure in the **Reconnection Interval after connection failure** entry field. The range is from 1 to 9999 seconds; the default value is 40 seconds.

5. Enter the number of seconds after which the primary controller transmits a connection failure if there is no message while it is connected, in the **Connection Inactivity Interval** entry field. The range is from 15 to 80 seconds; the default value is 80 seconds
6. Navigate to the **Miscellaneous** tab or **Save and Close** to save the cluster and begin configuring iSTAR Controllers.

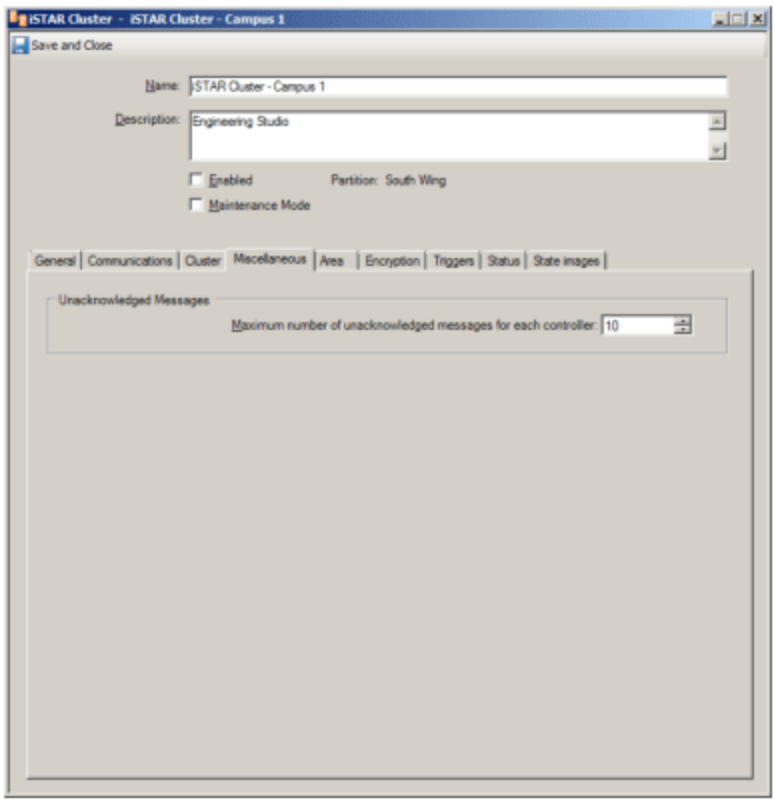
iSTAR Cluster Miscellaneous Tab

The iSTAR Cluster Miscellaneous tab allows you to set the maximum number of unacknowledged messages that are allowed for each iSTAR Controller

To Configure the iSTAR Cluster - Miscellaneous Tab

1. From the **iSTAR Controller** dialog box, click the **Miscellaneous** tab. The **Miscellaneous** tab opens, shown in Figure 29 on Page 101.

Figure 29: iSTAR Cluster Miscellaneous Tab



2. In the **Unacknowledged Messages** box specify the maximum number of unacknowledged messages that are allowed for each iSTAR Controller in the **Maximum number of unacknowledged messages for each controller** field.

   If you have a network with high latency, you may want to set this value to a higher number; if the network has low latency, the default value (10) should be sufficient.

NOTE

- This setting does not result in lost messages.
- For Proprietary Burglar Alarm applications, the Send state changes to the monitoring station option must be selected.
- The range is from 1 to 99 and the default value is 10. For UL applications, set the range to 99.

3. Navigate to the **Antipassback** tab or **Save and Close** to save the cluster and begin configuring iSTAR Controllers.

iSTAR Cluster Area Tab

The iSTAR Cluster Area tab allows you to configure the following:

- How Cluster Antipassback works for iSTAR Cluster Areas during a communications failure when the Cluster members lose communication with the Cluster master.
- Whether or not the Cluster is configured for both Global Antipassback and Cluster Antipassback or solely for Cluster Antipassback.

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

You configure how Global Antipassback works during a communications failure through a system variable in the iSTAR Driver section, "iSTAR Global Antipassback Communication Failure Mode". For more information, see the *C•CURE 9000 System Maintenance Guide*.

Cluster Antipassback Communications Failure Mode

As long as the communication within the Cluster is good, the Cluster members do not store any antipassback information. During communications failure, the Cluster members (the Controllers) begin to enforce antipassback locally, based on the Failure Mode you configure for the Area's Cluster on this tab.

For iSTAR Cluster Areas, all Doors and Readers must be within the same iSTAR Cluster. Adjacent Areas can be on any Cluster and can also be Cross-Cluster Areas.

Using Antipassback restricts access to Cluster Areas 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.

The violation triggered when personnel enter a specified Area is called an entry violation. The violation triggered when personnel exit a specified Area is an exit violation.

NOTE To ensure that personnel are always appropriately prevented from entering Lockout Areas, make sure that you configure the Communications Failure Mode for the Area's iSTAR Cluster as **No access** Mode, instead of **Local** Mode.

Global Antipassback for the Cluster

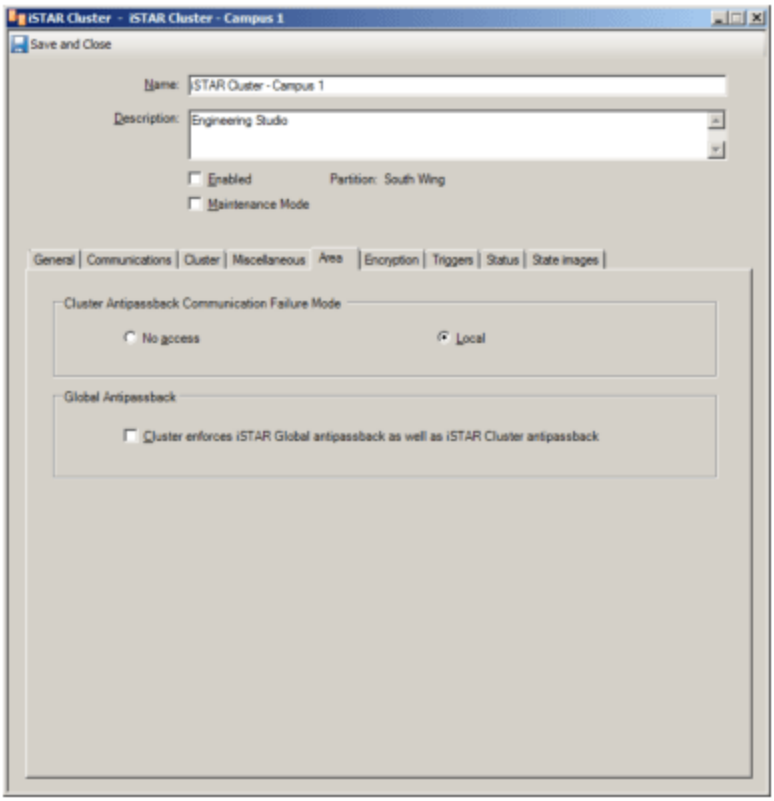
iSTAR Global Antipassback gives a higher level of security, but also means that when a person's card moves from one Cluster to another, the card must be transferred through the Host. Transfer through the Host is slower than within a Cluster and also requires the Cluster to Host network connections to be good. Access within the Cluster is faster since it only relies on the member-to-master network connections.

For more information on Areas and Antipassback, see the *C•CURE 9000 Areas and Zones Configuration Guide*.

To Configure the iSTAR Cluster - Area Tab for Cluster Antipassback Communications Failure Mode

1. From the **iSTAR Cluster** dialog box, click the **Area** tab. The **Area** tab opens, shown in Figure 30 on Page 103.

Figure 30: iSTAR Cluster Area Tab



2. In the **Cluster Antipassback Communication Failure Mode** box, click to select either the **No access** or **Local** option.

NOTE Make sure that you leave the **Cluster enforces iSTAR Global antipassback as well as iSTAR Cluster antipassback** check box **unselected**.

To Configure the iSTAR Cluster - Area Tab for both Global Antipassback and Cluster Antipassback

1. From the **iSTAR Cluster** dialog box, click the **Area** tab. The **Area** tab opens, shown in Figure 30 on Page 103.
2. In the **Global Antipassback** box, click to select the **Cluster enforces iSTAR Global antipassback as well as iSTAR Cluster antipassback** option.

Area Tab Field Definitions

Area tab definitions are listed in Table 8 on Page 104.

Table 8: Area Tab Definitions

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 (Hard)	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.)
Local (Soft)	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.
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.

iSTAR Cluster Encryption Tab

This tab allows you to configure the encryption mode for an Encrypted Cluster.

NOTE This tab is Read-only for a Non-encrypted Cluster, and does not apply. Non-encrypted Clusters do not use 256 bit AES (FIPS 197) encryption.

The iSTAR eX, iSTAR Edge, and encrypted iSTAR Ultra controllers always use 256-bit AES (FIPS 197) encryption by default.

The Encryption options on the iSTAR Cluster **Encryption** tab let you choose the FIPS 140-2 method for an Encrypted Cluster. The options on the iSTAR Cluster Encryption tab are only available for iSTAR Encrypted Clusters.

NOTE The 256 bit AES (FIPS 197) encryption method satisfies the Proprietary Burglar Alarm application requirements.

FIPS 140-2 mode requires a custom certificate key, either host based or controller based. Software House recommends a controller based certificate key. Once you set the cluster to FIPS 140-2 compliant mode, the iSTAR encrypted controllers will be in "dark mode." They will not be visible on the network.

NOTE Software House recommends that you configure the Tamper Input for a 'dark mode' controller to trigger an Alarm Event that will be displayed on the Monitoring State if the input changes state.

To Configure FIPS 140-2 Encryption for an iSTAR Encrypted Cluster

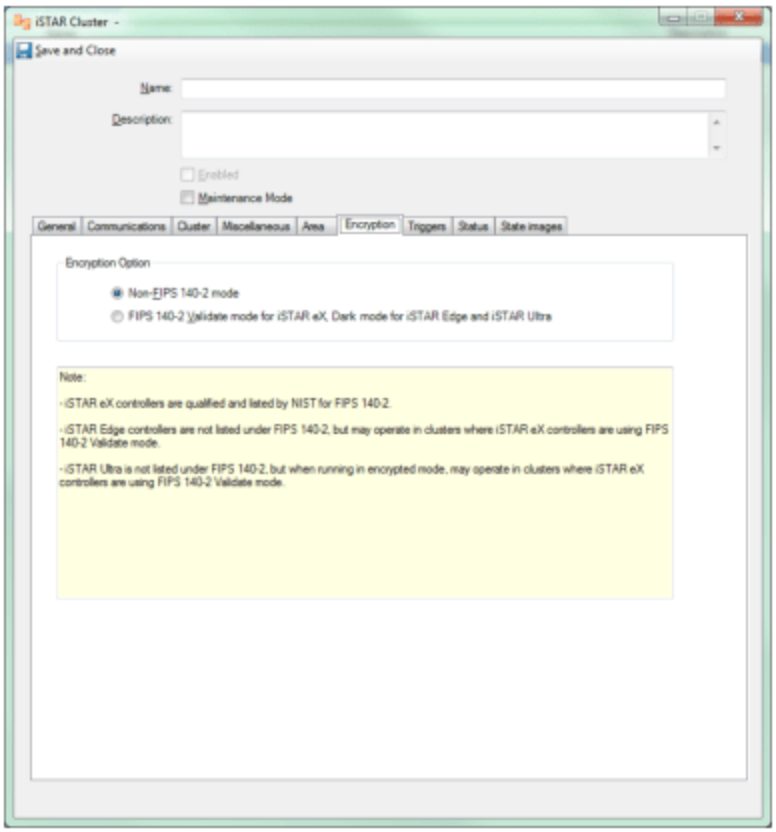
1. Open the **Encryption Options** dialog box in the **Options and Tools** pane and select from the following options:
   - **Controller-Based Encryption Mode**
   - **Host-Based Encryption Mode**
2. To use FIPS 140-2 mode, Software House recommends that you use the Controller-Based Encryption Mode.

NOTE Software House recommends Controller-based Encryption for 2 reasons:

1. Host-based Encryption requires a private key to be transmitted to the controllers non-encrypted. Controller-based Encryption does not. The tradeoff is that the controller-based method requires a signature at the host that recognizes the iSTAR to be valid.
2. The second reason is that it is much easier to recover from a controller-based error situation than to recover from a host-based area. Host based recovery of encryption keys is more difficult.

3. For more information, see the *C•CURE 9000 System Maintenance Guide* and the *iSTAR Installation and Configuration Guide*.
4. From the iSTAR Cluster dialog box, click the **Encryption** tab. The **Encryption** options are shown in Figure 31 on Page 106.

Figure 31: iSTAR Cluster Encryption Tab



5. Select from the available Encryption modes: **Non-FIPS 140-2** and **FIPS 140-2**.
6. Navigate to the **Triggers** tab or **Save and Close** to save the cluster and begin configuring iSTAR Controllers.

NOTE FIPS 140-2 compliant mode has not been evaluated by UL.

iSTAR Cluster Triggers Tab

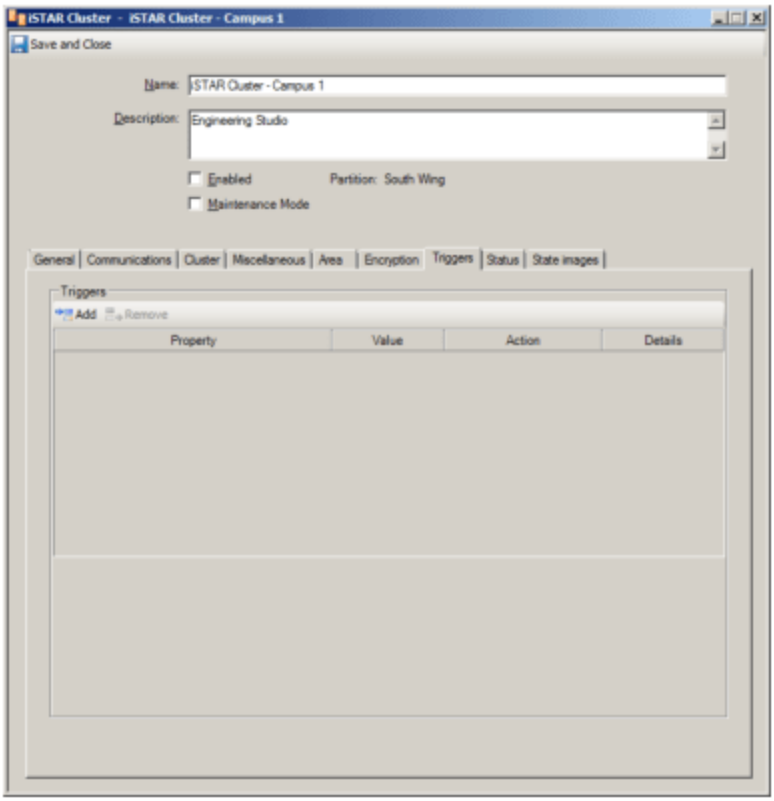
C•CURE 9000 uses **Triggers**, which are configured procedures used for activating security actions. A Trigger automatically executes a specified **Action** when a particular predefined condition occurs. When a Trigger is defined, the Actions available depend on the property selected. This section illustrates the use of Triggers to monitor a cluster master power failure.

NOTE The Triggers tab is not available for iSTAR Pro or iSTAR Ultra SE Pro Mode dialup configurations.

To Configure the iSTAR Cluster Triggers Tab

1. Navigate to the **Triggers** tab, shown in Figure 33 on Page 108.

Figure 32: iSTAR Cluster Triggers Tab



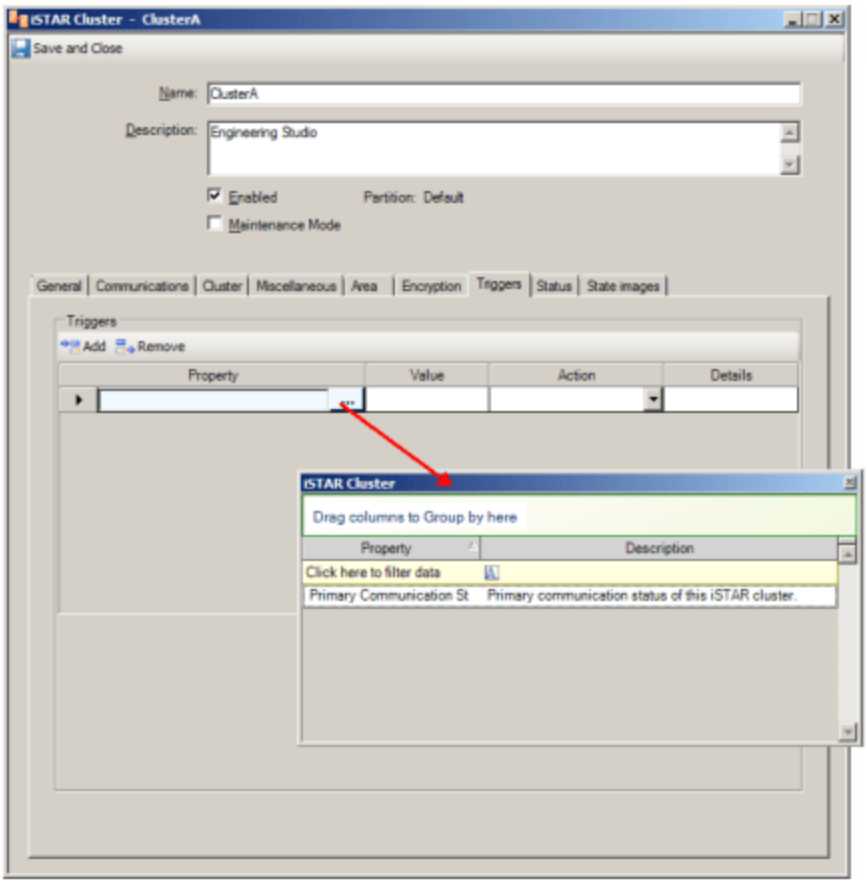
This tab provides you with ability to define the activation/deactivation, enable/disable, and arm/disarm, etc. of such objects as: events, inputs, outputs, camera actions, door status changes, etc. Triggers can also be used to launch events which also can be used to launch imports and exports, email and reports, viewer and message displays, personnel ID number state changes, controller downloads, sound activation, communication notifications, etc.

2. Click **Add** in the **Triggers** tab to create a new trigger.
   a. Click within the **Property** column to display [...].

      When you select this button, the **Property** browser opens presenting properties available for the controller.

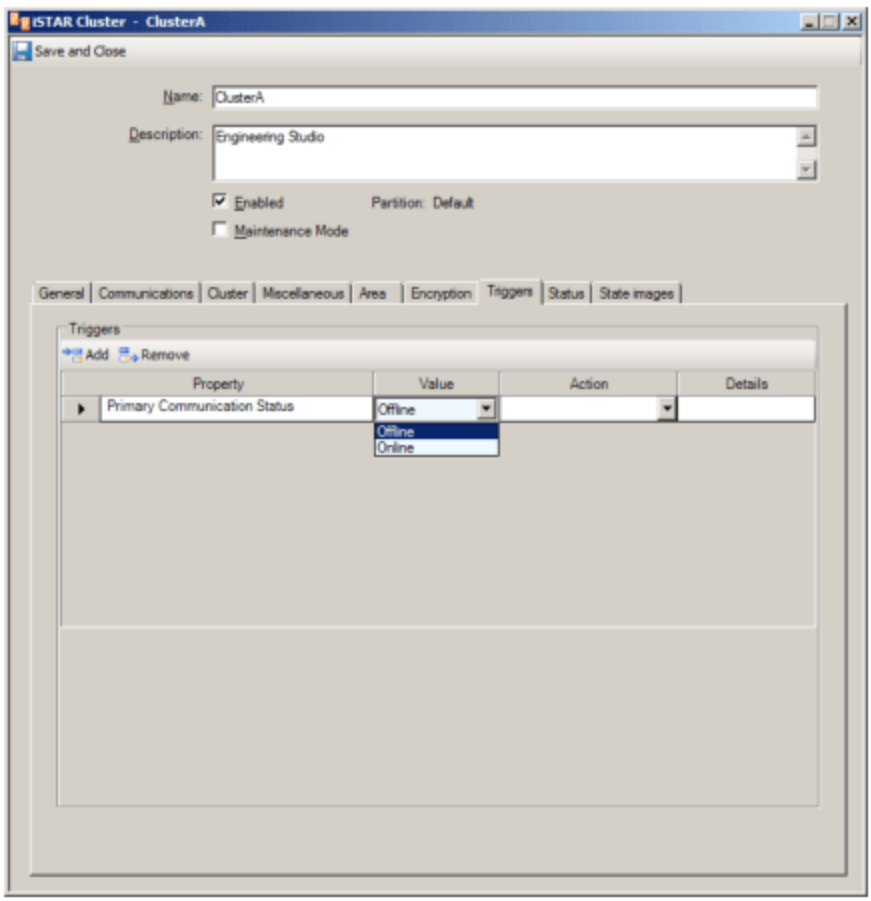
   b. Click a **Property** to select it and add it to the column (see Figure 33 on Page 108).

Figure 33: iSTAR Cluster Triggers Tab - Property Selection



c. Click within the **Value** column to display a drop-down list of Values associated with the **Property** that you have selected. Then click on a **Value** that you want to include as a parameter for the trigger to add it to the column (see Figure 34 on Page 109).

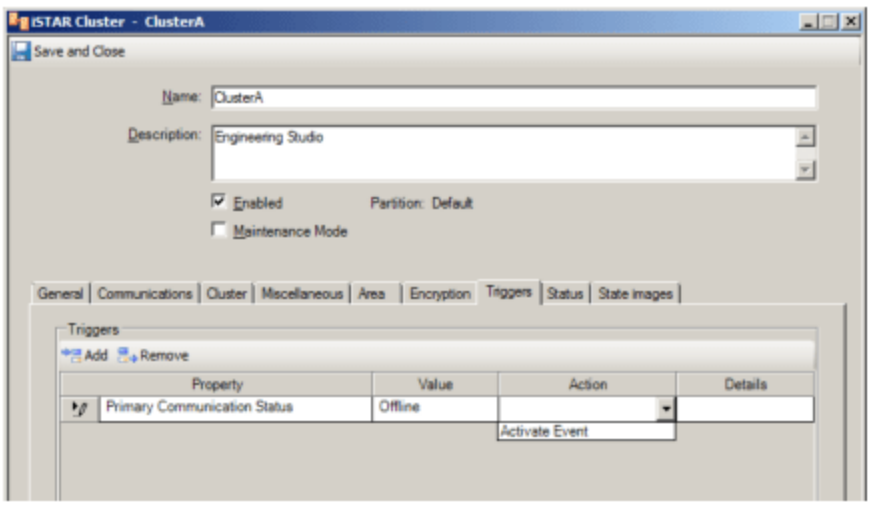
Figure 34: iSTAR Cluster Triggers Tab - Value



When a **Trigger** is added, an **Action** must be configured in the Action column. This is the Action that will occur when the object's selected **Property** receives the selected **Value**.

d. Click within the column to display a drop-down list of valid actions. Click an **Action** that you want to include as a parameter for the trigger to add it to the column (see Figure 35 on Page 110).

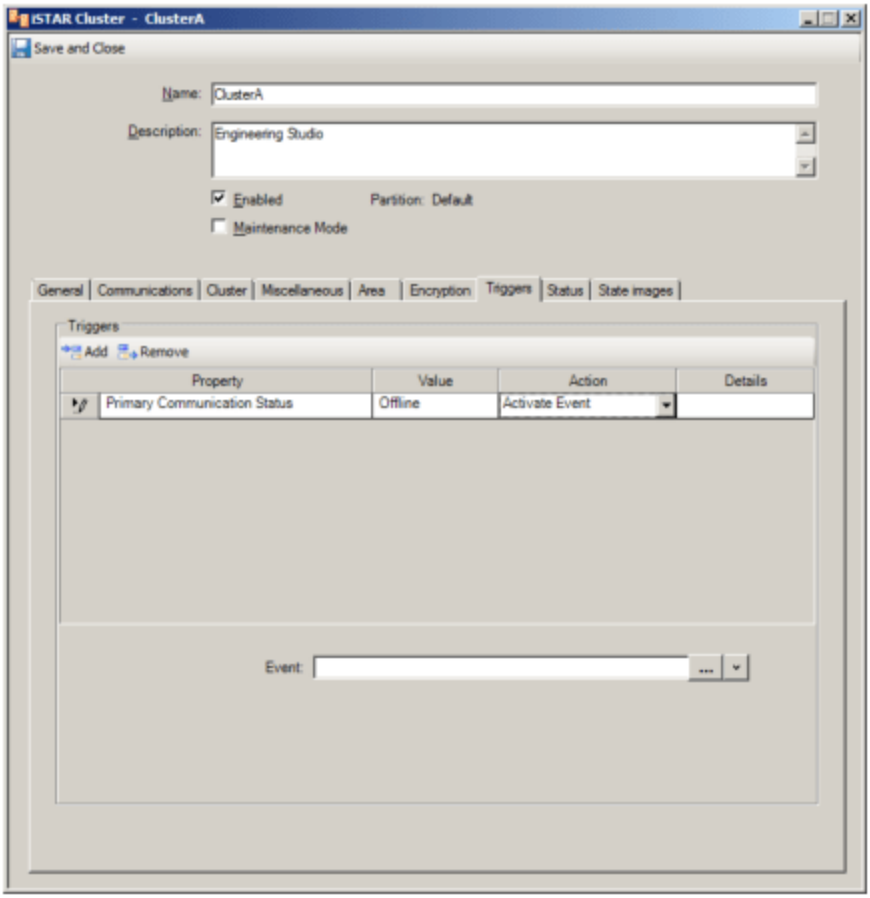
Figure 35: iSTAR Cluster Triggers Tab - Action



As the Action is selected, the lower pane in the Triggers box displays a corresponding entry field, or group of entry fields, specific to the selected Action, such as an Event or Output (see Figure 36 on Page 110).

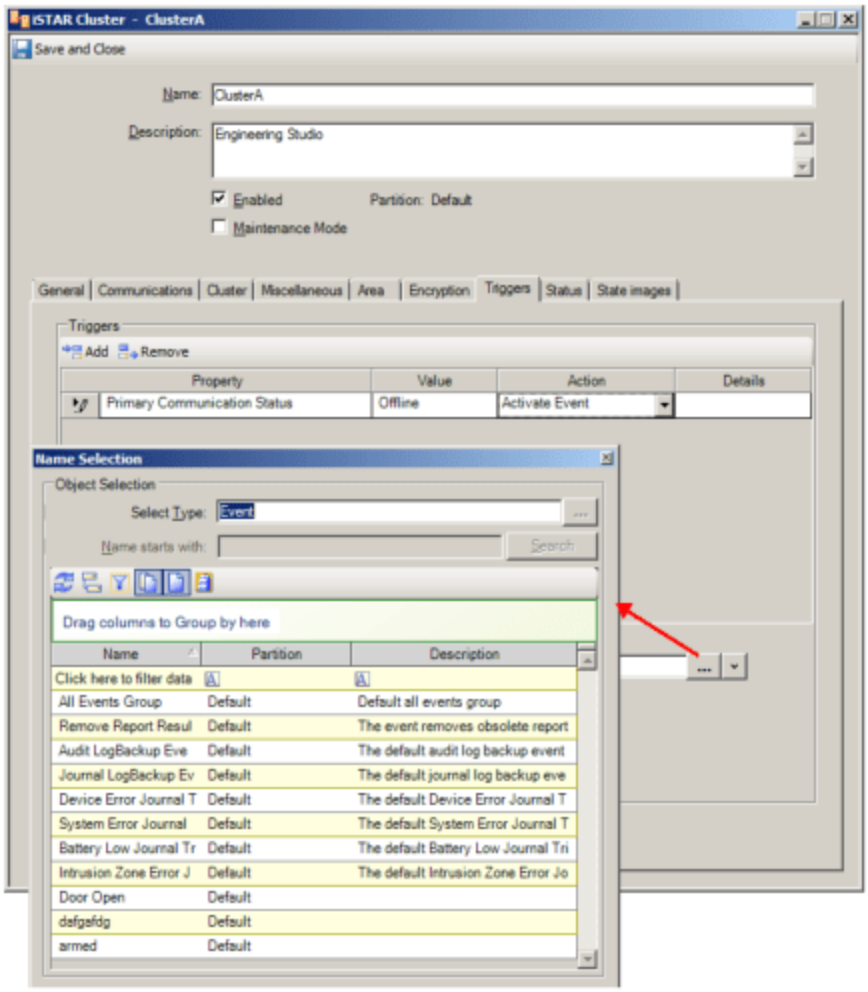
In the case of the **Primary Communications Status Property**, the available **Action** is to activate an event.

Figure 36: iSTAR Cluster Triggers Tab - Action Event



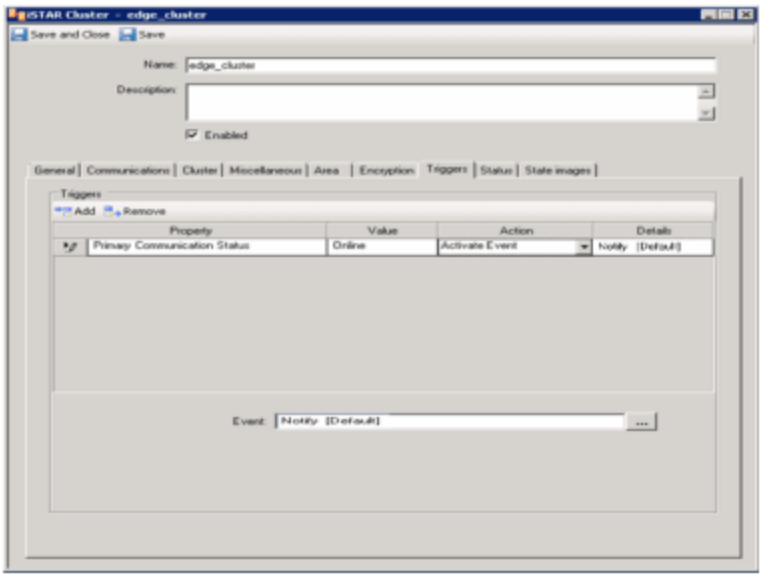
e. In the **Event** field, click [...] to select a **Event** that you want to associate with the trigger (see Figure 37 on Page 111). Events are created in the Configuration Pane. See the *C•CURE 9000 Software Configuration Guide* for more information.

Figure 37: iSTAR Cluster Triggers Tab - Event Selection



Once the field (or group of fields) is completed, the **Details** column will show information about how the Action has been configured.

Figure 38: iSTAR Cluster Triggers Tab - Finished



NOTE To activate or arm iSTAR Cluster events by a trigger condition, the schedule value is restricted to **Always**.

3. To Remove a Trigger, select the row using the button and click **Remove**.

   A completed Trigger that notifies you of communications failure in the cluster is shown in Figure 38 on Page 112.

4. Navigate to the **Status** tab or **Save and Close** to save the cluster and begin configuring iSTAR Controllers.

iSTAR Cluster Dialup Configuration Tab

The **Dialup Configuration** tab is used to configure a cluster to use dial-up on the iSTAR Pro or Ultra SE Pro Mode controller.

See Chapter 3: Configuring Dialup for the dial-up configuration sequence to follow and configuration information.

iSTAR Cluster Status Tab

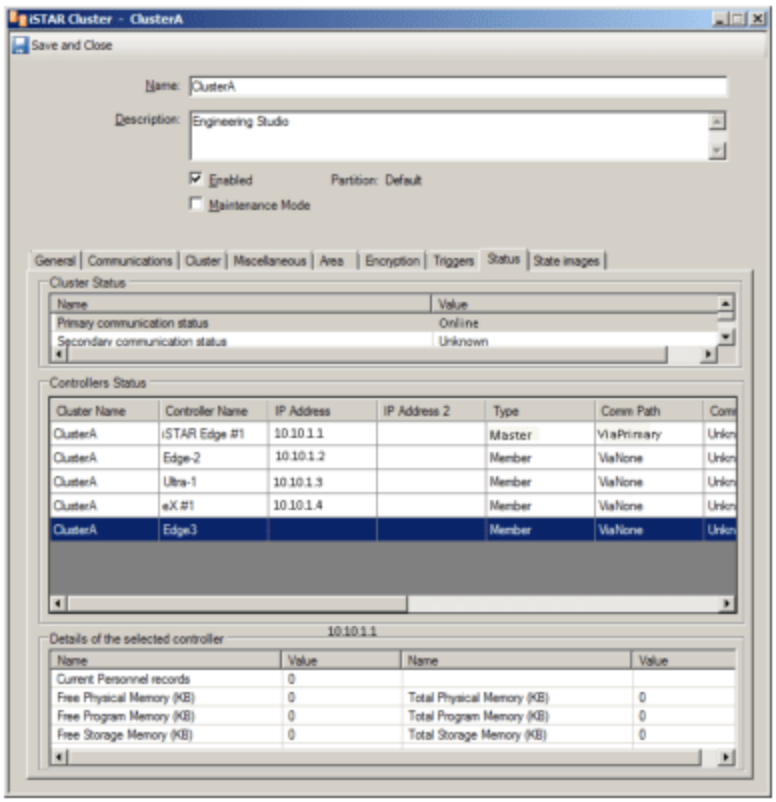
The **Status** tab provides a read-only listing of critical information about the operational status of the iSTAR controllers associated with the cluster. Such information includes:

- Cluster Name
- Controller Name
- IP Address
- IP Address 2
- Type
- Comm Path
- Comm State
- Conn Path
- Boards State
- Panel State
- Firmware Version
- Board Type

The **Details of the selected controller section** displays the same status fields that are displayed on that controller's Status tab. For more information on the status fields that are displayed for each controller type, see the iSTAR Controller Status Tab on Page 147.

The **Status** tab is shown in Figure 39 on Page 114.

Figure 39: iSTAR Cluster Status Tab



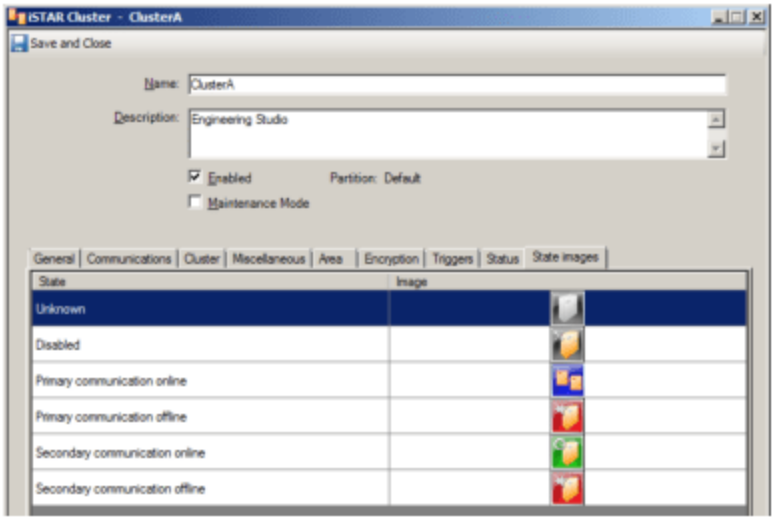
Using the Cluster Status Tab

1. The **Cluster Status** box displays Communications Status values for the iSTAR Cluster.
2. When you select an iSTAR Controller within the **Controllers Status** list, its status values are displayed in the **Details of selected controller** box.
3. Navigate to the **State Images** tab or **Save and Close** to save the cluster and begin configuring iSTAR Controllers.

iSTAR Cluster State Images Tab

The **State Images** tab, shown in Figure 40 on Page 115, provides a means to change the default images used to indicate Cluster states that are displayed in the Monitoring Station.

Figure 40: iSTAR Cluster State Images Tab



To Change an Image

1. Double-click the existing image.

   A **Windows Open** dialog box appears allowing you to browse for a folder in which you have placed replacement images.

2. When you locate the replacement image, select it to add it to the image listing.
3. To restore the default image, right-click the new image and select **Restore Default**.
4. Click **Save and Close** to save changes to the cluster state images.

5

Configuring C•CURE iSTAR Controllers

The C•CURE iSTAR controller is an intelligent controller for networked security systems. C•CURE iSTAR controllers communicate with the C•CURE 9000 server (acting as a database and journal host) and the system security hardware, providing direct control of events and system activity. This chapter explains how to configure iSTAR controllers, and the devices related to them, in the C•CURE 9000 System.

In this chapter

Understanding C•CURE iSTAR Controllers

The iSTAR controller is an intelligent, network-ready controller for security systems. The heart of the iSTAR controller is the **General Controller Module** (**GCM**) - an embedded microprocessor-based controller card. Add-on **Access Control Modules** (**ACM Boards**) provide access control functionality by supporting readers, outputs, and inputs. The iSTAR Ultra, Pro, and eX also support Schlage wireless readers and the Ultra also supports Assa Abloy Aperio wireless readers.

To install and configure the controller hardware and its connected devices see the following manuals:

- *iSTAR Pro Installation and Configuration Guide*
- *iSTAR eX Installation and Configuration Guide*
- *iSTAR Edge Installation and Configuration Guide*
- *iSTAR Ultra Installation and Configuration Guide*
- *iSTAR Ultra SE Installation and Configuration Guide*

For information on configuring host and panel Events for an iSTAR controller, see the Events chapter in the *C•CURE 9000 Software Configuration Guide*.

The following sections provide the information you need to configure the iSTAR Controllers.

- iSTAR Controller Tasks on Page 124
- Configuration Overview for iSTAR Controllers on Page 119
- iSTAR Controller Editor on Page 137

Configuration Overview for iSTAR Controllers

Configuring the iSTAR controllers involves setting up the hardware and configuring the software components. See the *iSTAR Hardware Installation Guides* for instructions about setting up controllers and related hardware.

NOTE Before configuring a controller, make sure you know the MAC address of the controller NIC you are using. The MAC address is built into the GCM and cannot be changed. You can find a controller's MAC address(es) on a label attached to the GCM.

To Configure an iSTAR Controller

1. Create an iSTAR Controller (see Creating an iSTAR Controller on Page 124) or edit an existing iSTAR Controller (see Editing an iSTAR Controller on Page 126. The iSTAR Controller General tab appears, as shown in Figure 47 on Page 142.
2. On the iSTAR Controller **General** tab, configure the basic communications settings for the Controller, such as the MAC address, the primary and optional secondary network connections, and the Controller Time Zone.
3. Click on each of the tabs for attached devices, such as the **Boards** tab for iSTAR Classic/Pro Controllers, or the **Readers** tab for iSTAR eX Controllers, and configure the devices and their settings.
   - For iSTAR Classic/Pro Controllers, refer to the iSTAR Pro Configuration Summary on Page 119.
   - For iSTAR eX/Edge Controllers, refer to the iSTAR eX and iSTAR Edge Configuration Summary on Page 121.
   - For iSTAR Ultra, refer to the iSTAR Ultra Configuration Summary on Page 122.
4. Click on the iSTAR **Triggers** tab to configure actions that can activate Events, lock or unlock Doors, sound audible alarms, or a wide range of other security functions.
5. Click on the iSTAR **State** Images tab to customize the images that are displayed on the Monitoring Station to represent the Controllers.
6. Click **Save and Close** to save your settings.

NOTE When using a multi-homed 9000 standalone server with multiple network adapters on multiple networks, use the VINCA IP address of the adapter selected for IP communication to ensure consistent communication with the iSTAR fast personnel download. Set the VINCA IP address as the host address for the iSTAR controllers and in the Options & Tools > System Variables > VINCA IP address field. Then restart the drivers.

iSTAR Pro Configuration Summary

Table 9 on Page 119 provides a summary of the tasks involved in configuring an iSTAR Pro Controller.

Table 9: iSTAR Pro Configuration Summary

Step	Task	Reference
1.	Create and save an iSTAR Pro Cluster for the Controller.	Creating an iSTAR Cluster on Page 88

Table 9: iSTAR Pro Configuration Summary (continued)

Step	Task	Reference
2.	Create an iSTAR Pro Controller under the iSTAR Cluster in the Hardware Tree.	Creating an iSTAR Controller on Page 124
3.	Use the iSTAR Controller General tab to configure the basic communications settings for the Controller and to assign Reader LCD Message Sets.	iSTAR Controller General Tab on Page 141
4.	Use the Boards tab to create and configure Inputs, Outputs, and ACM boards for the Controller.	iSTAR Controller Boards Tab (iSTAR Classic/Pro) on Page 156
5.	Open the iSTAR ACM Board Editor to create Inputs, Outputs, and Readers for the Controller.	iSTAR Classic/Pro Controller ACM Board Editor on Page 197
6.	Use the ACM Board Inputs tab to create Inputs.	iSTAR ACM Board Inputs Tab on Page 198
	• Click ... to open the iSTAR Input Editor to configure each Input.	iSTAR Input Editor on Page 232
7.	Use the ACM Board Outputs tab to create Outputs.	iSTAR ACM Board Outputs Tab on Page 199
	• Click ... to open the iSTAR Output Editor to configure each Output.	iSTAR Output Editor on Page 241
8.	Use the ACM Board Readers tab to create Readers.	iSTAR ACM Board Readers Tab on Page 200
	• Click ... to open the iSTAR Reader Editor to configure each Reader.	iSTAR Reader Editor on Page 248
9.	Use the ACM Board ACM EXT tab to create Input and Output Boards.	iSTAR ACM Board ACM Ext Tab on Page 201
10.	Use the iSTAR Input Board Editor to Configure an iSTAR Input Board.	iSTAR Input Board Editor on Page 203
	• Click ... to open the iSTAR Input Editor to configure each Input.	iSTAR Input Editor on Page 232
11.	Use the iSTAR Output Board Editor to Configure an iSTAR Output Board.	iSTAR Output Board Editor on Page 208
	• Click ... to open the iSTAR Output Editor to configure each Output.	iSTAR Output Editor on Page 241
12.	If you have Schlage Wireless PIMs and Readers, use the Schlage Wireless PIMs tab to configure these devices.	iSTAR Schlage Wireless PIMs Tab on Page 153
13.	From the Hardware Tree, create iSTAR Door objects for the Controller.	iSTAR Door Editor on Page 427
14.	From the Hardware Tree, create iSTAR Elevator objects for the Controller.	iSTAR Elevators on Page 505
15.	Use the iSTAR Triggers tab to create new triggers for the Controller.	iSTAR Controller Triggers Tab on Page 147
16.	Use the iSTAR State Images tab to customize the state images that are displayed on the Monitoring Station for the iSTAR Controller.	iSTAR Controller State Images Tab on Page 152

iSTAR eX and iSTAR Edge Configuration Summary

Table 10 on Page 121 provides a summary of the tasks involved in configuring an iSTAR eX or iSTAR Edge Controller.

Table 10: iSTAR eX/Edge Configuration Summary

Step	Task	Reference
1.	Create and save an iSTAR eX/Edge Cluster for the Controller.	Creating an iSTAR Cluster on Page 88
2.	Create an iSTAR eX/Edge Controller under the iSTAR Cluster in the Hardware Tree.	Creating an iSTAR Controller on Page 124
3.	Use the iSTAR Controller General tab to configure the basic communications settings for the Controller and to assign Reader LCD Message Sets.	iSTAR Controller General Tab on Page 141
4.	Use the iSTAR Controller Inputs tab to create the Inputs on the Controller.	iSTAR eX and Edge Controller Inputs Tab on Page 159
	• Click ... to open the iSTAR Input Editor to configure each Input.	iSTAR Input Editor on Page 232
5.	Use the iSTAR Controller Outputs tab to create the Outputs on the Controller.	iSTAR Edge/eX Controller Outputs Tab on Page 164
	• Click ... to open the iSTAR Output Editor to configure each Output.	iSTAR Output Editor on Page 241
6.	Use the iSTAR Controller Wiegand tab to create the direct connect Wiegand Readers on the Controller.	iSTAR eX Controller Wiegand Tab on Page 171
	• Click ... to open the iSTAR Reader Editor to configure each Reader.	iSTAR Reader Editor on Page 248
7.	Use the iSTAR Controller tabs to create the Input Boards, Output Boards, and Readers on the Controller.	iSTAR eX COM1/COM2 Tabs on Page 173 iSTAR Edge COM1/COM2/COM3 Tabs on Page 167
8.	Use the iSTAR Input Board Editor to Configure an iSTAR Input Board.	iSTAR Input Board Editor on Page 203
	• Click ... to open the iSTAR Input Editor to configure each Input.	iSTAR Input Editor on Page 232
9.	Use the iSTAR Output Board Editor to Configure an iSTAR Output Board.	iSTAR Output Board Editor on Page 208

Table 10: iSTAR eX/Edge Configuration Summary (continued)

Step	Task	Reference
	• Click ... to open the iSTAR Output Editor to configure each Output.	iSTAR Output Editor on Page 241
10.	Click ... to open the iSTAR Reader Editor to configure each Reader.	iSTAR Reader Editor on Page 248
11.	If you have Schlage Wireless PIMs and Readers, open the iSTAR PIM-485 Board editor to configure these devices.	iSTAR PIM-485 Board Editor on Page 226
12.	From the Hardware Tree, create iSTAR Door objects for the Controller.	iSTAR Door Editor on Page 427
13.	From the Hardware Tree, create iSTAR Elevator objects for the Controller.	iSTAR Elevators on Page 505
14.	Use the iSTAR Triggers tab to create new triggers for the Controller.	iSTAR Controller Triggers Tab on Page 147
15.	Use the iSTAR State Images tab to change the images that display on the Monitoring Station for the iSTAR Controller. You can substitute a .JPG image for any of the default state images.	iSTAR Controller State Images Tab on Page 152

iSTAR Ultra Configuration Summary

Table 11 on Page 122 provides a summary of the tasks involved in configuring a iSTAR Ultra Controller.

Table 11: iSTAR Ultra Configuration Summary

Step	Task	Reference
1	Create and save an iSTAR Ultra Cluster for the Controller.	Creating an iSTAR Cluster on Page 88
2	Create an iSTAR Ultra Controller under the iSTAR Cluster in the Hardware Tree.	Creating an iSTAR Controller on Page 124
3	Use the iSTAR Controller General tab to configure the basic communications settings for the Controller and to assign Reader LCD Message Sets.	iSTAR Controller General Tab on Page 141
4	Use the Boards tab to create and configure Inputs, Outputs, and ACM boards for the Controller.	iSTAR Controller Boards Tab (iSTAR Classic/Pro) on Page 156
5	Open the iSTAR ACM Board Editor to create Inputs, Outputs, and Readers for the Controller.	iSTAR Classic/Pro Controller ACM Board Editor on Page 197
6	Use the ACM Board Inputs tab to create Inputs.	iSTAR ACM Board Inputs Tab on Page 198
7	Click ... to open the iSTAR Input Editor to configure each Input.	iSTAR Input Editor on Page 232
8	Use the ACM Board Outputs tab to create Outputs.	iSTAR ACM Board Outputs Tab on Page 199
9	Click ... to open the iSTAR Output Editor to configure each Output.	iSTAR Output Editor on Page 241

Table 11: iSTAR Ultra Configuration Summary (continued)

Step	Task	Reference
10	Use the ACM Wiegand tab to create Wiegand-connected Readers.	iSTAR Ultra ACM Board Wiegand Tab on Page 184
11	Click ... to open the iSTAR Reader Editor to configure each Reader.	iSTAR Reader Editor on Page 248
12	Use the ACM Board RS-485 tab to create RS-485 Ports for Readers.	iSTAR Ultra ACM Board RS-485 Tab on Page 186
13	Click ... to open the iSTAR Device Port Editor to configure each RS-485 Reader and related Inputs.	iSTAR Ultra ACM RS-485 Device Port Editor on Page 188
14	Use the ACM Board RS-485 Device Port Reader tab to configure RS-485 Readers.	iSTAR Ultra RS-485 Device Port Readers Tab on Page 190
15	Use the ACM Board RS-485 Device Port ACM Ext tab to configure Input and Output Boards.	iSTAR Ultra RS-485 Device Port ACM EXT Tab on Page 192
16	Use the iSTAR Input Board Editor to Configure an iSTAR Input Board.	iSTAR Input Board Editor on Page 203
17	Click ... to open the iSTAR Input Editor to configure each Input.	iSTAR Input Editor on Page 232
18	Use the iSTAR Output Board Editor to Configure an iSTAR Output Board.	iSTAR Output Board Editor on Page 208
19	Click ... to open the iSTAR Output Editor to configure each Output.	iSTAR Output Editor on Page 241
20	Click the Com1 and Com2 tab to configure Aperio Hubs	iSTAR Ultra COM1/COM2 Tabs on Page 181
	Click ... to open the iSTAR Aperio RS-485 Hub Board editor to configure the Communications Fail Input and iSTAR Aperio Readers.	iSTAR Aperio RS-485 Hub Board Editor (iSTAR Ultra only) on Page 220
	Click ... to open the iSTAR Aperio Reader editor to configure iSTAR Aperio readers.	iSTAR Aperio Reader Editor on Page 264
	From the Hardware Tree, create iSTAR Door objects for your Controller.	iSTAR Door Editor on Page 427
	From the Hardware Tree, create iSTAR Elevator objects for your Controller.	iSTAR Elevators on Page 505
	Use the iSTAR Triggers tab to create new triggers for your Controller.	iSTAR Controller Triggers Tab on Page 147
	Use the iSTAR State Images tab to customize the state images that are displayed on the Monitoring Station for your iSTAR Controller.	iSTAR Controller State Images Tab on Page 152

iSTAR Controller Tasks

You can perform the following tasks to manage iSTAR Controllers.

Creating an iSTAR Controller

You can create a new iSTAR Controller only within an iSTAR Cluster of the appropriate type.

NOTE The iSTAR Ultra S1-1 encryption switch enables FIPS 197 AES 256-bit encryption. The switch setting must match the software configuration of the cluster and the controller. See the *iSTAR Ultra Installation and Configuration Guide* for more information.

To Create a iSTAR Controller

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Navigate to the Hardware folder that contains the iSTAR Cluster in which you want to create the new Controller.
3. Select the iSTAR Cluster and right-click to display the context menu.
4. Select the controller you wish to create:

NOTE For an iSTAR Ultra SE in Pro Mode, select **iSTAR Pro Controller**.

   - For an Encrypted Cluster, you can select:
     - **iSTAR Edge Controller>New**
     - **iSTAR eX Controller>New**
     - **iSTAR Ultra Controller>New**
   - For a Non-encrypted Cluster, you can select:
     - **iSTAR Classic Controller>New**
     - **iSTAR Pro Controller>New**
     - **iSTAR Ultra Controller>New**

   The iSTAR Controller Editor opens to allow you to configure the Controller (see iSTAR Controller General Tab on Page 141).
5. Type a unique name for the controller in the **Name** field.
6. Type a textual description (optional) in the **Description** field.

7. Enter the MAC Address of the iSTAR Controller in the MAC Address field (if you do not, you will receive an error when you try to save the Controller).
8. To save the new iSTAR controller, click **Save and Close**.

Creating a Controller Template

You can create a template for an iSTAR Controller. A Controller Template saves you time because you can save the configuration settings and re-use the template to create new Controller objects with the those settings pre-defined.

To Create a Controller Template

1. In the Navigation pane of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Navigate to the Hardware folder that contains the iSTAR Cluster in which you want to create the new Controller Template.
3. Select the iSTAR Cluster and right-click to display the context menu.
4. Select the iSTAR controller you wish to create a template for:
   - **iSTAR Edge Controller>New Template**.
   - **iSTAR eX Controller>New Template**.
   - **iSTAR Classic Controller>New Template**.
   - **iSTAR Pro Controller>New Template**.
   - **iSTAR Ultra Controller>New Template**.
5. The iSTAR Controller Editor opens a new Template.
6. Configure any settings you want to include in the Template.
7. To save the new iSTAR Controller Template, click **Save and Close**.

The new Controller template appears under —- *Templates* in the iSTAR Controller context menu drop-down list in the Hardware tree.

To Create an iSTAR Controller from a Template

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Navigate to the Hardware folder that contains the iSTAR Cluster in which you want to create the new Controller.
3. Select the iSTAR Cluster and right-click to display the context menu.
4. Select **iSTAR Controller** and click the Template you want to use from the context menu.
5. The iSTAR Controller Editor opens so that you can edit the new Controller. The settings from your Template are already configured.
6. Configure any additional settings. See Configuration Overview for iSTAR Controllers on Page 119 for more information.
7. To save the new iSTAR Controller, click **Save and Close**.

Deleting an iSTAR Controller

You can delete an iSTAR Controller from the Hardware tree, or one or more iSTAR Controllers from a Dynamic View.

To Delete an iSTAR Controller from the Hardware Tree

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Navigate to the iSTAR Cluster that contains the Controller that you want to delete.
3. Right-click on the iSTAR Controller that you want to delete and select **Delete** from the context menu.
4. Click **Yes** in the "**Are you sure you want to delete the selected iSTAR Controller object?**" message box. A dialog box appears showing the progress of the deletion.
5. When the object has been deleted, click one of the following buttons:
   - **OK** to close the dialog box.
   - **Print** to print the deletion message.
   - **Email** to send the deletion message to the email address you have configured in the Customer Support section of the C•CURE 9000 System Variables.

To Delete iSTAR Controllers from a Dynamic View

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Select iSTAR **Controller** from the **Hardware** pane drop-down list.
3. Click  to open a **Dynamic View** showing all **iSTAR Controller** objects.
4. Select one or more iSTAR controllers from the Dynamic View list of iSTAR Controllers.
5. Right-click one of the **Controllers** in the list that you want to delete and select **Delete** from the context menu.
6. Click **Yes** in the "**Are you sure you want to delete the selected iSTAR Controller object(s)?**" message box. A dialog box appears showing the progress of the deletion(s).
7. When the object(s) have been deleted, click one of the following buttons:
   - **OK** to close the dialog box.
   - **Print** to print the deletion message.
   - **Email** to send the deletion message to the email address you have configured in the Customer Support section of the C•CURE 9000 System Variables.

Editing an iSTAR Controller

You can edit an iSTAR Controller to change settings or add new Input, Output, or Reader objects to the Controller.

To Edit an Controller or Board

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Select **iSTAR Controller** from the **Hardware** pane drop-down list.

3. Click to open a **Dynamic View** showing all iSTAR Controller objects.
4. Double-click the **Controller** in the list that you want to modify and select **Edit** from the context menu. The iSTAR Controller editor opens (see iSTAR Controller Editor on Page 137).
5. See Configuration Overview for iSTAR Controllers on Page 119 for information about how to use the iSTAR Controller Editor to configure your iSTAR Controller.

Viewing a List of iSTAR Controllers

You can view a list of iSTAR Controllers in a Dynamic View.

To View a List of iSTAR Controllers

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Select iSTAR Controller from the **Hardware** pane drop-down list.
3. Click to open a **Dynamic View** showing all iSTAR Controller objects
4. You can filter, group, and print the list of iSTAR Controllers in the Dynamic View. See the *C•CURE 9000 Data Views Guide* for more information about using the features provided by Dynamic Views.
5. You can select one or more Controllers in the list (using **CTRL+Left-click** or **SHIFT+Left-click** for multiple selection) and right-click to display a context menu (see Viewing a List of iSTAR Controllers on Page 127).

Using the iSTAR Controller Context Menu

To access the controller context menu, right-click on a controller in the Hardware tree or in the Dynamic View.

The selections described in Table 1 on Page 127 are not available for all controllers.

Table 1: iSTAR Controller Context Menu

Selection	Description
Edit	Click this menu selection to edit the selected iSTAR Controller. The iSTAR Controller editor opens. You can rename the iSTAR Controller, change its description, and any other attributes.
Delete	Click this menu selection to delete the selected iSTAR Controller(s). A prompt appears asking you to confirm that you want to delete the iSTAR Controller. Click **Yes** to delete the Input or **No** to cancel the deletion. When you delete an iSTAR Controller, all of the child objects you have defined for the Controller are also deleted.

Table 1: iSTAR Controller Context Menu (continued)

Selection	Description
Set Property	Click this menu selection to change the value of a property in the selected controller(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 change the value of the following iSTAR Controller properties: • **Description** – You can change the textual description of the iSTAR Controller(s) by selecting this property and typing in a new value. • **Enabled** – You can determine whether or not the iSTAR Controller(s) are enabled to communicate to the Administration or Monitoring Station by selecting this property and selecting/clearing the value check box. • **Power Suppression** – Allows you to select or clear this value for the selected controller. See Using Set Property for an iSTAR Controller on Page 130.
Add to Group	Click this menu selection to add the iSTAR Controller to a Group.A dialog box listing the iSTAR Controller Groups in the system appears. Click on a Group in the list to add the iSTAR Controller(s) to that Group. See Add a Hardware Device to Group from a Dynamic View on Page 409.
Export Selection	Opens an Export dialog box from which you can export one or more records displayed in a Dynamic View to either an XML or a CSV file. This allows you to quickly and easily create XML/CSV reports on selected C•CURE 9000 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. 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. **Example:** \\Computer Name\Program Files\Software House\SWHouse\SWHSystem\Export.
Find in Audit Log	Opens 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 Controller. The results display in a separate Dynamic View. This selection is not available if you select multiple Controllers.
Update Firmware	Updates the firmware for an iSTAR controller. See Updating iSTAR Firmware (Ethernet Connections) on Page 130 and Updating iSTAR Firmware (Dial-up Connections) on Page 132. NOTE: If you are using dial-up to update the firmware, you must manually connect to the iSTAR before Update Firmware is visible in the context menu.

Table 1: iSTAR Controller Context Menu (continued)

Selection	Description
Find in Journal	Opens 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 Controller. The results display in a separate Dynamic View. This selection is not available if you select multiple Controllers.
Perform Full Controller Download	Downloads configuration and personnel records appropriate to the controller.
Diagnostics	Opens the iSTAR Diagnostics System web page for this Controller, providing you with the controller's status. This selection is not available if you select multiple Controllers.
Turn Maintenance Mode On	Opens the Maintenance Mode dialog box to put the iSTAR Controller and/or its components into Maintenance Mode. See Chapter 2: Maintenance Mode for more information.
Turn Maintenance Mode Off	Opens the Maintenance Mode dialog box to take the iSTAR Controller and/or its components out of Maintenance Mode. See Chapter 2: Maintenance Mode for more information.
Copy & Paste	Used to make a duplicate of a Cluster and its Child Objects on the same partition on the same system. See Copying, Pasting, and Renaming Clusters and Controllers on Page 40.
Copy To	Used to make a duplicate of a Cluster and its Child Objects on a different partition on the same system, using **Paste From**. See Copying, Pasting, and Renaming Clusters and Controllers on Page 40.
Paste From	The **Copy To** and **Paste From** context menu selections can be used to duplicate Clusters and Children on another system. See Copying, Pasting, and Renaming Clusters and Controllers on Page 40.
Monitor	Click this menu selection to view activity for the selected iSTAR Controller(s), and any Add-on Board, Door, Elevator, Input, Output, Reader, and Trigger-with-target-Event children, on an Admin Monitor Activity Viewer. NOTE: Which Add-on Boards display on the Monitor—as well as which of their Input, Output, Reader, and Trigger-with-target-Event children—Depends on the Controller type and what is turned on. For more information, see "Monitoring an Object from the Administration Station" in the *C•CURE 9000 Getting Started Guide*.
Connect Dialup Panel	This menu selection is only available for an iSTAR using dialup (Pro/Ultra SE Pro Mode). Click to open the Manual Action dialog box to enter a starting time, ending time, and priority to connect using dialup. It is recommended that you set the **Start** and **End** time to maintain a connection for a minimum of two hours.
Reset Dial-up Panel	This menu selection is only available on an iSTAR Master using dialup (Pro/Ultra SE Pro Mode). Click to reboot the iSTAR controller.
Reset All IP-ACM Panels	Resets all IP-ACMs configured on the controller.
Hardware Tree Only:	

Table 1: iSTAR Controller Context Menu (continued)

Selection	Description
iSTAR Door	Click to configure a new door or a door template.
Elevator	Click to configure a new elevator or an elevator template.
iSTAR Input	Click to configure a new input or an input template.
Output	Click to configure a new output or an output template.
iSTAR Reader	Click to configure a new reader or a reader template.

Using Set Property for an iSTAR Controller

You can use **Set Property** to quickly set a property for a Controller without opening the iSTAR Controller Editor. **Set Property** allows you to select multiple Controllers in a Dynamic View and right-click to set a specific property for all of them. So, for example, if you wanted to change a setting for 20 Controllers, you could select all of them and do it in one step.

To Set a Property for an iSTAR Controller

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Select iSTAR Controller from the **Hardware** pane drop-down list.
3. Click  to open a **Dynamic View** showing all iSTAR Controller objects.
4. Select the iSTAR Controllers in the list for which you want to set a property, using multiple selection (CTRL+Left-click to select more than one Controller, or SHIFT+Left-click to select a range of Controllers) as needed.
5. Right-click a selected iSTAR **Controller** and select **Set Property** from the context menu.
6. Click  in the **Property** field to open a selection dialog box and select the property you want to set.
7. Enter the value for the property in the **Value** field and click **OK**.

Updating iSTAR Firmware (Ethernet Connections)

You can update the iSTAR firmware on iSTAR panels using Ethernet connections from either the Administration Client or the Monitoring Station client.

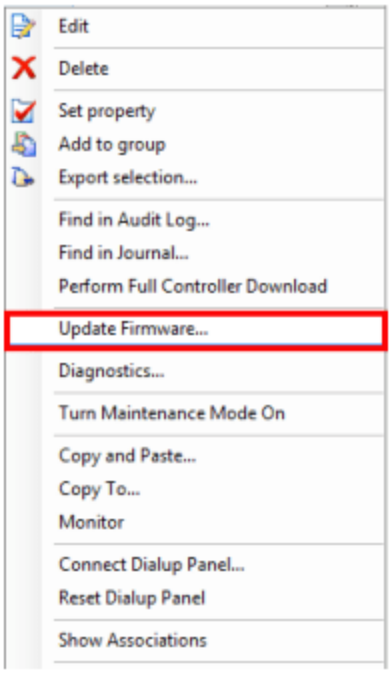
You can initiate a firmware update by right-clicking on the iSTAR controller:

- In the Hardware Tree
- In a Dynamic View in the Administration Client
- In the Status List - Controller in the Monitoring Station

To Update Firmware on an iSTAR Controller

1. Right-click on the controller and select **Update Firmware** from the context menu as shown in Figure 41 on Page 131.

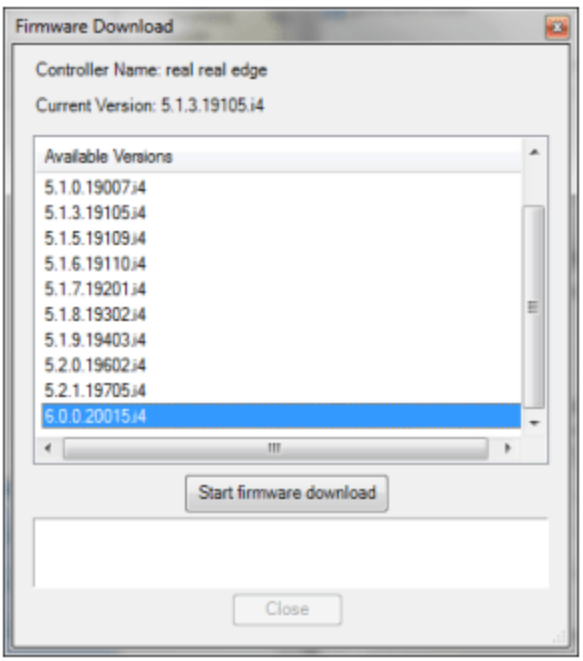
Figure 41: iSTAR Context Menu



NOTE Update Firmware will not appear on the context menu if the iSTAR is not Enabled or is off-line.

The Firmware Download dialog box, shown in Figure 42 on Page 132, opens.

Figure 42: Firmware Download Dialog Box



2. Select the firmware version that you want to download from the list in the dialog box.
3. Click **Start firmware download**. A progress bar shows you when the download is completed.
4. When the download has completed, click **Close** to close the dialog box.

Updating iSTAR Firmware (Dial-up Connections)

You can update the iSTAR firmware on iSTAR Pro and iSTAR Ultra SE Pro Mode panels using dial-up from either the Administration Client or the Monitoring Station client.

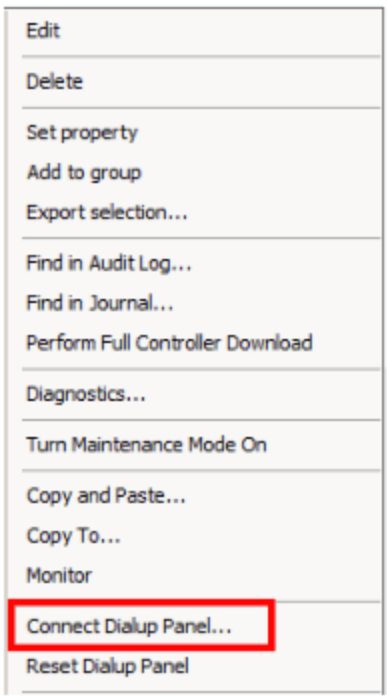
You can initiate a firmware update by right-clicking on the iSTAR controller:

- In the Hardware Tree
- In a Dynamic View in the Administration Client
- In the Status List - Controller in the Monitoring Station

To Update Firmware on an iSTAR Controller

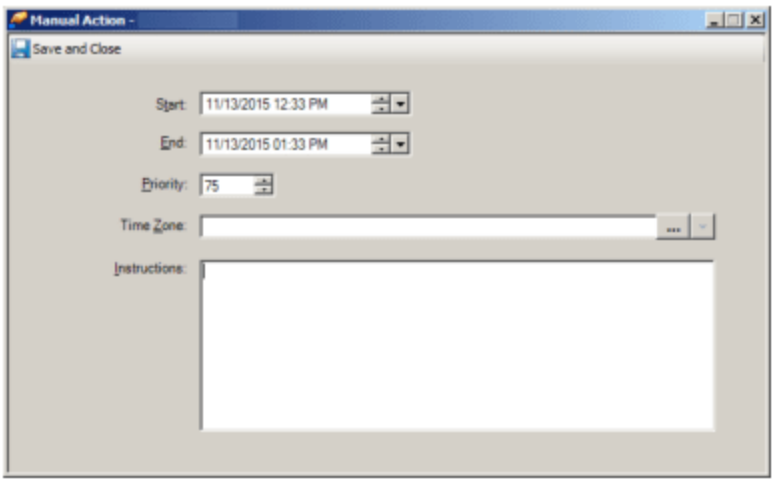
1. Manually connect to the dial-up iSTAR controller. Right-click on the dial-up iSTAR controller and select **Connect Dialup Panel** as shown in Figure 43 on Page 133.

Figure 43: iSTAR Context Menu - Dialup Connection



The Manual Actions dialog box, shown in Figure 44 on Page 133, opens.

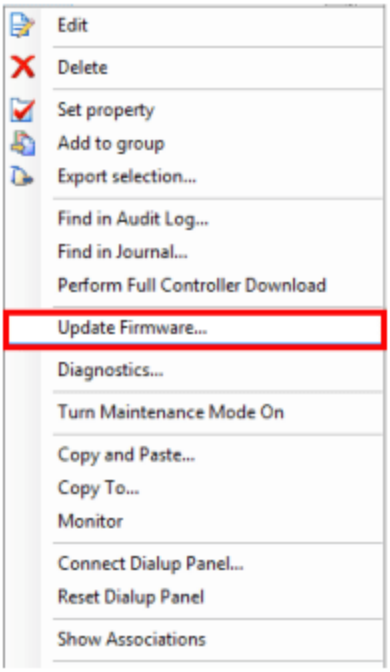
Figure 44: Manual Action Dialog Box



2. Ensure that the **Start** and **End** Time is set to a minimum of two hours.
3. Click **Save and Close**.
4. After the connection is established, right-click on the controller and select **Update Firmware** as shown in Figure 45 on Page 134.

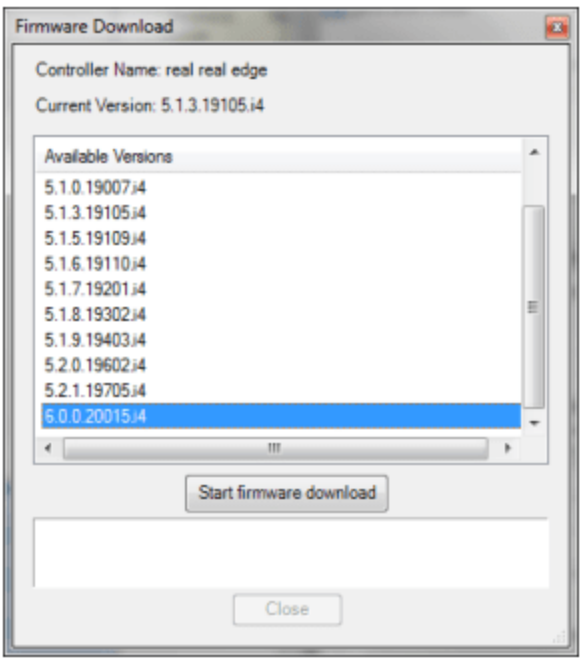
NOTE Update Firmware will not appear on the context menu if the iSTAR is not Enabled or is off-line.

Figure 45: iSTAR Context Menu - Update Firmware



The Firmware Download dialog box, shown in Figure 46 on Page 134, opens.

Figure 46: Firmware Download



5. Select the firmware version that you want to download from the list in the dialog box.
6. Click **Start firmware download**. A progress bar shows you when the download is completed.
7. When the download has completed, click **Close** to close the dialog box.

iSTAR Firmware Updates Using ICU

You can use the ICU (iSTAR Configuration Utility) to quickly download firmware updates to one or more controllers. Copy the new firmware file to **C:\Program Files (x86) Tyco\CrossFire\ServerComponents\istar\ICU\Firmware** (the default folder location) before starting the download process.

Before starting the firmware download, note the following:

- If you moved the ICU folder, then you must go back to the Controller dialog box and change the Server Root Directory to match that path. See the ICU help for information about changing the Server Root Directory.
- If the default Server HTTP Port (9701) that is used for firmware downloads is in use by another application, you have to specify another port to use for firmware downloads. See the ICU help for information about changing the Server Root Directory.

NOTE These procedures use default passwords. If you changed the default passwords, then you must use those.

To Download Firmware to the Controller Using the ICU

NOTE If you are downloading firmware to a controller using dialup, perform the following steps before you download the firmware:

1. Right-click on the controller an select **Connect to Controller**.
2. Monitor the connection in the Monitoring Station. Once complete, proceed to Step 1 below.

1. Click the **Options & Tools** pane.
2. Click **ICU**.
3. Enter the ICU password and click **OK**. The default password is **manager**. The ICU starts and the main window opens.
4. Select the controller(s) that you want to update. You can select multiple controllers by pressing the **Ctrl** key while you are selecting them.
5. After selecting the controller(s), right-click in the ICU window and select **Download Firmware** from the context menu.
6. You are prompted for a password if the iSTAR controller is an Ultra or Ultra SE.

   Enter **iSTAR**, the default password and click **OK**.
7. Click **Browse** and navigate to **C:\Program Files (x86) Tyco\CrossFire\ServerComponents\istar\ICU\Firmware** (the default folder location) .
8. Select the firmware image file and click **Open**. The selected file is displayed in the Firmware Image File to Download box.

6. Click **Start Download** to initiate the download to all controllers in the Download Firmware list.

   The firmware is downloaded simultaneously to all controllers in the list. The Progress bar on each line indicates when the download is complete for each controller.

NOTE The controller may reboot more than once during the upgrade process.

- To cancel a download, select the controller and right-click to select **Cancel Download** from the context menu.
- If a Controller returns a Download Failed message, you can select the controller and right-click to select **Retry** from the context menu to restart the firmware download.

9. When all of the downloads have completed, click **Exit** to close the Firmware Download dialog box.

Changing the Time Zone of an iSTAR Controller

You can change the value of the iSTAR controller **Time Zone** field only when the iSTAR Controller is not enabled (**Enabled** field is blank ☐). You must edit the controller, clear the **Enabled** field, save the controller, then re-open it to change the Time Zone.

If you change the Time Zone of the iSTAR controller, the Time Zone settings of all child objects of that iSTAR controller are changed as well. A warning message appears if you change the Time Zone and any Events or Triggers have controller-based actions on this iSTAR controller and the Event is configured to use a different Time Zone than this iSTAR controller.

Host-based actions with Schedules respect the controller Time Zone: a host-based Event that unlocks doors according to a Schedule uses the controller Time Zone to determine when the Schedule is active for devices on that controller.

However, if a Time Zone is assigned to the host-based Event itself, the Event actions will activate on the Schedule based on the host Time Zone.

Example:

With a C•CURE 9000 Server in the Eastern US Time Zone (GMT -5:00) and an iSTAR controller in the Central US Time Zone (GMT -6:00):

- A host Event that does not include an Event Time Zone unlocks specific Doors by Schedule on an iSTAR controller according to the controller Time Zone.
- A host Event that includes an Event Time Zone unlocks specific doors by Schedule on an iSTAR controller according to the C•CURE 9000 Server Time Zone.

To Change the Time Zone of an iSTAR Controller

1. From the **Hardware** pane, select the iSTAR controller you wish to change. Right-click and select **Edit**.
2. Clear the **Enabled** field (change ☑ to ☐).
3. Click **Save and Close** to save the change.
4. From the **Hardware** pane, select the iSTAR controller again. Right-click and select **Edit**.
5. When the iSTAR controller editor opens, the **Time Zone** field can be changed.
6. Click **Save and Close** to save the change.

iSTAR Controller Editor

The iSTAR Controller editor dialog box allows you to configure an iSTAR Controller and its attached devices.

You use the iSTAR Controller editor to configure the Controller settings and specify the Inputs, Outputs, and Readers that are connected to the Controller.

For information about the iSTAR Controller editor for a specific iSTAR model, see:

- iSTAR Classic Controller Editor on Page 137
- iSTAR Pro Controller Editor on Page 137
- iSTAR eX Controller Editor on Page 138
- iSTAR Edge Controller Editor on Page 139
- iSTAR Ultra Controller Editor on Page 139

iSTAR Classic Controller Editor

On iSTAR Classic Controllers, you can configure the GCM and any installed ACM Boards. Two ACM Boards can be installed on an iSTAR Classic Controller.

The iSTAR Classic Controller Editor has the tabs listed in Table 12 on Page 137.

Table 12: iSTAR Classic Controller Editor Tabs

Tab	See...
General Tab	iSTAR Controller General Tab on Page 141
Boards Tab	iSTAR Controller Boards Tab (iSTAR Classic/Pro) on Page 156
Schlage Wireless PIMs Tab	iSTAR Schlage Wireless PIMs Tab on Page 153
Triggers Tab	iSTAR Controller Triggers Tab on Page 147
Groups Tab	Groups Tab for Hardware Devices on Page 28
Status Tab	iSTAR Controller Status Tab on Page 147
User Defined Fields Tab	iSTAR Controller User Defined Fields Tab on Page 151
State Images Tab	iSTAR Controller State Images Tab on Page 152

iSTAR Pro Controller Editor

On iSTAR Pro Controllers, you can configure the GCM and any installed ACM Boards. Two ACM Boards can be installed on an iSTAR Pro Controller.

The iSTAR Pro Controller Editor has the tabs listed in Table 13 on Page 138.

Table 13: iSTAR Pro Controller Editor Tabs

Tab	See...
General Tab	iSTAR Controller General Tab on Page 141
Boards Tab	iSTAR Controller Boards Tab (iSTAR Classic/Pro) on Page 156
Schlage Wireless PIMs Tab	iSTAR Schlage Wireless PIMs Tab on Page 153
Triggers Tab	iSTAR Controller Triggers Tab on Page 147
Groups Tab	Groups Tab for Hardware Devices on Page 28
Status Tab	iSTAR Controller Status Tab on Page 147
User Defined Fields Tab	iSTAR Controller User Defined Fields Tab on Page 151
State Images Tab	iSTAR Controller State Images Tab on Page 152

iSTAR eX Controller Editor

On iSTAR eX Controllers, you can configure the GCM and any boards connected to the Power Management Board (PMB).

The tabs for the iSTAR eX Controller Editor are listed in Table 14 on Page 138.

Table 14: iSTAR eX Controller Editor Tabs

Tab	See...
General Tab	iSTAR Controller General Tab on Page 141
Inputs Tab	iSTAR eX and Edge Controller Inputs Tab on Page 159
Outputs Tab	iSTAR Edge/eX Controller Outputs Tab on Page 164
Wiegand Tab	iSTAR eX Controller Wiegand Tab on Page 171
COM1 Tab	iSTAR eX COM1/COM2 Tabs on Page 173
COM2 Tab	iSTAR eX COM1/COM2 Tabs on Page 173
Triggers Tab	iSTAR Controller Triggers Tab on Page 147
Groups Tab	Groups Tab for Hardware Devices on Page 28
Status Tab	iSTAR Controller Status Tab on Page 147
User Defined Fields Tab	iSTAR Controller User Defined Fields Tab on Page 151
State Images Tab	iSTAR Controller State Images Tab on Page 152

iSTAR Edge Controller Editor

The tabs for the iSTAR Edge Controller Editor are listed in Table 15 on Page 139.

Table 15: iSTAR Edge Controller Editor Tabs

Tab	See...
General Tab	iSTAR Controller General Tab on Page 141
Inputs Tab	iSTAR eX and Edge Controller Inputs Tab on Page 159
Outputs Tab	iSTAR Edge/eX Controller Outputs Tab on Page 164
Wiegand Tab	iSTAR Edge Controller Wiegand Tab on Page 169
COM1 Tab	iSTAR Edge COM1/COM2/COM3 Tabs on Page 167
COM2 Tab	iSTAR Edge COM1/COM2/COM3 Tabs on Page 167
COM3 Tab	iSTAR Edge COM1/COM2/COM3 Tabs on Page 167
Triggers Tab	iSTAR Controller Triggers Tab on Page 147
Groups Tab	Groups Tab for Hardware Devices on Page 28
Status Tab	iSTAR Controller Status Tab on Page 147
User Defined Fields Tab	iSTAR Controller User Defined Fields Tab on Page 151
State Images Tab	iSTAR Controller State Images Tab on Page 152

iSTAR Ultra Controller Editor

The tabs for the iSTAR Ultra Controller Editor tabs are listed in Table 16 on Page 139.

Table 16: iSTAR Ultra Controller Editor Tabs

Tab	See...
General Tab	iSTAR Controller General Tab on Page 141
Inputs	iSTAR Ultra Controller Editor Inputs Tab on Page 178
Boards Tab	iSTAR Ultra Controller Boards Tab on Page 179
IP ACM's Tab	iSTAR Ultra Controller IP-ACMs Tab on Page 181
COM1 Tab	iSTAR Ultra COM1/COM2 Tabs on Page 181
COM2 Tab	iSTAR Ultra COM1/COM2 Tabs on Page 181

iSTAR Ultra Controller Editor Tabs (continued)

Tab	See...
Triggers Tab	iSTAR Controller Triggers Tab on Page 147
Groups Tab	Groups Tab for Hardware Devices on Page 28
Status Tab	iSTAR Controller Status Tab on Page 147
User Defined Fields Tab	iSTAR Controller User Defined Fields Tab on Page 151
State Images Tab	iSTAR Controller State Images Tab on Page 152

iSTAR Controller Editor Tabs

The iSTAR Controller editor tabs available depend on the iSTAR Controller type.

The iSTAR Controller editor basic tabs and iSTAR specific tabs are listed below.

Basic Tabs

- iSTAR Controller General Tab on Page 141
- iSTAR Controller Boards Tab (iSTAR Classic/Pro) on Page 156
- iSTAR Controller Triggers Tab on Page 147
- iSTAR Controller Status Tab on Page 147
- iSTAR Controller State Images Tab on Page 152
- iSTAR Controller User Defined Fields Tab on Page 151

iSTAR Specific Tabs

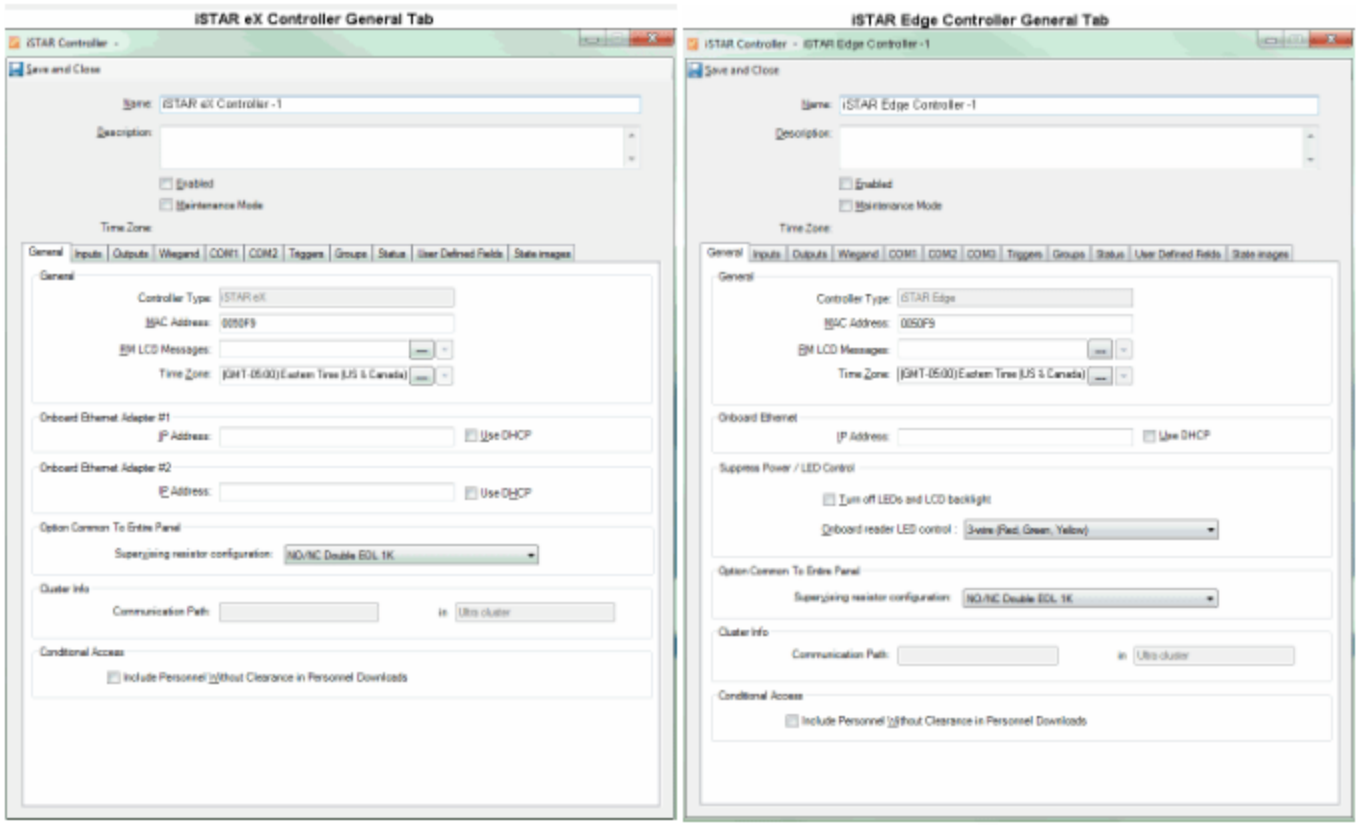
- iSTAR Schlage Wireless PIMs Tab on Page 153
- iSTAR eX and Edge Controller Inputs Tab on Page 159
- iSTAR Edge/eX Controller Outputs Tab on Page 164
- iSTAR Edge COM1/COM2/COM3 Tabs on Page 167
- iSTAR Edge Controller Wiegand Tab on Page 169
- iSTAR eX Controller Wiegand Tab on Page 171
- iSTAR eX COM1/COM2 Tabs on Page 173
- iSTAR Ultra Controller Editor Inputs Tab on Page 178
- iSTAR Ultra COM1/COM2 Tabs on Page 181
- iSTAR Ultra Controller IP-ACMs Tab on Page 181

iSTAR Controller General Tab

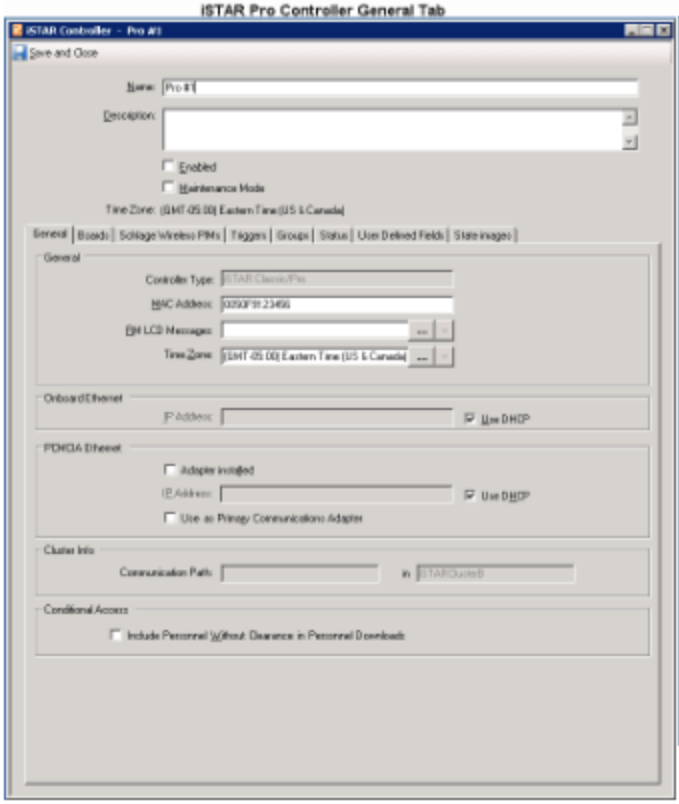
The iSTAR Controller General tab provides a means to set the controller's Onboard and PCMCIA Ethernet adapters, MAC address, RM LCD Messages, and Time Zone.

NOTE PCMCIA Ethernet adapters have not been evaluated by UL.

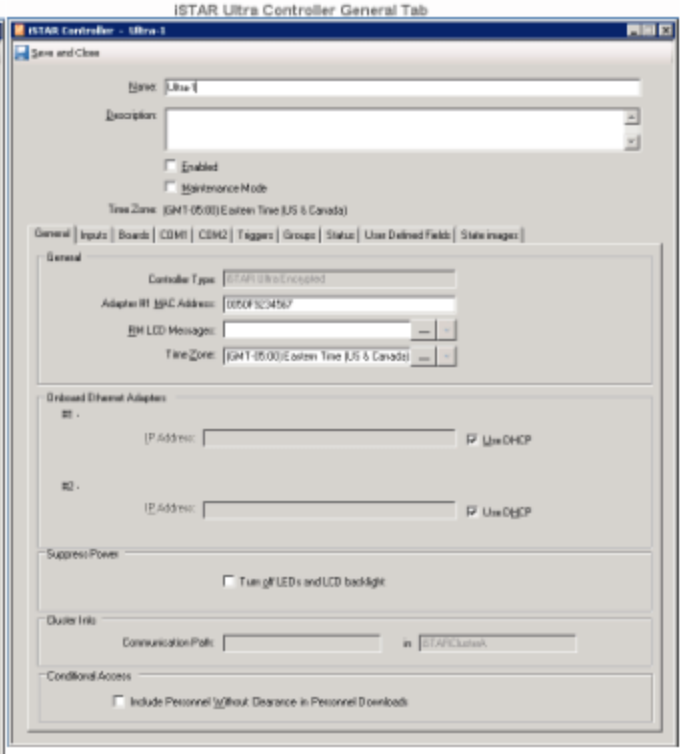
Figure 47: iSTAR Controller General Tab



iSTAR Pro Controller General Tab



iSTAR Ultra Controller General Tab



To Configure the iSTAR Controller General Tab

1. Create or edit an iSTAR Controller. See either:
   - Creating an iSTAR Controller on Page 124
   - Editing an iSTAR Controller on Page 126.
2. Enter a unique controller name in the **Name** field at the top of the **iSTAR Controller** dialog box.
3. Enter a textual description (optional) in the **Description** field.
4. Enter the last six hexadecimal characters after the vendor portion of the address in the **MAC Address** entry field for the controller. The first six characters of a controller's MAC address are set at 00-50-F9. The last six characters of a controller's MAC address must be within the range of hexadecimal values (i.e., 0-9 and a-f).
5. To select a particular customized set of LCD messages for the RM Readers, click ... to display a Reader LCD Message Set selection list. If you leave this field blank (the default), the Readers use the default messages. See Reader LCD Message Set Overview on Page 382 for more information.
6. If you are configuring iSTAR controllers that are located in different time zones, you can use the **Time Zone** entry field. Click ... to display a time zone selection. Greenwich Mean Time is equivalent to Zulu or Universal Time. If you leave the Time Zone field blank, the iSTAR is considered to be in the C•CURE 9000 server's Time Zone.

   You can only change the Time Zone setting for the iSTAR controller when the controller is not **Enabled** (☐). See Changing the Time Zone of an iSTAR Controller on Page 136.

7. You can type an **IP Address** in the **Onboard Ethernet IP Address** field, although it is recommended that you select **Use DCHP** to use the Dynamic Host Configuration Protocol (DHCP) option to automatically assign an IP address to the Controller.
8. For an iSTAR eX Controller, you can enter an IP Address for the **Onboard Ethernet Adapter #2**. Alternatively, you can select **Use DHCP**.

NOTE The DHCP Server has not been evaluated by UL.

9. For an iSTAR Classic/Pro Controller:
   a. If you have a PCMCIA Ethernet Adapter, select **Adapter Installed**.
   b. You can either enter an **IP Address** for the PCMCIA adapter or select **Use DHCP**.
   c. If you are using the PCMCIA Ethernet Adapter as the primary connection to the host, select **Use as Primary Communications Adapter**.
10. If you are configuring an iSTAR eX or iSTAR Edge Controller, you need to select the supervising resistor configuration for the GCM Inputs. The default setting is **NO/NC Double EOL 1K**. See Table 17 on Page 145 for more information.

NOTE The supervision method for Inputs on the iSTAR Ultra is configured for each separate Input on the Input Editor.

11. If any Doors on this controller need to be configured for Conditional Access, select the **Include Personnel Without Clearance in Personnel Downloads** option in the Conditional Access box. The **Conditional Access** tab is available on the **iSTAR Doors** Editor **only** if this option is selected. See iSTAR Door Conditional Access Tab on Page 436.

NOTE Since selecting this option causes a full Personnel download to the controller (including all credentials except for Lost, Stolen Not Active, and Expired), a warning displays about the 250,000-record-download limit.

12. You can optionally click other tabs on the iSTAR Controller Editor to configure other settings prior to saving the Controller.
13. Click the **Enabled** check box to put the controller online when you are finished configuring the iSTAR Controller General Tab. You must have entered a valid **MAC Address** and a setting for the **IP Address** before enabling the Controller or you will receive an error message if you try to save the Controller settings with **Enabled** selected.
14. Click **Save and Close** to save your settings for the Controller and close the iSTAR Controller Editor.

iSTAR Controller General Tab Definitions

Table 17 on Page 145 includes further information for fields in the **Controller** Editor **General** tab. The fields available differ by controller type, as indicated in this table.

Table 17: iSTAR Controller Editor General Tab Fields

Field	Description
Name	Enter a unique name up to 50 characters long for the controller. If you enter the name of an existing object, the system returns an error message indicating there is a conflict.
Description	Enter a textual comment about the controller, such as its location or purpose. This text is for information only.
Enabled	Click the **Enabled** check box to put the Controller online. You must specify the MAC address and IP address for the Controller prior to selecting **Enabled** or you will receive an error message when you save the Controller.
Maintenance Mode	Click to put the iSTAR Controller and/or its components into Maintenance Mode. See Chapter 2: Maintenance Mode for more information.
Partition	This read-only field identifies the Partition in which this Controller resides. If you are creating a new Controller, the Partition that is currently the New Object Partition for your Operator account is automatically assigned to each Controller you create. If you want to change the Partition of a Controller, you must move the Cluster in which the Controller resides. See Using Drag and Drop in the Hardware Tree on Page 27.
General (All Controller Types)	
Controller Type	This field displays the controller type: **iSTAR Classic/Pro**, **iSTAR Edge**, **iSTAR eX**, or **iSTAR Ultra**. The Controller Type is determined when you initially create the controller object. When you save the controller object, this field becomes read-only for all subsequent editing sessions.
Hardware (MAC) Address	Enter the Hardware MAC address for the controller. The MAC address is built into the GCM and cannot be changed. You can find a controller's MAC address on a label attached to the GCM or view the address using the iSTAR Configuration Utility. The first six nibbles (or characters) of a controller's MAC address are set at 00-50-F9. The last six nibbles (or characters) of a controller's MAC address must hexadecimal numbers between 0-9 and A-F.
RM LCD Messages	If you want customized LCD messages to display on the RM Readers, specify a Reader LCD Message Set. Click ... to display a Reader LCD Message Set selection list. By default, this field is blank indicating that the Readers are use the default messages. For more information, see Reader LCD Message Set Overview on Page 382.
Time Zone	If you are managing controllers in different time zones, specify a time zone for the controller. Click ... to display a time zone selection. The following objects are associated with the controller's time zone: • Inputs, outputs, and readers on the controller. • Doors and door groups with inputs, outputs, or readers on the controller. • Elevators and elevator groups with inputs, outputs, or readers on the controller. NOTE: Only Schedules and clearances that use the same time zone as the controller are downloaded to the controller. If you change the controller's time zone after a Schedule or clearance has been downloaded to the controller, a matching violation occurs. The time zone is downloaded to the controller, and the clearance is deleted from the controller. See the *C•CURE 9000 Software Configuration Guide* for more information.
Onboard Ethernet Adapter #1 (All Controller Types)	
IP Address	Enter the unique IP address for Onboard Ethernet #1 as 4 numbers between 0 and 255, separated by periods, such as 100.10.10.1.
Use DHCP	Select this check box to obtain an IP Address from a DHCP Server for the iSTAR Controller's Onboard Ethernet #1 Adapter.

Table 17: iSTAR Controller Editor General Tab Fields (continued)

Field	Description
Onboard Ethernet Adapter #2 (iSTAR eX and ISTAR Ultra only)	
IP Address	Enter the unique IP address for Onboard Ethernet #2 as 4 numbers between 0 and 255, separated by periods, such as 100.10.10.1.
Use DHCP	Select this check box to obtain an IP Address from a DHCP Server for the iSTAR Controller's Onboard Ethernet #2 Adapter.
PCMCIA Ethernet (iSTAR Classic/Pro only)	
Adapter Installed	Select this check box to indicate that an PCMCIA Ethernet adapter is installed.
IP Address	Enter the unique IP address for the PCMCIA Ethernet Adapter as 4 integers between 0 and 255, separated by periods, such as 100.10.10.1.
Use DHCP	Select this check box to obtain an IP Address from a DHCP Server for the PCMCIA Ethernet Adapter.
Use as Primary Ethernet Adapter	Select this check box to indicate that the PCMCIA Ethernet Adaptor is to be used as the Primary Ethernet Adapter.
Suppress Power / LED Control (iSTAR Edge and iSTAR Ultra only)	
Turn off LEDs and LCD backlight	You can to configure the LCD backlight and various status LEDs to always be off by selecting (☑), regardless of tamper state. Selecting this option does not affect the Power LED or the bright white external power indicator.
Onboard reader LED control	Specify the method used on this controller to drive the direct connect reader LEDs: • 3-wire (Red, Green, Yellow) • External Bi-Color (2-wire Red, Green) • 1-wire (A, B, C)
Option Common To Entire Panel (iSTAR eX and iSTAR Edge only)	
Supervising resistor configuration	All iSTAR eX GCM Inputs and iSTAR Edge inputs must be wired in the same way and use the same supervision method. All supervised settings assume either one or two end of line (EOL) resistors. You can use the **Reverse Sense** option if you need a particular Input to differ from the selected setting (for example, if you choose a NO setting here, but you need a door switch monitor Input to be NC, you can set that Input for **Reverse Sense** in the iSTAR Input Editor (see iSTAR Input Editor on Page 232 for more information). • NO = Normally Open • NC = Normally Closed • EOL = End of Line Select one of the resistor values in the drop-down list. NO/NC Double EOL 1K is the default, and the traditional Software House method

Table 17: iSTAR Controller Editor General Tab Fields (continued)

Field	Description
Cluster Info (All Controller Types)	
Cluster Info Communications Path	These read-only fields display the Communications Path and the name of the iSTAR Cluster through which this controller communicates with the C•CURE 9000 Server.
Conditional Access (All Controller Types)	
Include Personnel Without Clearance in Personnel Downloads	If you want to enable conditional access for Doors on this Controller—allow entry to Personnel without Clearances, click to select this option. The Conditional Access tab is available on the iSTAR Doors Editor **only** if this option is selected. For information, see iSTAR Door Conditional Access Tab on Page 436. NOTE: Since selecting this option causes a full Personnel download to the controller (including all credentials except for Lost, Stolen Not Active, and Expired), a warning displays about the 250,000-record-download limit.

iSTAR Controller Triggers Tab

C•CURE 9000 uses **Triggers**, which are configured procedures used for activating security actions. A Trigger automatically executes a specified **Action** when a particular predefined condition occurs. When a Trigger is defined, the Actions available depend on the property selected. The Triggers are usually used to activate an Event which can activate numerous actions.

See Triggers Tab for iSTAR Devices on Page 270 for information on creating Triggers for an iSTAR device.

iSTAR Controller Status Tab

The Status tab, as shown in Figure 48 on Page 149 provides a read-only listing of critical information about the operational status of the selected iSTAR controller. Such information includes:

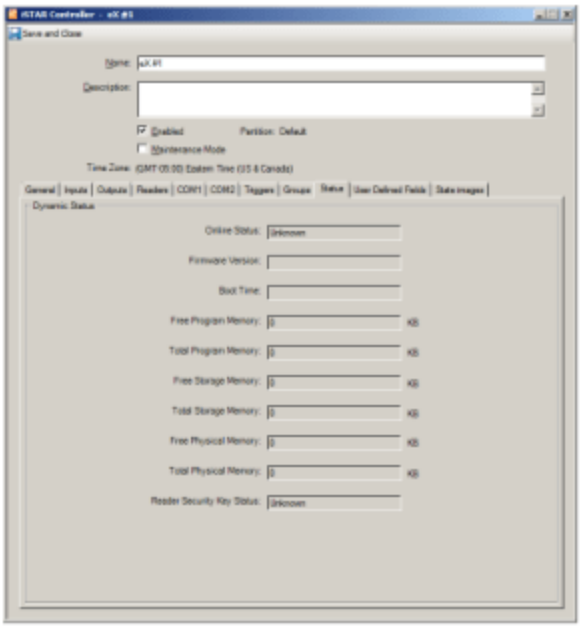
- Online Status - indicates whether the controller has been enabled (see the **General** tab).
- Firmware Version - the version of the firmware used by the controller.
- Boot Time - the last time the controller was restarted (GMT or Zulu time).
- Memory Usage for the controller's microprocessors:
  - Free and Total Program Memory
  - Free and Total Storage Memory
  - Free and Total Physical Memory
- Reader Security Key Status (for iSTAR eX).
- PoE Board Installed - True or False (for the iSTAR Edge/Ultra)
- Edge Model Status - 1-door, 2-door or 4-door (for the iSTAR Edge)
- Encryption Setting Status

The definitions for the Status tab for various controller types are:

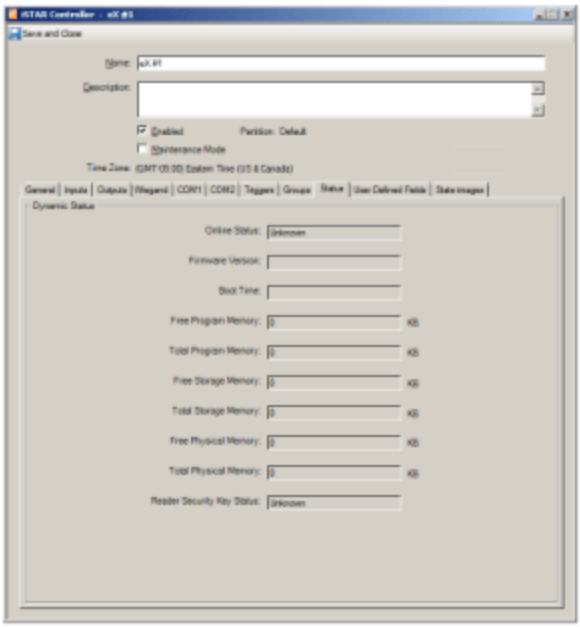
- iSTAR Controller Status Tab Definitions on Page 149

Figure 48: iSTAR Controller Status Tab

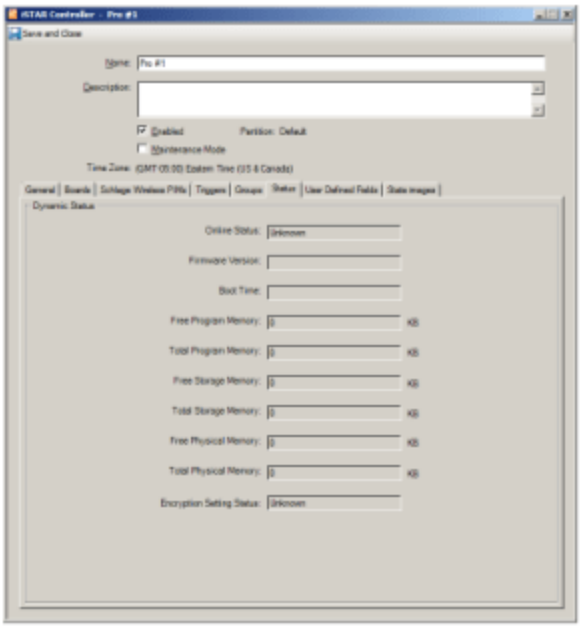
iSTAR eX Controller Status Tab



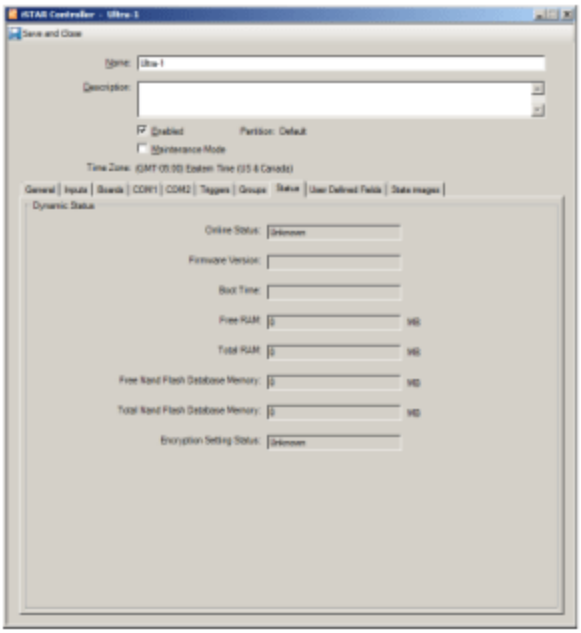
iSTAR Edge Controller Status Tab



iSTAR Pro Controller Status Tab



iSTAR Ultra Controller Status Tab



iSTAR Controller Status Tab Definitions

Table 18 on Page 150 provides definitions of the fields and buttons on the iSTAR Controller Status tab.

Table 18: iSTAR Controller Status Tab Definitions

Field/Button	Description
Online Status	Indicates whether the controller has been **Enabled** (see the **General** tab).
Firmware Version	The version of the firmware currently in use by the controller.
Boot Time	The last date/time the controller was restarted (GMT or Zulu time)
Free Program Memory	Unused program memory in the controller's microprocessor, in kilobytes.
Total Program Memory	Total storage memory in the controller's microprocessor, in kilobytes.
Free Storage Memory	Unused storage memory in the controller's microprocessor, in kilobytes.
Total Storage Memory	Total storage memory in the controller's microprocessor, in kilobytes.
Free Physical Memory	Unused physical memory in the controller's microprocessor, in kilobytes.
Total Physical Memory	Total physical memory in the controller's microprocessor, in kilobytes.
Reader Security Key Status (eX only)	This field applies only to iSTAR eX controllers. It displays whether or not the eX 8-Reader Security Key is in place. Possible status values are: **Detected** – the key is plugged in and 8 readers are operational on the iSTAR eX. **NotDetected** – the key is not plugged in, and only four Readers will be operational. **Unknown** – the key status cannot be determined (for example, the status is Unknown if the controller is out of communication with C•CURE 9000). You can determine the status by observing the LCD on the iSTAR eX.
Encryption Setting Status (iSTAR Edge, classic/Pro)	A Read-only field that displays the Encryption Setting. Encryption settings are Encrypted (AES), Unknown, or Not Encrypted.

iSTAR Edge Controller Status Tab Definitions

Table 19 on Page 150 provides definitions of the fields and buttons unique to the iSTAR Edge Controller Status tab.

Table 19: iSTAR Edge Controller Status Tab Definitions

Field/Button	Description
PoE Board Installed	The field displays whether the Power over Ethernet (PoE) Board is installed. Possible status values are **True** or **False**.
Edge Model Status	The field displays the iSTAR Edge Model Status, either 2-door or 4-door.

iSTAR Ultra Controller Status Tab Definitions

Table 20 on Page 151 provides definitions of the fields and buttons unique to the iSTAR Ultra Controller Status tab.

Table 20: iSTAR Ultra Controller Status Tab Definitions

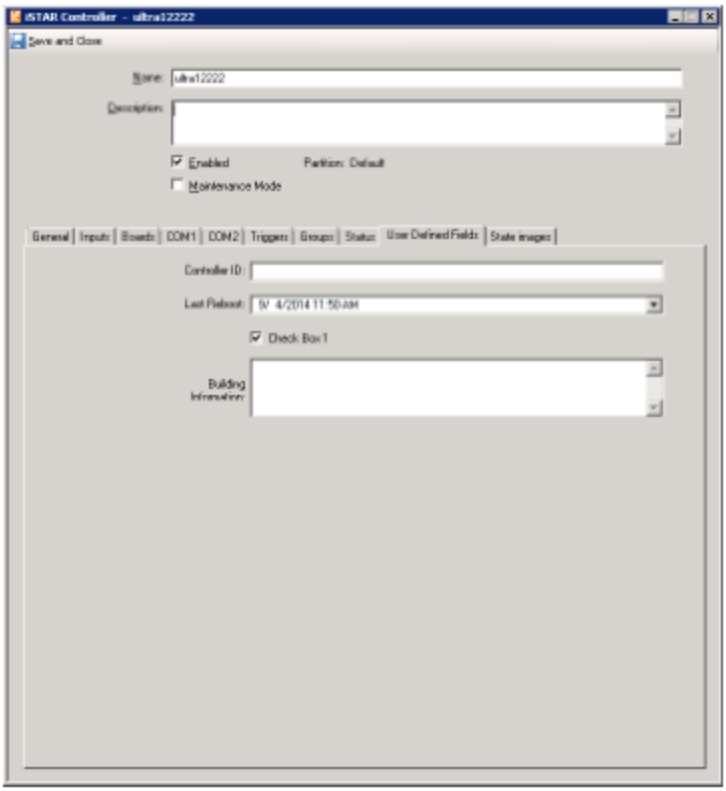
Field/Button	Description
Free RAM	Unused program memory available to the microprocessor in megabytes.
Total RAM	Total storage memory available to the microprocessor in megabytes.
Free Nand Flash Database Memory	Unused flash memory in megabytes.
Total Nand Flash Database Memory	Total flash memory in megabytes.
PoE Board Installed	The field displays whether the Power over Ethernet (PoE) Board is installed. Possible status values are **True** or **False**.

iSTAR Controller User Defined Fields Tab

The User Defined Fields tab, shown in Figure 1 on Page 152, displays user-defined fields in the system for hardware. User-defined fields are configured in the **Configuration** pane. If there are no user-defined fields configured, then the tab is empty.

See the *C•CURE 9000 Software Configuration Guide* for more information.

Figure 1: iSTAR User Defined Fields Tab



iSTAR Controller State Images Tab

The **State Images** tab provides a means to change the default images that are displayed on the C•CURE 9000 Monitoring Station to indicate controller states. See State Images Tab for iSTAR Devices on Page 274 for information on using the State Images tab for your iSTAR Controller.

iSTAR Controller State Images Tab Definitions

Table 21 on Page 152 shows the iSTAR Controller States and the default State Images.

Table 21: iSTAR Controller State Images Tab Definitions

Icon	Description		Icon	Description
	Unknown			Download in Progress
	Online			Comm Fail

iSTAR Controller State Images Tab Definitions (continued)

Icon	Description		Icon	Description
	Disabled			Database Back Up
	Power Failure			Fire Alarm Supervision State (Used only by iSTAR Edge)
	Battery Low			FAI Relay Control (iSTAR Edge/Ultra)
	Tamper			FAI Key Supervision State (Used only by iSTAR Edge)
	Download Error			Internal Battery Fault (iSTAR Edge and Ultra)

iSTAR Schlage Wireless PIMs Tab

This tab allows you to configure up to 16 Schlage Wireless Panel Interface Modules (PIMs) on an iSTAR Classic/Pro.

An iSTAR controller can support up to 16 Schlage Wireless readers. The number of PIM boards needed to support your readers can vary, depending upon Reader type and the physical location of the reader/lock hardware. You could connect 16 readers to a single PIM if all readers are within the range/distance specifications for wireless readers. If some readers are farther away, additional PIMs may be needed to place a PIM within wireless range of each reader. You can configure no more than 16 PIMs and 16 Readers per controller.

The AD300 series readers have an integrated PIM in the reader/lock hardware - these readers require you to configure an iSTAR PIM board with only that reader attached to the PIM.

NOTE Support for the following Schlage features requires C•CURE 9000 2.10 R2 Patch 1 or later, and iSTAR firmware 5.2.1 or later.

- Wake on Radio
- Keypad support
- Manual Lock Override
- Push Button

PIM and Reader Addresses

Each PIM has an address between 0 (zero) and 15. On an iSTAR, boards are numbered starting at 1, not 0. As a result, a PIM with address 0 is configured on the iSTAR as PIM #1.

Each Reader has a reader address between 0 (zero) and 15. On an iSTAR, readers are numbered starting at 1, not 0. As a result, a reader with address 0 is configured on the iSTAR as reader #1.

Example

If you have PIMs with addresses of 4, 8, 12, and 15, you should configure these PIMs on the iSTAR as PIM5, PIM9, PIM13, and PIM16.

If you have readers with addresses 0 through 5, you should configure these readers on the iSTAR as iSTAR PIM 485 Reader1 through iSTAR PIM 485 Reader6.

Once you have assigned a reader address to one PIM, that reader address will be unavailable on all other PIM boards on the iSTAR.

Example

You configure Reader address #1 on PIM Board #1. On every other PIM Board you configure on this iSTAR, Reader address #1 is unavailable (grayed out).

The address ranges for readers connected to PIMs cannot overlap. If you set up your PIM hardware so that a specific PIM controls reader addresses 0 through 5, you cannot assign a different PIM to control any of the addresses in between.

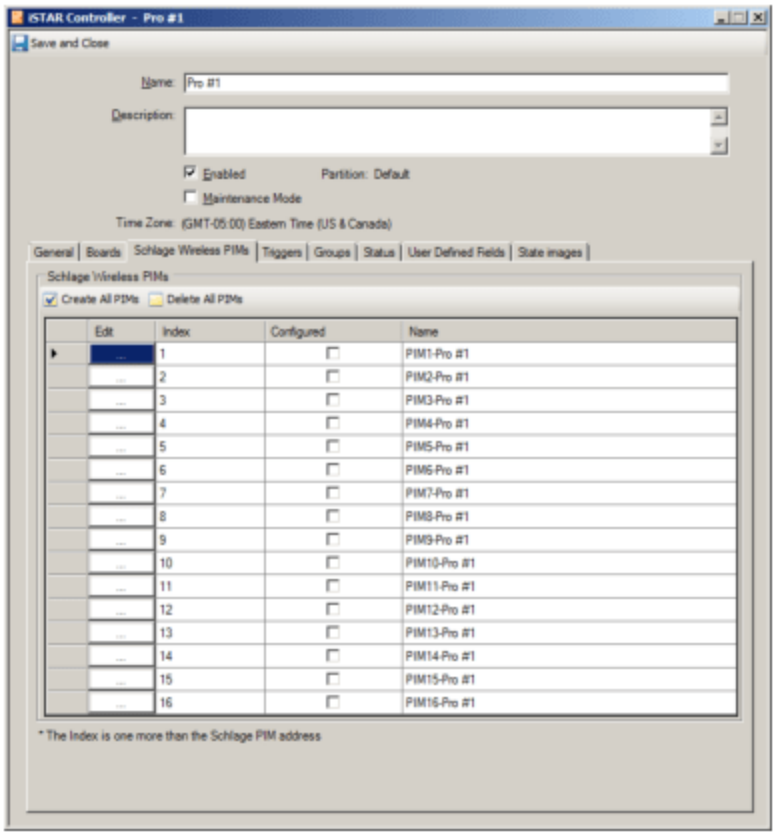
Example

You have two PIMs. You set one to control Reader addresses 0 through 5 (readers 1 through 6 on the iSTAR). You other PIM must be setup to control readers outside this range, such as Reader addresses 8 through 11 (Readers 9 through 12 on the iSTAR).

If you add another PIM, that PIM cannot be assigned to control any of the already assigned addresses, even if the address are not in use at this time by one of the two existing PIMs. The new PIM could only be assigned Reader addresses 6 and 7 (Readers 7 and 8) and/or Reader addresses 12 through 15 (Readers 13 through 16)

Figure 49 on Page 155 shows the iSTAR Schlage Wireless PIM tab.

Figure 49: iSTAR Schlage Wireless PIMs Tab



iSTAR Schlage Wireless PIMs Tab Definitions

The fields and buttons on the iSTAR Schlage Wireless PIMs tab are described in Table 22 on Page 155.

Table 22: iSTAR Schlage Wireless PIM Tab

Field/Button	Description
Create All PIMs	Click to create all 16 PIMs. When you click **Create All PIMs** the Configured column check boxes are selected, and you can click ... in the **Edit** column to open the iSTAR PIM-485 Board Editor to configure a PIMs.
Delete All PIMs	When you click **Delete All PIMs**, the check boxes in the **Configured** column are cleared for all 16 PIMs, and all 16 PIM boards are immediately deleted (any settings you have configured are lost).
Edit column	Click ... in the **Edit** column to open the iSTAR PIM-485 Board Editor to configure a PIM. See iSTAR PIM-485 Board Editor on Page 226.
PIM Index column	This column displays the number of each PIM Board.
Configured column	Click in this column to create a PIM Board (make it available to be edited).

Field/Button	Description
Name column	Displays the name for this PIM Board The name is system-generated by default, but you can edit this name by clicking in this field.
Save and Close	Click to save your configuration changes and close the iSTAR Controller editor.

iSTAR Controller Boards Tab (iSTAR Classic/Pro)

The Boards tab is available for iSTAR Classic and iSTAR Pro Controllers only.

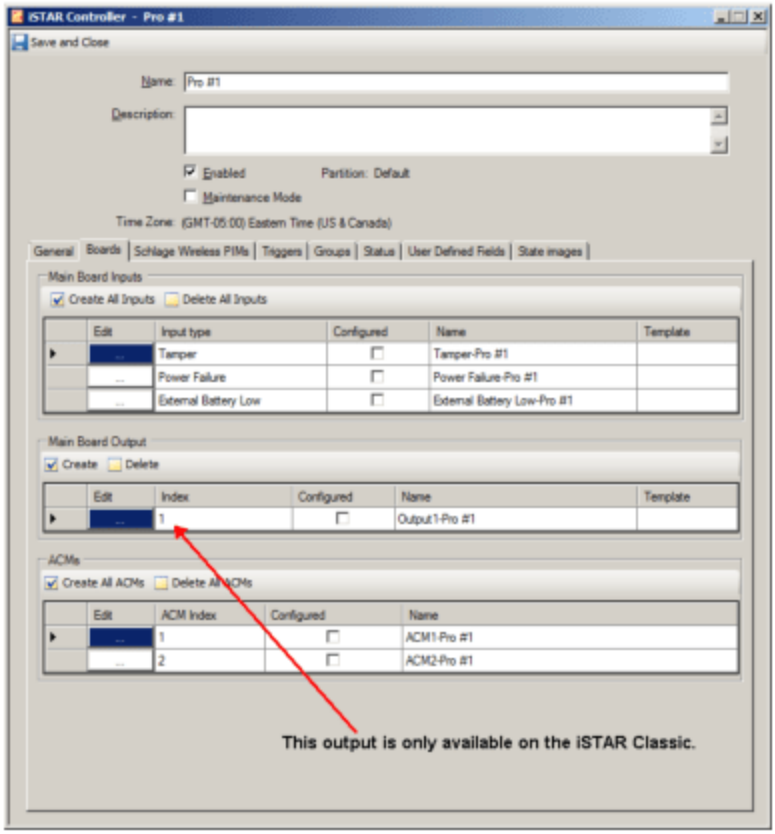
The Boards tab in the iSTAR Controller Editor lets you configure the following inputs, outputs, and ACM boards.

- Main Board Inputs on the GCM.
  - **Tamper** - this input activates when the controller cabinet is opened.
  - **Power Failure** - this input monitors for AC power failure of the apS or UPS supplying power to the controller. When this alarm input activates, it specifies that the GCM has lost its primary power source, and is operating on batteries.
  - **External Battery Low** (iSTAR Ultra/Classic/Pro) - this input activates when the external emergency battery (from the apS or UPS) is running low on power.
  - **Internal Battery Fault** (iSTAR Ultra only) - this is a logical input that reports the state of the onboard battery.
  - **General** (iSTAR Ultra only) - this input is a general purpose Supervised Input on the GCM.
- Main Board Output on the GCM (iSTAR Classic only).
- ACM 1 and ACM 2 Boards for the Controller (iSTAR Classic/Pro only).

  Add-on Access Control Modules (**ACM Boards**) provide access control functionality by supporting readers, outputs and inputs.
- ACM 1 and ACM 2 Boards on SPI port 1 (iSTAR Ultra only) - used to configure Inputs, Outputs, and Readers on an iSTAR ACM Board attached to SPI port 1 on an iSTAR Ultra Controller.
- ACM 1 and ACM 2 Boards on SPI port 2 (iSTAR Ultra only) - used to configure Inputs, Outputs, and Readers on an iSTAR ACM Board attached to SPI port 2 on an iSTAR Ultra Controller.

The iSTAR Controller Boards tab is shown in Figure 50 on Page 157.

Figure 50: iSTAR Controller Editor Boards Tab



To Configure the iSTAR Controller Boards Tab

1. From the iSTAR Controller editor, click the **Boards** tab.
2. Create the **Main Board Inputs** that you need by clicking **Create All Inputs** or by selecting the **Configured** check box for only the Inputs you wish to create.
3. To use an existing Input Template to create one or more of the Main Board Inputs, click in the **Template** Column, then click [...]. A list of available iSTAR Input Templates appears. Click on the Template you wish to use. See Using Templates for Controller Inputs, Outputs, and Readers on Page 37 for more detailed information about using Templates to create Controller Inputs.
4. Click [...] in the **Edit** column to configure individual Main Board Inputs. See the definitions of the Main Board Inputs in Table 23 on Page 158.
5. Create the **Main Board Output** if needed by clicking **Create Output** or by selecting the **Configured** check box for the Main Board Output.
6. Click [...] in the **Edit** column to configure the Main Board Output. See the definition of the Main Board Output in Table 23 on Page 158 and see iSTAR Output Editor on Page 241 for configuration instructions.
7. Create the **ACM Boards** that you need by clicking **Create All ACMs** or by selecting the **Configured** check box for only the ACMs you wish to create.
8. Click [...] in the **Edit** column to configure an ACM. See iSTAR Classic/Pro Controller ACM Board Editor on Page 197 for configuration instructions.

9. Click **Save and Close** to save the settings you have configured on the iSTAR Controller Boards tab, or click another tab in the iSTAR Controller Editor to perform additional configuration.

iSTAR Controller Boards Tab Definitions

The iSTAR Controller Boards tab includes the fields and buttons described in Table 23 on Page 158.

Table 23: iSTAR Controller Boards Tab Definitions

Field/Button	Description
Main Board Inputs	
Create All Inputs	Click to create the three Main Board Inputs. When you click **Create All Inputs** the Configured column check boxes are selected, and you can click ... in the **Edit** column to open the iSTAR Input Editor to configure an Input.
Delete All Inputs	When you click **Delete All Inputs**, the check boxes in the **Configured** column are cleared for all three Main Board Inputs, and all three Inputs are immediately deleted (any settings you have configured are lost).
Tamper	The Tamper input activates when the controller cabinet is opened or removed from its mounting surface. NOTE: For UL applications, this field must be enabled. Select the check box in the **Configured** column and click ... located in the **Edit** column to open the iSTAR Input Editor General tab to configure the Tamper input. From the Input Editor you can configure the Options, Triggers, Groups, Status and State Images that are associated with the Tamper Input. The **Template** column shows the template name chosen if you selected a Template prior to creating the Input.
Power Failure	The AC power failure input monitors the AC power failure output of a battery backup unit, such as the Advanced Power System (apS). When this alarm input activates, it specifies that the GCM has lost its primary power source, and is operating on batteries. NOTE: For UL applications, this field must be enabled. Select the check box in the **Configured** column and click ... located in the **Edit** column to open the iSTAR Input Editor General tab to configure the AC Power Fail Input. From the Input Editor you can configure the Options, Triggers, Groups, Status and State Images that are associated with the AC Power Fail Input. The **Template** column shows the template name chosen if you selected a Template prior to creating the Input.
External Battery Low (iSTAR Classic/Pro)	The External Battery Low input activates when the emergency battery is running low on power. NOTE: For UL applications, this field must be enabled. NOTE: This field for iSTAR Pro and Classic is on the Boards Tab. For iSTAR eX and Edge, this field is on the Inputs Tab.
External Battery Low (iSTAR eX/Edge/Ultra)	Select the check box in the **Configured** column and click ... located in the **Edit** column to open the iSTAR Input Editor General tab to configure the Options, Triggers, Groups, Status and State Images that are associated with the Battery Low Input. The **Template** column shows the template name chosen if you selected a Template prior to creating the Input.

Table 23: iSTAR Controller Boards Tab Definitions (continued)

Field/Button	Description
Internal Battery Fault (iSTAR Ultra)	A logical input that reports the state of the onboard battery. This Input is configured (☑) by default when the controller is created.
General (iSTAR Ultra)	A physical input that can be used to monitor a condition, particularly useful for Ultra configurations that are GCM only.
Main Board Output (Classic and Ultra only)	
Create	Click to create the Main Board Output. When you click **Create** the **Configured** column check box is selected, and you can click ... in the **Edit** column to open the iSTAR Output Editor to configure the Output.
Delete (iSTAR Classic/Ultra)	When you click **Delete**, the check box in the Configured column is cleared for the Main Board Output, and the Output is immediately deleted (any settings you have configured are lost).
1	Select the check box in the **Configured** column and click ... located in the **Edit** column to open the iSTAR Output Editor General tab to configure the Options, Groups, Status and State Images that are associated with the Main Board Output. The **Template** column shows the template name chosen if you selected a Template prior to creating the Output.
ACMs	
Create All ACMs (iSTAR Classic/Pro only)	Click to create all the ACM Boards. When you click **Create All ACMs** the Configured column check boxes are selected, and you can click ... in the **Edit** column to open the iSTAR ACM Board Editor to configure an ACM Board.
Delete All ACMs (iSTAR Classic/Pro only)	When you click **Delete All ACMs**, the check boxes in the Configured column are cleared for both Main Board ACM Boards, and both ACM Boards are immediately deleted (any settings you have configured are lost).
Board1	Select the check box in the **Configured** column and click ... located in the **Edit** column to open the iSTAR ACM Editor General tab to configure the Inputs, Outputs, and Readers that are associated with the first ACM board.
Board2	Select the check box in the **Configured** column and click ... located in the **Edit** column to open the iSTAR ACM Editor General tab to configure the Inputs, Outputs, and Readers that are associated with the second ACM board.

iSTAR eX and Edge Controller Inputs Tab

The iSTAR Controller Inputs tab is available only on the iSTAR eX Controller editor and the iSTAR Edge Controller editor.

The Inputs tab (shown in Figure 51 on Page 162) lets you define the Special Purpose and General Purpose Inputs for the Controller.

All of the inputs support event triggers based on their active or inactive states. These triggers can activate alarms, send emails, run a Roll Call Report, etc.

iSTAR eX Controller Inputs

Special Purpose Inputs

- **Tamper** input – Activates when the controller cabinet is opened.
- **Power Failure** input – Monitors the AC power failure output of the PMB. When this alarm input activates, it indicates that the PMB has had an AC Power Failure and is now supplying battery power to the controller.

  Similarly, if the eX is the NPS (No Power Supply) version, the Power Fail output of the UPS or apS is monitored with the same result.
- **External Battery Low** input – Activates when the battery connected to the PMB emergency battery has reached a yellow warning level. This will be followed, after some further use, with a Backup Now condition (Battery really low) which will backup the configuration and data and then shut down the controller.

  If the eX is the NPS (No Power Supply) version, the Battery Low output of the UPS or apS is monitored and will signal low battery. It is recommended to shut down the unit being powered by the low battery.

NOTE Tamper, AC power fail, and Low battery inputs must be programmed for UL applications.

General Purpose Inputs

- iSTAR eX provides 16 general purpose inputs.

iSTAR Edge Controller Inputs

Special Purpose Inputs

- **Tamper** input – Activates when the controller cabinet is opened.
- **Power Failure** input – Monitors the AC power failure output of the UPS (Un-interruptible Power Supply) or apS and indicates an AC Power Failure resulting in the UPS or apS supplying battery power to the controller.
- **Battery Low** input – Activates when the UPS or apS emergency battery has reached a yellow warning level. It is recommended to shut down the unit being powered by the low battery. Do not confuse this input with **Onboard Battery Low**.

NOTE Tamper, AC power fail, and Low battery inputs must be programmed for UL applications.

- **Onboard Battery Low** input – This input activates when the voltage of all four onboard AA alkaline batteries in series reaches 4.6 volts, or if a battery is missing or disconnected.

NOTE The following Fire Alarm Interface (FAI) features are only supported on these iSTAR Edge models:

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

- **FAI Supervision State** input – This input represents the F (Fire) Input State - the state of the F (Fire) input coming into J40 of the iSTAR Edge. In other words, this is the fire alarm. The Fire Alarm Interface activates the relays on the iSTAR Edge when the F input goes True. This input is supervised as NC (Normally Closed).
- **FAI Relay Control** input – The FAI relay control is a pseudo input that indicates the state of the Relay Drive signal that activates or latches the selected relays when the F (Fire) input is True.

- **FAI Key Supervision State**input – This input represents the K (Key) Input State. The K input is used to unlatch the latched relays, which removes the relay drive signal, once it is clear that the fire emergency is over. The K (Key) input is usually a momentary contact key switch. The K input is supervised as NO (Normally Open).

General Purpose Inputs

- iSTAR Edge provides eight general purpose inputs.

Fire Alarm Interface

FAI (Fire Alarm Interface) is a hardware feature on the iSTAR Edge that is typically used to perform the following tasks when a fire alarm signal is present.

- Unlock all doors when fire is present.
- Remove power from various devices when fire is present.

All three of the FAI Inputs support Event triggers based on their active or inactive states. These Event triggers can be configured to activate alarms, send emails, run a Roll Call Report, etc based on the state changes of the three FAI inputs.

FAI Modes

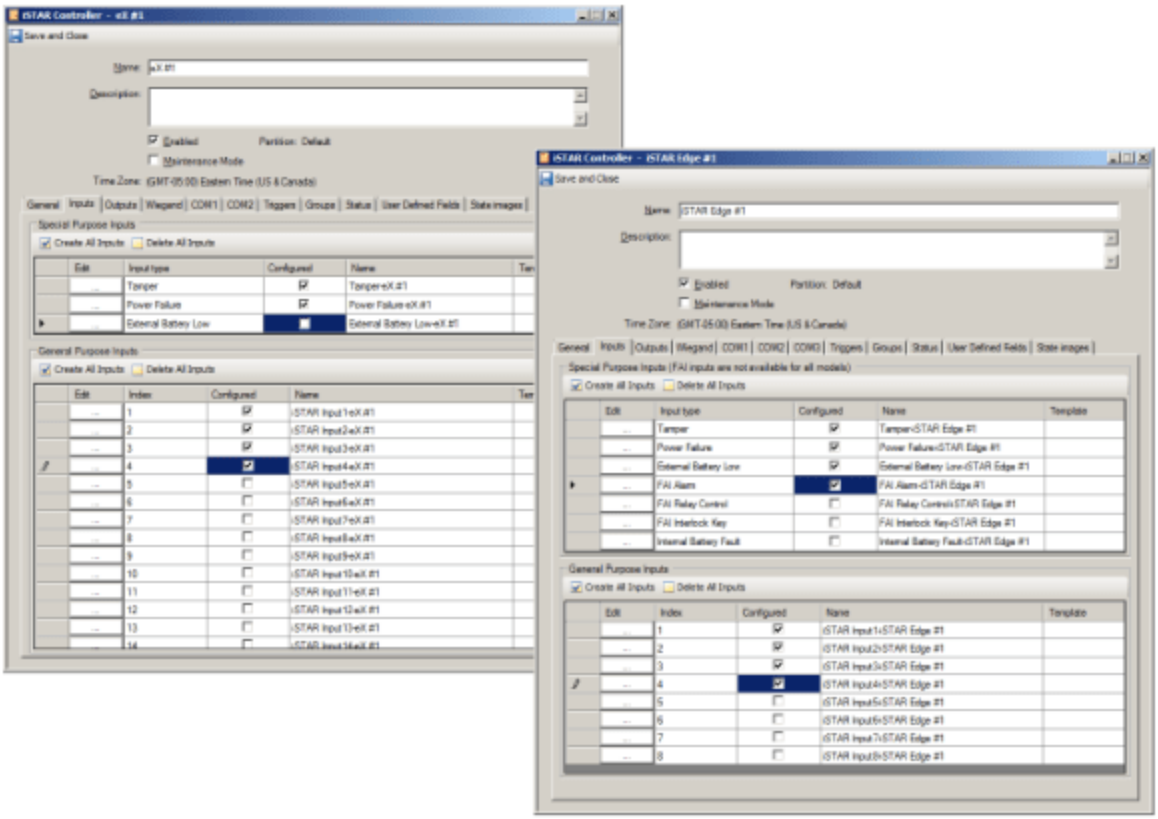
There are two basic FAI modes that can be configured at the controller.

- FAI without Latch - This method requires the F (Fire) input (NC) of J40 plus the individual enable switches for each relay (SW2 through SW5).
- FAI with Latch and subsequent Unlatch - This method requires the F (Fire) input of J40 plus the individual enable switches for each relay (SW2 through SW5), plus SW6 to enable the Latch and J40 K (Key) input (NO) to reset the Latch.

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

The FAI mode chosen at the controller will determine how you might want to use the Triggers and Actions available in the software to provide notification of a fire alarm and related actions. See the *iSTAR Edge Installation and Configuration Guide* for detailed information about wiring the FAI inputs.

Figure 51: iSTAR eX and iSTAR Edge Controller Editor Inputs Tab



To Configure the iSTAR eX/Edge Controller Inputs Tab

1. From the iSTAR Ex/Edge Controller Editor, click the **Inputs** tab.
2. Create the **Special Purpose Inputs** that you need by clicking **Create All Inputs** or by selecting the **Configured** check box for only the Inputs you wish to create.
3. Click [...] in the **Edit** column to configure individual Special Purpose Inputs. See the definitions of the Special Purpose Inputs in Table 24 on Page 163 and see iSTAR Input Editor on Page 232 for configuration instructions.
4. Create the **General Purpose Inputs** that you need by clicking **Create All Inputs** or by selecting the **Configured** check box for only the Inputs you wish to create.
5. Click [...] in the **Edit** column to configure individual General Purpose Inputs. See the definitions of the General Purpose Inputs in Table 24 on Page 163 and see iSTAR Input Editor on Page 232.
6. Click **Save and Close** to save the settings you have configured on the iSTAR Controller Inputs tab, or click another tab in the iSTAR Controller Editor to perform additional configuration.

iSTAR eX/Edge Controller Inputs Tab Definitions

The iSTAR eX and iSTAR Edge Inputs tabs include the fields and buttons detailed in Table 24 on Page 163.

Table 24: iSTAR eX and iSTAR Edge Inputs Tab Definitions

Field/Button	Description
Special Purpose Inputs	
Create All Inputs	Click to create all the Special Purpose Inputs. When you click **Create All Inputs** the Configured column check boxes are selected, and you can click ... in the **Edit** column to open the iSTAR Input Editor to configure an Input.
Delete All Inputs	When you click **Delete All Inputs**, the check boxes in the **Configured** column are cleared for all Special Purpose Inputs, and all these Inputs are immediately deleted (any settings you have configured are lost). You will need to confirm each deletion.
Edit column	Click ... in the **Edit** column to open the iSTAR Input Editor to configure a Special Purpose Input. See iSTAR Input Editor on Page 232.
Input Type column	This column displays the type of each Special Purpose Input.
Configured column	Click ☐ in this column to create an input (make it available to be edited).
Name column	Displays the name for this Input. The name is system-generated by default, but you can edit this name by clicking in this field.
Template column	Click in this column, then click ... to select an Input template to use for creating this Input from the list of available Input templates.You can only select a Template prior to creating the input.
Tamper	The **Tamper** input activates when the controller cabinet is opened or removed from its mounting surface. Select the check box in the **Configured** column and click ... in the **Edit** column to open the iSTAR Input Editor. From the Input Editor you can configure the settings and link to events through triggers.
Power Failure	The **Power Failure** input monitors the AC power failure output of a battery backup unit, such as the Advanced Power System (apS). When this alarm input activates, it specifies that the GCM has lost its primary power source, and is operating on batteries.
Battery Low	The **Battery Low** input activates when the emergency DC battery is running low on power.
FAI Supervision State	(iSTAR Edge only) – This is the F (Fire) Input State. Indicates the state of the F (Fire) input coming into J40 of the iSTAR Edge. In other words, this is the fire alarm.
FAI Key Supervision State	(iSTAR Edge only) – This is the K (Key) input state. Indicates the state of the K (Key) switch at J40 of the iSTAR Edge.
FAI Relay Control	(iSTAR Edge only) – This pseudo input indicates the state of the Relay Drive signal that activates or latches the selected relays when the F (Fire) input is true,
Onboard Battery Low (iSTAR Edge only)	The **Onboard Battery Low** activates when the voltage of all four onboard AA alkaline batteries in series reaches 4.6 volts, or if a battery is missing or disconnected. Upon loss of external or PoE power to the Edge, data is written to onboard flash. Four onboard non-rechargeable alkaline AA batteries provide power for the backup process and maintaining the clock afterwards. Backup is valid for the period the onboard batteries can maintain the clock. The period has been tested for >3 days, but should reasonably last for 2 weeks.

iSTAR eX and iSTAR Edge Inputs Tab Definitions (continued)

Field/Button	Description
General Purpose Inputs	
Create All Inputs	Click to create all the General Purpose Inputs. When you click **Create All Inputs** the **Configured** column check boxes are selected, and you can click ... in the **Edit** column to open the iSTAR Input Editor to configure an Input.
Delete All Inputs	When you click **Delete All Inputs**, the check boxes in the Configured column are cleared for all General Purpose Inputs, and all these Inputs are immediately deleted (any settings you have configured are lost).
Edit column	Click ... in the **Edit** column to open the iSTAR Input Editor to configure a General Purpose Input. See iSTAR Input Editor on Page 232.
Index column	This column displays the number of each General Purpose Input.
Configured column	Click in this column to create an input (make it available to be edited).
Name column	Displays the name for this Input. The name is system-generated by default, but you can edit this name by clicking in click in this field.
Template column	Click in this column, then click ... to select an Input template to use for creating this Input from the list of available Input templates.You can only select a Template prior to creating the input.
Index 1 - 8 (iSTAR Edge) Index 1 - 16 (iSTAR eX)	The General Purpose Inputs can be configured in an iSTAR Door as door switch monitor or request to exit inputs. Select the check box in the **Configured** column and click ... in the **Edit** column to open the iSTAR Input Editor. From the editor you can configure the settings for a General Purpose Input.

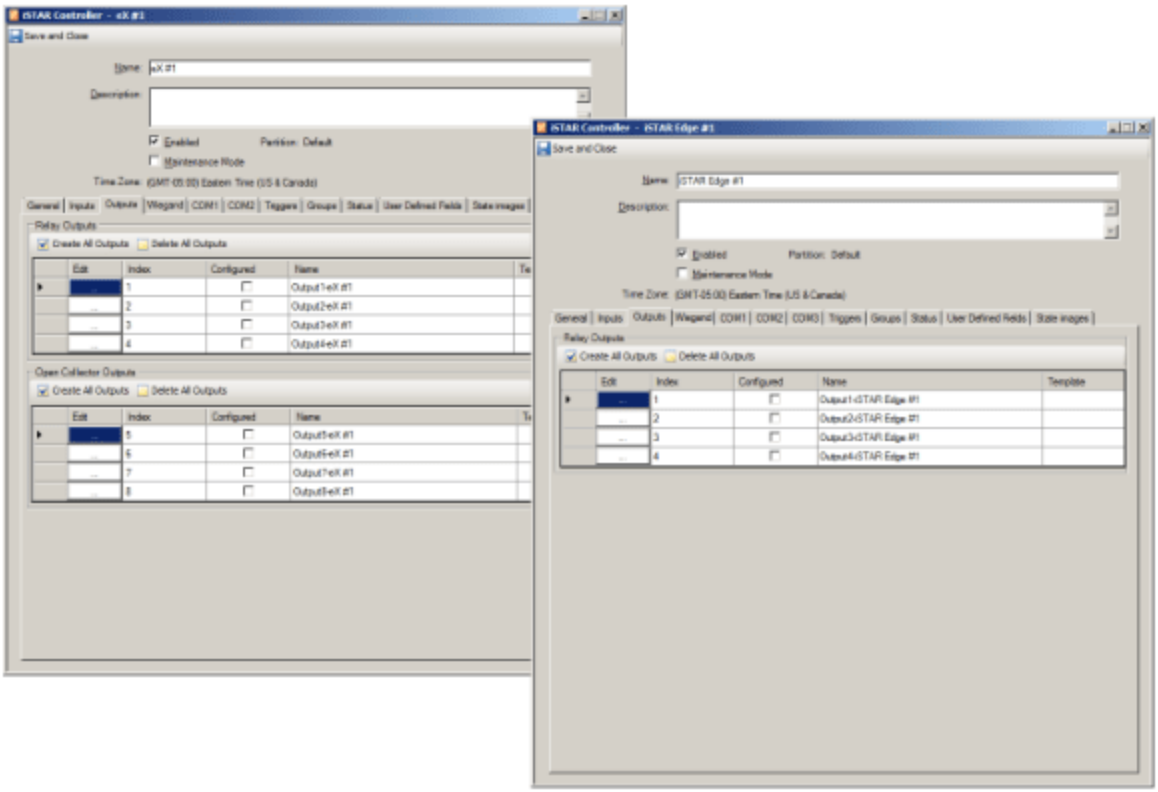
iSTAR Edge/eX Controller Outputs Tab

The iSTAR Controller Outputs tab is available only on the iSTAR eX Controller editor and the iSTAR Edge Controller editor.

The Outputs tab in the iSTAR Controller Editor lets you define four Relay Outputs and four Open Collector Outputs (on the iSTAR eX only).

The iSTAR ex and iSTAR Edge Outputs tabs are shown in Figure 52 on Page 165.

Figure 52: iSTAR eX and iSTAR Edge Controller Editor Outputs Tab



To Configure the iSTAR eX/Edge Outputs Tab

1. From the iSTAR Ex/Edge Controller Editor, click the Outputs tab.
2. Create the **Relay Outputs** that you need by clicking **Create All Outputs** or by selecting the **Configured** check box for only the Outputs you wish to create.
3. Click ... in the **Edit** column to configure individual Relay Outputs. See the definitions of the Relay Outputs in Table 25 on Page 166 and see iSTAR Output Editor on Page 241 for configuration instructions.
4. On an iSTAR eX, create the **Open Collector Outputs** that you need by clicking **Create All Outputs** or by selecting the **Configured** check box for only the Outputs you wish to create.
5. Click ... in the **Edit** column to configure individual Open Collector Outputs. See the definitions of the Open Collector Outputs in Table 25 on Page 166 and see iSTAR Output Editor on Page 241 for configuration instructions.
6. Click **Save and Close** to save the settings you have configured on the iSTAR Controller Outputs tab, or click another tab in the iSTAR Controller Editor to perform additional configuration.

iSTAR eX/Edge Controller Outputs Tab Definitions

The iSTAR eX and iSTAR Edge Outputs tab includes the fields and buttons detailed in Table 25 on Page 166.

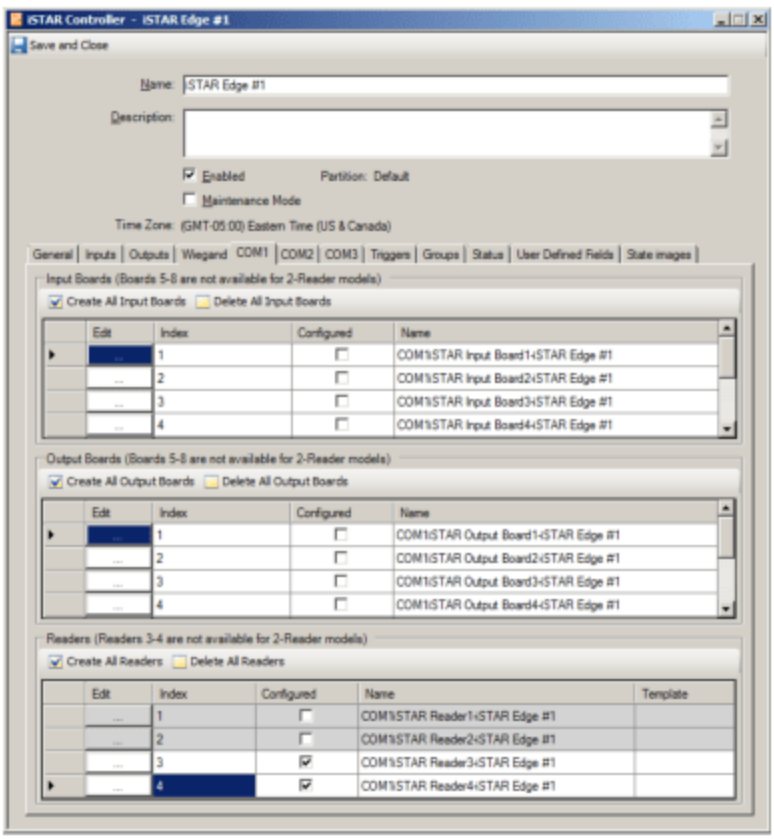
Table 25: iSTAR eX and iSTAR Edge Outputs Tab Definitions

Box	Description
Relay Outputs (iSTAR ex and iSTAR Edge)	
Create All Outputs	Click to create all the Relay Outputs. When you click **Create All Outputs** the **Configured** column check boxes are selected, and you can click ... in the **Edit** column to open the iSTAR Output Editor to configure an Output.
Delete All Inputs	When you click **Delete All Outputs**, the check boxes in the **Configured** column are cleared for all Relay Outputs, and all these Outputs are immediately deleted (any settings you have configured are lost).
Edit column	Click ... in the **Edit** column to open the iSTAR Output Editor to configure a Relay Output. See iSTAR Output Editor on Page 241.
Index column	This column displays the number of each Relay Output.
Configured column	Click ☐ in this column to create an Output (make it available to be edited).
Name column	Displays the name for this Output. The name is system-generated by default, but you can edit this name by clicking in this field.
Template column	Click in this column, then click ... to select an Output template to use for creating this Output from the list of available Output templates.You can only select a Template prior to creating the Output.
Relay Outputs 1 - 4	Select the check box in the **Configured** column and click ... located in the **Edit** column to open the iSTAR Output Editor. From the editor you can configure the settings for the Relay Output.
Open Collector Outputs (iSTAR eX Only)	
Create All Outputs	Click to create all the Open Collector Outputs. When you click **Create All Outputs** the **Configured** column check boxes are selected, and you can click ... in the **Edit** column to open the iSTAR Output Editor to configure an Output.
Delete All Outputs	When you click **Delete All Outputs**, the check boxes in the **Configured** column are cleared for all Open Collector Outputs, and all these Outputs are immediately deleted (any settings you have configured are lost).
Edit column	Click ... in the **Edit** column to open the iSTAR Output Editor to configure an Open Collector Output. See iSTAR Output Editor on Page 241.
Index column	This column displays the type of each Open Collector Output.
Configured column	Click ☐ in this column to create an Output (make it available to be edited).
Name column	Displays the name for this Output. The name is system-generated by default, but you can edit this name by clicking in this field.
Template column	Click in this column, then click ... to select an Output template to use for creating this Output from the list of available Output templates.You can only select a Template prior to creating the Output.
Open Collector Outputs 5 - 8	Select the check box in the **Configured** column and click ... located in the **Edit** column to open the iSTAR Output Editor. From the editor you can configure the settings for an Open Collector Output.

iSTAR Edge COM1/COM2/COM3 Tabs

The COM1, COM2, and COM3 tabs in the iSTAR Edge Controller Editor let you define security objects that are connected to the COM1, COM2, and COM3 ports. RM readers, I/8s, and R/8s can be connected to the COMx ports.

Figure 53: iSTAR Edge Controller COM Tabs



The iSTAR Edge can support either two or four Readers, depending on the model.

These Readers can be configured on either the Readers tab or on the COM1, COM2, or COM3 tabs in any combination, as long as the total number of Readers does not exceed the maximum allowed.

The number of I/8 and R/8 bus modules that are supported on the COMx ports depend upon the model:

- Four I/8 s and four R/8s are supported on the two-reader model.
- Eight I/8 s and eight R/8s are supported on the four-reader model.

To Configure the iSTAR Edge COM1, COM2, or COM3 Tab

1. From the iSTAR Edge Controller Editor, click the COMx tab.
2. In the Input Boards table, create the **Input Boards** that you need by clicking **Create All Input Boards** or by selecting the **Configured** check box for only the Input Boards you wish to create.
3. Click [...] in the Edit column to configure individual Input Boards. See the definitions of the Input Boards in Table 29 on Page 176 and see iSTAR Input Board Editor on Page 203 for configuration instructions.

4. In the Output Boards table, create the **Output Boards** that you need by clicking **Create All Outputs** or by selecting the **Configured** check box for only the Output boards you wish to create.
5. Click [...] in the Edit column to configure individual Output Boards. See the definitions of the Output Boards in Table 29 on Page 176 and see iSTAR Output Board Editor on Page 208 for configuration instructions.
6. In the Reader Boards table, create the **Readers** that you need by clicking **Create All Readers** or by selecting the **Configured** check box for only the Reader you wish to create.
7. Click [...] in the Edit column to configure individual Readers. See the definitions of the Readers in Table 29 on Page 176 and see iSTAR Reader Editor on Page 248 for configuration instructions.
8. Click **Save and Close** to save the settings you have configured on the iSTAR Controller COM tabs, or click another tab in the iSTAR Controller Editor to perform additional configuration.

iSTAR Edge COM Tabs Definitions

Table 26: iSTAR Edge COM Tabs Definitions

Box	Description
Input Boards	
Create All Input Boards	Click to create all the Input Boards. When you click **Create All Input Boards** the Configured column check boxes are selected, and you can click [...] in the Edit column to open the iSTAR Input Board Editor to configure an Input Board.
Delete All Inputs Boards	When you click **Delete All Input Boards**, the check boxes in the Configured column are cleared for all Input Boards, and all these Input Boards are immediately deleted (any settings you have configured are lost).
Edit column	Click [...] in the **Edit** column to open the iSTAR Input Board Editor to configure an Input Board. See iSTAR Input Board Editor on Page 203.
Index column	This column displays the number of each Input Board.
Configured column	Click [ ] in this column to create an Input Board (make it available to be edited).
Name column	Displays the name for this Input Board. The name is system-generated by default, but you can edit this name by clicking in this field.
Input Boards 1 - 8	Select the check box in the **Configured** column and click [...] in the **Edit** column to open the iSTAR Input Board Editor. From the editor you can configure the settings for the Input Board.
Output Boards	
Create All Output Boards	Click to create all the Output Boards. When you click **Create All Output Boards** the Configured column check boxes are selected, and you can click [...] in the Edit column to open the iSTAR Output Board Editor to configure an Output Board.

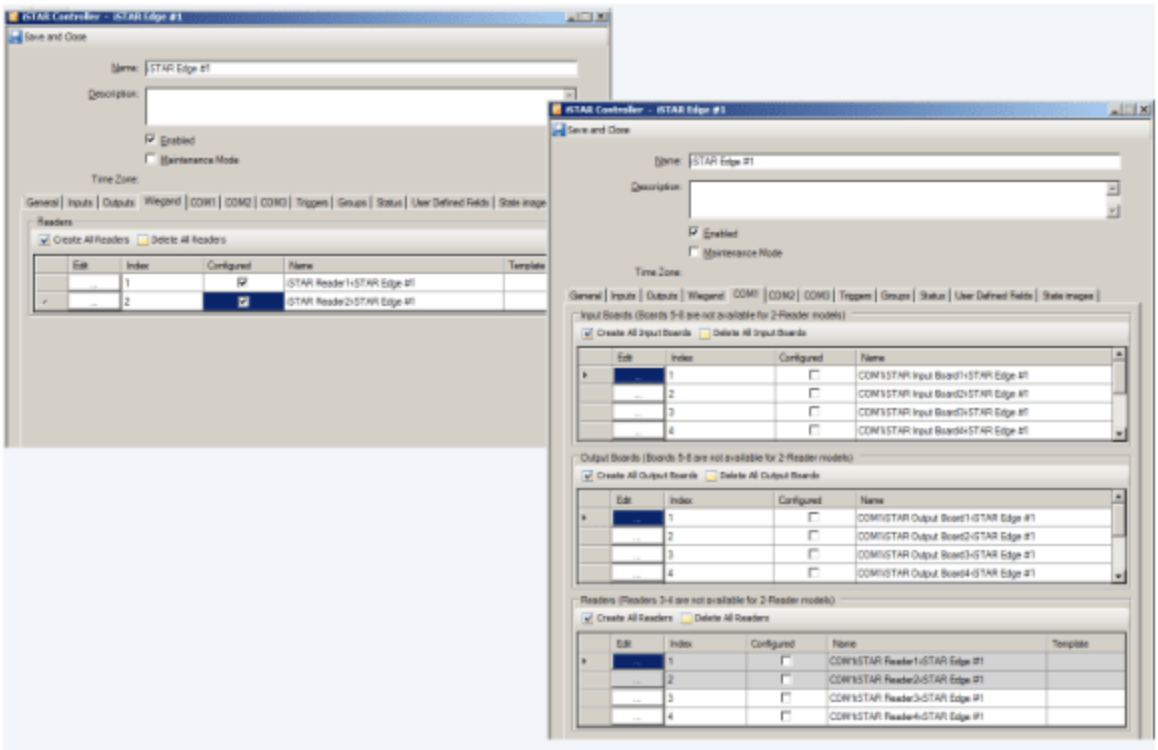
Table 26: iSTAR Edge COM Tabs Definitions (continued)

Box	Description
Delete All Output Boards	When you click **Delete All Output Boards**, the check boxes in the Configured column are cleared for all Output Boards, and all these Output Boards are immediately deleted (any settings you have configured are lost).
Output Boards 1 - 8	Select the check box in the **Configured** column and click ... in the **Edit** column to open the iSTAR Output Board Editor. From the editor you can configure the settings for the Output Board.
Readers	
Create All Readers	Click to create all the Readers. When you click **Create All Readers** the **Configured** column check boxes are selected, and you can click ... in the **Edit** column to open the iSTAR Reader Editor to configure a Reader.
Delete All Readers	When you click **Delete All Readers**, the check boxes in the **Configured** column are cleared for all Readers, and all these Readers are immediately deleted (any settings you have configured are lost).
Readers 1 - 4	Select the check box in the **Configured** column and click ... in the **Edit** column to open the iSTAR Reader Editor. From the editor you can configure the settings for the Reader. You can create up to four Readers in this table for an iSTAR Edge, but if your iSTAR Edge is not a 4-reader model, Readers 3 - 4 will not function. The Template column shows the template name if you selected a Template prior to creating the Reader.

iSTAR Edge Controller Wiegand Tab

The iSTAR Edge Controller Editor Wiegand tab, shown in Figure 54 on Page 170, allows you to configure direct connect Reader devices. Readers that are not connected directly are configured on the COM1, COM2, or COM3 tabs.

Figure 54: iSTAR Edge Controller Editor Wiegand and COM1 Tabs



The Readers can be configured on either the **Wiegand** tab or on the **COM1**, **COM2**, or **COM3** tab in any combination, as long as the total number of Readers does not exceed the maximum allowed.

The iSTAR Edge supports a maximum of either two readers or four readers depending on the model.

You can configure up to two Readers on the Wiegand tab, and the remaining Readers, in any combination, on the COM1, COM2, and COM3 tabs. See the *iSTAR Edge Installation and Configuration Guide* for more information about the two models.

Example:

If you configure two Readers on the iSTAR Edge Wiegand tab, the iSTAR Edge Controller Editor makes the Reader 1 - 2 objects on the COM1 and COM2 tabs unavailable (shaded gray) leaving Reader 3 - 4 objects available.

To Configure the iSTAR Edge Wiegand Tab

1. From the iSTAR Edge Controller Editor, click the Wiegand tab.
2. Create the **Readers** that you need by clicking **Create All Readers** or by selecting the **Configured** check box for only the Readers you wish to create.
3. Click [...] in the **Edit** column to configure individual Readers. See the definitions of the Readers in Table 27 on Page 171 and see iSTAR Reader Editor on Page 248 for configuration instructions.
4. Click **Save and Close** to save the settings you have configured on the iSTAR Controller Wiegand tab, or click another tab in the iSTAR Controller Editor to perform additional configuration.

iSTAR Edge Controller Wiegand Tab Definitions

The iSTAR Edge Wiegand tab includes the fields and buttons detailed in Table 27 on Page 171.

Table 27: iSTAR Edge Wiegand Tab Definitions

Box	Description
Create All Readers	Click to create all the Readers. When you click **Create All Readers**, the **Configured** column check boxes are selected, and you can click ... in the **Edit** column to open the iSTAR Reader Editor to configure a Reader.
Delete All Readers	When you click **Delete All Readers**, the check boxes in the **Configured** column are cleared for all Readers, and all these Readers are immediately deleted (any settings you have configured are lost).
Edit column	Click ... in the **Edit** column to open the iSTAR Reader Editor to configure a Reader. See iSTAR Reader Editor on Page 248.
Index column	This column displays the number for each reader. This number is the physical port number for a Direct Connect Wiegand reader.
Configured column	Click in this column to create a reader (make it available to be edited).
Name column	Displays the name for this Reader. The name is system-generated by default, but you can edit this name by clicking in this field.
Template column	Click in this column prior to creating the Reader, then click ... to select a Reader template from the list of available Reader templates. The **Template** column shows the template name chosen if you selected a Template prior to creating the Reader.
Readers 1 - 2	Select the check box in the **Configured** column for a Reader and click ... located in the **Edit** column to open the iSTAR Reader Editor General tab to configure the Options, Triggers, Groups, Status and State Images that are associated with a Reader. See iSTAR Reader Editor on Page 248 for detailed instructions for configuring iSTAR Readers. If the row in this table for a particular reader is unavailable for selection (shaded gray) it indicates that this reader number is configured on one of the COM tabs in the iSTAR Controller Editor. The **Name** column displays a name comprised of the Reader Type and the iSTAR Controller name. You can click in this column to edit the Reader name.

iSTAR eX Controller Wiegand Tab

The iSTAR eX Wiegand tab, shown in Figure 55 on Page 172, allows you to configure direct connect Reader devices. Readers that are not connected directly are configured on the COM1 or COM2 tabs.

The iSTAR eX can support up to a total of eight Readers if an iSTAR eX Security Key is installed, or four Readers without the Security Key.

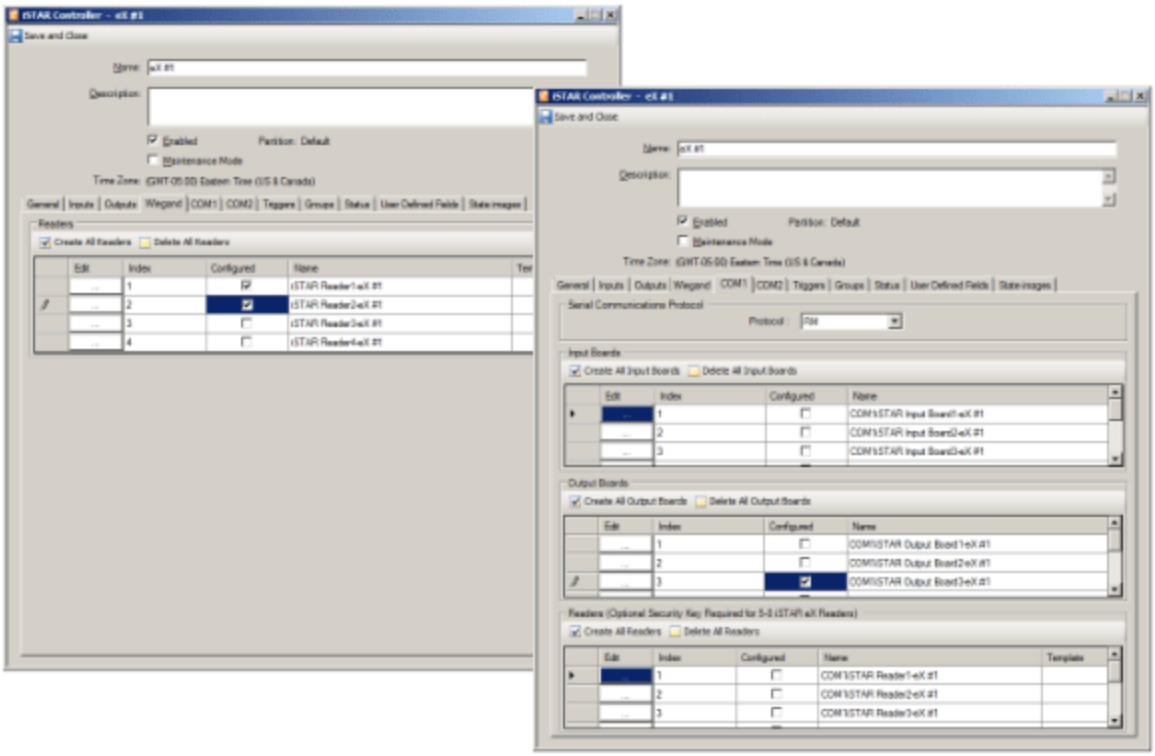
These Readers can be configured on either the Readers tab or on the COM1 or COM2 tabs in any combination, as long as the total number of Readers does not exceed the maximum allowed.

For iSTAR eX, you can configure up to four of these Readers on the iSTAR eX Wiegand tab, and the remaining Readers, in any combination, on the COM1 and COM2 tabs. See the *iSTAR eX Installation and Configuration Guide* for more information about the iSTAR eX Security Key.

Example:

If you configure Readers 1 and 2 on the iSTAR eX Wiegand tab, the iSTAR eX Controller Editor makes the Reader 1 and 2 objects on the COM1 and COM2 tabs unavailable (shaded gray). Conversely, when you add Readers 3 and 4 to one of the COMx tabs, the corresponding readers on the Wiegand tab are unavailable.

Figure 55: iSTAR eX Wiegand and COMx Tabs



To Configure the iSTAR eX Wiegand Tab

1. From the iSTAR eX Controller Editor, click the Wiegand tab.
2. Create the **Readers** that you need by clicking **Create All Readers** or by selecting the **Configured** check box for only the Readers you wish to create.
3. Click [...] in the **Edit** column to configure individual Readers. See the definitions of the Readers in Table 28 on Page 173 and see iSTAR Reader Editor on Page 248 for configuration instructions.
4. Click **Save and Close** to save the settings you have configured on the iSTAR Controller Wiegand tab, or click another tab in the iSTAR Controller Editor to perform additional configuration.

iSTAR eX Controller Wiegand Tab Definitions

The iSTAR eX Wiegand tab includes the fields and buttons detailed in Table 28 on Page 173.

Table 28: iSTAR eX Wiegand Tab Definitions

Box	Description
Create All Readers	Click to create all the Readers. When you click **Create All Readers**, the **Configured** column check boxes are selected, and you can click ... in the **Edit** column to open the iSTAR Reader Editor to configure a Reader.
Delete All Readers	When you click **Delete All Readers**, the check boxes in the **Configured** column are cleared for all Readers, and all these Readers are immediately deleted (any settings you have configured are lost).
Edit column	Click ... in the **Edit** column to open the iSTAR Reader Editor to configure a Reader. See iSTAR Reader Editor on Page 248.
Index column	This column displays the number for each reader. This number is the physical port number for a Direct Connect Wiegand reader.
Configured column	Click in this column to create a reader (make it available to be edited).
Name column	Displays the name for this Reader. The name is system-generated by default, but you can edit this name by clicking in this field.
Template column	Click in this column prior to creating the Reader, then click ... to select a Reader template from the list of available Reader templates. The **Template** column shows the template name chosen if you selected a Template prior to creating the Reader.
Readers 1 - 8 Readers 5 - 8 are only available if the 8 reader USB key is present in the GCM.	Select the check box in the **Configured** column for a Reader and click ... located in the **Edit** column to open the iSTAR Reader Editor General tab to configure the Options, Triggers, Groups, Status and State Images that are associated with a Reader. See iSTAR Reader Editor on Page 248 for detailed instructions for configuring iSTAR Readers. If the row in this table for a particular reader is unavailable for selection (shaded gray) it indicates that this reader number is configured on one of the COM tabs in the iSTAR Controller Editor. In Figure 55 on Page 172, for example, Reader #4 is configured on another tab. The **Name** column displays a name comprised of the Reader Type and the iSTAR Controller name. You can click in this column to edit the Reader name.

iSTAR eX COM1/COM2 Tabs

The COM1 and COM2 tabs in the iSTAR eX Controller Editor, let you define security objects that are connected to the COM1 and COM2 ports.

The iSTAR eX Contoller COM1 and COM2 tabs have a **Protocol** drop-down list that lets you choose the type of serial communications board is connected to the controller:

- COM1 or COM2 Schlage Wireless PIM on Page 173
- COM1 or COM2 RM Communications on Page 174

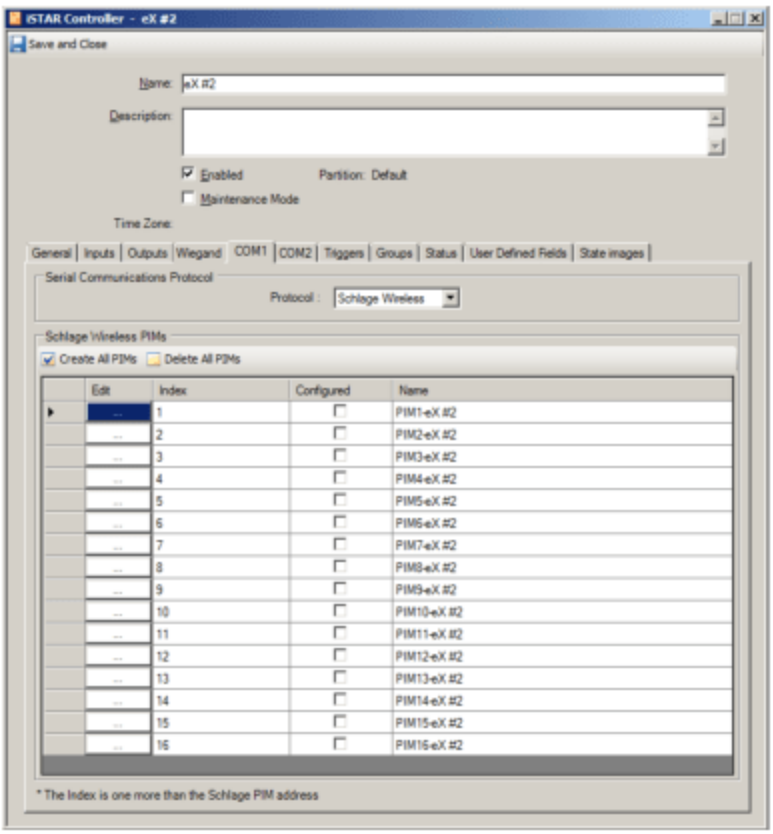
The options available on the COM1 or COM2 tab depend upon which Serial Communications option you select.

COM1 or COM2 Schlage Wireless PIM

If you select **Schlage Wireless** from the Protocol drop-down list, the COM1 or COM2 tab displays 16 possible PIM Boards that you can configure.

See Figure 56 on Page 174, which shows the COM1 and COM2 tabs for an iSTAR eX.

Figure 56: iSTAR eX Controller COM Tab with Schlage PIM Boards



To Configure the iSTAR eX COM1 or COM2 Tab for Schlage Wireless PIMs

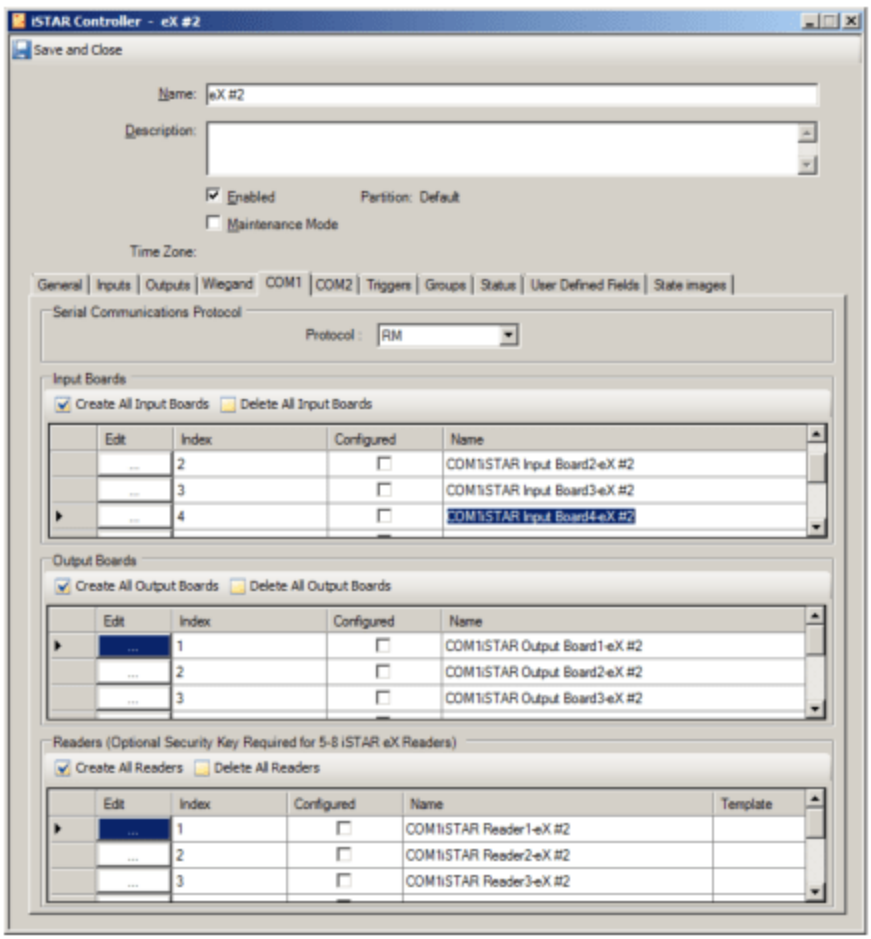
1. From the iSTAR Ex Controller Editor, click one of the COM tabs.
2. Select **Schlage Wireless** from the **Protocol** drop-down list.
3. In the Schlage Wireles PIMs table that appears, create the **PIMs** that you need by clicking **Create All PIMs** or by selecting the **Configured** check box for only the PIMs you wish to create.
4. Click [...] in the Edit column to configure individual PIMs. See:
   - iSTAR Schlage Wireless PIMs Tab Definitions on Page 155 for definitions for the PIM board fields and buttons.
   - iSTAR PIM-485 Reader I/O Tab on Page 261 for configuration instructions.
5. Click **Save and Close** to save the settings you have configured on the iSTAR Controller COM tabs.

COM1 or COM2 RM Communications

If you select the **RM** option from the Protocol drop-down list, the COM1 or COM2 tab displays 4 Input Boards, 4 Output Boards, and up to 8 RM Readers that you can configure.

Figure 57 on Page 175 shows the COM1 and COM2 tabs for an iSTAR eX.

Figure 57: iSTAR eX Controller COM Tabs



The iSTAR eX can support up to four Readers, and an additional four Readers if equipped with an iSTAR eX Security Key.

These Readers can be configured on either the Readers tab or on the COM1 or COM2 tabs, in any combination, as long as the total number of Readers does not exceed the maximum allowed.

Example:

If you configure two Readers on the iSTAR eX Controller Readers tab and two Readers on the COM1 tab, the Editor makes the remaining Reader connections on the Reader, COM1, and COM2 tabs unavailable. Sections of the COM tab are shaded gray (unavailable) to signify that these devices are configured on another tab.

If you select the RM option from the **Protocol** drop-down list, COM1 and COM2 are configured to support RM bus readers. The iSTAR eX can support up to four RM reader devices (or eight Readers if the iSTAR eX Security Key is installed). A total of eight I/8 and eight R/8 devices can also be configured on the iSTAR eX on COM1 and/or COM2.

NOTE However you configure iSTAR eX Readers, they must match the setting of the S1 switch on the PMB. The S1 switches define which COM port the RM ports are connected to in the hardware. See the *iSTAR eX Installation and Configuration Guide*.

To Configure the iSTAR eX COM1 or COM2 Tab

1. From the iSTAR Ex Controller Editor, click one of the COM tabs.
2. Select RM from the **Protocol** drop-down list.
3. In the Input Boards table, create the **Input Boards** that you need by clicking **Create All Input Boards** or by selecting the **Configured** check box for only the Input Boards you wish to create.
4. Click [...] in the Edit column to configure individual Input Boards. See the definitions of the Input Boards in Table 29 on Page 176 and see iSTAR Input Board Editor on Page 203 for configuration instructions.
5. In the Output Boards table, create the **Output Boards** that you need by clicking **Create All Outputs** or by selecting the **Configured** check box for only the Output boards you wish to create.
6. Click [...] in the Edit column to configure individual Output Boards. See the definitions of the Output Boards in Table 29 on Page 176 and see iSTAR Output Board Editor on Page 208 for configuration instructions.
7. In the Readers Boards table, create the **Readers** that you need by clicking **Create All Readers** or by selecting the **Configured** check box for only the Reader you wish to create.
8. Click [...] in the Edit column to configure individual Readers. See the definitions of the Readers in Table 29 on Page 176 and see iSTAR Reader Editor on Page 248 for configuration instructions.
9. Click **Save and Close** to save the settings you have configured on the iSTAR Controller COM tabs, or click another tab in the iSTAR Controller Editor to perform additional configuration.

iSTAR eX COM Tabs Definitions

Table 29 on Page 176 contains definitions for the fields and buttons on the iSTAR eX COM tabs.

Table 29: iSTAR eX COM Tabs Definitions

Box	Description
Input Boards	
Create All Input Boards	Click to create all the Input Boards. When you click **Create All Input Boards** the Configured column check boxes are selected, and you can click [...] in the Edit column to open the iSTAR Input Board Editor to configure an Input Board.
Delete All Inputs Boards	When you click **Delete All Input Boards**, the check boxes in the Configured column are cleared for all Input Boards, and all these Input Boards are immediately deleted (any settings you have configured are lost).
Edit column	Click [...] in the **Edit** column to open the iSTAR Input Board Editor to configure an Input Board. See iSTAR Input Board Editor on Page 203.
Index column	This column displays the number of each Input Board.
Configured column	Click [ ] in this column to create an Input Board (make it available to be edited).

Table 29: iSTAR eX COM Tabs Definitions (continued)

Box	Description
Name column	Displays the name for this Input Board. The name is system-generated by default, but you can edit this name by clicking in this field.
Input Boards 1 - 8	Select the check box in the **Configured** column and click ... in the **Edit** column to open the iSTAR Input Board Editor. From the editor you can configure the settings for the Input Board.
Output Boards	
Create All Output Boards	Click to create all the Output Boards. When you click **Create All Output Boards** the Configured column check boxes are selected, and you can click ... in the Edit column to open the iSTAR Output Board Editor to configure an Output Board.
Delete All Output Boards	When you click **Delete All Output Boards**, the check boxes in the Configured column are cleared for all Output Boards, and all these Output Boards are immediately deleted (any settings you have configured are lost).
Output Boards 1 - 8	Select the check box in the **Configured** column and click ... in the **Edit** column to open the iSTAR Output Board Editor. From the editor you can configure the settings for the Output Board.
Readers	
Create All Readers	Click to create all the Readers. When you click **Create All Readers** the **Configured** column check boxes are selected, and you can click ... in the **Edit** column to open the iSTAR Reader Editor to configure a Reader.
Delete All Readers	When you click **Delete All Readers**, the check boxes in the **Configured** column are cleared for all Readers, and all these Readers are immediately deleted (any settings you have configured are lost).
Readers 1 - 8	Select the check box in the **Configured** column and click ... in the **Edit** column to open the iSTAR Reader Editor. From the editor you can configure the settings for the Reader. You can create up to eight Readers in this table for an iSTAR eX, but if your iSTAR eX does not have an iSTAR eX Security key, Readers 5-8 will not function. The Template column shows the template name if you selected a Template prior to creating the Reader.

iSTAR Ultra Controller Editor Inputs Tab

The Inputs tab (shown in Figure 2 on Page 178) lets you define the Main Board (GCM) inputs for the Controller.

All of the inputs support event triggers based on their active or inactive states. These triggers can activate alarms, send emails, run a Roll Call Report, etc.

The Input tab fields and buttons are described in Table 2 on Page 178.

Figure 2: Inputs Tab

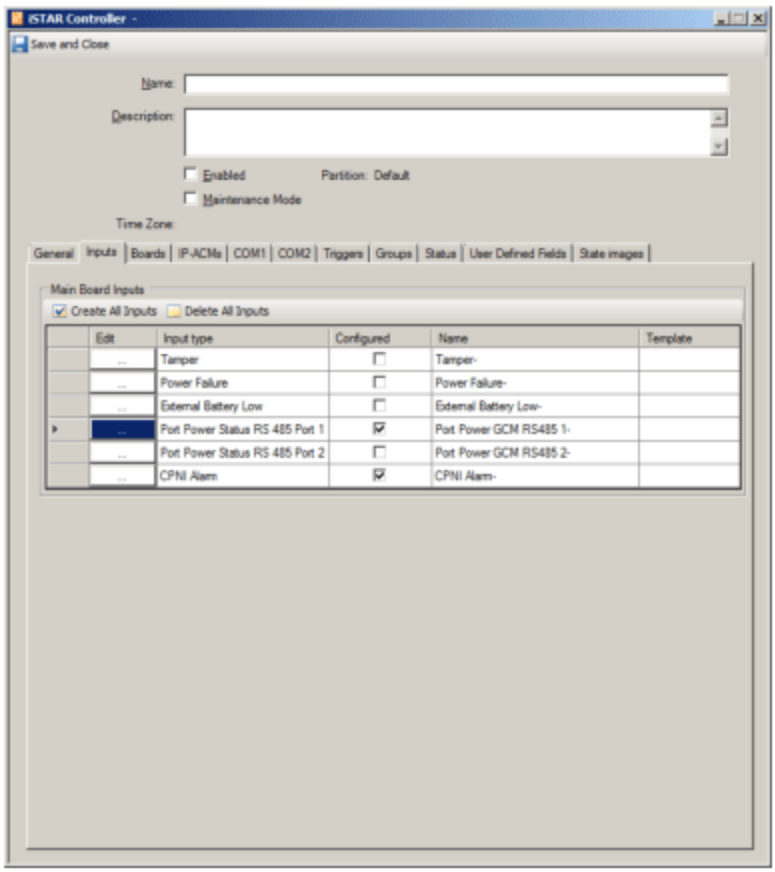


Table 2: Ultra Inputs Tab Definitions

Field/Button	Description
Main Board Inputs	
Create All Inputs	Click to create all the Main Board Inputs. When you click **Create All Inputs** the Configured column check boxes are selected, and you can click ... in the **Edit** column to open the iSTAR Input Editor to configure an Input.
Delete All Inputs	When you click **Delete All Inputs**, the check boxes in the **Configured** column are cleared for all Main Board Inputs, and all these Inputs are immediately deleted (any settings you have configured are lost). You will need to confirm each deletion.

Ultra Inputs Tab Definitions (continued)

Field/Button	Description
Edit column	Click ... in the **Edit** column to open the iSTAR Input Editor to configure a Main Board Input. See iSTAR Input Editor on Page 232.
Input Type column	This column displays the type of each Main Board Input.
Configured column	Click in this column to create an input (make it available to be edited).
Name column	Displays the name for this Input. The name is system-generated by default, but you can edit this name by clicking in this field.
Template column	Click in this column, then click ... to select an Input template to use for creating this Input from the list of available Input templates.You can only select a Template prior to creating the input.
Input Type	
Tamper	Activates when the controller cabinet is opened or removed from its mounting surface. Select the check box in the **Configured** column and click ... in the **Edit** column to open the iSTAR Input Editor. From the Input Editor you can configure the settings and link to events through triggers.
Power Failure	Monitors the AC power failure output of a battery backup unit. When this alarm input activates, it specifies that the GCM has lost its primary power source, and is operating on batteries.
External Battery Low	Activates when the emergency DC battery is running low on power.
Port Power RS 485 Port 1/2	Activates if there is a problem with the power on the port.
CPNI Alarm	Activates if the CPNI (Centre for the Protection of National Infrastructure) switch S1-2 is changed.

NOTE Tamper, AC power fail, and Low battery inputs must be programmed for UL applications.

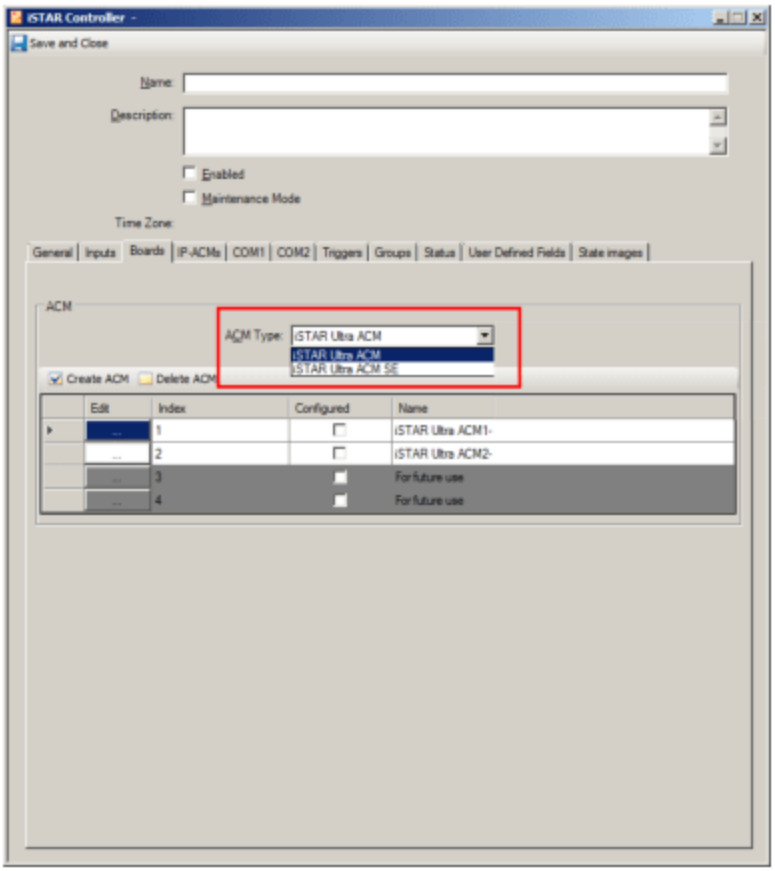
iSTAR Ultra Controller Boards Tab

Use the iSTAR Controller Editor Boards tab, shown in Figure 3 on Page 180, to select the ACM type and to open the iSTAR ACM Board editor to configure readers, outputs and inputs.

NOTE You must select the correct ACM type used by the controller:

- iSTAR Ultra - select **iSTAR Ultra ACM**.
- iSTAR Ultra SE - select **iSTAR Ultra SE ACM**.

Figure 3: iSTAR Controller Boards Tab



To Configure the iSTAR Controller Boards Tab

1. From the iSTAR Controller editor, click the **Boards** tab.
2. Select the iSTAR ACM type from the **ACM Type** drop-down menu.
   - iSTAR Ultra - select **iSTAR Ultra ACM**.
   - iSTAR Ultra SE - select **iSTAR Ultra SE ACM**.
3. Create the **ACM Boards** that you need by clicking **Create All ACMs**, or by selecting the **Configured** check box for only the ACMs you wish to create.
4. Click [...] in the **Edit** column to configure an ACM. See iSTAR Ultra Controller ACM Board Editor on Page 184
5. Click **Save and Close**.

Table 3: iSTAR Controller Boards Tab Definitions

Field/Button	Description
ACM Type	Select the iSTAR ACM type from the **ACM Type** drop-down menu. • iSTAR Ultra - select **iSTAR Ultra ACM**. • iSTAR Ultra SE - select **iSTAR Ultra SE ACM**
Create ACM	When you click **Create ACM** the Configured column check boxes are selected, and you can click [...] in the **Edit** column to open the iSTAR Ultra ACM Editor to configure the ACM.
Delete ACM	When you click **Delete ACM**, the check boxes in the **Configured** column are cleared for all ACMs, and are deleted (all configuration settings are lost).
Index	Select the check box in the **Configured** column and click [...] located in the **Edit** column to open the iSTAR Ultra ACM Editor to configure the Inputs, Outputs, and Readers that are associated with the ACM board.

iSTAR Ultra Controller IP-ACMs Tab

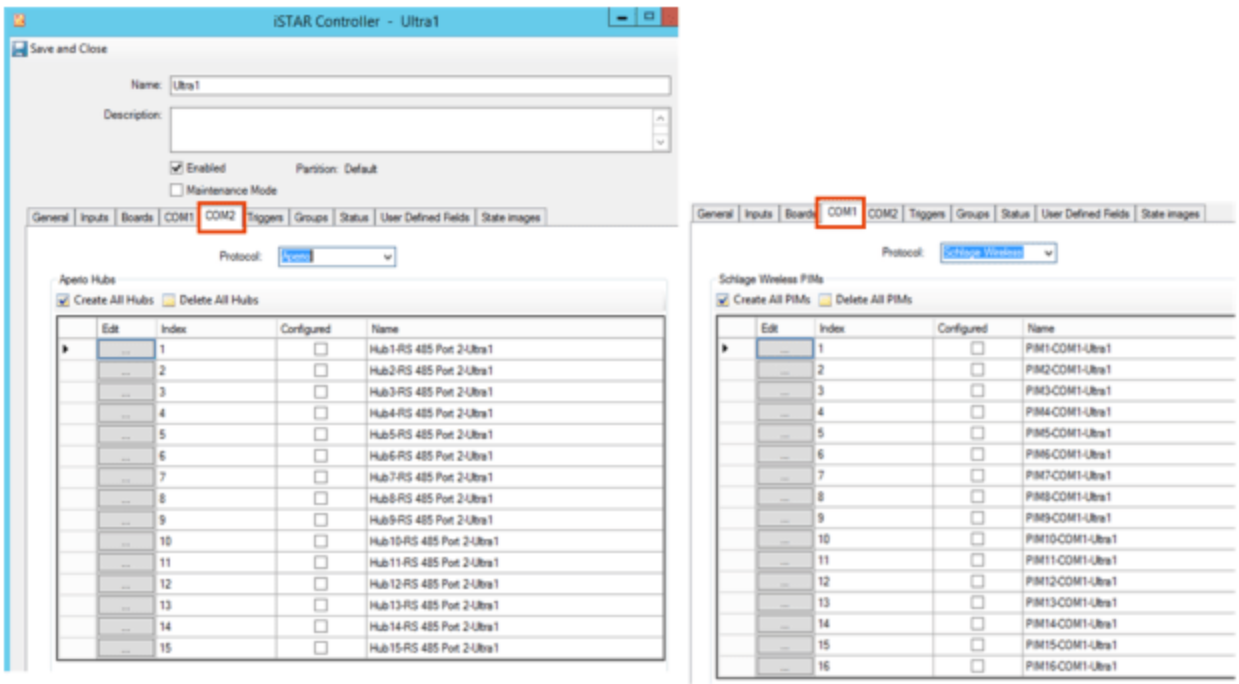
The IP-ACMs tab is used to configure the IP-ACM Offline Mode, readers, inputs, outputs, and triggers.

See Chapter 6, Configuring the IP-ACM for information about configuring the IP-ACM.

iSTAR Ultra COM1/COM2 Tabs

The COM1 and COM2 tabs in the iSTAR Ultra Controller Editor let you define security objects that are connected to the COM1 and COM2 ports. Aperio Hubs and Schlage PIMs can be configured for the COM1 and COM2 ports.

Figure 58: iSTAR Ultra Controller COM Tabs



The iSTAR Ultra can support up to 32 Readers. There can be up to 16 ACM Readers and up to 32 Aperio Readers or Schlage Readers, but the total number of readers cannot exceed 32. If you try to configure any additional readers, an error message appears. The iSTAR Ultra supports either Aperio or Schlage Wireless Readers. There cannot be a mixture of the two readers on one iSTAR Ultra.

The ACM Readers can be configured as Wiegand direct connect or RM bus as long as the total number of Readers does not exceed eight per ACM or sixteen per iSTAR Ultra.

The Aperio Readers can be configured on any of the possible 30 Hubs, in any combination, as long as the total number of Readers does not exceed 32.

There can be up to 15 Aperio Hubs per COMx port, allowing for a total of 30 Hubs per iSTAR Ultra. Each Hub can support up to 8, or 1, Assa Abloy Readers with a maximum of 16 readers per COMx port. This provides for a maximum of 32 readers per iSTAR Ultra.

NOTE If using a 1 Reader Hub, the maximum is 30 Aperio Readers (i.e., 1 Reader per Hub).

To Configure the iSTAR Ultra COM1 or COM2 Tab for Aperio

1. From the iSTAR Ultra Controller Editor, click the **COM**x tab.
2. Select **Aperio** in the **Protocol** field. This will also select Aperio in the other COMx tab.
3. In the **Aperio Hubs** table, create the **Aperio Hubs** that you need by by selecting the **Configured** check box for only the Hubs you wish to create.
4. Click [...] in the Edit column to configure individual Hubs. See the definitions of the Hubs in iSTAR Ultra COM Tabs Definitions on Page 183 and see iSTAR Aperio RS-485 Hub Board Editor (iSTAR Ultra only) on Page 220 for configuration instructions.
5. Click **Save and Close** to save the settings you have configured on the iSTAR Controller COM tabs, or click another tab in the iSTAR Controller Editor to perform additional configurations.

To Configure the iSTAR Ultra COM1 or COM2 Tab for Schlage

1. From the iSTAR Ultra Controller Editor, click the **COM**x tab.
2. Select **Schlage** in the **Protocol** field. This will also select Schlage in the other COMx tab.
3. In the **Schlage Wireless PIMs** table, create the **Schlage PIMs** that you need by by selecting the **Configured** check box for only the PIMs you wish to create.
4. Click [...] in the Edit column to configure individual PIMS.
5. Click **Save and Close** to save the settings you have configured on the iSTAR Controller COM tabs, or click another tab in the iSTAR Controller Editor to perform additional configurations.

iSTAR Ultra COM Tabs Definitions

Table 30: iSTAR Ultra COM Tabs Definitions

Box	Description
Aperio Hubs	
Create All Hubs	Click to create all the Aperio Hubs. When you click **Create All Hubs** the **Configured** column check boxes are selected, and you can click ... in the **Edit** column to open the iSTAR Aperio RS-485 Hub Board Editor to configure an Aperio Hub.
Delete All Hubs	When you click **Delete All Hubs**, the check boxes in the Configured column are cleared for all Hubs, and all these Hubs are deleted after you confirm each deletion (any settings you have configured are lost).
Protocol	Select **Aperio**.
Edit column	Click ... in the **Edit** column to open the iSTAR Aperio RS-485 Hub Board Editor to configure an Aperio Hub. See iSTAR Aperio RS-485 Hub Board Editor (iSTAR Ultra only) on Page 220.
Index column	This column displays the number of each Hub (from 1 to 15).
Configured column	Click ☐ in this column to create an Aperio Hub (make it available to be edited).
Name column	Displays the name for this Aperio Hub. The name is system-generated by default, but you can edit this name by clicking in this field.
Hubs 1 - 15	Select the check box in the **Configured** column and click ... in the **Edit** column to open the iSTAR Aperio RS-485 Hub Board editor. From the editor you can configure the settings for the Hub.
Schlage PIMs	
Create All PIMs	Click to create all the Schlage PIMs. When you click **Create All PIMs** the **Configured** column check boxes are selected, and you can click ... in the **Edit** column to open the iSTAR Schlage RS-485 PIM Board Editor to configure a Schlage PIM.
Delete All PIMs	When you click **Delete All PIMs**, the check boxes in the **Configured** column are cleared for all PIMs, and all these PIMs are deleted after you confirm each deletion (any settings you have configured are lost).
Edit column	Click ... in the **Edit** column to open the iSTAR Schlage RS-485 PIM Board Editor to configure a Schlage PIM.
Index column	This column displays the number of each PIM (from 1 to 16).
Configured column	Click ☐ in this column to create a Schlage PIM (make it available to be edited).
Name column	Displays the name for this Schlage PIM. The name is system-generated by default, but you can edit this name by clicking in this field.
PIMs 1 - 16	Select the check box in the **Configured** column and click in the **Edit** column to open the iSTAR Schlage RS-485 PIM Board editor. From the editor you can configure the settings for the PIM.

iSTAR Ultra Controller ACM Board Editor

Add-on Access Control Modules (ACM Boards) provide access control functionality by supporting readers, outputs and inputs.

The iSTAR Ultra ACM Board dialog box is accessed from the iSTAR Controller editor Boards tab.

iSTAR Ultra ACM Board Editor

The iSTAR Ultra ACM Board editor allows you to define and configure inputs, outputs and readers for an ACM Board. The ACM Wiegand tab allows you to configure Wiegand readers, while the ACM RS-485 tab lets you configure RS-485-connected devices.

The iSTAR Ultra ACM Board editor has six tabs:

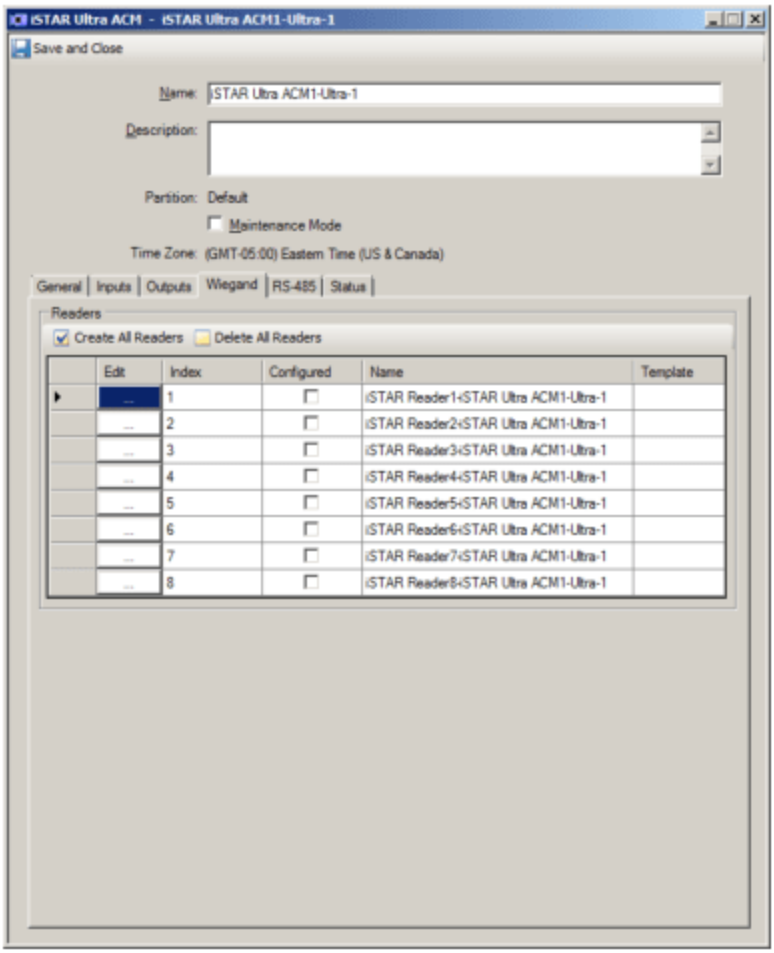
- iSTAR ACM Board General Tab on Page 197
- iSTAR ACM Board Inputs Tab on Page 198
- iSTAR ACM Board Outputs Tab on Page 199
- iSTAR Ultra ACM Board Wiegand Tab on Page 184
- iSTAR Ultra ACM Board RS-485 Tab on Page 186
- iSTAR Ultra ACM Board Status Tab on Page 195

For more information see the *iSTAR Ultra Installation and Configuration Guide*.

iSTAR Ultra ACM Board Wiegand Tab

The iSTAR Ultra ACM Board Wiegand tab, shown in Figure 59 on Page 185, provides configuration for Wiegand readers connected to the iSTAR Ultra ACM Board.

Figure 59: iSTAR Ultra ACM Board Wiegand Tab



iSTAR Ultra ACM Board Wiegand Tab Definitions

Table 31 on Page 185 provides definitions of the fields and buttons on the iSTAR Ultra ACM Board Wiegand Tab.

Table 31: iSTAR Ultra ACM Board Wiegand Tab.Definitions

Box	Description
Create All Readers	Click to create all the Readers. When you click **Create All Readers**, the **Configured** column check boxes are selected, and you can click ... in the **Edit** column to open the iSTAR Reader Editor to configure a direct connect Wiegand Reader.
Delete All Readers	When you click **Delete All Readers**, the check boxes in the **Configured** column are cleared for all Readers, and all these Readers are immediately deleted (any settings you have configured are lost).
Edit column	Click ... in the **Edit** column to open the iSTAR Reader Editor to configure a Reader. See iSTAR Reader Editor on Page 248.
Index column	This column displays the number for each reader. This number is the physical port number for a Direct Connect Wiegand reader.

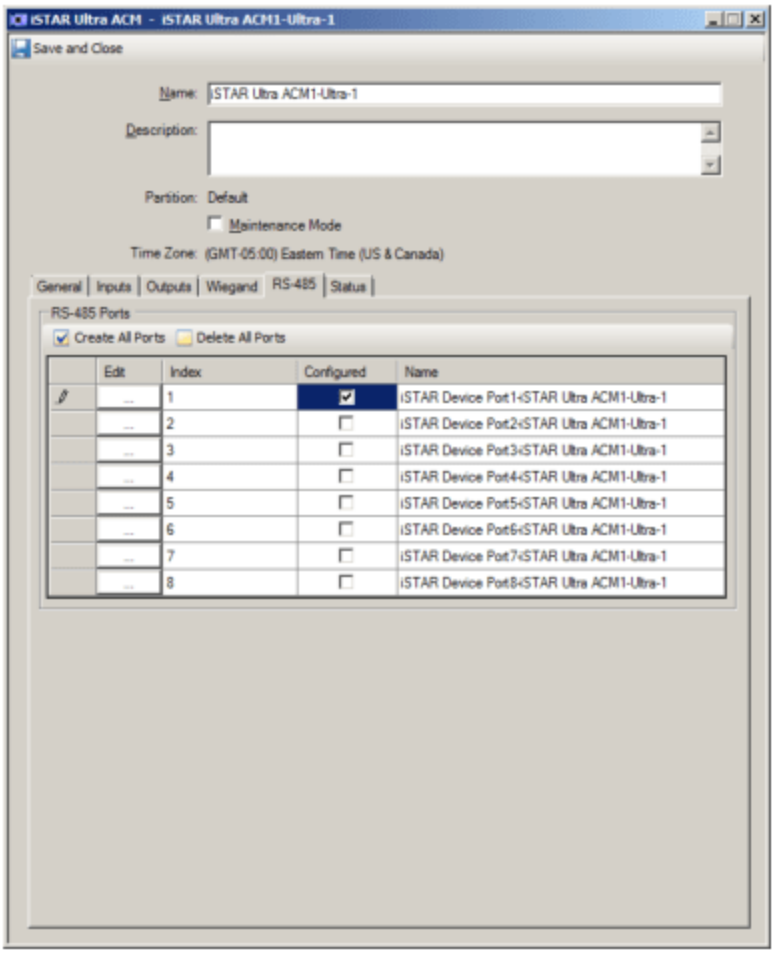
Table 31: iSTAR Ultra ACM Board Wiegand Tab.Definitions (continued)

Box	Description
Configured column	Click in this column to create a reader (make it available to be edited).
Name column	Displays the name for this Reader. The name is system-generated by default, but you can edit this name by clicking in this field.
Template column	Click in this column prior to creating the Reader, then click ... to select a Reader template from the list of available Reader templates. The **Template** column shows the template name chosen if you selected a Template prior to creating the Reader.
Readers 1 - 8	Select the check box in the **Configured** column for a Reader and click ... located in the **Edit** column to open the iSTAR Reader Editor General tab to configure the Keypad, Triggers, Groups, Status and State Images that are associated with a Reader. See iSTAR Reader Editor on Page 248 for detailed instructions for configuring iSTAR Readers. The **Name** column displays a name comprised of the Reader Type and the iSTAR Controller name. You can click in this column to edit the Reader name.

iSTAR Ultra ACM Board RS-485 Tab

The iSTAR Ultra ACM Board RS-485 tab, shown in Figure 60 on Page 187,provides configuration for RS-485 devices connected to the iSTAR Ultra ACM Board.

Figure 60: iSTAR Ultra ACM Board RS-485 Tab



iSTAR Ultra ACM Board RS-485 Tab Definitions

Table 32 on Page 187 provides definitions of the fields and buttons on the iSTAR Ultra ACM Board RS-485 Tab.

Table 32: iSTAR Ultra ACM Board RS-485 Tab Definitions

Field/Button	Description
RS-485 Ports	
Create All Ports	Click to create the RS-485 Ports. When you click **Create All Ports** the Configured column check boxes are selected, and you can click [...] in the **Edit** column to open the iSTAR Device Port Editor to configure an RS-485 Port.
Delete All Ports	When you click **Delete All Ports**, the check boxes in the **Configured** column are cleared for all Ports, and allPorts are immediately deleted (any settings you have configured are lost).
Edit column	Click [...] in the **Edit** column to open the iSTAR Device Port Editor to configure Device Ports for the iSTAR Ultra. See iSTAR Reader Editor on Page 248.

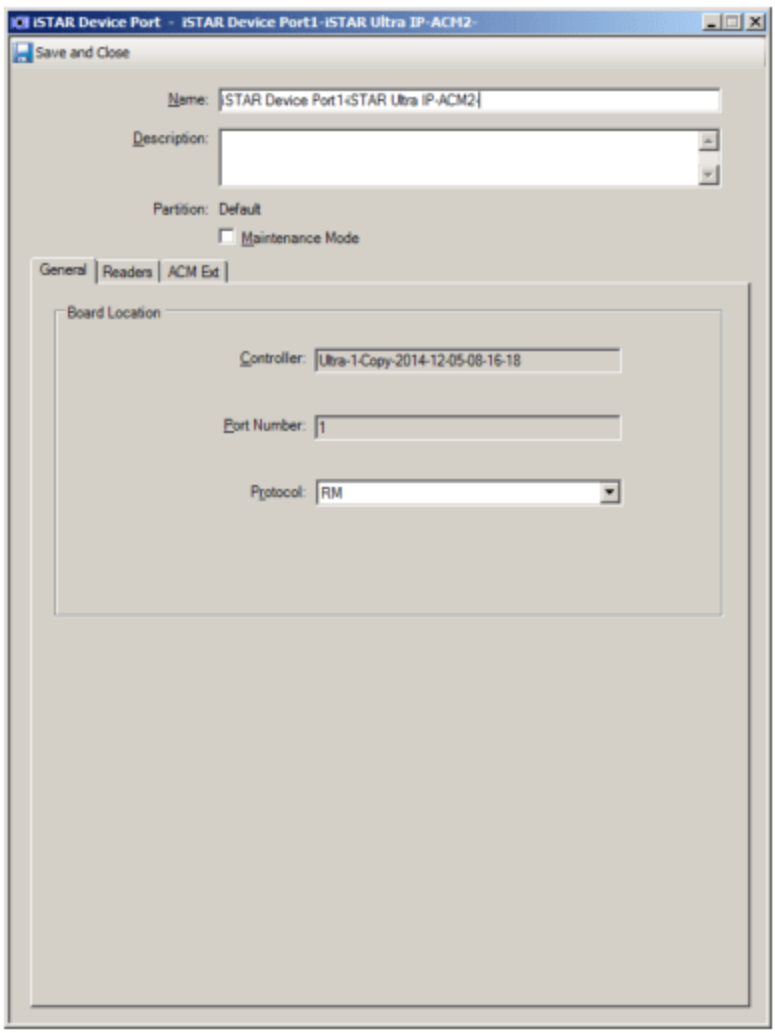
Table 32: iSTAR Ultra ACM Board RS-485 Tab Definitions (continued)

Field/Button	Description
Index column	This column displays the number for each Device Port.
Configured column	Click ☐ in this column to create a Device Port (make it available to be edited).
Name column	Displays the name for this Device Port. The name is system-generated by default, but you can edit this name by clicking in click in this field.
Device Ports 1 - 8	Select the check box in the **Configured** column for a Device Port and click ... located in the **Edit** column to open the iSTAR Device Port Editor General tab to configure the Readers and ACM extensions that are associated with the Device Port. See iSTAR Reader Editor on Page 248 for detailed instructions for configuring iSTAR Device Ports. The **Name** column displays a name comprised of the Device Port and the iSTAR Controller name. You can click in this column to edit the Device Port name.

iSTAR Ultra ACM RS-485 Device Port Editor

The iSTAR Ultra ACM RS-485 Device Port Editor lets you create and configure RM Readers, BLE readers, and direct-connect Wiegand Readers.

Figure 61: iSTAR Ultra ACM RS-485 Device Port Editor



iSTAR Ultra ACM RS-485 Device Port Tabs

- iSTAR Ultra ACM/IP-ACM RS-485 Device Port General Tab on Page 189
- iSTAR Ultra RS-485 Device Port Readers Tab on Page 190
- iSTAR Ultra RS-485 Device Port ACM EXT Tab on Page 192

iSTAR Ultra ACM/IP-ACM RS-485 Device Port General Tab

The iSTAR Ultra RS-485 Device Port General tab displays three Read-only fields that identify the Controller, Port Number, and Protocol for the RM reader and Wiegand Reader Device Port. Table 33 on Page 190 describes the fields on this tab.

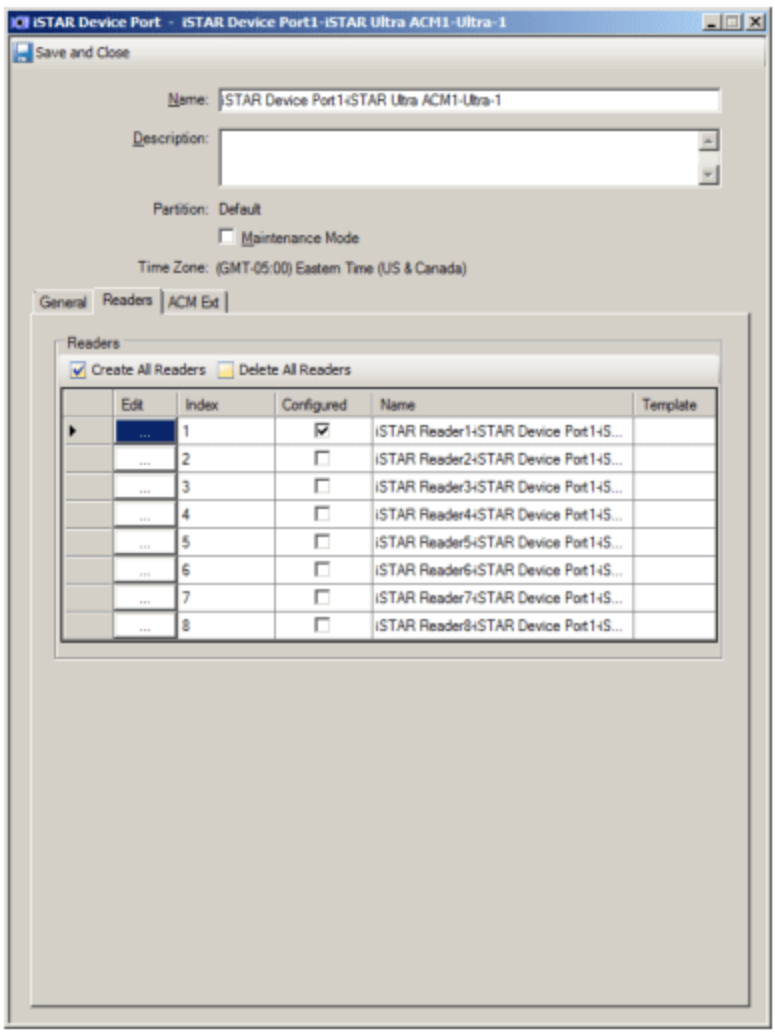
Table 33: iSTAR Ultra ACM RS-485 Device Port General Tab Definitions

Field	Description
Controller	This field identifies the controller for this ACM RS-485 Device Port.
Port Number	This field identifies the index number of the Device Port on the ACM for the Readers.
Protocol	Click on the drop-down menu to select the Protocol type. • **RM** (Software House Reader Protocol) • **BLE** (Bluetooth Low Energy), • **OSDP** (Open Supervised Device Protocol) Default: RM

iSTAR Ultra RS-485 Device Port Readers Tab

The iSTAR Ultra RS-485 Device Port Readers tab lets you create and configure the Readers that are attached to an RS-485 port on the iSTAR Ultra.

Figure 62: iSTAR Ultra RS-485 Device Port Readers Tab



You can use an existing Reader Template to create one or more of the RS-485 Readers. Click in the **Template** Column, then click [...]. A list of available iSTAR Reader Templates appears. Click on the Template you wish to use. See Using Templates for Controller Inputs, Outputs, and Readers on Page 37 for more detailed information about using Templates to create Readers.

iSTAR Ultra RS-485 Device Port Readers Tab Definitions

Table 34 on Page 191 provides definitions for the buttons and fields on the iSTAR Ultra RS-485 Device Port Readers tab.

Table 34: iSTAR Ultra RS-485 Device Port Readers Tab Definitions

Field/Button	Description
Create All Readers	Click to create all the readers. When you click **Create All Readers** the Configured column check boxes are selected, and you can click [...] in the Edit column to edit that reader.

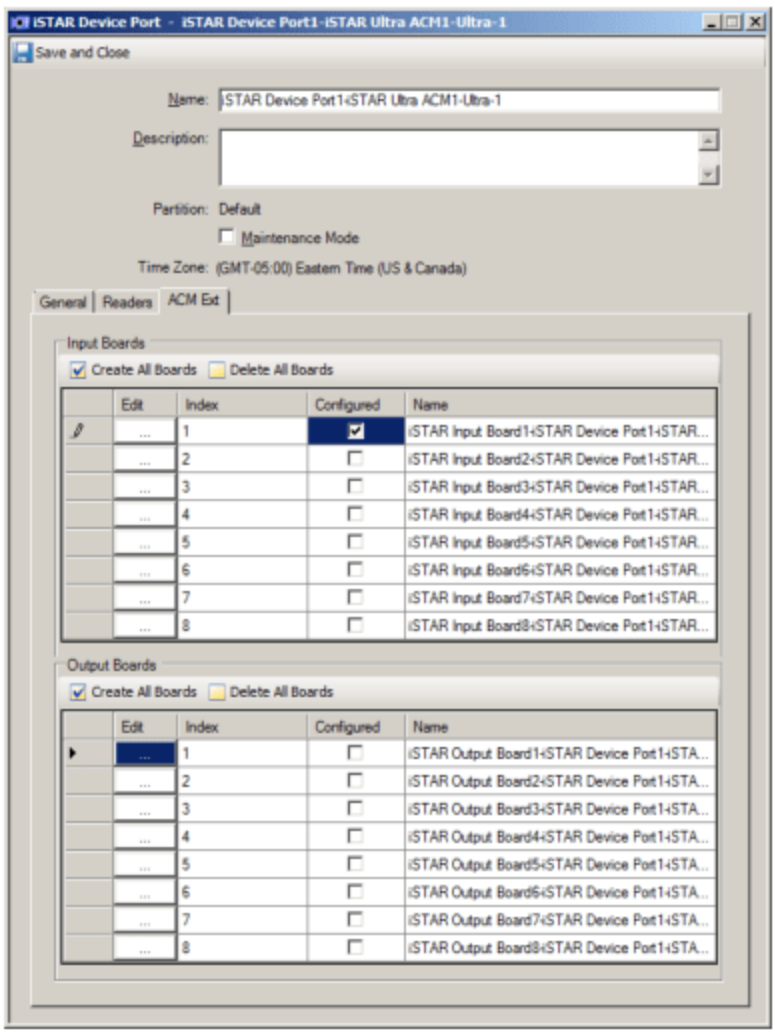
iSTAR Ultra RS-485 Device Port Readers Tab Definitions (continued)

Field/Button	Description
Delete All Readers	When you click **Delete All Readers**, the check boxes in the Configured column are cleared for all readers, and all these readers are immediately deleted (any settings you have configured are lost).
Edit column	Click ... in the **Edit** column to open the iSTAR Reader Editor to configure an Reader. See iSTAR Reader Editor on Page 248.
Index column	This column displays the number of each Reader.
Configured column	Click in this column to create a Reader (make it available to be edited).
Name column	Displays the name for this Reader. The name is system-generated by default, but you can edit this name by clicking in click in this field.
Template column	The Template column shows the template name if you selected a Template prior to creating the Readers. Click in this column, then click ... to select a Reader template to use for creating this Reader from the list of available Reader templates.You can only select a Template prior to creating the Reader.

iSTAR Ultra RS-485 Device Port ACM EXT Tab

The iSTAR Ultra RS-485 Device Port ACM Ext tab lets you create and configure the Input boards and Output boards that are attached to this iSTAR Ultra RS-485 Device Port.

Figure 63: iSTAR Ultra RS-485 Device Port ACM Ext Tab



Configuring the iSTAR Ultra RS-485 Device Port ACM Ext Tab

When you configure the iSTAR Ultra RS-485 Device Port ACM Ext tab, you are defining the Input boards and Output boards that are attached to the port. You can then click to open the Input Boards Editor to configure individual Input Boards, or open the Output Boards Editor to configure individual Output Boards.

To Configure the iSTAR Ultra RS-485 Device Port ACM Ext Tab

1. From the iSTAR Ultra Boards tab, create an ACM on either SPI Port 1 or SPI Port 2 by clicking in the **Configure** column.
2. Click [...] to open the iSTAR Ultra ACM Board editor. Access the Input Board Editor for the Input Board you wish to edit (see iSTAR Ultra Controller ACM Board Editor on Page 184).
3. Click the RS-485 tab.
4. Create an RS-485 port by clicking in the **Configure** column, then click [...] to open the iSTAR Ultra Device Port editor.

5. Click the ACM Ext tab.
6. Create an Input board by clicking in the **Configure** column for one of the Input Boards (1-8), then click [...] to open the iSTAR Input Board editor. See the iSTAR Input Board Editor on Page 203 for configuration instructions.
7. Create an Output board by clicking in the **Configure** column for one of the Output Boards (1-8), then click [...].to open the iSTAR Output Board editor. See the iSTAR Output Board Editor on Page 208 for configuration instructions.
8. When you have finished configuring the Inputs on the iSTAR Ultra RS-485 Device Port ACM Ext tab, click **Save and Close** to save the settings you have configured.

iSTAR Ultra RS-485 Device Port ACM Ext tab Definitions

Table 42 on Page 202 provides definitions for the buttons and fields on the iSTAR Ultra RS-485 Device Port ACM Ext tab.

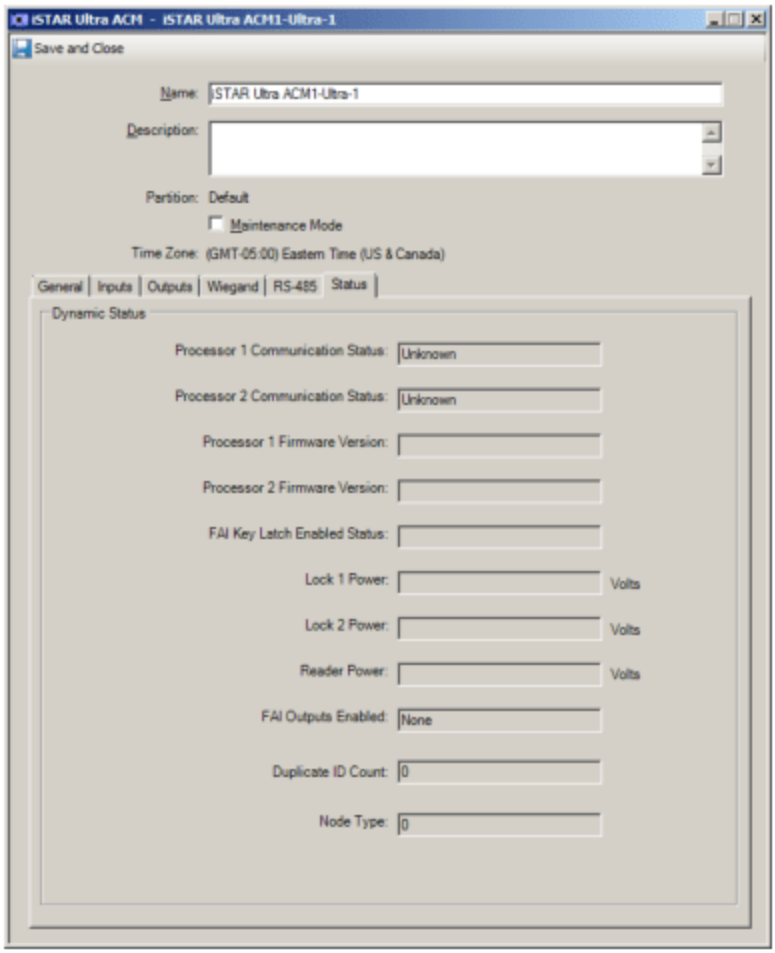
Table 35: iSTAR Ultra RS-485 Device Port ACM Ext Tab Definitions

Field/Button	Description
Input Boards	
Create All Boards	Click to create all the Input Boards. When you click **Create All Boards** the Configured column check boxes are selected, and you can click [...] in the Edit column to edit that Input Board.
Delete All Boards	When you click **Delete All Boards**, the check boxes in the Configured column are cleared for all Input Boards, and all these Input Boards are immediately deleted (any settings you have configured are lost).
Edit column	Click [...] in the **Edit** column to open the iSTAR Input Board Editor. See iSTAR Input Board Editor on Page 203.
Index column	This column displays the number of each Input Board.
Configured column	Click [ ] in this column to create an Input Board (make it available to be edited).
Name column	Displays the name for this Input board. The name is system-generated by default, but you can edit this name by clicking in click in this field.
Output Boards	
Create All Boards	Click to create all the Output Boards. When you click **Create All Boards** the Configured column check boxes are selected, and you can click [...] in the Edit column to edit that Output Board.
Delete All Boards	When you click **Delete All Boards**, the check boxes in the Configured column are cleared for all Output Boards, and all these Output Boards are immediately deleted (any settings you have configured are lost).
Edit column	Click [...] in the **Edit** column to open the iSTAR Output Board Editor. See iSTAR Output Board Editor on Page 208.
Index column	This column displays the number of each Output Board.
Configured column	Click [ ] in this column to create an Output Board (make it available to be edited).
Name column	Displays the name for this Output board. The name is system-generated by default, but you can edit this name by clicking in click in this field.

iSTAR Ultra ACM Board Status Tab

The iSTAR Ultra ACM Board Status tab, shown in Figure 64 on Page 195,provides a read-only listing of information about the operational status of the selected iSTAR Ultra ACM Board.

Figure 64: iSTAR Ultra ACM Board Status Tab



iSTAR Ultra ACM Board Status Tab Definitions

Table 36 on Page 195 provides definitions of the fields and buttons on the iSTAR Ultra ACM Board Status tab.

Table 36: iSTAR Ultra ACM Board Status Tab Definitions

Field/Button	Description
Processor 1 Communications Status	Offline or Online.
Processor 2 Communications Status	Offline or Online.
Processor 1 Firmware Version	Processor firmware, such as 00.00.36.00008

Table 36: iSTAR Ultra ACM Board Status Tab Definitions (continued)

Field/Button	Description
Processor 2 Firmware Version	Processor firmware, such as 00.00.36.00008
FAI Key Latch Enabled Status	Enabled or disabled.
Lock 1 Power (Volts)	Lock power in Volts. Possible vales are: 0.0V, 12.0V, 24.0V.
Lock 2 Power (Volts)	Lock power in Volts. Possible vales are: 0.0V, 12.0V, 24.0V.
Reader Power	Voltage reported for Readers. Reader power is the basic power to the GCM and ACMs. Typically reads about 13.8V.
FAI Outputs Enabled	List of Outputs with FAI enabled.

iSTAR Classic/Pro Controller ACM Board Editor

Add-on Access Control Modules (ACM Boards) provide access control functionality by supporting readers, outputs and inputs.

The ACM Board dialog box is accessed from the iSTAR Controller editor Boards tab.

iSTAR Classic/Pro ACM Board Editor

The iSTAR Classic/Pro ACM Board editor allows you to define and configure inputs, outputs and readers for the ACM Board. The ACM Extension (ACM Ext) tab allows you to configure the I/8 input and R/8 output boards connected to the ACM Board.

The iSTAR Classic/Pro ACM Board editor has five tabs:

- iSTAR ACM Board General Tab on Page 197
- iSTAR ACM Board Inputs Tab on Page 198
- iSTAR ACM Board Outputs Tab on Page 199
- iSTAR ACM Board Readers Tab on Page 200
- iSTAR ACM Board ACM Ext Tab on Page 201

For more information see the *iSTAR Pro Installation and Configuration Guide*.

iSTAR ACM Board General Tab

The ACM Board General tab identifies the ACM Board. The fields on this tab are read-only.

iSTAR ACM Board General Tab Definitions

Table 37 on Page 197 provides definitions for the fields on the iSTAR ACM Board General tab.

Table 37: iSTAR ACM Board General Tab Definitions

Field/Button	Description
Name	Displays the name for this ACM board. The name is system-generated by default, but you can edit this name by clicking in this field.
Description	Enter a textual comment about the ACM board, such as its location or purpose. This text is for information only.
Maintenance Mode	Click to put the iSTAR ACM board into Maintenance Mode. See Chapter 2: Maintenance Mode for more information.
Partition	This read-only field identifies the Partition in which the iSTAR Controller for this ACM Board resides.
Board Location	

iSTAR ACM Board General Tab Definitions (continued)

Field/Button	Description
Controller	This read-only field identifies the Controller to which this board is attached.
ACM Number	This read-only field displays the number of the ACM board.
Board Type	This read-only field displays the iSTAR ACM type.

iSTAR ACM Board Inputs Tab

The ACM Board Inputs tab lets you create and configure the Inputs that are attached to this ACM Board.

You can use an existing Input Template to create one or more of the ACM Board Inputs. Click in the **Template** Column, then click [...]. A list of available iSTAR Input Templates appears. Click on the Template you wish to use. See Using Templates for Controller Inputs, Outputs, and Readers on Page 37 for more detailed information about using Templates to create Inputs.

iSTAR ACM Board Inputs Tab Definitions

- Table 38 on Page 198 provides definitions for the buttons and fields on the ACM Board Inputs tab.
- Table 39 on Page 199 provides definitions for the iSTAR Ultra ACM Board Inputs tab.

Table 38: iSTAR Pro/Classic ACM Board Inputs Tab Definitions

Field/Button	Description
Create All Inputs	Click to create all the Inputs. When you click **Create All Inputs** the Configured column check boxes are selected, and you can click [...] in the Edit column to edit that Input.
Delete All Inputs	When you click **Delete All Inputs**, the check boxes in the Configured column are cleared for all Inputs, and all these Inputs are immediately deleted (any settings you have configured are lost).
Edit column	Click [...] in the **Edit** column to open the iSTAR Input Editor to configure an Input. See iSTAR Input Editor on Page 232.
Index column	This column displays the number of each Input.
Configured column	Click [ ] in this column to create an Input (make it available to be edited).
Name column	Displays the name for this Input. The name is system-generated by default, but you can edit this name by clicking in this field.
Template column	The Template column shows the template name if you selected a Template prior to creating the Input. Click in this column, then click [...] to select an Input template to use for creating this Input from the list of available Input templates. You can only select a Template prior to creating the input.
Inputs 1 through 16	These standard general purpose supervised inputs are available on iSTAR Pro ACM boards.

iSTAR Ultra ACM Board Inputs Tab Definitions

Table 39 on Page 199 provides definitions for the buttons and fields on the iSTAR Ultra ACM Board Inputs tab.

Table 39: iSTAR Ultra ACM Board Inputs Tab Definitions

Field/Button	Description
Special Purpose Inputs (iSTAR Ultra only)	
Tamper	The **Tamper** input activates when the controller cabinet is opened or removed from its mounting surface. NOTE: For UL applications, this field must be enabled. Select the check box in the **Configured** column and click [...] located in the **Edit** column to open the iSTAR Input Editor General tab to configure the Tamper input. From the Input Editor you can configure the Options, Triggers, Groups, Status and State Images that are associated with the Tamper Input. The **Template** column shows the template name chosen if you selected a Template prior to creating the Input.
Comm Fail Processor 1	A logical unsupervised input that reflects the state of the communication between the GCM board and Processor-A on this ACM board.
Comm Fail Processor 2	A logical unsupervised input that reflects the state of the communication between the GCM board and Processor-B on this ACM board.
FAI Alarm	This is the Fire Alarm Input signal. It is NC supervised.
FAI Relay Control	FAI Relay Control. When the FAI signal is true, the HW drives all selected relays to activate. Each relay has a switch indicating whether it is selected to behave in this way.
FAI Interlock Key	The FAI K input is usually a key switch. It is supervised as NO. It is used in conjunction with Latch mode. If latching is enabled, the F signal will turn on all selected outputs. They will stay that way until the Fire Chief inserts the key in the key switch and announces all clear.
Port 1 Power Status through Port 8 Power Status	Power indicator input for each RM port.
General Purpose Inputs (iSTAR Ultra only)	
Inputs 1 through 24 (Ultra) Inputs 1 though 16 Ultra SE (Ultra Mode)	These standard general purpose supervised inputs are available on iSTAR Ultra ACM boards.

iSTAR ACM Board Outputs Tab

The ACM Board Outputs tab lets you create and configure the Outputs that are attached to this ACM Board.

You can use an existing Output Template to create one or more of the ACM Board Outputs. Click in the **Template** Column, then click [...]. A list of available iSTAR Output Templates appears. Click on the Template you wish to use.

See Using Templates for Controller Inputs, Outputs, and Readers on Page 37 for more detailed information about using Templates to create Outputs.

iSTAR ACM Board Outputs Tab Definitions

Table 40 on Page 200 provides definitions for the buttons and fields on the iSTAR ACM Board Outputs tab.

Table 40: iSTAR ACM Board Outputs Tab Definitions

Field/Button	Description
Create All Outputs	Click to create all the outputs. When you click **Create All Outputs** the Configured column check boxes are selected, and you can click [...] in the Edit column to edit that output.
Delete All Outputs	When you click **Delete All Outputs**, the check boxes in the Configured column are cleared for all outputs, and all these outputs are immediately deleted (any settings you have configured are lost).
Edit column	Click [...] in the **Edit** column to open the iSTAR Output Editor to configure an Output. See iSTAR Output Editor on Page 241.
Index column	This column displays the number of each Output.
Configured column	Click [ ] in this column to create an Output (make it available to be edited).
Name column	Displays the name for this Output. The name is system-generated by default, but you can edit this name by clicking in this field.
Template column	The Template column shows the template name if you selected a Template prior to creating the Outputs. Click in this column, then click [...] to select an Output template to use for creating this Output from the list of available Output templates.You can only select a Template prior to creating the Output.
Primary Relay Outputs	
Outputs 1 through 8	These outputs can be used for a Fire Alarm Interface (FAI). They are rated at 5 Amps, and are socket mounted. Click [ ] in the **Configure** column, then click [...] in the **Edit** column to open the iSTAR Output Editor to configure a Primary Output. See iSTAR Output Board Editor on Page 208
Secondary Relay Outputs	
Outputs 1 through 8	These outputs cannot be used for a Fire Alarm Interface (FAI). They are rated at 0.75 or 1 Amp, and are permanently soldered to the ACM. Click [ ] in the **Configure** column, then click [...] in the **Edit** column to open the iSTAR Output Editor to configure a Secondary Output. See iSTAR Output Board Editor on Page 208

iSTAR ACM Board Readers Tab

The ACM Board Readers tab lets you create and configure the Readers that are attached to this ACM Board.

You can use an existing Reader Template to create one or more of the ACM Board Readers. Click in the **Template** Column, then click [...]. A list of available iSTAR Reader Templates appears. Click on the Template you wish to use. See Using Templates for Controller Inputs, Outputs, and Readers on Page 37 for more detailed information about using Templates to create Readers.

iSTAR ACM Board Readers Tab Definitions

Table 41 on Page 201 provides definitions for the buttons and fields on the iSTAR ACM Board Readers tab.

Table 41: iSTAR ACM Board Readers Tab Definitions

Field/Button	Description
Create All Readers	Click to create all the readers. When you click **Create All Readers** the Configured column check boxes are selected, and you can click ... in the Edit column to edit that reader.
Delete All Readers	When you click **Delete All Readers**, the check boxes in the Configured column are cleared for all readers, and all these readers are immediately deleted (any settings you have configured are lost).
Edit column	Click ... in the **Edit** column to open the iSTAR Reader Editor to configure an Reader. See iSTAR Reader Editor on Page 248.
Index column	This column displays the number of each Reader.
Configured column	Click ☐ in this column to create a Reader (make it available to be edited).
Name column	Displays the name for this Reader. The name is system-generated by default, but you can edit this name by clicking in this field.
Template column	The Template column shows the template name if you selected a Template prior to creating the Readers. Click in this column, then click ... to select a Reader template to use for creating this Reader from the list of available Reader templates.You can only select a Template prior to creating the Reader.

iSTAR ACM Board ACM Ext Tab

The ACM Board ACM Ext tab lets you create and configure the Input boards and Output boards that are attached to this ACM Board.

Configuring the iSTAR ACM Board ACM Ext Tab

When you configure the iSTAR ACM Board ACM Ext tab, you are defining the Input boards and Output boards that are attached to the ACM. You can then click to open the Input Boards Editor to configure individual Input Boards, or open the Output Boards Editor to configure individual Output Boards.

To Configure the iSTAR ACM Board ACM EXT Tab

1. From the iSTAR controller Boards tab, create an ACM and click ... to access the iSTAR ACM Board Editor.
2. Click the ACM EXT tab.
3. Create the **Input Boards** that you need by clicking **Create All Boards** or by selecting the **Configured** check box for only the Input Boards you wish to create.
4. Click ... in the **Edit** column to open the iSTAR Input Board editor to configure individual Inputs. See the iSTAR Input Board Editor on Page 203 for configuration instructions.
5. Create the **Output Boards** that you need by clicking **Create All Boards** or by selecting the **Configured** check box for only the Output Boards you wish to create.

6. Click [...] in the **Edit** column to open the iSTAR Output Board editor to configure individual Outputs. See the iSTAR Output Board Editor on Page 208 for configuration instructions.
7. When you have finished configuring the Input Boards and Output Boards, click **Save and Close** to save the settings you have configured.

iSTAR ACM Board ACM Ext Tab Definitions

Table 42 on Page 202 provides definitions for the buttons and fields on the iSTAR ACM Board ACM Ext tab.

Table 42: iSTAR ACM Board ACM Ext Tab Definitions

Field/Button	Description
Input Boards	
Create All Boards	Click to create all the Input Boards. When you click **Create All Boards** the Configured column check boxes are selected, and you can click [...] in the Edit column to edit that Input Board.
Delete All Boards	When you click **Delete All Boards**, the check boxes in the Configured column are cleared for all Input Boards, and all these Input Boards are immediately deleted (any settings you have configured are lost).
Edit column	Click [...] in the **Edit** column to open the iSTAR Input Board Editor. See iSTAR Input Board Editor on Page 203.
Index column	This column displays the number of each Input Board.
Configured column	Click [ ] in this column to create an Input Board (make it available to be edited).
Name column	Displays the name for this Input board. The name is system-generated by default, but you can edit this name by clicking in this field.
Output Boards	
Create All Boards	Click to create all the Output Boards. When you click **Create All Boards** the Configured column check boxes are selected, and you can click [...] in the Edit column to edit that Output Board.
Delete All Boards	When you click **Delete All Boards**, the check boxes in the Configured column are cleared for all Output Boards, and all these Output Boards are immediately deleted (any settings you have configured are lost).
Edit column	Click [...] in the **Edit** column to open the iSTAR Output Board Editor. See iSTAR Output Board Editor on Page 208.
Index column	This column displays the number of each Output Board.
Configured column	Click [ ] in this column to create an Output Board (make it available to be edited).
Name column	Displays the name for this Output board. The name is system-generated by default, but you can edit this name by clicking in this field.

iSTAR Input Board Editor

The iSTAR Input Board editor lets you configure an iSTAR Input Board that you created on the iSTAR Classic/Pro ACM Board ACM Ext tab or the iSTAR eX and iSTAR Edge COM1, COM2, and COM3 tabs.

The iSTAR Input Board editor (see Figure 65 on Page 203) has the following tabs:

- **iSTAR Input Board General Tab**

  Lists the Inputs and Status Inputs on an I/8 board that is connected to an iSTAR Classic/Pro, iSTAR eX, or iSTAR Edge. See iSTAR Input Board General Tab on Page 206.

- **iSTAR Input Board Group Tab**

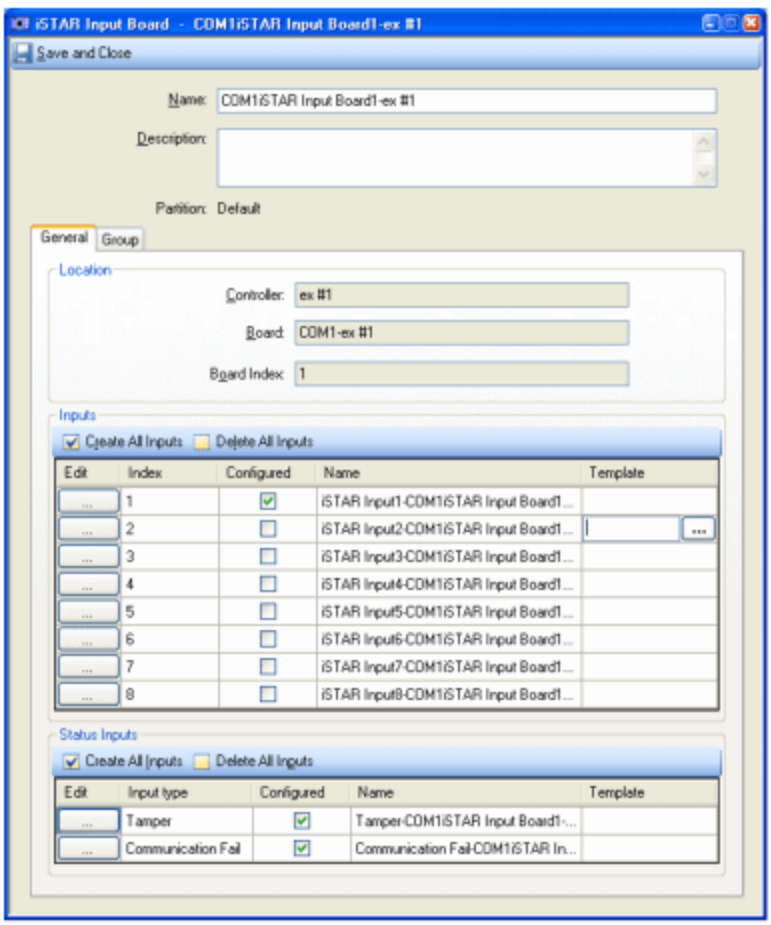
  If you have created a Group containing iSTAR Input Boards and added this Input Board to it, the iSTAR Input Board editor also displays a Group tab.

  This tab lists the Input Board groups to which this Input Board belongs. See Groups Tab for Hardware Devices on Page 28 for information on using the Group tab for the iSTAR Input board.

ISTAR Input Board editor Tasks:

- Accessing the iSTAR Input Board Editor on Page 204
- Configuring iSTAR Input Boards on Page 205

Figure 65: iSTAR Input Board Editor



Accessing the iSTAR Input Board Editor

You can access the iSTAR Input Board Editor in three ways:

- To Access the iSTAR Input Board Editor (iSTAR eX/Edge Controller) on Page 204
- To Access the iSTAR Input Board Editor (iSTAR Classic/Pro Controller) on Page 204
- To Access the iSTAR Input Board Editor from the Hardware Tree on Page 204

To Access the iSTAR Input Board Editor (iSTAR eX/Edge Controller)

1. From the iSTAR Controller Editor, click on the appropriate COM tab (COM1, COM2, or COM3).
2. In the Input Boards table on this tab, click [...] in the **Edit** column for the Input board you want to Edit.
3. The iSTAR Input Board Editor opens.

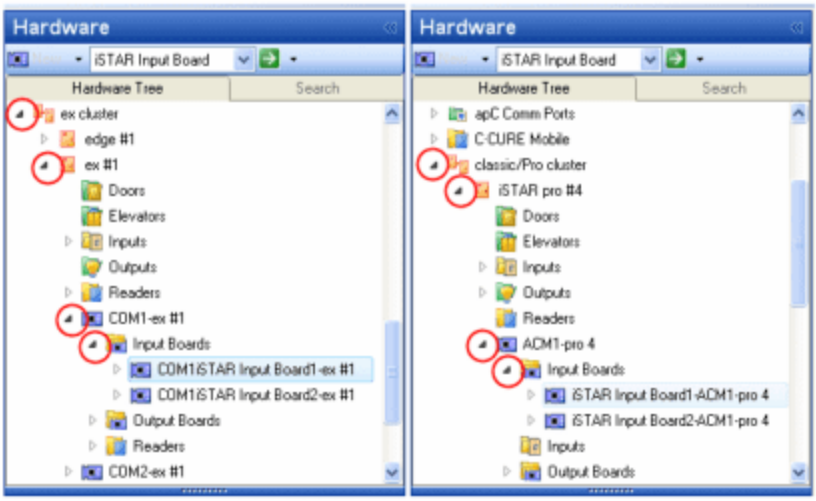
To Access the iSTAR Input Board Editor (iSTAR Classic/Pro Controller)

1. From the iSTAR Controller Editor, click on the Boards tab.
2. In the ACMs table on this tab, click [...] in the **Edit** column for the ACM that contains the Input board you want to Edit. The ACM Board Editor opens.
3. Click the ACM Ext tab.
4. In the Input Boards table on this tab, click [...] in the **Edit** column for the Input board you want to Edit.
5. The iSTAR Input Board Editor opens.

To Access the iSTAR Input Board Editor from the Hardware Tree

1. Navigate from your iSTAR Controller in the Hardware Tree to the appropriate COM Board (on an iSTAR eX or iSTAR Edge Controller) or ACM Board (iSTAR Classic/Pro Controller).
2. Click on **Input Boards**, as shown in Figure 66 on Page 205. This figure shows the hardware tree for an iSTAR eX on the left and an iSTAR Pro on the right.

Figure 66: iSTAR Input Board in the Hardware Tree



3. Double-click on the Input Board you wish to edit. The iSTAR Input Board Editor opens.

Configuring iSTAR Input Boards

When you configure an iSTAR Input Board, you are defining the Inputs that are attached to a particular I/8 board. You can then click to open the Inputs Editor to configure individual Inputs.

To Configure an iSTAR Input Board Tab

1. Access the Input Board Editor for the Input Board you wish to edit (see Accessing the iSTAR Input Board Editor on Page 204).
2. If you wish to use an Input Template to configure one or more of the I/8 board Inputs, click in the **Template** column, then click [...] to open a dialog box listing the available Input Templates. See Using Templates for Controller Inputs, Outputs, and Readers on Page 37 for more information.
3. Create the **Inputs** that you need by clicking **Create All Inputs** or by selecting the **Configured** check box for only the Inputs you wish to create.
4. Click [...] in the **Edit** column to open the iSTAR Input Editor to configure individual Inputs. See the iSTAR Input Editor on Page 232 for configuration instructions.
5. If you wish to use an Input Template to configure one or more of the I/8 board Status Inputs, click in the **Template** column, then click [...] to open a dialog box listing the available Input Templates. See Using Templates for Controller Inputs, Outputs, and Readers on Page 37 for more information.
6. Create the Status Inputs that you need by clicking **Create All Inputs** or by selecting the **Configured** check box for only the Inputs you wish to create.
7. Click [...] in the **Edit** column to configure individual Status Inputs. See the definitions of the Status Inputs in Table 43 on Page 206 and see iSTAR Input Editor on Page 232.
8. When you have finished configuring the Inputs on the Input Board Editor General tab, click **Save and Close** to save the settings you have configured on the iSTAR Input Board editor.

iSTAR Input Board General Tab

The iSTAR Input Board General tab allows you to configure the Inputs on an I/8 board attached to your iSTAR Controller, as well as the Status Inputs for Tamper and Communications Failure.

iSTAR Input Board General Tab Definitions

Table 43 on Page 206 lists the fields and buttons that appear on the iSTAR Input Board General tab.

Table 43: iSTAR Input Board General Tab Definitions

Field/Button	Description
Identification	
Name	Displays the name for this Input board. The name is system-generated by default, but you can edit this name by clicking in this field.
Description	Enter a textual comment about the Input Board, such as its location or purpose. This text is for information only.
Maintenance Mode	Click to put the Input Board into Maintenance Mode. See Chapter 2: Maintenance Mode for more information.
Partition	This read-only field identifies the Partition in which this Input board resides.
Controller	This read-only field identifies the iSTAR Controller to which this Input board is attached.
Location	
Board	This read-only field identifies the iSTAR Controller board to which this Input board is attached.
Board Index	This read-only field identifies the board index (which represents the SW1 address switch setting on the I/8 board) for this Input board.
Inputs	
Create All Inputs	Click to create all eight Inputs. The check boxes in the **Configured** column are set to ☑.
Delete All Inputs	Click to delete all eight Inputs. The check boxes in the **Configured** column are set to ☐.
Edit column	Click ... in this column to open the iSTAR Input Editor to edit this Input.
Index column	This read-only field identifies the position of each Input (P1 - P8) on the I/8 board.
Configured column	☑ indicates that the Input has been configured. ☐ indicates that the Input has not been configured.
Name column	Displays the system-generated name for this Input. You can edit this name by clicking in the field.

Table 43: iSTAR Input Board General Tab Definitions (continued)

Field/Button	Description
Template column	Displays the Template used for creating this Input. If the Input is not yet configured, you can click in this column, then click to select an Input Template. If the **Configured** column displays ☑, this field cannot be edited.
Status Inputs	
Create All Inputs	Click to create the Tamper and Communications Fail Inputs. The check boxes in the **Configured** column are set to ☑.
Delete All Inputs	Click to delete the Tamper and Communications Fail Inputs. The check boxes in the **Configured** column are set to ☐.
Edit column	Click ... in this column to open the iSTAR Input Editor to edit this Input.
Input Type column	The Input Type Column displays: **Tamper** – Represents the Tamper Input on the I/8 board. NOTE: For UL applications, the **Tamper** Input on the iSTAR Input Board General tab must be enabled. **Communications Fail** – Represents the Communications Fail Input on the I/8 board. NOTE: For UL applications, the Communications Failure Input on the iSTAR Input Board General tab must be enabled.
Configured column	☑ indicates that the Input has been configured. ☐ indicates that the Input has not been configured.
Name column	Displays the system-generated name for this Input. You can edit this name by clicking in the field.
Template column	Displays the Template used for creating this Input. If the Input is not yet configured, you can click in this column, then click to select an Input Template. If the **Configured** column displays ☑, this field cannot be edited.

iSTAR Output Board Editor

The iSTAR Output Board editor lets you configure an iSTAR Output Board that you created on the iSTAR Classic/Pro ACM Board ACM Ext tab or the iSTAR eX and iSTAR Edge COM1, COM2, and COM3 tabs.

The iSTAR Output Board editor (see Figure 67 on Page 208) has the following tabs:

- **iSTAR Output Board General Tab**

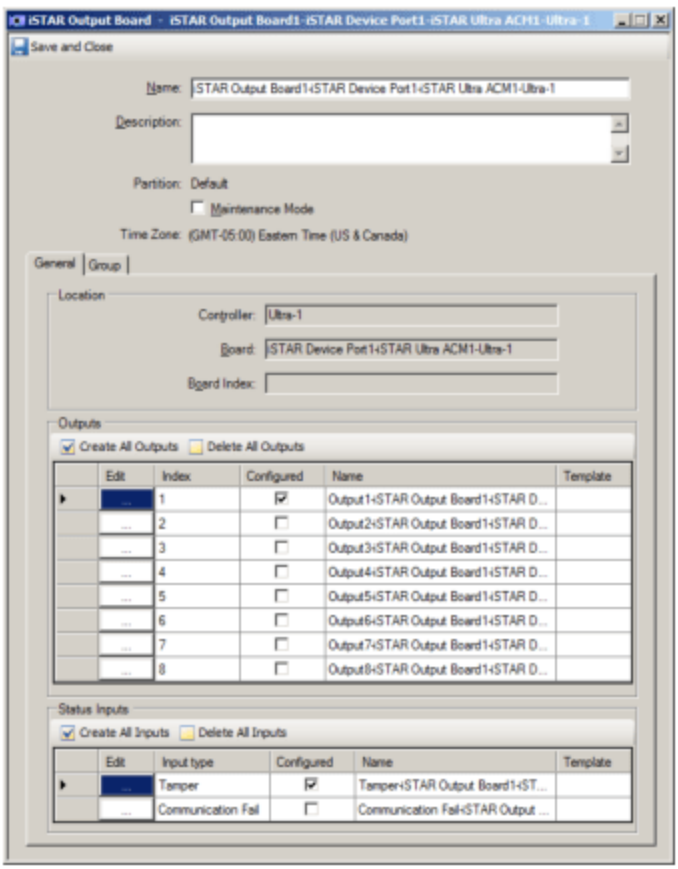
  Lists the Outputs and Status Inputs on an R/8 board that is connected to an iSTAR Classic/Pro, iSTAR eX, or iSTAR Edge. See iSTAR Output Board General Tab on Page 210.

- **iSTAR Output Board Group Tab**

  If you have created a Group containing iSTAR Output Boards and added this Output Board to it, the iSTAR Output Board editor also displays a Group tab.

  This tab lists the Output Board groups to which this Output Board belongs. See Groups Tab for Hardware Devices on Page 28 for information on using the Group tab for the iSTAR Output Board.

Figure 67: iSTAR Output Board Editor



Accessing the iSTAR Output Board Editor

You can access the iSTAR Output Board Editor in three ways:

- To Access the iSTAR Output Board Editor (iSTAR eX/Edge Controller) on Page 209

To Access the iSTAR Output Board Editor (iSTAR eX/Edge Controller)

1. From the iSTAR Controller Editor, click on the appropriate COM tab (COM1, COM2, or COM3).
2. In the Output Boards table on this tab, click [...] in the **Edit** column for the Output board you want to Edit.
3. The iSTAR Output Board Editor opens (see iSTAR Output Board Editor on Page 208).

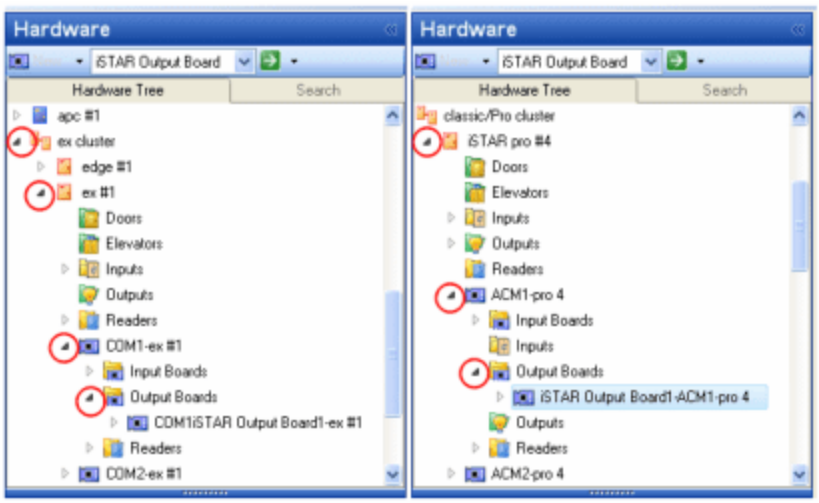
To Access the iSTAR Output Board Editor (iSTAR Classic/Pro Controller)

1. From the iSTAR Controller Editor, click on the Boards tab.
2. In the ACMs table on this tab, click [...] in the **Edit** column for the ACM that contains the Output board you want to Edit. The ACM Board Editor opens.
3. Click the ACM Ext tab.
4. In the Output Boards table on this tab, click [...] in the **Edit** column for the Output board you want to Edit.
5. The iSTAR Output Board Editor opens (see iSTAR Output Board Editor on Page 208).

To Access the iSTAR Output Board Editor from the Hardware Tree

1. Navigate from your iSTAR Controller in the Hardware Tree to the appropriate COM Board (on an iSTAR eX or iSTAR Edge Controller) or ACM Board (iSTAR Classic/Pro Controller).
2. Click on **Output Boards**, as shown in Figure 68 on Page 209. This figure shows the hardware tree for an iSTAR eX on the left and an iSTAR Pro on the right.

Figure 68: iSTAR Output Board in the Hardware Tree



3. Double-click on the Output Board you wish to edit. The iSTAR Output Board Editor opens (see iSTAR Output Board Editor on Page 208).

Configuring iSTAR Output Boards

When you configure an iSTAR Output Board, you are defining the Outputs that are attached to a particular R/8 board. You can then click to open the Outputs Editor to configure individual Outputs.

To Configure an iSTAR Output Board

1. Access the Output Board Editor for the Output Board you wish to edit (see Accessing the iSTAR Output Board Editor on Page 208).
2. If you wish to use an Output Template to configure one or more of the R/8 board Outputs, click in the **Template** column, then click [...] to open a dialog box listing the available Output Templates. See Using Templates for Controller Inputs, Outputs, and Readers on Page 37 for more information.
3. Create the **Outputs** that you need by clicking **Create All Outputs** or by selecting the **Configured** check box for only the Outputs you wish to create.
4. Click [...] in the **Edit** column to open the iSTAR Output Editor to configure individual Outputs. See the iSTAR Output Editor on Page 241 for configuration instructions.
5. If you wish to use an Output Template to configure one or more of the R/8 board Status Inputs, click in the **Template** column, then click [...] to open a dialog box listing the available Input Templates. See Using Templates for Controller Inputs, Outputs, and Readers on Page 37 for more information.
6. Create the Status Inputs that you need by clicking **Create All Inputs** or by selecting the **Configured** check box for only the Inputs you wish to create.
7. Click [...] in the **Edit** column to configure individual Status Inputs. See the definitions of the Status Inputs in Table 44 on Page 210 and see iSTAR Input Editor on Page 232.
8. When you have finished configuring these Outputs and Inputs on the Output Board Editor General tab, click **Save and Close** to save the settings you have configured on the iSTAR Output Board editor.

iSTAR Output Board General Tab

The iSTAR Output Board General tab allows you to configure the Outputs on an R/8 board attached to your iSTAR Controller, as well as the Status Inputs for Tamper and Communications Failure.

iSTAR Output Board General Tab Definitions

Table 44 on Page 210 lists the fields and buttons that appear on the iSTAR Output Board General tab.

Table 44: iSTAR Output Board General Tab Definitions

Field/Button	Description
Identification	
Name	Displays the name for this Output board. The name is system-generated by default, but you can edit this name by clicking this field.

Table 44: iSTAR Output Board General Tab Definitions (continued)

Field/Button	Description
Description	Enter a textual comment about the Output board, such as its location or purpose. This text is for information only.
Maintenance Mode	Click to put the iSTAR Outboard Board into Maintenance Mode. See Chapter 2: Maintenance Mode for more information.
Partition	This read-only field identifies the Partition in which this Output board resides.
Location	
Controller	This read-only field identifies the iSTAR Controller to which this Output board is attached.
Board	This read-only field identifies the iSTAR Controller board to which this Output board is attached.
Board Index	This read-only field identifies the board index (which represents the SW1 address switch setting on the R/8 board) for this Output board.
Outputs	
Create All Outputs	Click to create all eight Outputs. The check boxes in the **Configured** column are set to ☑.
Delete All Outputs	Click to delete all eight Outputs. The check boxes in the **Configured** column are set to ☐.
Edit column	Click ... in this column to open the iSTAR Output Editor to edit this Output.
Index column	This read-only field identifies the position of each Output (P1 - P8) on the R/8 board.
Configured column	☑ indicates that the Output has been configured. ☐ indicates that the Output has not been configured.
Name column	Displays the system-generated name for this Output. You can edit this name by clicking in the field.
Template column	Displays the Template used for creating this Output. If the Output is not yet configured, you can click in this column, then click to select an Output Template. If the **Configured** column displays ☑, this field cannot be edited.
Status Inputs	
Create All Inputs	Click to create the Tamper and Communications Fail Inputs. The check boxes in the **Configured** column are set to ☑.
Delete All Inputs	Click to delete the Tamper and Communications Fail Inputs. The check boxes in the **Configured** column are set to ☐.
Edit column	Click ... in this column to open the iSTAR Input Editor to edit this Input.

Table 44: iSTAR Output Board General Tab Definitions (continued)

Field/Button	Description
Index column	The Input Type Column displays: **Tamper** – Represents the Tamper Input on the R/8 board. NOTE: For UL applications, the Tamper Input on the iSTAR Output Board General tab must be enabled. **Communications Fail** – Represents the Communications Fail Input on the R/8 board. NOTE: For UL applications, the Communications Failure Input on the iSTAR Output Board General tab must be enabled.
Configured column	☑ indicates that the Input has been configured. ☐ indicates that the Input has not been configured.
Name column	Displays the system-generated name for this Input. You can edit this name by clicking in the field.
Template column	Displays the Template used for creating this Input. If the Input is not yet configured, you can click in this column, then click to select an Input Template. If the **Configured** column displays ☑, this field cannot be edited.

iSTAR Ultra Wireless Readers

The iSTAR Ultra supports either Assa Abloy Aperio or IR Schlage wireless readers. The interface is through the RS-485 ports on the Ultra GCM board. The default setting is Aperio, with Schlage as the only other option currently. Both ports must use the protocol, and they are synchronized so that both ports change whenever the protocol changes on either of them.

NOTE The protocol cannot be changed while any Schlage PIM or Aperio Hub exists.

Assa Abloy Aperio™ Hubs and Wireless Readers

- Each RS-485 port (i.e., GCM Port1, Port2) supports up to 15 Hubs. The iSTAR Ultra supports up to 32 readers paired to any of the 30 Hubs.
- If there are fewer than 32 Aperio readers, there can be up to 16 usual (RM bus or direct Wiegand) readers on the iSTAR Ultra. If only Aperio readers are used, there is no need for an ACM on the Ultra.
- Either 8 Port or 1 Port Hubs can be used, but usually 8 Port Hubs are configured.
- There are 11, plus a generic, types of locks that can be configured on the Ultra GCM.

IR Schlage™ PIMs and Wireless Readers

- Each RS-485 port (i.e., GCM Port1, Port2) supports up to 16 PIMs. The iSTAR Ultra supports up to 32 readers connected to any of the 32 PIMs. Schlage use a proprietary protocol named RS-485 RSI for communication on the bus.
- If there are fewer than 32 Schlage readers, there can be up to 16 usual (RM bus or direct Wiegand) readers on the iSTAR Ultra. If only Schlage readers are used, there is no need for an ACM on the Ultra.
- When assigning reader numbers, it is best practice to use sequential numbers, If you configure reader 1 and reader 5, Schlage will not use readers 2, 3, and 4. Although, those reader numbers are available for the up to 16 ACM RM or Wiegand readers.

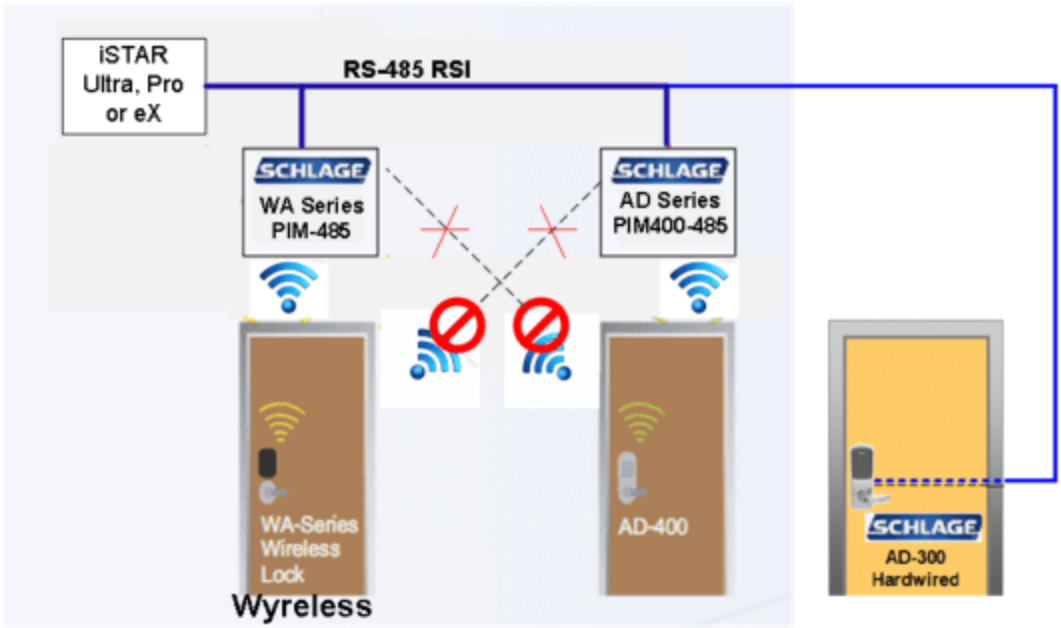
NOTE Schlage addresses are one less than the C•CURE index. For example, if you setup a reader on Schlage address 1, then it's C•CURE index 2.

- There are 3 types of PIMs that can be connected to Port 1 or Port 2.
  - PIM400-485 (AD-400 Series Locks)
  - AD-300 (AD-300 Series Locks)
  - PIM-485 (WA Series Locks)

NOTE The iSTAR eX and iSTAR Pro support the same PIMs and Locks through the RS-485 ports on the Pro GCM and the eX PMB board. The RM ports on the eX PMB are multiplexed to the COM1 and COM2 ports that are visible in the C•CURE 9000 software.

Figure 4 on Page 214 shows Schlage wireless connection methods.

Figure 4: Schlage Wireless Connection Methods



iSTAR Ultra Schlage Wireless Types of Connections

The Schlage Readers interface to C•CURE hardware using one of seven basic methods:

1. PIM400-485 (AD400 Wireless to Ultra GCM, Pro GCM and eX PMB)
2. PIM400-485 TD2 (AD400 Wireless to all iSTARs and all apCs) (Can use Wiegand or Magnetic signaling)
3. AD300 Built-in PIM (AD300 Wired to Ultra, Pro and eX)
4. AD300 PIB300 (AD300 Wired to all iSTARs and all apCs)
5. PIM485 (Wyreless Wireless to Ultra GCM, Pro GCM and eX PMB)
6. PIM TD2 (Wyreless Wireless to all iSTARs and all apCs) (2 Reader - Can use Wiegand or Magnetic signaling)
7. PIM TD4 (Wyreless Wireless to all iSTARs and all apCs) (4 reader - Can use Wiegand or Magnetic signaling)

Each of the first four methods are repeated for FIPS-201:

1. PIM401-485 (AD400 Wireless to Ultra, Pro and eX)
2. PIM401-485 TD2 (AD400 Wireless to all iSTARs and all apCs)
3. AD301 Built-in PIM (AD300 Wired to Ultra, Pro and eX)
4. AD301 PIB301 (AD301 Wired to all iSTARs and all apCs)

Wireless - PIM400 and PIM400-TD2

- Up to 16 AD400 wireless readers can be associated with 1 PIM400. Up to 2 AD400 wireless readers can be associated with 1 PIM400-TD2.

- The PIM400 interfaces with iSTAR Ultra, Pro and eX using RS-485 RSI.
- The PIM400-TD2 interfaces with either Wiegand signaling or Clock/Data Magnetic ABA2 signaling. The method is determined by the type of reader.
- A magnetic card reader (swipe or insertion) will use Clock and Data which will be passed through the TD2 to the C•CURE hardware. The magnetic signaling must be connected to an RM4/4E and then to an RM port.
- A Wiegand signaling reader will use Data 1 and Data 0 which will also be passed through the TD2. the Wiegand signaling can be connected to any direct Wiegand port or to an RM4/4E.
- In addition to AD400 Readers, the PIM400-485 can also communicate with WRI400, WPR400, and TK400 devices.

Summary Tables

The tables in this section provides a matrix of the possible connections between Schlage devices and iSTARs and apCs.

AD400 Wireless

Table 4: AD400 Series

Controller/Panel	Locks Supported	RS485 RSI Chain	Wiegand Signal (D0/D1) to Panel	Magnetic Signal (CLK/DATA) to Panel
iSTAR Ultra iSTAR Pro iSTAR Classic	AD400 (All styles)	PIM400-485 RSI to GCM	PIM400-TD2 to ACM Wiegand PIM400-TD2 to RM4x to ACM RM	PIM400-TD2 to RM4x to ACM RM
iSTAR eX	AD400 (All styles)	PIM400-485 RSI to PMB	PIM400-TD2 to GCM Wiegand PIM400-TD2 to RM4x to PMB RM	PIM400-TD2 to RM4x to PMB RM
iSTAR Edge	AD400 (All styles)		PIM400-TD2 to Edge Wiegand PIM400-TD2 to RM4x to Edge RM	PIM400-TD2 to RM4x to Edge RM
apC/8X	AD400 (All styles)		PIM400-TD2 to WPSC Wiegand PIM400-TD2 to RM4x to apC RM	PIM400-TD2 to RM4x to apC RM
apC/L	AD400 (All styles)		PIM400-TD2 to RM4x to apC/L RM	PIM400-TD2 to RM4x to apC/L RM

AD401 Wireless (FIPS-201)

NOTE The AD401 (FIPS-201) configuration only supports a Multi-technology reader with Keypad and Wiegand signaling.

The reader appears as a standard Wiegand reader connected to:

- iSTAR ACM Wiegand Port

- iSTAR eX GCM Wiegand Port
- iSTAR Edge Wiegand Port
- apC/8X WPSC Wiegand Port
- RM4 or RM4E to any RM Port on iSTAR or apC.

The PIB401-TD2 is used for all connections.

Table 5: AD401 Series

Controller/Panel	Locks Supported	RS485 RSI Chain	Wiegand Signal (D0/D1) to Panel	Magnetic Signal (CLK/DATA) to Panel
iSTAR Ultra iSTAR Pro iSTAR Classic	AD401 (Multi-Technology with keypad only)	N/A	PIM401-TD2 to ACM Wiegand PIM401-TD2 to RM4x to ACM RM	N/A
iSTAR eX	AD401 (Multi-Technology with keypad only)	N/A	PIM401-TD2 to GCM Wiegand PIM401-TD2 to RM4x to PMB RM	N/A
iSTAR Edge	AD401 (Multi-Technology with keypad only)		PIM401-TD2 to Edge Wiegand PIM401-TD2 to RM4x to Edge RM	N/A
apC/8X	AD401 (Multi-Technology with keypad only)		PIM401-TD2 to WPSC Wiegand PIM401-TD2 to RM4x to apC RM	N/A
apC/L	AD401 (Multi-Technology with keypad only)		PIM401-TD2 to RM4x to apC/L RM	N/A

AD300 Hard Wired

Table 6: AD300 Series

Controller/Panel	Locks Supported	RS485 RSI Chain	Wiegand Signal (D0/D1) to Panel	Magnetic Signal (CLK/DATA) to Panel
iSTAR Ultra iSTAR Pro iSTAR Classic	AD300 (All styles)	Built in PIM400-485 RSI to GCM	PIB300-TD2 to ACM Wiegand PIB300-TD2 to RM4x to ACM RM	PIB300-TD2 to RM4x to ACM RM
iSTAR eX	AD300 (All styles)	Built in PIM400-485 RSI to PMB	PIB300-TD2 to GCM Wiegand PIB300-TD2 to RM4x to PMB RM	PIB300-TD2 to RM4x to PMB RM

Table 6: AD300 Series (continued)

Controller/Panel	Locks Supported	RS485 RSI Chain	Wiegand Signal (D0/D1) to Panel	Magnetic Signal (CLK/DATA) to Panel
iSTAR Edge	AD300 (All styles)		PIB300-TD2 to Edge Wiegand PIB300-TD2 to RM4x to Edge RM	PIB300-TD2 to RM4x to Edge RM
apC/8X	AD300 (All styles)		PIB300-TD2 to WPSC Wiegand PIB300-TD2 to RM4x to apC RM	PIB300-TD2 to RM4x to apC RM
apC/L	AD300 (All styles)		PIB300-TD2 to RM4x to apC/L RM	PIB300-TD2 to RM4x to apC/L RM

AD301 Hard Wired FIPS-201

NOTE The AD301 (FIPS-201) configuration only supports a Multi-technology reader with Keypad and Wiegand signaling.

The reader appears as a standard Wiegand reader connected to:

- iSTAR ACM Wiegand Port
- iSTAR eX GCM Wiegand Port
- iSTAR Edge Wiegand Port
- apC/8X WPSC Wiegand Port
- RM4 or RM4E to any RM Port on iSTAR or apC

The PIB301-TD2 is used for all connections.

Table 7: AD301 Series

Controller/Panel	Locks Supported	RS485 RSI Chain	Wiegand Signal (D0/D1) to Panel	Magnetic Signal (CLK/DATA) to Panel
iSTAR Ultra iSTAR Pro iSTAR Classic	AD301 (Multi-Technology with keypad only)	N/A	PIB301-TD2 to ACM Wiegand PIB301-TD2 to RM4x to ACM RM	N/A
iSTAR eX	AD301 (Multi-Technology with keypad only)	N/A	PIB301-TD2 to GCM Wiegand PIB301-TD2 to RM4x to PMB RM	N/A

Table 7: AD301 Series (continued)

Controller/Panel	Locks Supported	RS485 RSI Chain	Wiegand Signal (D0/D1) to Panel	Magnetic Signal (CLK/DATA) to Panel
iSTAR Edge	AD301 (Multi-Technology with keypad only)		PIB301-TD2 to Edge Wiegand PIB301-TD2 to RM4x to Edge RM	N/A
apC/8X	AD301 (Multi-Technology with keypad only)		PIB301-TD2 to WPSC Wiegand PIB301-TD2 to RM4x to apC RM	N/A
apC/L	AD301 (Multi-Technology with keypad only)		PIB301-TD2 to RM4x to apC/L RM	N/A

Readers per Controller/Panel

Aperio Wireless Readers

Table 8: Aperio Wireless Readers

Controller/Panel	Interface Device	Max # of Aperio Hubs	Max # of Non-Aperio Readers	Max # of Aperio Readers	Max # of both Combined	Notes
iSTAR Ultra	Aperio Hub (8 Port or 1 Port)	30 15 per RS-485 Port	16	32	32	iSTAR Ultra is the only iSTAR that supports Wireless Aperio Hubs.

Schlage Wireless Readers

Table 9: Readers per Controller/Panel - including Schlage Readers

Controller/Panel	Interface Device	Max # of Non-Schlage Readers	Max # of Schlage Readers	Max # of both Combined	Notes
iSTAR Ultra	PIM, AD300 to GCM	16	32	32	Max of 32 PIM(s) and 32 Readers
iSTAR Pro	PIM, AD300 to GCM	16	16	16	Max of 16 PIM(s) and 16 Readers
iSTAR eX 4 door	PIM, AD300 to PMB	4	16	16	16, but non-Schlage readers must be numbered 1-4

Table 9: Readers per Controller/Panel - including Schlage Readers (continued)

Controller/Panel	Interface Device	Max # of Non-Schlage Readers	Max # of Schlage Readers	Max # of both Combined	Notes
iSTAR eX 8 door	PIM, AD300 to PMB	8	16	16	16, but non-Schlage Readers must be numbered 1-8
iSTAR Pro Direct	TD2, PIB to ACM	16	16	16	2 Readers per TD2 or PIB
iSTAR eX 4 door Direct	TD2, PIB to GCM or PMB	4	4	4	2 Readers per TD2 or PIB
iSTAR eX 8 door Direct	TD2, PIB to GCM or PMB	8	8	8	Requires USB key 2 Readers per TD2 or PIB
iSTAR Edge 1 door Direct	TD2, PIB to Edge board	1	1	1	2 Readers per TD2 or PIB
iSTAR Edge 2 door Direct	TD2, PIB to Edge board	2	2	2	2 Readers per TD2 or PIB
iSTAR Edge 4 door Direct	TD2, PIB to Edge board	4	4	4	2 Readers per TD2 or PIB
apC/8X Direct	TD2, PIB to apC, WPSC, or Star Coupler	8	8	8	2 Readers per TD2 or PIB
apC/L Direct	TD2, PIB to apC/L	2	2	2	2 Readers per TD2 or PIB

iSTAR Aperio RS-485 Hub Board Editor (iSTAR Ultra only)

The iSTAR Aperio RS-485 Hub Board editor allows you to configure wireless Aperio Readers on the Hub. The Hub supports either one or eight Aperio wireless readers.

The iSTAR Aperio RS-485 Hub Board Editor has three tabs:

- General tab - see iSTAR Aperio RS-485 Hub Board Editor General Tab on Page 220
- Inputs tab - see iSTAR Aperio Hub Board Editor Input Tab on Page 222
- Readers tab - see iSTAR Aperio Hub Board Editor Readers Tab on Page 223

iSTAR Aperio RS-485 Hub Board Editor General Tab

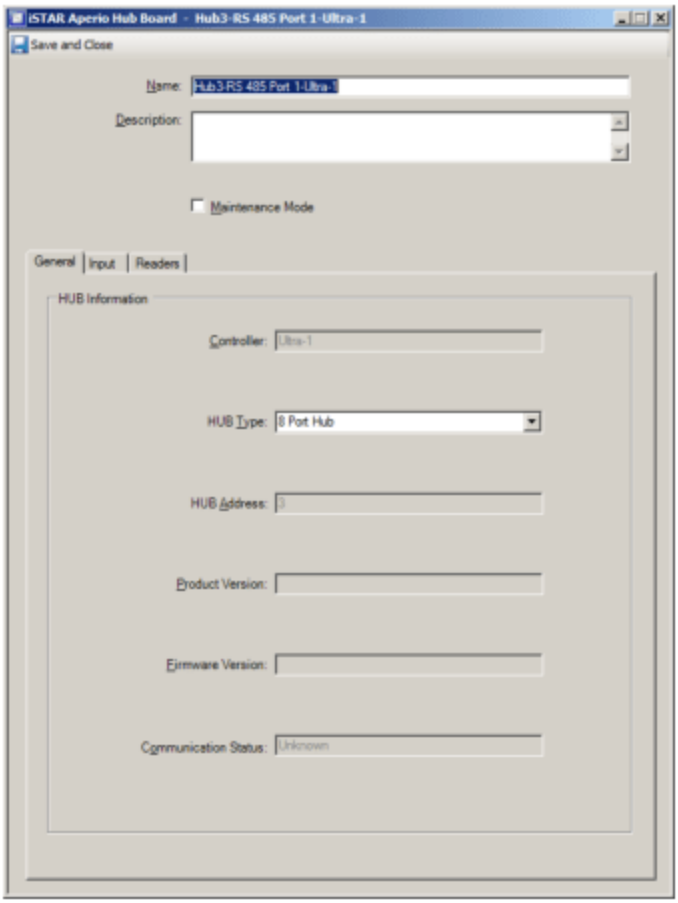
The iSTAR Aperio RS-485 Hub Board editor General tab lets you specify the Aperio RS-485 Hub on which you can create Aperio readers.

You select the type of Hub you want to configure by choosing a type from the HUB Type drop-down list. That selection determines the options that are available on the other tabs.

To access the iSTAR Aperio RS-485 Hub Board editor General tab, click on the COM 1 or COM 2 tab in the iSTAR Controller editor dialog box. Then, click on **Edit** in the row name of the RS-485 Port that you want to edit.

Figure 69 on Page 221 shows the iSTAR Aperio RS-485 Hub Board General tab.

Figure 69: iSTAR Aperio RS-485 Hub Board General Tab



iSTAR Aperio Hub Board Editor General Tab Definitions

The fields and buttons on the iSTAR Aperio RS-485 Board editor General tab are described in Table 45 on Page 221.

Table 45: iSTAR Aperio RS-485 Board Editor General Tab

Field/Button	Description
Name	This field displays the name of the Aperio Hub
Description	You can enter a textual description of the Aperio Board in the **Description** field.
Maintenance Mode	Click to put the Aperio RS-485 Hub Board into Maintenance Mode. See Chapter 2: Maintenance Mode for more information.
Controller	The name of the iSTAR Ultra controller; this is a read-only field.
HUB Type	This drop-down list allows you to select the type of Aperio board you are configuring. The default selection is 8 Port Hub
HUB Number	This read-only field contains the HUB number - the same HUB Index number as shown on the iSTAR Ultra COM1/COM2 Tabs on Page 181.

iSTAR Aperio RS-485 Board Editor General Tab (continued)

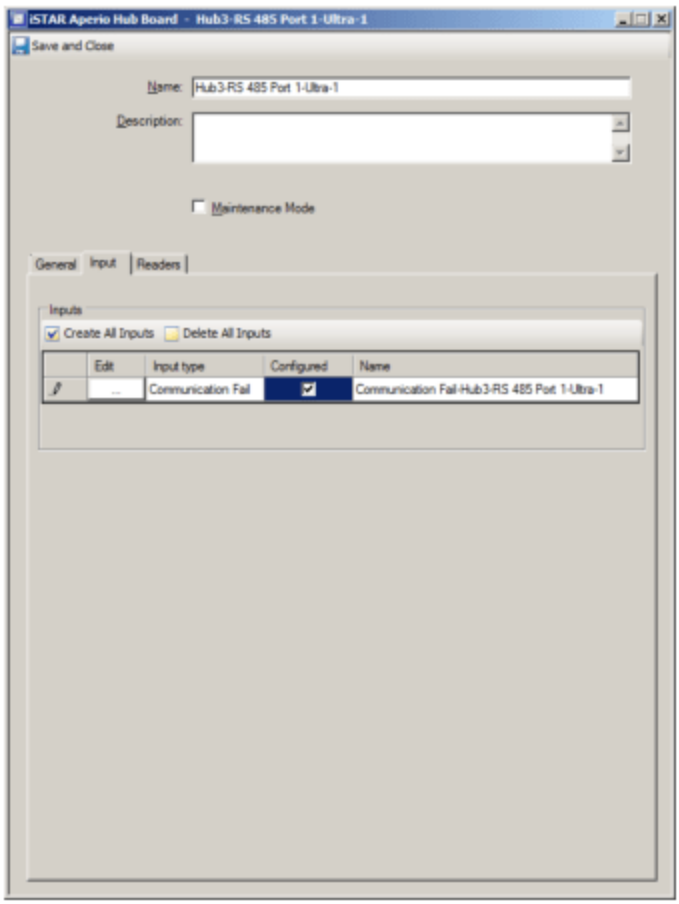
Field/Button	Description
Product Version	Displays the Product Version. For example, 2.0.0.
Firmware Version	Displays the Firmware Version. For example: 6.2.28176.
Communication Status	This read-only field displays whether the controller is in Online, Offline or Unknown state.
Save and Close	Click to save your configuration changes and close the iSTARAperio Hub Board editor.

iSTAR Aperio Hub Board Editor Input Tab

This tab allows you to configure a Communications Fail input for the Aperio Hub board.

Figure 70 on Page 222 shows the iSTAR Aperio Hub Board Input tab.

Figure 70: iSTAR Aperio Hub Board Input Tab



iSTAR Aperio Hub Board Editor Input Tab Definitions

The fields and buttons on the iSTAR Aperio Board editor Input tab are described in Table 46 on Page 223.

Table 46: iSTAR Aperio RS-485 Board Editor

Field/Button	Description
Create All Inputs	Click to create the Communication Fail Input. When you click **Create All Inputs**, the **Configured** column check box is selected, and you can click ... in the **Edit** column to open the iSTAR Input editor (see iSTAR Input Editor on Page 232.
Delete All Inputs	When you click **Delete Input**, the check box in the **Configured** column is cleared for the Communications Fail Input, and the Input is deleted (any settings you have configured are lost).
Edit column	Click ... in the **Edit** column to open the Input Editor to configure the Communications Fail Input. See iSTAR Input Editor on Page 232.
Input type column	This column displays the input type (Communications Fail).
Configured column	Click in this column to create the Communications Fail Input (make it available to be edited).
Name column	Displays the name for this Input. The name is system-generated, but you can edit the name.
Save and Close	Click to save your configuration changes and close the Aperio Hub Board editor.

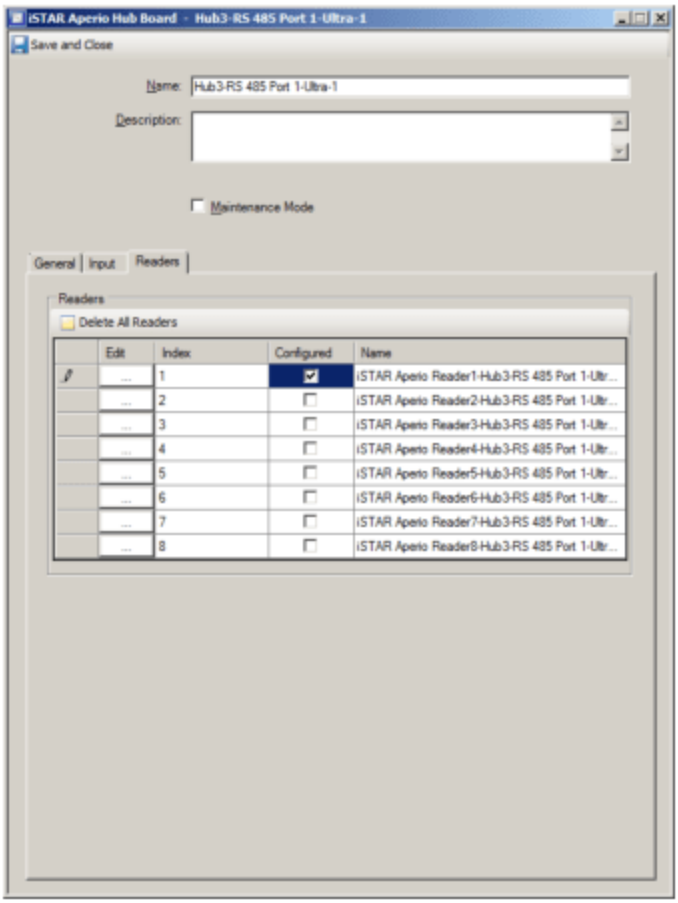
iSTAR Aperio Hub Board Editor Readers Tab

The iSTAR Aperio Hub Board editor Readers tab allows you to identify the readers you want to configure, and to access the iSTAR Aperio Reader editor to configure the readers.

The following Aperio Reader types can be configured: C100, E100, L100, PR100, IN100, A100, K100, M100, KS100, R100, AS100, and Generic types.

Figure 71 on Page 224 shows the iSTAR Aperio Hub Board Readers tab.

Figure 71: iSTAR Aperio Hub Board Readers Tab



iSTAR Aperio RS-485 Board Hub Editor Readers Tab Definitions

The fields and buttons on the iSTAR Aperio RS-485 Board editor Readers tab are described in Table 47 on Page 224.

Table 47: iSTAR Aperio RS-485 Board Editor Readers Tab

Field/Button	Description
Create All Readers	Click to create all 8 readers. When you click **Create All Readers** the Configured column check boxes are selected, and you can click [...] in the **Edit** column to open the iSTAR Aperio Reader Editor to configure a Reader. See iSTAR Aperio Reader Editor on Page 264.
Delete All Readers	When you click **Delete All Readers**, the check boxes in the **Configured** column are cleared for all 8 Readers, and all 8 Readers are deleted (any settings you have configured are lost). NOTE: If you **Delete all Readers** on this tab, the Aperio Door objects that were created automatically for these readers are also deleted.
Edit column	Click [...] in the **Edit** column to open the iSTAR Aperio Reader editor to configure a Reader. See iSTAR Aperio Reader Editor on Page 264.

iSTAR Aperio RS-485 Board Editor Readers Tab (continued)

Field/Button	Description
Reader Index column	This column displays the number of each Reader.
Configured column	Click ☐ in this column to create a Reader (make it available to be edited). Clearing this check box deletes this Aperio Reader, and any automatically created Aperio Door associated with this Reader, after you click **Yes** to confirm the deletion in the Warning box that appears.
Name column	Displays the name for this Reader. The name is system-generated, and the Name field is editable.
Save and Close	Click to save your configuration changes and close the iSTAR Aperio Hub Board editor.

iSTAR PIM-485 Board Editor

The iSTAR PIM-485 Board editor on iSTAR Pro or iSTAR eX allows you to configure Schlage Wireless Readers that are connected to a PIM-485 Panel Interface Module (PIM). This board supports up to 16 wireless readers connected via RS-485.

The following PIMs are supported:

- PIM400-485 (AD400 Series Locks)
- AD300 (AD300 Series Locks)
- PIM-485 (WA Series Locks)

The iSTAR PIM-485 Board Editor has three tabs:

- General tab - see iSTAR PIM-485 Board Editor General Tab on Page 226
- Inputs tab - see iSTAR PIM-485 Board Editor Input Tab on Page 228
- Readers tab - see iSTAR PIM-485 Board Editor Readers Tab on Page 229

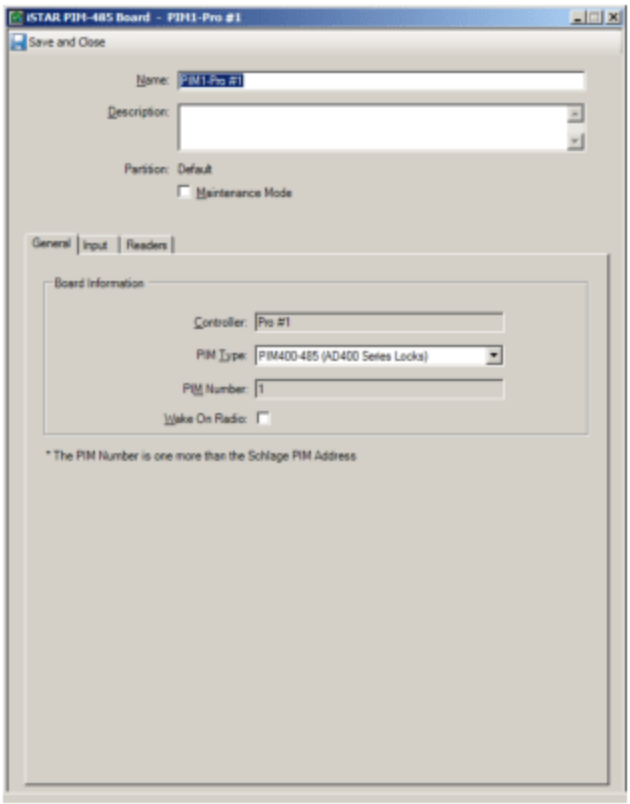
iSTAR PIM-485 Board Editor General Tab

The iSTAR PIM-485 Board editor General tab lets you specify the type of PIM Board to which you can configure Schlage Wireless readers. You select the type of PIM you want to configure by choosing a type from the PIM Type drop-down list. That selection determines the options that are available on the other tabs.

If you choose the AD300 (AD300 Series Locks), the Input tab is removed, because the AD300 does not support a Tamper Input.

Figure 72 on Page 227 shows the iSTAR PIM-485 Board General tab.

Figure 72: iSTAR PIM-485 Board General Tab



iSTAR PIM-485 Board Editor General Tab Definitions

The fields and buttons on the iSTAR PIM-485 Board editor General tab are described in Table 48 on Page 227.

Table 48: iSTAR PIM-485 Board Editor General Tab

Field/Button	Description
Name	This field displays the name of the PIM Board
Description	You can enter a textual description of the PIM Board in the **Description** field.
Maintenance Mode	Click to put the iSTAR PIM-485 Board into Maintenance Mode. See Chapter 2: Maintenance Mode for more information.
Controller	The name of the controller; this is a read-only field.
PIM Type	This drop-down list allows you to select the type of PIM board you are configuring. • PIM400-485 (AD400 Series Locks) • AD300 (AD300 Series Locks) • PIM-485 (WA Series Locks)

iSTAR PIM-485 Board Editor General Tab (continued)

Field/Button	Description
PIM Number	This read-only field contains the PIM number - the same PIM Index number as shown on the iSTAR Schlage Wireless PIMs Tab on Page 153 or the iSTAR eX COM1/COM2 Tabs on Page 173.
Wake on Radio	Wake on Radio allows a battery-powered lock device to receive an immediate command from the iSTAR panel that is out of sequence with the regular heartbeat communications between the panel and the lock (the default heartbeat interval is 10 minutes). The Wake on Radio interval is 10 seconds. Enabling this feature allows the reader and lock to respond more quickly (within ten seconds rather than within ten minutes) to manual actions. Typically the command from the iSTAR panel to the device will be for a lock or unlock.
Save and Close	Click to save your configuration changes and close the iSTAR PIM-485 Board editor.

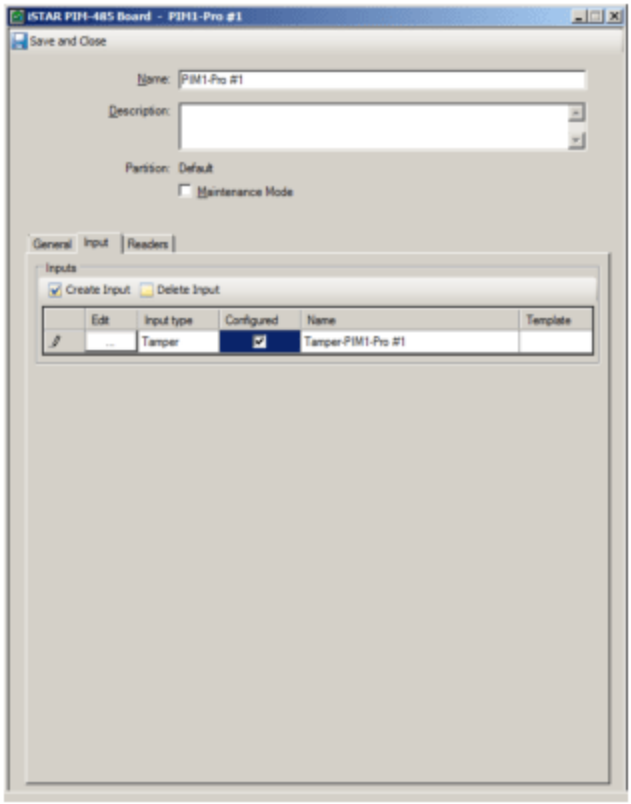
iSTAR PIM-485 Board Editor Input Tab

This tab allows you to configure a Tamper input for the PIM400-485 and PIM-485.

If you select the AD300 series lock in the PIM Type Drop-down list on the General tab, the Input tab is removed because the AD300 series does not have a Tamper Input.

Figure 73 on Page 228 shows the iSTAR PIM-485 Board Input tab.

Figure 73: iSTAR PIM-485 Board Input Tab



iSTAR PIM-485 Board Editor Input Tab Definitions

The fields and buttons on the iSTAR PIM-485 Board editor Input tab are described in Table 49 on Page 229.

Table 49: iSTAR PIM-485 Board Editor

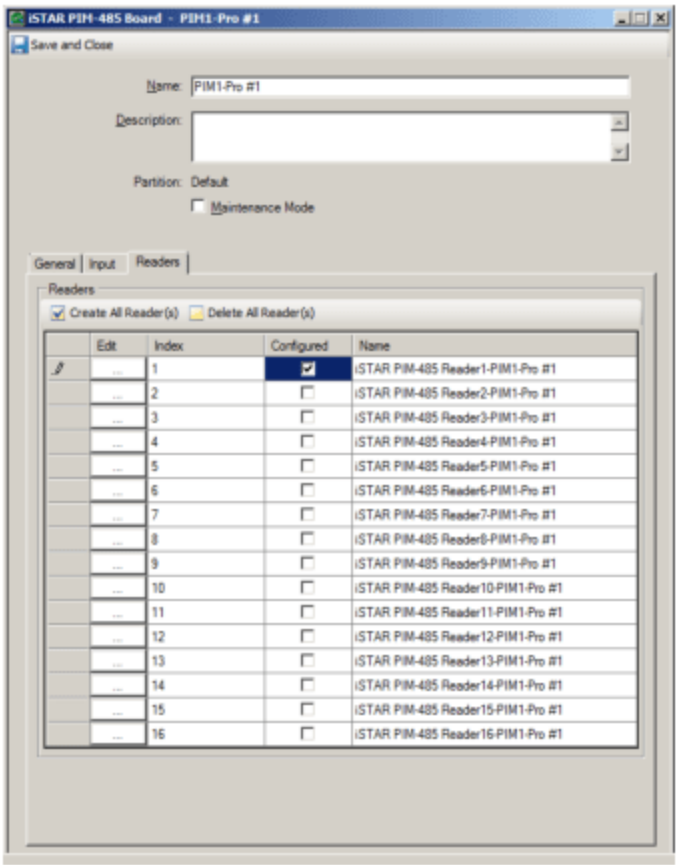
Field/Button	Description
Create Input	Click to create the Tamper Input. When you click **Create Input**, the **Configured** column check box is selected, and you can click ... in the **Edit** column to open the iSTAR Input editor (see iSTAR Input Editor on Page 232.
Delete Input	When you click **Delete Input**, the check box in the **Configured** column is cleared for the Tamper Input, and the Tamper Input is immediately deleted (any settings you have configured are lost).
Edit column	Click ... in the **Edit** column to open the Input Editor to configure the Tamper Input. See iSTAR Input Editor on Page 232.
Input type column	This column displays the input type (Tamper).
Configured column	Click ☐ in this column to create the Tamper Input (make it available to be edited).
Name column	Displays the name for this Input. The name is system-generated and is read-only.
Template Column	Displays the Template used for creating this Input. If the Input is not yet configured, you can click in this column, then click to select an Input Template. If the **Configured** column displays ☑, this field cannot be edited.
Save and Close	Click to save your configuration changes and close the iSTAR PIM-485 Board editor.

iSTAR PIM-485 Board Editor Readers Tab

The iSTAR PIM-485 Board editor Readers tab allows you to identify the readers you want to configure, and to access the iSTAR PIM-485 Reader editor to configure the readers.

Figure 74 on Page 230 shows the iSTAR PIM-485 Board Readers tab.

Figure 74: iSTAR PIM-485 Board Readers Tab



iSTAR PIM-485 Board Editor Readers Tab Definitions

The fields and buttons on the iSTAR PIM-485 Board editor Readers tab are described in Table 50 on Page 230.

Table 50: iSTAR PIM-485 Board Editor Readers Tab

Field/Button	Description
Create All Readers	Click to create all 16 readers. When you click **Create All Readers** the Configured column check boxes are selected, and you can click [...] in the **Edit** column to open the iSTAR PIM-485 Board Editor to configure a Reader. See iSTAR PIM-485 Reader Editor on Page 260.
Delete All Readers	When you click **Delete All Readers**, the check boxes in the **Configured** column are cleared for all 16 Readers, and all 16 Readers are immediately deleted (any settings you have configured are lost).
Edit column	Click [...] in the **Edit** column to open the iSTAR PIM-485 reader Editor to configure a Reader. See iSTAR PIM-485 Reader Editor on Page 260.
Reader Index column	This column displays the number of each Reader.

iSTAR PIM-485 Board Editor Readers Tab (continued)

Field/Button	Description
Configured column	Click ☐ in this column to create a Reader (make it available to be edited).
Name column	Displays the name for this Reader. The name is system-generated, and the field is read-only.
Save and Close	Click to save your configuration changes and close the iSTAR PIM-485 Board editor.

iSTAR Input Editor

The iSTAR Input editor lets you configure an iSTAR Input that you created on an iSTAR Input Board.

The iSTAR Input editor (see Figure 75 on Page 233) has the following tabs:

- **iSTAR Input General Tab on Page 236**

  Identifies the Controller and Board this Input is configured on, the type of the Input (such as Door Switch), and the object the Input is assigned to, such as a Door.

- **iSTAR Input Intrusion Zone Tab on Page 237**

  This tab appears only if you have included this iSTAR Controller in an Intrusion Zone and added this Input as a Controlled Input.

- **iSTAR Input Triggers Tab on Page 239**

  This tab lets you define Triggers that can activate C•CURE 9000 Events and activate outputs.

  See Triggers Tab for iSTAR Devices on Page 270 for information on creating Triggers for an iSTAR device.

- **Groups Tab for Hardware Devices on Page 28**

  If you have created a Group containing iSTAR Inputs and added this Input to it, the iSTAR Input editor also displays a Group tab.

  This tab lists the Input groups to which this Input belongs. for information on using the Group tab for your iSTAR Input.

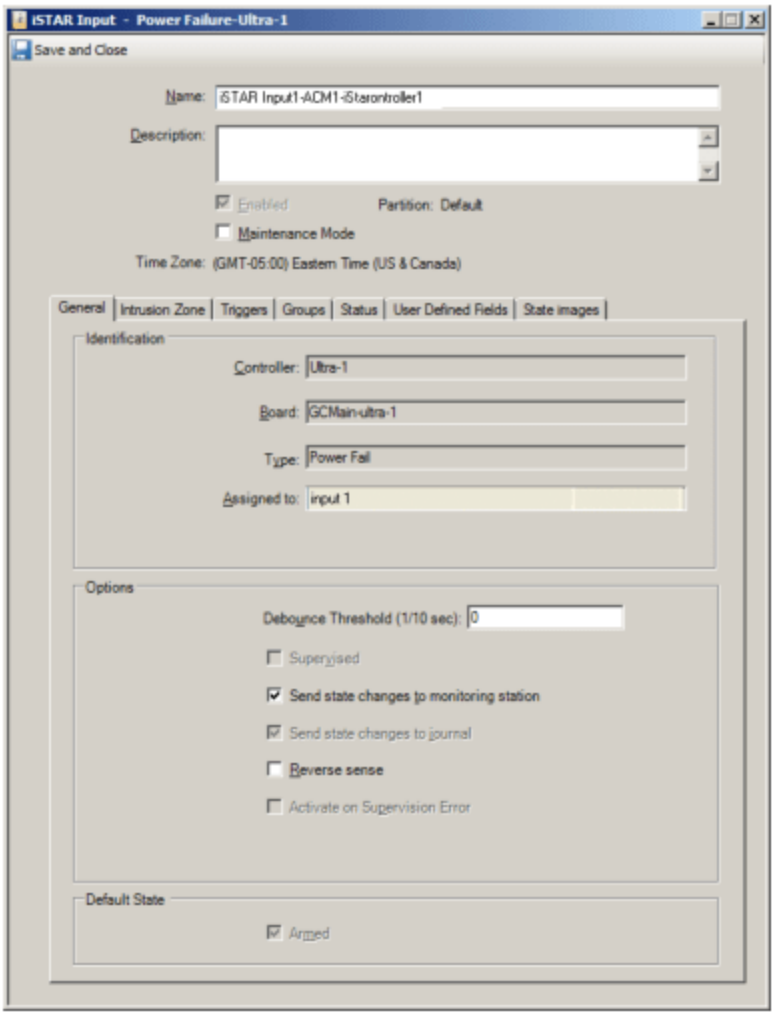
- **iSTAR Input Status Tab on Page 239**

  This tab displays several read-only fields that report the Active, Armed, Hardware, and Supervision status of the Input.

- **iSTAR Input State Images Tab on Page 239**

  This tab shows the images that are displayed in the Monitoring Station to represent this input. You can change the image used for any of the Input states.

Figure 75: iSTAR Input Editor



Accessing the iSTAR Input Editor

You can access the iSTAR Input Editor in several ways:

- To Access the iSTAR Input Editor (iSTAR eX/Edge Controller) on Page 233.
- To Edit a Main Board Input (iSTAR Classic/Pro Controller) on Page 234.
- To Edit an ACM Board Input (iSTAR Classic/Pro Controller) on Page 234.
- To Edit an Input on an ACM Ext I/8 Board (iSTAR Classic/Pro Controller) on Page 234.
- To Edit a Main Board Input from the Hardware Tree on Page 234.
- To Edit a COM1/COM2/COM3 or ACM Input from the Hardware Tree on Page 235

To Access the iSTAR Input Editor (iSTAR eX/Edge Controller)

1. From the iSTAR Controller Editor, click on the appropriate tab (Inputs, COM1, COM2, or COM3).
2. Click in the **Configured** column to create a Main Board or General Purpose Input.

3. Click the **Edit** button [...] for the Input you want to edit.
   - To edit a Main Board or General Purpose Input from the Inputs tab, click [...] in the **Edit** column for the Input you want to edit.
   - To edit I/8 Inputs from the COM1/COM2/COM3 tab, click [...] in the **Edit** column for the Input Board containing the Input you want to Edit. The iSTAR Input Board Editor opens. Click [...] in the **Edit** column for the Input you want to edit.

   The iSTAR Input Editor opens (see iSTAR Input Editor on Page 232).

To Edit a Main Board Input (iSTAR Classic/Pro Controller)

1. From the iSTAR Controller Editor, click on the Boards tab.
2. Click [...] in the **Edit** column for the Input you want to edit.

   The iSTAR Input Editor opens (see iSTAR Input Editor on Page 232).

To Edit an ACM Board Input (iSTAR Classic/Pro Controller)

1. From the iSTAR Controller Editor, click on the Boards tab.
2. Click [...] in the **Edit** column for the ACM that contains the Input you want to Edit. The ACM Board Editor opens.
3. Click the Inputs tab.
4. Click [...] in the **Edit** column for the Input you want to edit.

   The iSTAR Input Editor opens (see iSTAR Input Editor on Page 232).

To Edit an Input on an ACM Ext I/8 Board (iSTAR Classic/Pro Controller)

1. From the iSTAR Controller Editor, click on the Boards tab.
2. Click [...] in the **Edit** column for the ACM that contains the Input you want to Edit. The ACM Board Editor opens.
3. Click the ACM Ext tab.
4. Click [...] in the **Edit** column for the Input board that contains the Input.
5. In the Inputs table on this tab, click [...] in the **Edit** column for the Input you want to Edit.

   The iSTAR Input Editor opens (see iSTAR Input Editor on Page 232).

To Edit a Main Board Input from the Hardware Tree

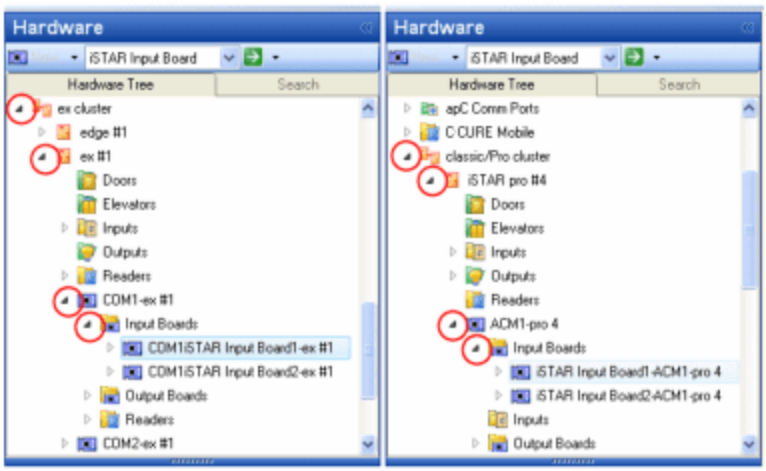
1. Navigate to your iSTAR Controller in the Hardware Tree and click ▷.
2. Click the **Inputs** folder.
3. Double-click on the Input you want to edit.

   The iSTAR Input Editor opens (see iSTAR Input Editor on Page 232).

To Edit a COM1/COM2/COM3 or ACM Input from the Hardware Tree

1. Navigate from your iSTAR Controller in the Hardware Tree to the appropriate COM Board (on an iSTAR eX or iSTAR Edge Controller) or ACM Board (on an iSTAR Classic/Pro Controller).
2. Click ▷ on **Input Boards**, as shown in Figure 68 on Page 209.

Figure 76: iSTAR Input Boards in the Hardware Tree



3. Click ▷ on the Input board that contains the Input you wish to edit.
4. Click ▷ on **Inputs** under that board.
5. Double-click on the Input you wish to edit.

   The iSTAR Input Editor opens.

Configuring an iSTAR Input

When you configure an iSTAR Input, you use the Input Editor tabs to define the Options, Default State, Triggers, and State Images for the Input.

To Configure an iSTAR Input

1. Access the Input Editor for the Input you wish to edit (see Accessing the iSTAR Input Editor on Page 233).
2. Click the Input General tab:
   - Modify the name of the Input in the **Name** field, if desired.
   - Add a textual description of the Input to the **Description** field.
   - Enable the Input by clicking the **Enabled** field.
   - Modify the Options settings for the Input. See the definitions for the Options fields in on Page 236.
   - Set the Default State for the Input to **Armed** (☑) or not **Armed** (☐).
3. Click the Intrusion Zone tab (if available) to view the name of the **Intrusion Zone** this Input is part of, and the **Display Name** used by the Intrusion Zone for this Input.

4. Click the Input Triggers tab. iSTAR Input Triggers Tab on Page 239 defines the Input Properties you can use in triggers. Configure the triggers you need for this Input by following the steps in Triggers Tab for iSTAR Devices on Page 270.
5. Click the Input Status tab to view the Active, Armed, Hardware, and Supervision status of the Input.
6. Click the Input State Images tab to view the state images for this Input. If you wish to customize the state images for this Input, follow the steps in State Images Tab for iSTAR Devices on Page 274.
7. When you have finished configuring this Input in the Input Editor, click **Save and Close** to save the settings you have configured.

iSTAR Input General Tab

The iSTAR Input General tab displays information that identifies the Input and allows you to configure the Options and Default State for the input.Figure 75 on Page 233 shows the iSTAR Input General tab.

iSTAR Input General Tab Definitions

Table 51 on Page 236 lists the fields and buttons that appear on the iSTAR Input General tab.

Table 51: iSTAR Input General Tab Definitions

Field/Button	Description
Name	Displays the name for this Input. The name is system-generated by default, but you can edit this name by clicking in this field.
Description	Enter a textual comment about the Input, such as its location or purpose. This text is for information only.
Enabled	Click ☑ to enable the Input.
Maintenance Mode	Click to put the iSTAR Input into Maintenance Mode. See Chapter 2: Maintenance Mode for more information.
Partition	This read-only field identifies the Partition in which this Input resides.
Identification	
Controller	This read-only field identifies the iSTAR Controller to which this Input is attached.
Board	This read-only field identifies the iSTAR Controller board to which this Input is attached.
Type	Reflects whether the Input has been assigned to a Door or other object. These include: • General • Door Switch • Request to Exit • Elevator
Assigned to	Displays the Elevator or Door object name with which this Input is configured.
Connection	Identifies the Input number on the hardware board to which this Input is connected.

Table 51: iSTAR Input General Tab Definitions (continued)

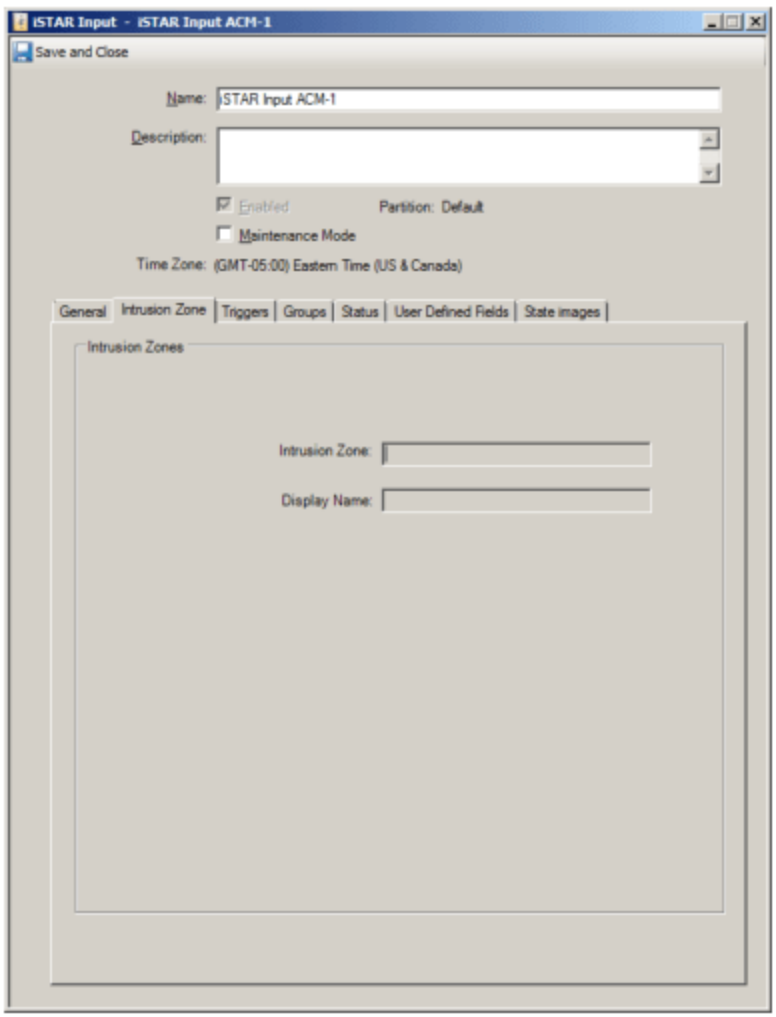
Field/Button	Description
Options	
Debounce Threshold (1/10 sec)	In this field, enter the time that an input must be in a particular state before it is reported as a state change. It is used to filter out spurious changes. The units range from 0 – 60 seconds, the default is 0. NOTE: For Proprietary Burglar Alarm applications, the **Debounce Threshold** field must be programmed for a maximum of 90 seconds.
Supervised	This field indicates that the inputs on the board are Supervised. This is a read-only field. NOTE: For Proprietary Burglar Alarm applications, the **Supervised** check box must be selected.
Send state changes to monitoring station	To have a notification of changes in state of the Input sent to the guard station, select the **Send state changes to the monitoring station** check box. NOTE: For Proprietary Burglar Alarm applications, the **Send state changes to the monitoring station** option must be selected.
Send state change to journal	To have a notification of changes in state of the Input sent to the journal, select the **Send state changes to journal** check box. This option will be selected by default.
Reverse sense	When this option is selected, the interpretation of the board's Supervised Resistors is reversed.
Activate on Supervision Error	When this option is selected, the Input will be activated on a Supervision error.
Default State	
Armed	When this option is selected, the Input is armed by default. This is useful if you are not providing arming via an event.

iSTAR Input Intrusion Zone Tab

The iSTAR Input Intrusion Zone tab appears only if the iSTAR Input is included in an Intrusion Zone. Figure 77 on Page 238 shows the iSTAR Input Intrusion Zone tab.

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. 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 77: iSTAR Input Intrusion Zone Tab



The iSTAR Input Intrusion Zone tab displays read-only fields that give Intrusion Zone assignment information for this Input.

Table 52: iSTAR Input Intrusion Zone Tab Definitions

Field/Button	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. NOTE: This is the unique LCD display name for this Input that is used whenever the Intrusion Zone needs to display this door as an 'offnormal' point on the Reader LCD.

NOTE The Dynamic View for iSTAR Inputs also allows you to add a column that identifies the Intrusion Zone to which the Inputs belong.

iSTAR Input Triggers Tab

You can create iSTAR Input Triggers for the properties shown in Table 53 on Page 239.

For iSTAR Main Board and Special Purpose Inputs such as Tamper, Power Failure, and Battery Low, you can only create Triggers for the **Active Status** property.

Table 53: iSTAR Input Trigger Properties

Property	Description
Active Status	Values that you can use for Triggers are "Active" and "Inactive".
Armed Status	Values that you can use for Triggers are "Armed" and "No Error".
Supervision Error Status	Values that you can use for Triggers are "Error" and "No Error".

See Triggers Tab for iSTAR Devices on Page 270 for information on creating Triggers for an iSTAR device.

iSTAR Input Status Tab

The iSTAR Input Status tab displays several Input properties in read-only fields. Table 54 on Page 239 lists the fields on the iSTAR Input Status tab.

Table 54: iSTAR Input Status Tab Definitions

Field/Button	Description
Active Status	Displays whether the Input is Active or Inactive.
Armed Status	Displays whether the Input is Armed or Disarmed.
Hardware Status	Displays the Hardware Status value for the Input. Possible values are Secure, Active, Open Loop, Shorted Loop, Fault, or Ground.
Supervision Status	Displays the Supervision Status value for the Input. Possible values are: • Unknown - the host has not received the input status reported from the panel yet. • Uninitialized - the panel reports no error on the input. • Error - the input is in error state, and the detail can be seen in the Hardware Status field.

iSTAR Input State Images Tab

The iSTAR Input State Images tab provides a means to change the default images that are displayed on the C•CURE 9000 Monitoring Station to indicate iSTAR Input states.

See State Images Tab for iSTAR Devices on Page 274 for information on using the State Images tab for an iSTAR Input.

iSTAR Input State Images Tab Definitions

Table 55 on Page 240 shows the iSTAR Input States and the default State Images.

Table 55: STAR Input State Images Tab Definitions

Icon	Description
	Unknown
	Active
	Armed Enabled
	Disarmed Enabled
	Supervision Error
	Disabled
	Update Disabled

iSTAR Output Editor

The iSTAR Output editor lets you configure an iSTAR Output that you created on an iSTAR Output Board.

The iSTAR Output editor (see on Page 241) has the following tabs:

- **iSTAR Output General tab**

  Identifies the Controller and Board this Output is configured on, the type of the Output (such as Alternate Shunt Relay), and the object the Input is assigned to, such as a Door. See iSTAR Output General Tab on Page 245.

- **iSTAR Output Groups tab**

  If you have created a Group containing iSTAR Outputs and added this Output to it, the iSTAR Output editor also displays a Group tab.

  This tab lists the Output groups to which this Output belongs. See Groups Tab for Hardware Devices on Page 28 for information on using the Group tab for the iSTAR Output.

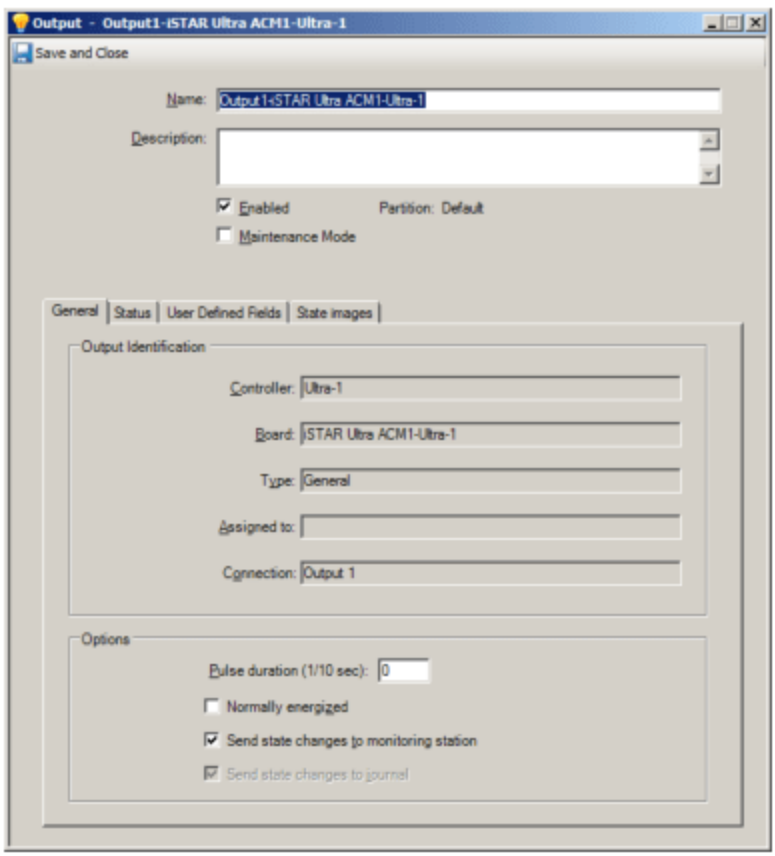
- **iSTAR Output Status tab**

  This tab displays several read-only fields that report the Active, Armed, Hardware, and Supervision status of the Output. See iSTAR Output Status Tab on Page 246.

- **iSTAR Output State Images tab**

  See iSTAR Output State Images Tab on Page 246.

Figure 78: iSTAR Output Editor



Accessing the iSTAR Output Editor

You can access the iSTAR Output Editor in several ways:

- To Access the iSTAR Output Editor (iSTAR eX/Edge Outputs Tab) on Page 242.
- To Access the iSTAR Output Editor (iSTAR eX/Edge COM Tabs) on Page 242.
- To Edit a Main Board Output (iSTAR Classic/Pro Boards Tab) on Page 242.
- To Access the iSTAR Output Editor (iSTAR Classic/Pro ACM Board Outputs Tab) on Page 242
- To Access the iSTAR Output Editor (iSTAR Classic/Pro ACM Board ACM Ext Tab) on Page 243
- To Edit a Main Board Output from the Hardware Tree on Page 243.
- To Edit a COM1/COM2/COM3 or ACM Output from the Hardware Tree on Page 243

To Access the iSTAR Output Editor (iSTAR eX/Edge Outputs Tab)

1. From the iSTAR Controller Editor, click on the Outputs tab.
2. Click in the **Configured** column to create a Relay Output or an Open Collector Output.
3. Click the **Edit** button [...] for the Output you want to edit.

   The iSTAR Output Editor opens (see iSTAR Output Editor on Page 241).

To Access the iSTAR Output Editor (iSTAR eX/Edge COM Tabs)

1. From the iSTAR Controller Editor, click on the COM1, COM2, or COM3 (iSTAR Edge only) tab.
2. Click in the **Configured** column of the Output Boards table to create an Output Board.
3. Click [...] in the **Edit** column for the Output board you want to edit.

   The iSTAR Output Board Editor opens (see iSTAR Output Board Editor on Page 208).
4. Click in the **Configured** column of the Outputs table to create an Output.
5. Click the **Edit** button [...] for the Output you want to edit.

   The iSTAR Output Editor opens (see iSTAR Output Editor on Page 241).

To Edit a Main Board Output (iSTAR Classic/Pro Boards Tab)

1. From the iSTAR Controller Editor, click on the Boards tab.
2. Click in the **Configured** column to create a Main Board Output.
3. Click [...] in the **Edit** column for the Main Board Output.

   The iSTAR Output Editor opens (see iSTAR Output Editor on Page 241).

To Access the iSTAR Output Editor (iSTAR Classic/Pro ACM Board Outputs Tab)

1. From the iSTAR Controller Editor, click on the Boards tab.
2. Click in the **Configured** column of the ACMs table to create an ACM Board.

3. Click ... in the **Edit** column for the ACM Board that contains the Input you want to Edit. The ACM Board Editor opens.
4. Click the Outputs tab on the ACM Board Editor.
5. Click in the **Configured** column to create an Output.
6. In the Outputs table on this tab, click ... in the **Edit** column for the Output you want to Edit.

   The iSTAR Output Editor opens (see iSTAR Output Editor on Page 241).

To Access the iSTAR Output Editor (iSTAR Classic/Pro ACM Board ACM Ext Tab)

1. From the iSTAR Controller Editor, click on the Boards tab.
2. Click in the **Configured** column of the ACMs table to create an ACM Board.
3. Click ... in the **Edit** column for the ACM Board that contains the Input you want to Edit. The ACM Board Editor opens.
4. Click the ACM Ext tab on the ACM Board Editor.
5. Click in the **Configured** column of the Output Boards table to create an Output Board.
6. In the Output Boards table on this tab, click ... in the **Edit** column for the Output Board you want to Edit.

   The iSTAR Output Board Editor opens (see iSTAR Output Board Editor on Page 208).
7. Click in the **Configured** column of the Outputs table to create an Output .
8. In the Output Boards table on this tab, click ... in the **Edit** column for the Output Board you want to Edit.

   The iSTAR Output Editor opens (see Figure 78 on Page 241).

To Edit a Main Board Output from the Hardware Tree

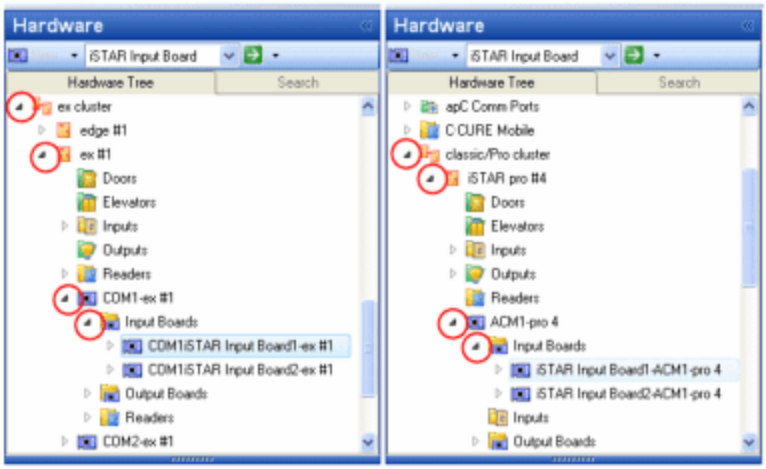
1. Navigate to your iSTAR Controller in the Hardware Tree and click ▷.
2. Click the **Outputs** folder.
3. Double-click on the Output you want to edit.

   The iSTAR Output Editor opens (see iSTAR Output Editor on Page 241).

To Edit a COM1/COM2/COM3 or ACM Output from the Hardware Tree

1. Navigate from your iSTAR Controller in the Hardware Tree to the appropriate COM Board (on an iSTAR eX or iSTAR Edge Controller) or ACM Board (on an iSTAR Classic/Pro Controller).
2. Click ▷ on **Output Boards**, as shown in Figure 79 on Page 244.

Figure 79: iSTAR Output Boards in the Hardware Tree



3. Click ▷ on the Output board that contains the Input you wish to edit.
4. Click ▷ on **Outputs** under that board.
5. Double-click on the Output you wish to edit.

   The iSTAR Output Editor opens (see iSTAR Output Editor on Page 241).

Configuring an iSTAR Output

When you configure an iSTAR Output, you use the Output Editor tabs to define the Options and State Images for the Output.

To Configure an iSTAR Output

1. Access the Output Editor for the Output you wish to edit (see Accessing the iSTAR Output Editor on Page 242).
2. Click the Output General tab:
   - Modify the name of the Output in the **Name** field, if desired.
   - Add a textual description of the Output to the **Description** field.
   - Enable the Output by clicking the **Enabled** field.
   - Modify the Options settings for the Output. See the definitions for the Options fields in Table 56 on Page 245.
3. Click the Output Status tab to view the **Active Status** of the Output.
4. Click the Output State Images tab to view the state images for this Output. If you wish to customize the state images for this Output, follow the steps in State Images Tab for iSTAR Devices on Page 274.
5. When you have finished configuring this Output in the Output Editor, click **Save and Close** to save the settings you have configured.

iSTAR Output General Tab

The iSTAR Output General tab displays information that identifies the Output and allows you to configure the Options for the Output. Figure 78 on Page 241 shows the iSTAR Output General tab.

iSTAR Output General Tab Definitions

Table 56 on Page 245 lists the fields and buttons that appear on the iSTAR Output General tab.

Table 56: iSTAR Output General Tab Definitions

Field/Button	Description
Identification	
Name	Displays the name for this Output. The name is system-generated by default, but you can edit this name by clicking in click in this field.
Description	Enter a textual comment about the Output, such as its location or purpose. This text is for information only.
Enabled	Click ☑ to enable the Output.
Maintenance Mode	Click to place the iSTAR Output into Maintenance Mode. See Chapter 2: Maintenance Mode for more information.
Partition	This read-only field identifies the Partition in which this Output resides.
Output Identification	
Controller	This read-only field identifies the iSTAR Controller to which this Output is attached.
Board	This read-only field identifies the iSTAR Controller board to which this Output is attached.
Type	Reflects whether the Output has been assigned to a Door or other object. These include: • General • Door Lock • Shunt Expiration Relay • Alternate Shunt Relay • Elevator Button NOTE: The Elevator output assignment has not been evaluated by UL.
Assigned to	Displays the Elevator or Door object name with which this Output is configured.
Connection	Identifies the Input number on the hardware board to which this Output is connected.
Options	
Pulse Duration (1/10 sec)	This is a momentary activation which is entered in second intervals with a default of 0 seconds.

Table 56: iSTAR Output General Tab Definitions (continued)

Field/Button	Description
Normally energized	This field is used to specify whether the Output is wired such that current is normally on or not. The default setting (not selected) signifies that the Output is wired so that the current is normally off and when the Output is in an On state, the circuit is energized.
Send state changes to monitoring station	To have a notification of changes in state of the Output sent to the Monitoring station, select the Send state changes to the monitoring station check box. NOTE: For Proprietary Burglar Alarm applications, the **Send state changes to the monitoring station** option must be selected. This selection is unavailable for an iSTAR Door Output. State changes for a Door Output are not sent to the Monitoring Station.
Send state changes to journal	To have a notification of changes in state of the Output sent to the journal, select **Send state changes to journal**. This option is selected by default. This selection is unavailable for an iSTAR Door Output. State changes for a Door Output are not sent to the journal.

iSTAR Output Status Tab

The iSTAR Output Status tab displays the State of the Output.

Table 57: iSTAR Output Status Tab Definitions

Field/Button	Description
Active Status	Displays the status of the Output - either Active or Inactive.

iSTAR Output State Images Tab

The iSTAR Output State Images tab provides a means to change the default images that are displayed on the C•CURE 9000 Monitoring Station to indicate iSTAR Output states.

See State Images Tab for iSTAR Devices on Page 274 for information on using the State Images tab for an iSTAR Output.

iSTAR Output State Images Tab Definitions

Table 58 on Page 246 shows the iSTAR Output States and the default State Images.

Table 58: iSTAR Output State Images Tab Definitions

Icon	Description		Icon	Description
	Unknown			Inactive

Table 58: iSTAR Output State Images Tab Definitions (continued)

Icon	Description		Icon	Description
	Active			Disabled
	Flashing			

iSTAR Reader Editor

The iSTAR Reader editor lets you configure an iSTAR Reader that you created on an iSTAR Controller.

The iSTAR Reader editor (see Figure 80 on Page 249) has the following tabs:

- **iSTAR Reader General tab**

  Lists the Reader name, connections, and card formats for a reader connected to an iSTAR. See iSTAR Reader General Tab on Page 250.

- **iSTAR Reader I/O tab**

  This tab lets you configure the available Inputs and Outputs for the Reader. See iSTAR Reader I/O Tab on Page 252.

- **iSTAR Reader Keypad tab**

  This tab lets you configure the settings and options for the Reader Keypad. See iSTAR Reader Keypad Tab on Page 253.

- **iSTAR Reader Triggers tab**

  See Triggers Tab for iSTAR Devices on Page 270 for information on creating Triggers for an iSTAR device.

- **iSTAR Reader Groups tab**

  If you have created a Group containing iSTAR readers and added this Reader to it, the iSTAR Reader editor also displays a Group tab.

  This tab lists the Reader groups to which this Reader belongs. See Groups Tab for Hardware Devices on Page 28 for information on using the Group tab for the iSTAR Reader.

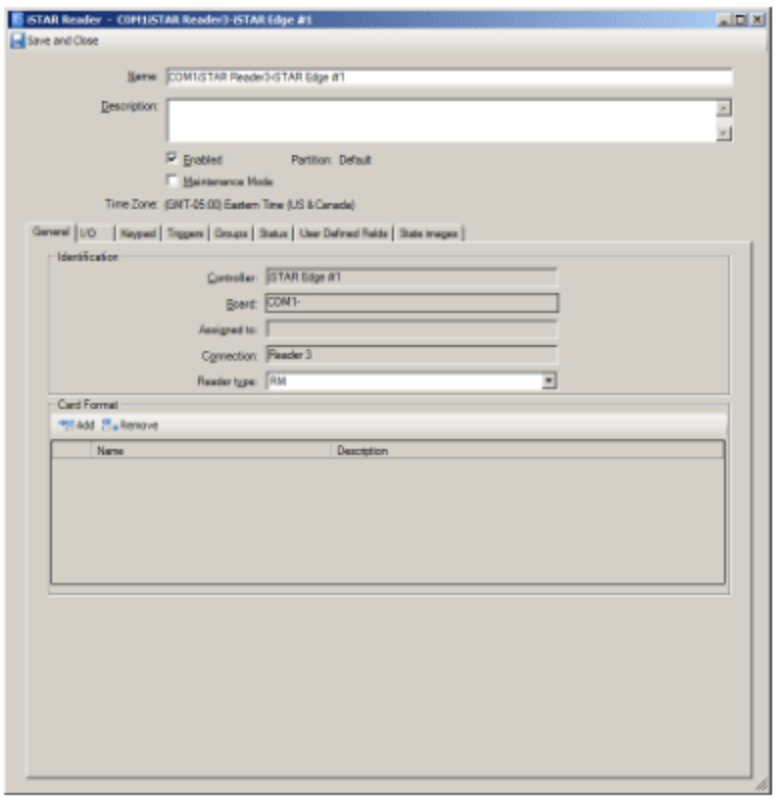
- **iSTAR Reader Status tab**

  This tab displays several read-only fields that report the Communications, PIN Required, and Keypad Command Allow Status of the Reader. See iSTAR Reader Status Tab on Page 256.

- **iSTAR Reader State Images tab**

  This tab displays the default images used to depict this reader in the Monitoring Station. You can use this tab to customize these state images. See iSTAR Reader State Images Tab on Page 258.

Figure 80: iSTAR Reader Editor



You can add or remove Card Formats from multiple Readers via an iSTAR Reader Dynamic View. See Add or Remove Reader Card Formats on Page 25 for more information.

Accessing the iSTAR Reader Editor

You can access the iSTAR Reader editor in several ways:

- From the iSTAR eX Controller Wiegand Tab on Page 171 or iSTAR Edge Controller Wiegand Tab on Page 169.
- From the iSTAR eX COM1/COM2 Tabs on Page 173 or iSTAR Edge COM1/COM2/COM3 Tabs on Page 167
- From the iSTAR Classic/Pro Controller iSTAR ACM Board Readers Tab on Page 200.
- From the iSTAR Ultra iSTAR Controller Boards Tab (iSTAR Classic/Pro) on Page 156, iSTAR Ultra Controller IP-ACMs Tab on Page 181, and iSTAR Ultra COM1/COM2 Tabs on Page 181.
- From the iSTAR PIM-485 Board Editor Readers Tab on Page 229.
- From the Hardware Tree, edit a Reader on a COM board or ACM board.

In each case, you must select the **Configure** column to configure ☑ the reader, then click [...] to open the iSTAR Reader editor.

Configuring iSTAR Readers

When you configure an iSTAR Reader, you use the Reader Editor tabs to define the Options and State Images for the Reader.

To Configure an iSTAR Reader

1. Access the Reader Editor for the Reader you wish to edit (see Accessing the iSTAR Reader Editor on Page 249).
2. Click the Reader **General** tab:
   - Modify the name of the Reader in the **Name** field, if desired.
   - Add a textual description of the Reader to the **Description** field.
   - Enable the Reader by clicking the **Enabled** field.
   - For some Readers, you need to select the correct Reader type from the drop-down list.
   - Add the Card Formats that the Reader uses to the Card Format table. See Configuring iSTAR Readers on Page 250.
3. Click the Reader Status tab to view the **Active Status** of the Reader.
4. Click the Reader State Images tab to view the state images for this Reader. If you wish to customize the state images for this Reader, follow the steps in State Images Tab for iSTAR Devices on Page 274.
5. When you have finished configuring this Reader in the Reader Editor, click **Save and Close** to save the settings you have configured.

NOTE See the *C•CURE 9000 Getting Started Guide* for a list of UL approved card formats.

iSTAR Reader General Tab

The iSTAR Reader General tab displays information that identifies the Reader and allows you to configure the Options for the Reader. Figure 80 on Page 249 shows the iSTAR Reader General tab.

iSTAR Reader General Tab Definitions

Table 59 on Page 250 lists the fields and buttons that appear on the iSTAR Reader General tab.

Table 59: iSTAR Reader General Tab Definitions

Field/Button	Description
Identification	
Name	Displays the name for this Reader. The name is system-generated by default, but you can edit this name by clicking in click in this field.
Description	Enter a textual comment about the Reader, such as its location or purpose. This text is for information only.

iSTAR Reader General Tab Definitions (continued)

Field/Button	Description
Enabled	Click ☑ to enable the Reader.
Maintenance Mode	Click to put the iSTAR Reader into Maintenance Mode. See Chapter 2: Maintenance Mode for more information.
Partition	This read-only field identifies the Partition in which this reader resides.
Controller	This read-only field identifies the iSTAR Controller to which this reader is attached.
Board	This read-only field identifies the iSTAR Controller board to which this reader is attached.
Assigned to	Displays the Elevator or Door object name with which this reader is configured.
Connection	Identifies the Reader number on the hardware board to which this reader is connected.
Device ID	The 15-character ID of the Aperio Reader. (Aperio Reader only.)
Reader Type	Click on the drop-down menu to select the reader type. • **RM** (Software House Reader Protocol) • **BLE** (Bluetooth Low Energy) • **OSDP** (Open Supervised Device Protocol) Default: RM
Authentication Required	Only available for BLE readers. Click to enable authentication. You will need to be logged into the BLE application on your mobile device for access. Default: Disabled - does not require authorization.
Card Format	
Add	Click **Add** to add a Card Format. If the card format you desire is not in the Name Selection dialog box list, click ... in the **Select Type** field to select a card format.
Remove	Click the row selector ▸ to select one or more Card Format rows (hold down **SHIFT** or **Ctrl** to select multiple rows), then click **Remove** to delete the row(s) for this field.
Name	Displays the Name of each Card Format you have chosen for this Reader.
Description	Displays the Description for the Card Format. This field is read-only.

iSTAR General Tab Definitions for iSTAR Ultra Wiegand Readers

The iSTAR Reader General tab for readers defined on the Wiegand tab of the iSTAR Ultra ACM Board has additional fields that allow you to configure Reader Options.

Table 60 on Page 252 lists the additional fields and buttons that appear on the iSTAR Reader General tab for iSTAR Ultra Wiegand Readers.

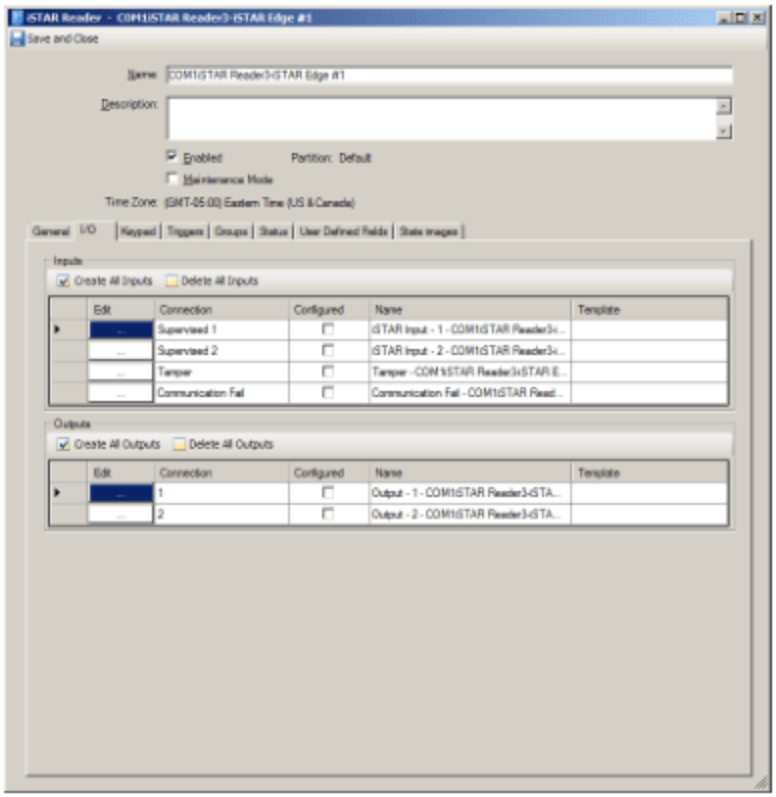
Table 60: iSTAR Ultra Wiegand Reader General Tab Definitions

Field/Button	Description
Reader Options	
LED Control	You can select the LED control setting that corresponds with the wiring method used to control the reader LEDs: • 3-wire (Red, Yellow, Green) • External Bi-color (2-wire Red, Green) • 1-wire (A,B, C0)
Beep on Card Read	Click to configure the reader to beep when a Card Read occurs.

iSTAR Reader I/O Tab

The iSTAR Reader I/O tab displays information that identifies the Reader and allows you to configure the Options for the Reader. Figure 81 on Page 252 shows the iSTAR Reader I/O tab.

Figure 81: iSTAR Reader I/O Tab



iSTAR Reader I/O Tab Definitions

Definitions for the fields and buttons on the Reader I/O tab are described in Table 61 on Page 253.

Definitions for the Inputs on the iSTAR Aperio Reader I/O Tab are described in iSTAR Aperio Reader I/O Tab on Page 266.

The fields on this tab vary depending upon the type of Reader you are configuring. For example, a Direct Connect Wiegand Reader displays only the Communications Fail Input on the I/O tab.

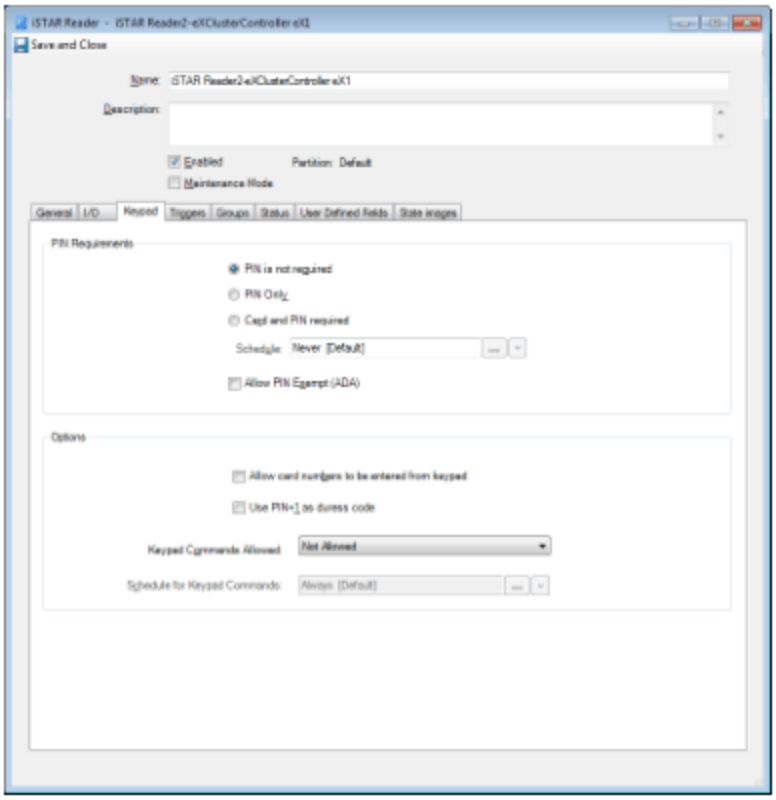
Table 61: iSTAR Reader I/O Tab Definitions

Field/Button	Description
Inputs	
Create All Inputs	Click to create all eight Inputs. The check boxes in the **Configured** column are set to ☑.
Delete All Inputs	Click to delete all eight Inputs. The check boxes in the **Configured** column are set to ☐.
Edit	Click ... in this column to open the iSTAR Input Editor to edit this Input.
Connection	This read-only field identifies the position of each Input on the I/O tab.
Configured	☑ indicates that the Input has been configured. ☐ indicates that the Input has not been configured.
Name	Displays the system-generated name for this Input. You can edit this name by clicking in the field.
Template	Displays the Template used for creating this Input. If the Input is not yet configured, you can click in this column, then click to select an Input Template. If the **Configured** column displays ☑, this field cannot be edited.
Supervised 1	Represents Supervised Input #1 on iSTAR Readers. Not available on direct connect Wiegand Readers.
Supervised 2	Represents Supervised Input #2 on iSTAR Readers. Not available on direct connect Wiegand Readers.
Tamper	Represents the Tamper Input on iSTAR Readers. Not available on direct connect Wiegand Readers.
Communications Fail	Represents the Communications Failure Input on iSTAR Readers.
Outputs	
Create All Outputs	Click to create all Outputs. The check boxes in the **Configured** column are set to ☑.
Delete All Outputs	Click to delete all Outputs. The check boxes in the **Configured** column are set to ☐.
1	Represents Output #1 on iSTAR Readers.
2	Represents Output #2 on iSTAR Readers. Not available on direct connect Wiegand Readers and MRM Readers.

iSTAR Reader Keypad Tab

The iSTAR Reader Keypad tab allows you to configure settings for the keypad on the Reader. You can specify how the Reader accepts PIN entries, and whether the Reader accepts Keypad Commands.

Figure 82: iSTAR Reader Keypad Tab



iSTAR Reader Keypad Tab Definitions

Table 62: iSTAR Reader Keypad Tab Definitions

Field/Button	Description
PIN is not required	If selected, only a card swipe is required for successful access to the door connected to this reader.
PIN only	If selected, this reader can be used for PIN-Only access. NOTE: **PIN only** cannot be used as a Query filter value for the PIN Required Status field.
Card and PIN required	If selected, this reader requires both a card swipe and a PIN entry at the keypad for access.
Schedule	If **Card and PIN Required** is selected, you can select a Schedule object to determine when Card and PIN Required is enforced. When the Schedule is active, both Card and PIN are required for access. When the Schedule is inactive, only a card swipe is required.
Allow PIN Exempt (ADA)	If **Card and PIN Required** is selected, Personnel records configured with **PIN Exempt (ADA)** are exempt from having to enter a PIN for access.

Table 62: iSTAR Reader Keypad Tab Definitions (continued)

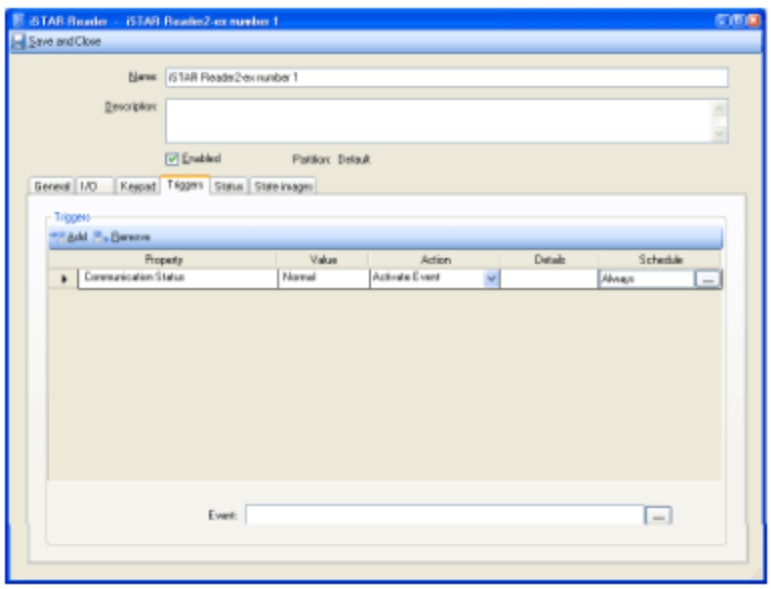
Field/Button	Description
Allow card numbers to be entered from keypad	If you have selected **PIN is not required** or **Card and PIN required**, you can enable **Allow card numbers to be entered from the keypad** by selecting the check box. If you chose **PIN Only**, this option is unavailable (because the Keypad must be used to enter a PIN).
Use PIN+1 as duress code	If you have selected **PIN is not required** or **Card and PIN required**, you can enable **Use PIN+1 as duress code** by selecting the check box. If you chose **PIN Only**, this option is unavailable.
Keypad Commands Allowed	Indicates whether or not Keypad Commands can be entered on this Reader's Keypad and when. Select one of the following options from the drop-down list. The default is **Not Allowed**. • **Not Allowed** – Keypad Commands cannot be used at the Reader • **Always Allowed** – Keypad Commands can always be used at the Reader • **Allowed during specified schedule** – Keypad Commands can be used at the Reader during the period specified in the following field. (When you select this option, the Schedule for Keypad Commands field becomes available.)
Schedule for Keypad Commands	Select a Schedule from the list to specify when Keypad Commands can be used at this Reader. When the Schedule is active, Keypad Commands can be used. When the Schedule is inactive, Keypad Commands cannot be used.

iSTAR Reader Triggers Tab

The iSTAR Reader Triggers tab allows you to configure triggers for the Reader. You can set up triggers based on Communication Status, PIN Required Status, and Tamper Status.

Figure 83 on Page 255 shows the iSTAR Reader Triggers tab.

Figure 83: iSTAR Reader Triggers Tab



See Triggers Tab for iSTAR Devices on Page 270 for information on creating Triggers for an iSTAR device.

For iSTAR Readers you can create Triggers for the properties shown in Table 63 on Page 256.

Table 63: iSTAR Reader Trigger Properties

Property	Description
Communication Status	Possible values are **Normal** or **Comm Fail**.
PIN Required Status	Possible values are **Not Required** or **Card and PIN Required**, based on the setting for PIN Requirements on the Keypad tab.
Tamper Status	Boolean value; **True** if the Tamper input has been activated, or **False** if the Tamper Input has not been activated.

iSTAR Reader Status Tab

The iSTAR Reader Status tab displays read-only status fields that allow you to see the current status of the Reader. The type of reader determines the fields displayed on this tab.

- iSTAR Reader Status Tab Definitions on Page 256.
- iSTAR PIM-485 Reader Status Tab Definitions on Page 257.
- iSTAR Aperio Reader Status Tab Definitions on Page 257

iSTAR Reader Status Tab Definitions

Table 64: iSTAR Reader Status Tab Definitions

Field/Button	Description
Firmware Version	The version number of the reader firmware.
Communications	Communications displays the value Normal if the Controller can communicate with the Reader or Comm Fail if the Controller cannot communicate with the Reader.
PIN Required	PIN Required displays the value **True** if **PIN Required** has been selected on the Keypad tab or **False** otherwise.
Tamper	Displays the status of the Tamper Input. Not available on Direct Connect Wiegand readers.
Keypad Command Allow Status	This field displays status of the **Keypad Commands Allowed** setting from the Reader Editor Keypad tab: • Not Allowed • Allowed • Allowed during specified schedule.

iSTAR PIM-485 Reader Status Tab Definitions

Table 65: iSTAR PIM-485 Reader Status Tab Definitions

Field/Button	Description
Firmware Version	The version number of the reader firmware.
Communications	Communications displays the value Normal if the Controller can communicate with the Reader or Comm Fail if the Controller cannot communicate with the Reader.
PIN Required	PIN Required displays the value **True** if **PIN Required** has been selected on the Keypad tab or **False** otherwise.
Tamper	**True** if a Tamper status is detected for the PIM Reader, or **False** if no Tamper condition is detected.
Keypad Command Allow Status	This field displays status of the **Keypad Commands Allowed** setting from the Reader Editor Keypad tab: • Not Allowed • Allowed • Allowed during specified schedule.
[PIM1-pro 1] - PIM Tamper	**True** if a Tamper status is detected for the PIM-485 board to which this reader is attached, or **False** if no Tamper condition is detected.
Motor Stall	**True** if a Motor Stall condition (a problem with the latching mechanism of the door strike) is detected, or **False** if no Motor Stall condition is detected. Available only for PIM-485 WA Series Locks, not for other AD Locks.
Low Battery	**True** if a Low Battery condition is detected for the PIM Reader, or **False** if no Low Battery condition is detected. Available only for PIM-485 connected Readers.
Manual Lock Override	**True** if the Manual Lock Overrride has been activated (unlocked by a physical key), or **False** if the Manual Lock Override has not been activated. Available only for PIM-485 connected Readers.
Push Button	**True** if the Push Button on the lock panel (inside the room) has been pressed, or **False** if the Push Button has not been pressed. Available only for PIM-485 connected Readers.

iSTAR Aperio Reader Status Tab Definitions

Table 66: iSTAR Aperio Reader Status Tab Definitions

Field/Button	Description
Communications	Communications displays the value **Normal** if the Controller can communicate with the Reader or **Comm Fail** if the Controller cannot communicate with the Reader.
Tamper	**True** if a Tamper status is detected for the Reader, or **False** if no Tamper condition is detected.
Low Battery	**True** if a Low Battery condition is detected for the Reader, or **False** if no Low Battery condition is detected.

iSTAR Reader State Images Tab

The State Images tab for a Reader provides a means to change the default images used to indicate iSTAR Reader device states on the Monitoring Station.

See State Images Tab for iSTAR Devices on Page 274 for information on using the State Images tab for an iSTAR Reader.

See Table 67 on Page 258 for default State Images for an iSTAR RM reader

See Table 68 on Page 258 for default State Images for an iSTAR PIM-485 reader (Schlage wireless lock and reader).

iSTAR Reader State Images Tab Definitions

Table 67: iSTAR Reader State Images Tab Definitions

Icon	Description		Icon	Description
	Unknown			Tampered
	Comm Fail			Normal

Table 68: iSTAR PIM 485 Reader State Images Definitions

Icon	Description		Icon	Description	Icon	Description
	Unknown			Normal		Low Battery
	Comm Fail			Motor Stall (Schlage Wireless Only)		Manual Lock Override (Schlage Wireless Only)
	Tampered			PIM Tamper (Schlage Wireless Only)		Push Button (Schlage Wireless Only)

Table 69: iSTAR Aperio Reader State Images Definitions

Icon	Description		Icon	Description
	Unknown			Key Cylinder Override (Aperio only)

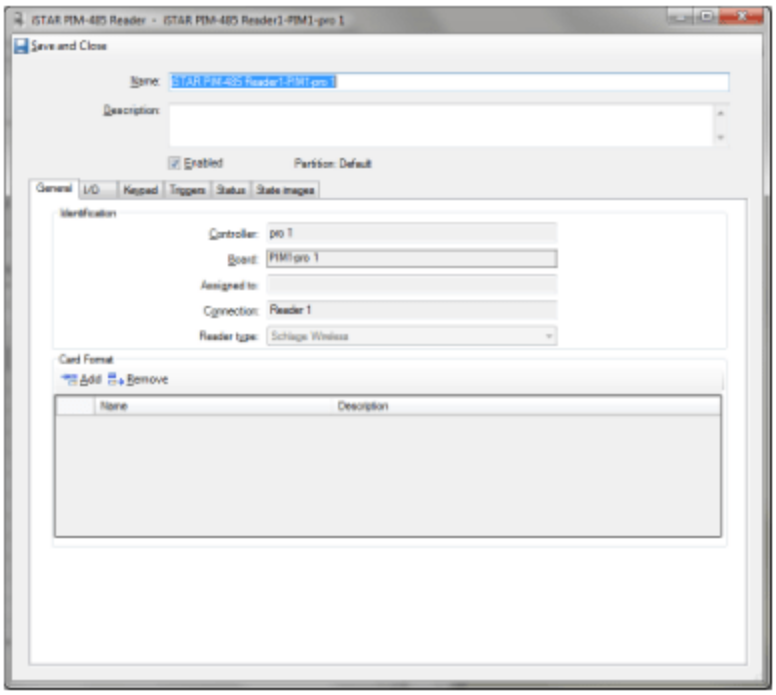
Icon	Description		Icon	Description
	Comm Fail			Lock State Locked (Aperio only)
	Tampered			Lock State Jammed (Aperio only)
	Normal			

iSTAR PIM-485 Reader Editor

The iSTAR PIM-485 Reader Editor allows you to configure the settings for a Schlage PIM-485 reader/lock wirelessly connected to an iSTAR Pro or eX controller PIM-485 board.

The iSTAR PIM-485 Reader editor is shown in Figure 84 on Page 260.

Figure 84: iSTAR PIM-485 Reader Editor



The iSTAR PIM-485 Reader editor dialog box has the following tabs.

- **iSTAR Reader General tab**

  Lists the Reader name, connections, and card formats for a reader connected to an iSTAR Classic/Pro, or iSTAR eX. See iSTAR Reader General Tab on Page 250.

- **iSTAR PIM-485 Reader I/O tab**

  This tab lets you configure the available Inputs and Outputs for the Reader. See the iSTAR PIM-485 Reader I/O Tab on Page 261.

- **iSTAR Reader Keypad tab**

  This tab lets you configure the settings and options for the Reader Keypad on iSTAR Schlage Readers. See iSTAR Reader Keypad Tab on Page 253.

  Only Schlage Keypad Mode 1 keypad output format (4 data bits per key with no parity) is supported. The mode is configured on the Schlage device.

- **iSTAR Reader Triggers tab**

  See the Triggers Tab for iSTAR Devices on Page 270 for information on creating Triggers for an iSTAR device.

  You can define triggers for the following Properties of the iSTAR PIM-485 Reader:

Property	Value
Communication Status	Normal or Comm Fail
Low Battery	Active ☑ or inactive ☐
Manual Lock Override	Active ☑ or inactive ☐
Motor Stall	Active ☑ or inactive ☐
Parent PIM Tamper	Active ☑ or inactive ☐
PIN Required Status	Not Required, Card and PN Required, or PIN Only
Push Button	Active ☑ or inactive ☐
Tamper Status	Active ☑ or inactive ☐

- **iSTAR Reader Groups tab**

  If you have created a Group containing iSTAR readers and added this Reader to it, the iSTAR Reader editor also displays a Groups tab.

  This tab lists the Reader groups to which this Reader belongs. See the Groups Tab for Hardware Devices on Page 28 for information on using the Group tab for the iSTAR Reader.

- **iSTAR Reader Status tab**

  This tab displays several read-only fields that report the Communications, PIN Required, and Keypad Command Allow Status of the Reader. See the iSTAR Reader Status Tab on Page 256.

- **iSTAR Reader State Images tab**

  This tab displays the default images used to depict this reader in the Monitoring Station. You can use this tab to customize these state images. See the iSTAR Reader State Images Tab on Page 258.

You can add or remove Card Formats from multiple Readers via an iSTAR PIM-485 Reader Dynamic View. See Add or Remove Reader Card Formats on Page 25 for more information.

iSTAR PIM-485 Reader I/O Tab

The iSTAR PIM-485 Reader I/O tab lets you configure the inputs and outputs for the reader. Each input and output is pre-assigned to a specific function for the reader. Typically you can use the **Create All** buttons to create the inputs and outputs, and then click the button in the **Edit** column to configure each input and output individually.

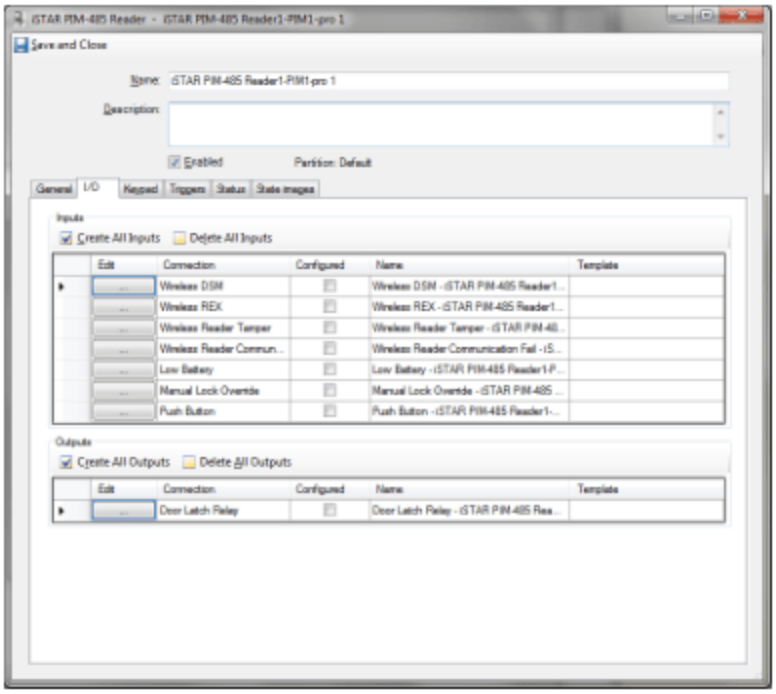
You can configure these inputs and outputs by clicking on [...] in the **Edit** column. You can then create triggers that can activate Events based on state changes.

Example:

You can create a trigger to activate an Event if the **Low Battery** Input status changes to Active (indicating that the reader battery charge is low). See Triggers Tab for iSTAR Devices on Page 270.

Figure 85 on Page 262 shows the iSTAR PIM-485 Reader I/O tab.

Figure 85: iSTAR PIM-485 Reader I/O Tab



Definitions for the fields and buttons on the Reader I/O tab are described in Table 70 on Page 262.

Table 70: iSTAR Reader I/O Tab Definitions

Field/Button	Description
Inputs	
Create All Inputs	Click to create all eight Inputs. The check boxes in the **Configured** column are set to ☑.
Delete All Inputs	Click to delete all eight Inputs. The check boxes in the **Configured** column are set to ☐.
Edit	Click ... in this column to open the iSTAR Input editor to edit the Input.
Connection	This read-only field identifies the position of each Input on the I/O tab.
Configured	☑ indicates that the Input has been configured. ☐ indicates that the Input has not been configured.
Name	Displays the system-generated name for this Input. You can edit this name by clicking in the field.
Template	Displays the Template used for creating this Input. If the Input is not yet configured, you can click in this column, then click to select an Input Template. If the **Configured** column displays ☑, this field cannot be edited.
Wireless DSM	Represents the Wireless Door Switch Monitor (DSM) for the door.
Wireless REX	Represents the Wireless Request To Exit (REX) for the door.

Table 70: iSTAR Reader I/O Tab Definitions (continued)

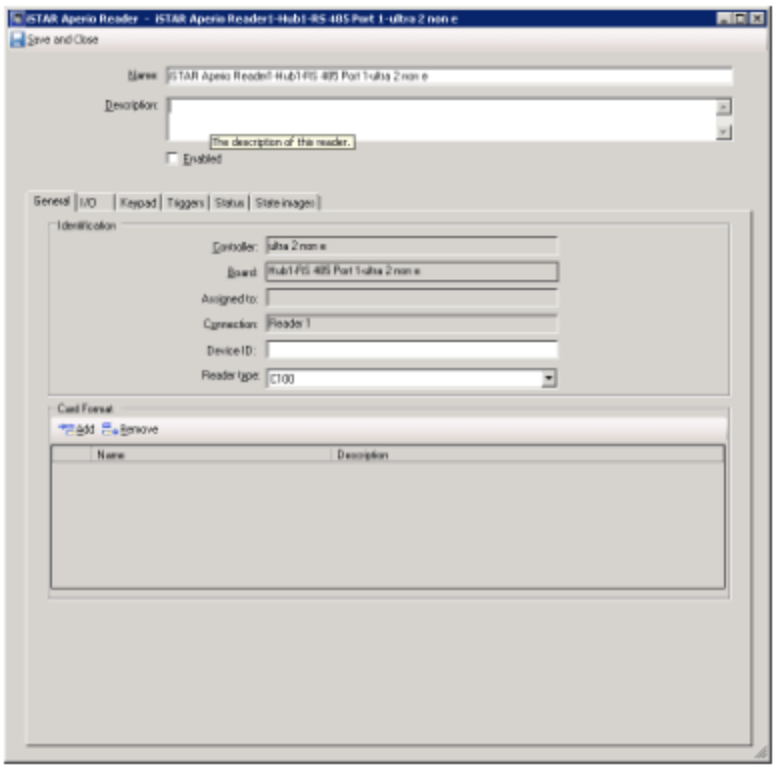
Field/Button	Description
Wireless Reader Tamper	Represents the Tamper Input on the Wireless Reader.
Wireless Reader Communications Fail	Represents the Communications Failure Input on the Wireless Reader.
Motor Stall	Represents the Motor Stall Input on the Wireless Reader.
Low Battery	Represents the Low Battery Input on the Wireless Reader.
Manual Lock Override	When this input is active, it indicates that the lock has been unlocked by a physical key. The Manual Lock Override status is available on the Status tab for this reader. This property is available for use in triggers.
Push Button	When this input is active, it indicates that the push button on the lock panel (inside the room) has been pushed. The Push Button Input status is available on the Status tab for this reader. This property is available for use in triggers.
Outputs	
Create All Outputs	Click to create all Outputs. The check boxes in the **Configured** column are set to ☑.
Delete All Outputs	Click to delete all Outputs. The check boxes in the **Configured** column are set to ☐.
Door Latch Relay	Represents the Door Latch Relay Output that is used to unlock the door.
Edit	Click ... in this column to open the iSTAR Output editor to edit the Output.
Connection	This read-only field identifies the position of the Output on the I/O tab.
Configured	☑ indicates that the Output has been configured. ☐ indicates that the Output has not been configured.
Name	Displays the system-generated name for this Output. You can edit this name by clicking in the field.
Template	Displays the Template used for creating this Output. If the Output is not yet configured, you can click in this column, then click to select an Output Template. If the **Configured** column displays ☑, this field cannot be edited.

iSTAR Aperio Reader Editor

The iSTAR Aperio Reader editor allows you to configure the settings for an Aperio reader/lock wirelessly connected to an iSTAR Ultra controller Aperio RS-485 Hub board.

The iSTAR Aperio Reader editor is shown in Figure 86 on Page 264.

Figure 86: iSTAR Aperio Reader Editor

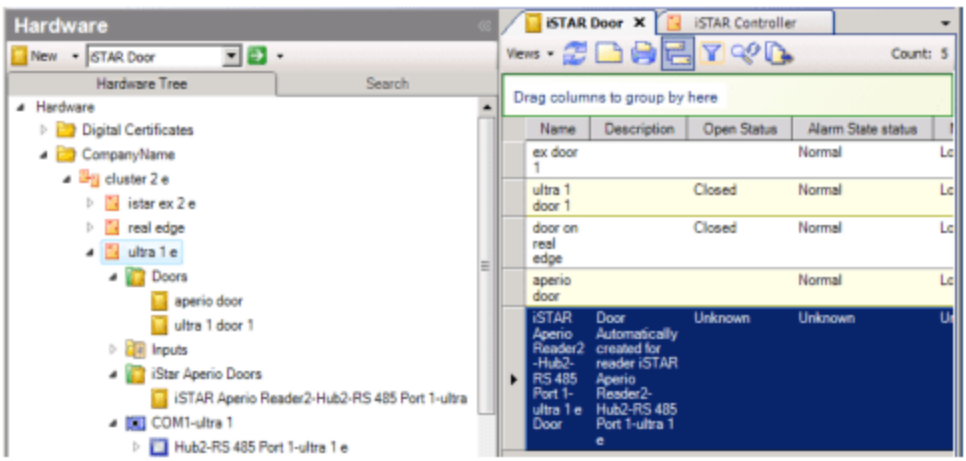


When you add an iSTAR Aperio Reader, **Enable** it in the Aperio Reader editor, and **Save and Close** the editor, a Door object for that reader is added to the parent Ultra controller in the iSTAR Aperio Doors folder in the Hardware tree.

If you delete an iSTAR Aperio Reader, the iSTAR Aperio Door associated with the reader is also deleted.

If you display a list of iSTAR Doors, the new Aperio Door appears on the list. See iSTAR Aperio Door Editor on Page 455 for more information on Aperio Doors.

Figure 87: iSTAR Aperio Doors



The iSTAR Aperio Reader editor dialog box has the following tabs.

- **iSTAR Reader General tab**

  Lists the Ultra controller name, Hub board, Assigned to Door, Reader number, Device ID, and Reader type. See iSTAR Reader General Tab on Page 250.

- **iSTAR Aperio Reader I/O tab**

  This tab lets you configure the available Inputs and Outputs for the Reader. See the iSTAR Aperio Reader I/O Tab on Page 266.

- **iSTAR Reader Keypad tab**

  This tab lets you configure the settings and options for the Reader Keypad on iSTAR Aperio Readers. See iSTAR Aperio Reader Keypad Tab on Page 268.

- **iSTAR Reader Triggers tab**

  See the Triggers Tab for iSTAR Devices on Page 270 for information on creating Triggers for an iSTAR Ultra device.

  You can define triggers for the following Properties of the iSTAR Aperio Reader:

Property	Value
Communication Status	Normal or Comm Fail
Key Cylinder Override	Active ☑ or inactive ☐
Lock State Jammed	Active ☑ or inactive ☐
Lock State Locked	Active ☑ or inactive ☐
Low Battery Status	Active ☑ or inactive ☐
Tamper Status	Active ☑ or inactive ☐

- **iSTAR Reader Status tab**

This tab displays several read-only fields that report the Communications, Tamper, and Low Battery status of the Reader. See the iSTAR Reader Status Tab on Page 256.

- **iSTAR Reader State Images tab**

  This tab displays the default images used to depict this reader in the Monitoring Station. You can use this tab to customize these state images. See the iSTAR Reader State Images Tab on Page 258.

You can add or remove Card Formats from multiple Readers via an iSTAR Aperio Reader Dynamic View. See Add or Remove Reader Card Formats on Page 25 for more information.

iSTAR Aperio Reader I/O Tab

The iSTAR Aperio Reader I/O tab lets you configure the inputs for the reader. Each input is pre-assigned to a specific function for the reader. Typically you can use the **Create All** buttons to create the inputs, and then click the button in the **Edit** column to configure each input individually.

The number of inputs available on this tab varies, depending upon the reader model configured on the General tab in the **Reader Type** field.

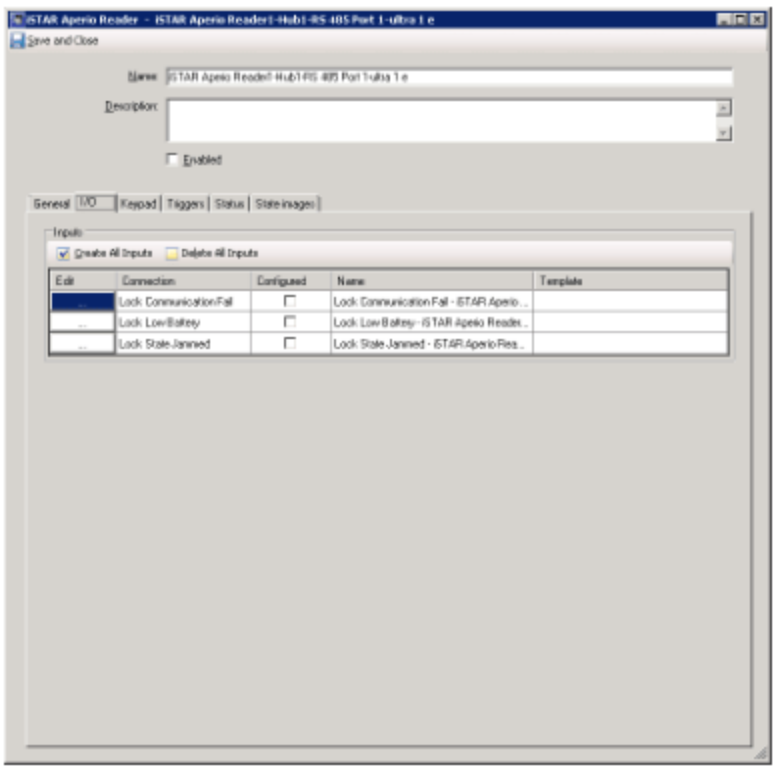
You can configure these inputs by clicking on ... in the **Edit** column. You can then create triggers that can activate Events based on state changes.

Example:

You can create a trigger to activate an Event if the **Lock Low Battery** Input status changes to Active (indicating that the reader battery charge is low). See Triggers Tab for iSTAR Devices on Page 270.

Figure 88 on Page 267 shows a typical iSTAR Aperio Reader I/O tab.

Figure 88: iSTAR Aperio Reader I/O Tab



Definitions for the fields and buttons on the Reader I/O tab are described in Table 71 on Page 267.

Definitions for the input types are described in Table 72 on Page 268.

Table 71: iSTAR Reader I/O Tab Definitions

Field/Button	Description
Create All Inputs	Click to create all Inputs. The check boxes in the **Configured** column are set to ☑.
Delete All Inputs	Click to delete all Inputs. The check boxes in the **Configured** column are set to ☐.
Edit	Click ... in this column to open the iSTAR Input editor to edit the Input.
Connection	This read-only field indicates the three standard inputs (Comm Fail, Low Battery, and Lock State Jammed.
Configured	☑ indicates that the Input has been configured. ☐ indicates that the Input has not been configured.
Name	Displays the system-generated name for this Input. You can edit this name by clicking in the field.
Template	Displays the Template used for creating this Input. If the Input is not yet configured, you can click in this column, then click to select an Input Template. If the **Configured** column displays ☑, this field cannot be edited.

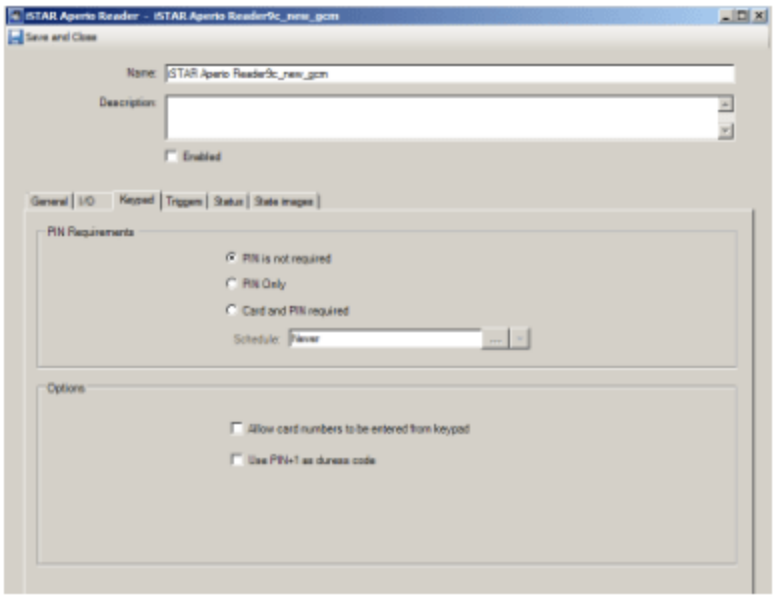
Table 72: iSTAR Reader I/O Tab Input Definitions

Field/Button	Description
Lock Reader Tamper	Represents the state of the Tamper input on the lock.
Handle State / Request to Exit	Represents the state of the Request to Exit input associated with the door handle.
Lock State Locked	Represents the
Key Cylinder Override	Represents the state of the Key Cylinder Override.
Door Position State	Represents state of the Door Switch Monitor for the door associated with this reader.
Lock Communications Fail	Represents the Lock Communications Failure Input on the Aperio Reader.
Lock State Jammed	Represents the Lock State Jammed Input on the Aperio Reader.
Lock Low Battery	Represents the Lock Low Battery Input on the Aperio Reader.

iSTAR Aperio Reader Keypad Tab

The iSTAR Reader Keypad tab allows you to configure settings for the keypad on the Reader. You can specify how the Reader accepts PIN entries.

Figure 89: iSTAR Aperio Reader Keypad Tab



iSTAR Aperio Reader Keypad Tab Definitions

Table 73: iSTAR Aperio Reader Keypad Tab Definitions

Field/Button	Description
PIN is not required	If selected, only a card swipe is required for successful access to the door connected to this reader.
PIN only	If selected, this reader can be used for PIN-Only access. NOTE: **PIN only** cannot be used as a Query filter value for the PIN Required Status field.
Card and PIN required	If selected, this reader requires both a card swipe and a PIN entry at the keypad for access.
Schedule	If **Card and PIN Required** is selected, you can select a Schedule object to determine when Card and PIN Required is enforced. When the Schedule is active, both Card and PIN are required for access. When the Schedule is inactive, only a card swipe is required.
Allow card numbers to be entered from keypad	If you have selected **PIN is not required** or **Card and PIN required**, you can enable **Allow card numbers to be entered from the keypad** by selecting the check box. If you chose **PIN Only**, this option is unavailable (because the Keypad must be used to enter a PIN).
Use PIN+1 as duress code	If you have selected **PIN is not required** or **Card and PIN required**, you can enable **Use PIN+1 as duress code** by selecting the check box. If you chose **PIN Only**, this option is unavailable.

Triggers Tab for iSTAR Devices

C•CURE 9000 uses Triggers, which are configured procedures for activating actions, to activate Events or Outputs for an iSTAR device. A Trigger automatically executes a specified Action when a particular Condition occurs (when the object Property specified in the Trigger reports the Value specified in the Trigger).

Example:

To provide an audible and visible alarm for a power failure condition, you can create two triggers for the AC Power Fail Input on an iSTAR controller that are activated when the Input's status changes:

Activate Output that energizes an audible sounder.

Activate Output that energizes an LED alarm light installed near an arming/disarming keypad reader.

Figure 90 on Page 270 shows the Triggers tab for an iSTAR Input, which is typical for an iSTAR device.

Figure 90: Typical iSTAR Triggers Tab

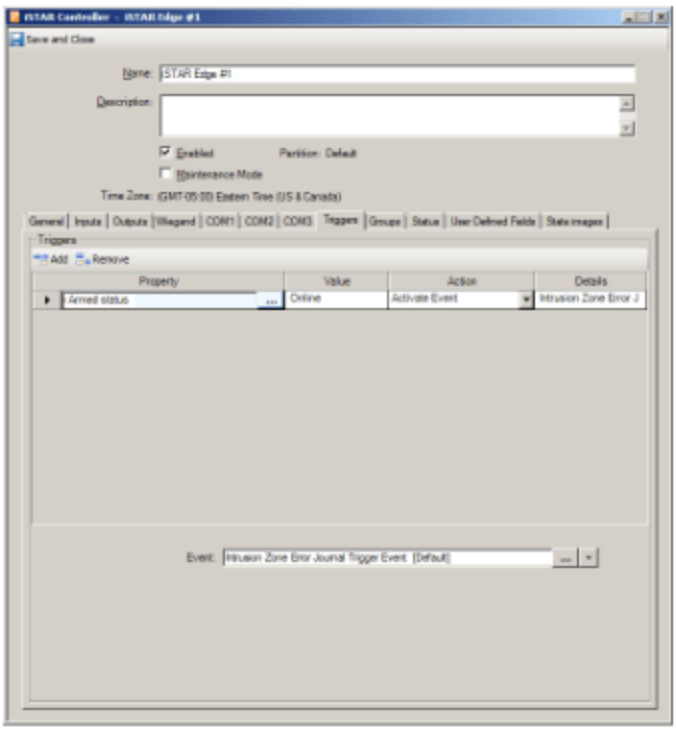


Table 74 on Page 270 provides an example of a configured iSTAR Trigger.

Table 74: Triggers Tab Settings Example

The following Triggers Tab settings:					
Property	**Value**	**Action**	**Details**	**Schedule**	**Time Zone**
Active Status	Active	Activate Event	iSTAR Input Event	Always	Time Zone of the iSTAR controller

Table 74: Triggers Tab Settings Example (continued)

Would create the following Trigger: Any time (**Always Schedule**) the Active Status (**Property**) equals Active (**Value**), activate the event (**Action**) named iSTAR Input Event (**Details**). iSTAR Input Event is an Event that you would need to create using the Event Editor.

NOTE You cannot assign a Schedule to an iSTAR Controller trigger. Effectively, iSTAR Controller triggers use an **Always** Schedule.

From the Triggers tab of an iSTAR device (such as a Controller, Input, or Reader), you can perform the following tasks.

- Defining a Trigger for an iSTAR Device on Page 271.
- Removing a Trigger on Page 272.

iSTAR Triggers Tab Definitions on Page 272 provides definitions for the fields and buttons on an iSTAR Device Triggers tab.

Defining a Trigger for an iSTAR Device

You can use the Triggers tab to define a Trigger for an iSTAR device. The typical usage for an iSTAR Trigger is to activate an Event or an Output as the result of a state change of an iSTAR device Property.

Example:

When an iSTAR Tamper Input changes from the Inactive (normal) to Active (abnormal) state, you wish to activate an Event and activate an audible alarm (an iSTAR Output).

Time Zones for iSTAR Triggers

If you specify a Time Zone in your Trigger definition, you can control when the Schedule for the Trigger is active. You can only select the C•CURE 9000 server Time Zone or the Time Zone of the iSTAR you are editing.

Example:

If you have iSTAR controllers that are in different Time Zones than your C•CURE 9000 server, you may want to have some Triggers activate according to the iSTAR controller's Time Zone, while other Triggers are activated according to the server Time Zone.

When you specify the Time Zone for a Trigger definition to be the same as the iSTAR controller Time Zone, the Schedule activation times for the Trigger occur according to the iSTAR controller Time Zone.

If you have an iSTAR controller in the Pacific Time Zone (GMT - 08:00) and a server in the Eastern Time Zone (GMT - 05:00), a Schedule that is active from Midnight to 6:00 AM is activated from Midnight to 6:00 AM in Pacific Time (GMT - 08:00) rather than Eastern time (three hours later).

To Define a Trigger for an iSTAR Device

1. Click on the Triggers tab for your iSTAR device.
2. Click **Add** on the Triggers tab to create a new Trigger.

3. Click ... within the **Property** column to open the Property dialog box showing the Properties available for the device.
4. Click a Property in the list to select it and add it to the **Property** column.
5. Click ... within the **Value** column to display a drop-down list of Values associated with the Property that you have selected. Click a **Value** that you want to include as a parameter for the trigger to add it to the column. (If there is no set list of Values, you can type in a Value.)
6. Click ... within the **Action** column to display a drop-down list of valid actions. Click an Action that you want to include as a parameter for the trigger to add it to the column.
7. When you select an Action, the lower pane in the Triggers box displays an entry field or group of entry fields, specific to the selected Action, so that you can configure the Details for the Action.
8. Once you define the Action details, the **Details** column displays information about how the Action has been configured.
9. For example, if an Event field is displayed in **Details**, you can click to select an Event that you want to associate with the Trigger.
10. If the Triggers tab includes a **Time Zone** column, click within the **Time Zone** column to display a drop-down list of available Time Zones. Most of the time, you will want to select a Time Zone that is the same as the iSTAR controller Time Zone. If you do not select a Time Zone, the Time Zone of the C•CURE 9000 server is used by default.
11. Click **Save and Close** to save the iSTAR Trigger.

Removing a Trigger

If you no longer need a Trigger defined for a Device, you can remove the Trigger.

To Remove a Trigger

1. Click the Triggers tab for your device.
2. Click the row selector ▸ to select a Trigger row.
3. Click **Remove** to delete the selected row.
4. Click **Save and Close** to save the device.

iSTAR Triggers Tab Definitions

Table 75 on Page 272 provides definitions for the fields and buttons on an iSTAR Triggers tab.

Table 75: iSTAR Triggers Tab Definitions

Field/Button	Description
Add	Click **Add** in the Triggers tab to create a new trigger.
Remove	Click the Row Selector ▸, then click **Remove** in the Triggers tab to delete a trigger.

Table 75: iSTAR Triggers Tab Definitions (continued)

Field/Button	Description
▸	Click the Row Selector to select a row in the Triggers table.
Property	Click within the **Property** column, and then click [...]. The Property browser opens presenting properties available for the Comm Port. Click a Property to select it and add it to the column.
Value	Click within the **Value** column to display a drop-down list of Values associated with the Property that you have selected. Click a Value that you want to include as a parameter for the trigger to add it to the column.
Action	Click [...] within the **Action** column to display a drop-down list of valid actions. Click an Action that you want to include as a parameter for the trigger to add it to the column. As you select an Action, a corresponding entry field, or group of entry fields, appear at the bottom of the dialog box. Click to select entries for these fields.
Details	Displays details about how the Action was configured.
Schedule	Click within the **Schedule** column to select a Schedule. Click [...] to select a Schedule that you want to associate with the trigger. Schedules are created in the Configuration Pane. Refer to the *C•CURE 9000 Software Configuration Guide* for more information on creating Schedules.
Time Zone	Click within the **Time Zone** column to select a Time Zone for Schedule activation. Click [...] to select a Time Zone that you want to associate with the trigger Schedule. Typically you can chose either the C•CURE 9000 server (host) Time Zone or the Time Zone of the iSTAR controller. If you specify a Time Zone, the Schedule start and end times are calculated using that Time Zone. **Example:** A Schedule that becomes active at 3:00 AM would become active at 3:00 AM in the Pacific Time Zone, if that Time Zone was specified. Refer to the *C•CURE 9000 Software Configuration Guide* for more information on Time Zones and Events.

State Images Tab for iSTAR Devices

The State Images tab provides a means to change the default images used to indicate iSTAR device states on the Monitoring Station.

From the State Images tab of an iSTAR device (such as a Controller, Input, Output, or Reader), you can perform the following tasks.

- Customizing State Images for an iSTAR Device on Page 274
- Restore a Default State Image on Page 275

You can replace the default images with JPG formatted files of your choice, to uniquely identify your objects when activities are displayed on the Monitoring Station Client.

iSTAR State Images Tabs Definitions on Page 274 provides definitions for the fields and buttons on an iSTAR Device State Images tab.

iSTAR State Images Tabs Definitions

iSTAR State Images Tabs have the State Images tabs as shown in Table 76 on Page 274.

Table 76: iSTAR State Images Tabs Definitions

Field/Button	Description
State	This column lists the states that are defined for this iSTAR device. These are the states that are reported on the Monitoring Station to reflect the status of this iSTAR device.
Image	This column shows the images that are assigned to each of the iSTAR device states. There are images assigned by default to every iSTAR device you create. For any individual iSTAR device, you can use the State Images tab to substitute a different.JPG/JPEG image for the default image. See Customizing State Images for an iSTAR Device on Page 274 for instructions.
Save and Close	After you have made changes to any settings for the iSTAR device, click **Save and Close** to save those changes and Close the editor for the device.

Customizing State Images for an iSTAR Device

From the State Images tab, you can change the images that appear in the Monitoring Station to represent an iSTAR device.

To Customize an iSTAR Device State Image

1. Navigate to the State Images tab for the iSTAR device.
2. Double-click the existing image.

   A Windows Open dialog box appears, allowing you to browse for a folder in which you have placed replacement images.
3. When you locate the replacement image, select it and click **Open** to replace the default image with this image.
4. When you are done editing the device, click **Save and Close** to save the configuration.

Restore a Default State Image

You can restore the default state image for any of the states of an iSTAR device.

To Restore the Default State Image

1. From the State Images tab, select an existing image.
2. Right-click the image and select **Restore Default**.
3. Click **Save and Close** to save the configuration.

6

Configuring the IP-ACM

This chapter explains how to configure the IP-ACM in C•CURE 9000.

In this chapter

IP-ACM Overview

The IP-ACM provides connection and management of access control for two doors. Two readers can be configured on each IP-ACM.

The IP-ACM acts as its own entity if it becomes disconnected from the iSTAR. Readers will remain active, with limitations. Offline access operation is buffered, and will be reported to the iSTAR Controller when communication is restored (determined by available memory.)

Limitations

- C•CURE 9000 only supports two readers (any combination of RM/Wiegand/BLE readers) connected to an IP-ACM.
- The IP-ACM is supported on the iSTAR Ultra and the iSTAR Ultra SE in Ultra Mode.
- Offline mode is supported for RM readers and Wiegand readers connected to the IP-ACM.
- Offline mode is not supported for BLE readers connected to the IP-ACM.

IP-ACM Offline Mode

Offline Mode allows a limited level of access and control if communication is interrupted between the IP-ACM and the iSTAR. Offline Access stores a set of credentials in non-volatile memory on the IP-ACM. Clearances are not downloaded to the IP-ACM and are not stored. IP-ACM

Offline Mode is configured in the iSTAR Controller dialog box using the IP-ACMs tab.

See the following:

- Stored Credentials on Page 279
- Door Configuration on Page 280

Stored Credentials

Predefined Credentials

Predefined credentials are downloaded from the iSTAR controller in the form of raw data (Static Card Data). During offline, access will be granted when the predefined credentials (from the Static Card Data stored on the IP-ACM) are presented to the readers.

The following restrictions apply to stored predefined credentials:

- Personnel groups configured for Offline Mode must all share the same card format and facility code.
- Card formats supported are:
  - Wiegand 26
  - Wiegand 37
  - Two-parity bit style formats
  - 32-bit serial number type formats.
- Static records can only be deleted from the iSTAR Controller.

Credentials Last Granted Access

In offline mode, the IP-ACM board will admit cards that are among the last *xxx* previous admitted cards in addition to a pre-defined personnel group.

- A total of 1000 credentials (not personnel) for both previous admitted credentials and credentials in the personnel group.
- Maximum 100 personnel in the personnel group.
- If you set the **Personnel** system variable "**Maximum Cards Per Person**", then that value must be taken into consideration.

Example:

If you set the "Maximum Cards Per Person" value to 3, then only 1000 - 100 x 3 = 700 is allowed in the "Admit the last admitted cards" field for configuration. This is true, even if the personnel count in the personnel group selected is less than 100.

Door Configuration

Doors must have their readers, inputs, and outputs connected to the IP-ACM and configured as follows:

- Readers that are not IP-ACM readers cannot be used.
- Entry reader must be connected as Reader 1 on Serial Port 2.
- Exit reader must be connected to Wiegand Port 2.
- DSM (Door State Monitor) must be connected to the IP-ACM onboard Input 1.
- REX (Request to Exit) must be connected to the IP-ACM onboard Input 2.
- Door lock must be connected to the IP-ACM onboard Output 1.

The door operation parameters are fixed when the IP-ACM goes into Offline Mode and cannot be changed. The door parameters will go back to their configured settings when the IP-ACM goes back online.

Offline fixed parameters:

- Shunt time: 10 seconds
- Unlock time: 5 seconds
- Relock delay time: ½ second
- Debounce time: ½ second
- Unlock on RTE: Enabled
- Shunt on RTE: Enabled
- DSM shunted full shunt time: Disabled
- Delay Relock full shunt time: Disabled

NOTE The Offline door will not provide access if the Tamper input is active.

IP-ACM Configuration Sequence

The IP-ACM configuration sequence is described in Table 1 on Page 280.

Table 1: IP-ACM Configuration Sequence

Step	Task	See...
1	Connect the IP-ACM to the network.	*IP-ACM Hardware Configuration Guide*
2	Add the IP-ACM to the subnet: 1. Open the iSTAR Configuration Utility (ICU). 2. Click IP-ACM to discover all IP-ACMs in the subnet. 3. Right-click on the IP-ACM in the list and select **Configure IP-ACM**.	*iSTAR Configuration Utility User Guide*

Table 1: IP-ACM Configuration Sequence (continued)

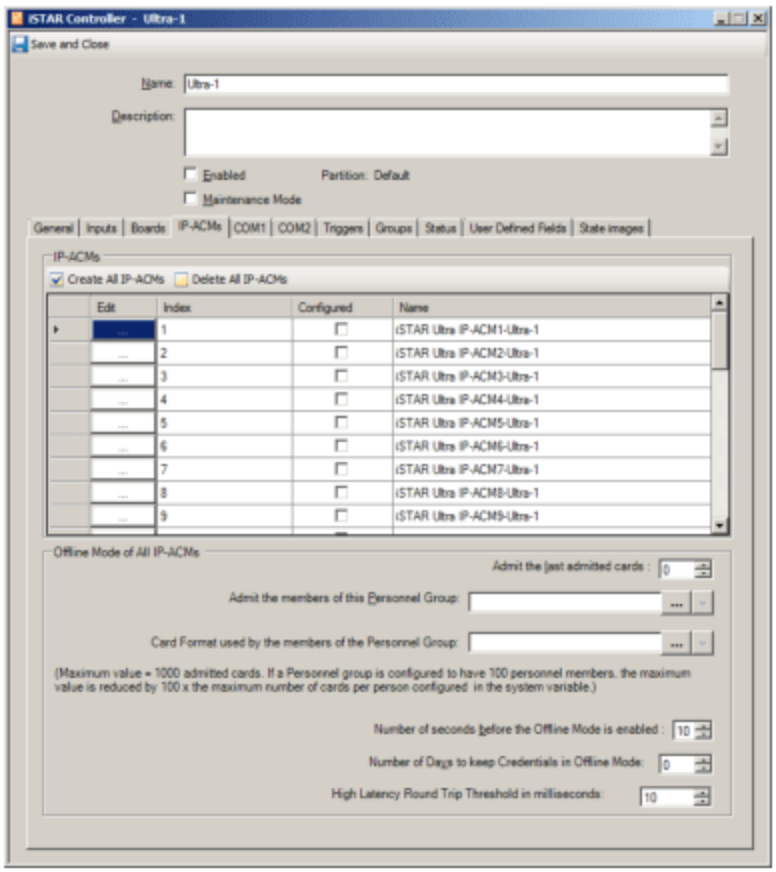
Step	Task	See...
3	Ensure that the iSTAR Controller (Ultra or Ultra SE in Ultra Mode) is configured in the C•CURE 9000.	Creating an iSTAR Controller on Page 124
4	Access the iSTAR Controller dialog box **IP-ACM**s tab: 1. Add the IP-ACM(s) to the controller. 2. Configure the IP-ACMs Offline Mode. 3. Configure the readers to connect to the IP-ACM. 4. Configure the inputs, outputs, and triggers.	iSTAR Controller IP-ACMs Tab on Page 282 iSTAR Ultra IP-ACM Editor on Page 285
5	Configure a door with the readers in the IP-ACM.	iSTAR Door Editor on Page 427

Configuring the IP-ACM

The IP-ACM configuration is accessed through the iSTAR Controller dialog box IP-ACMs tab, as shown in Figure 1 on Page 282.

See Table 2 on Page 283 for descriptions of the fields.

Figure 1: iSTAR Controller IP-ACMs Tab



To Configure the IP-ACM

1. From the iSTAR Ultra Controller editor, click the **IP ACMs** tab, as shown in Figure 1 on Page 282.
2. Click on the **Configured** check box in the Index row that you want to add/edit.
3. Click [...] in the **Edit** column of the Index row to open the iSTAR Ultra IP-ACM Editor on Page 285. The iSTAR Ultra IP-ACM editor is used to configure the inputs, outputs, and readers (Wiegand, RM, BLE, and OSDP).
4. Configure the **Offline Mode of All IP-ACM's** configured on this controller.

   See Table 2 on Page 283 for descriptions of the fields.
5. When the IP-ACM(s) configuration is complete, click in the **Enabled** check box, and click **Save and Close**.

Table 2: iSTAR Controller IP-ACMs Tab Definitions

Field/Button	Description
IP-ACMs	
Create All IP-ACMs	Click to create the IP-ACMs. When you click **Create All IP ACMs** the Configured column check boxes are selected, and you can click ... in the **Edit** column to open the iSTAR Ultra IP ACM Editor to configure the IP ACM.
Delete All IP-ACMs	When you click **Delete All IP-ACMs**, the check boxes in the **Configured** column are cleared for all IP-ACMs. When the configuration is save, you are prompted to confirm deletion of each IP-ACM.
Offline Mode of All IP-ACMs	
NOTE: The selections made in the Offline Mode of All IP-ACMs section will apply to all IP-ACMs configured on the controller. In offline mode, the IP-ACM board will admit cards that are among the last *xxx* previous admitted cards in addition to a pre-defined personnel group. - A total of 1000 credentials (not personnel) for both previous admitted credentials and credentials in the personnel group. - Maximum 100 personnel in the personnel group. - If you set the **Personnel** system variable "**Maximum Cards Per Person**", then that value must be taken into consideration. Example:If you set the "Maximum Cards Per Person" value to 3, then only 1000 - 100 x 3 = 700 is allowed in the "Admit the last admitted cards" field for configuration. This is true, even if the personnel count in the personnel group selected is less than 100.	
Admit the last admitted cards	Select a number from the menu that will apply to the previous cards that were admitted. Default: 0 Value: 0 to 1000
Card Format used by the members of the Personnel Group	Select a card format to be used for personnel when in office mode. Only individual card formats are selectable. The card format is used to determine the card data stream for each person in the personnel group. Al personnel will use the same card format. The first facility code and site code in the list will be used if that format has multiple values.
Admit the members of this personnel group	Click ... to select a pre-configured personnel group. NOTE: The maximum value is 1000 admitted cards. If a Personnel Group is configured to have 100 personnel members, the maximum value is reduced by 100 times the maximum number of cards per person configured in the System Variable.
Number of seconds before Offline Mode is enabled.	The time in seconds that the IP ACM waits to enter offline mode after it loses communication with the GCM board. This setting will apply to all IP ACMs on this controller unless specified in the iSTAR Ultra IP ACM Editor General tab. Default: 10 seconds. Range: 5 to 30 seconds.
Number of Days to Keep Credentials in Offline Mode	The number of days a credential is kept while in offline mode. A value of 0 indicates not to keep a credential when in offline mode. Default: 30 days Range: 0 to 9999 days

Table 2: iSTAR Controller IP-ACMs Tab Definitions (continued)

Field/Button	Description
High Latency Threshold in milliseconds	The number of milliseconds that will cause a round-trip latency alarm. This value will apply to all IP-ACM's configured for this controller. Default: 500 milliseconds (0.5 seconds) Range: 100- 2000 milliseconds (0.1 to 2 seconds)

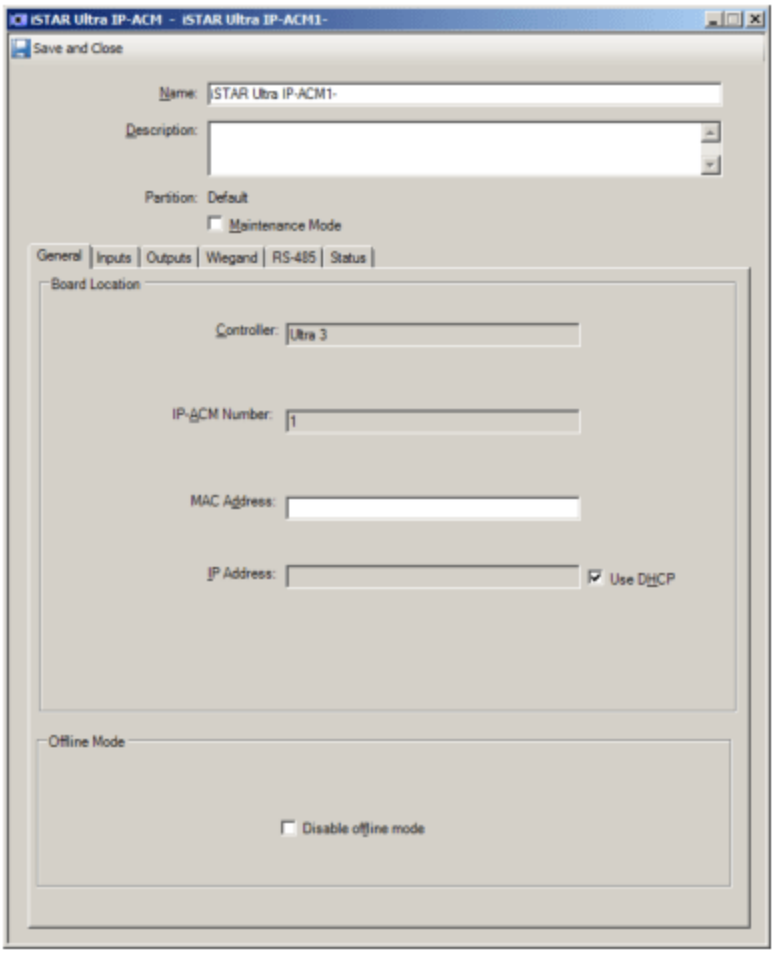
iSTAR Ultra IP-ACM Editor

The iSTAR Ultra IP-ACM editor, shown in Figure 2 on Page 285, is used to configure readers, inputs and outputs.

See the following for more information:

- Accessing the iSTAR Ultra IP-ACM Editor on Page 285
- iSTAR Ultra IP-ACM Inputs Tab on Page 291
- iSTAR Ultra IP-ACM Outputs Tab on Page 286
- iSTAR Ultra IP-ACM Wiegand Tab on Page 288
- iSTAR Ultra IP-ACM RS-485 Tab on Page 290
- iSTAR Ultra IP-ACM Status Tab on Page 293

Figure 2: iSTAR Ultra IP-ACM Editor



Accessing the iSTAR Ultra IP-ACM Editor

To Access the iSTAR Ultra IP-ACM Editor

1. From the iSTAR Ultra Controller editor dialog box, click the **IP ACMs** tab.

2. Click on the **Configured** check box in the Index row that you want to add/edit.
3. Click [...] in the **Edit** column of the Index row to open the iSTAR Ultra IP-ACM editor.

Table 3: iSTAR Ultra Controller IP-ACM Editor General Tab Definitions

Field/Button	Description
Partition	This read-only field identifies the Partition.
Maintenance Mode	Click to put the IP-ACM into Maintenance Mode. See Chapter 2: Maintenance Mode for more information.
Board Location	
Controller	This field is read-only.
IP-ACM Number	This field is read-only.
MAC Address	Enter the MAC address of the IP-ACM. NOTE: You will not be able to edit this field after you enter the IP address and save the configuration. **To change the MAC Address, you will need to delete the IP-ACM configuration and create a new one.**
IP Address	The IP address of the IP-ACM if not using DHCP.
Use DHCP	Click the check box to use DHCP. Deselect the check box to enter an IP Address. Default: DHCP is enabled.
Offline Mode	
Disable offline mode	Click the check box to disable offline mode on this IP-ACM. NOTE: This selection will override the **Offline Mode of all IP-ACMs** selections in the iSTAR Controller Editor IP-ACMs tab for this IP-ACM.

iSTAR Ultra IP-ACM Outputs Tab

The Outputs tab allows you to configure the Outputs for the IP-ACM.

Table 4 on Page 287 provides definitions of the fields and buttons on the iSTAR Ultra IP-ACM Board Outputs tab.

Figure 3: iSTAR Ultra IP-ACM Outputs Tab

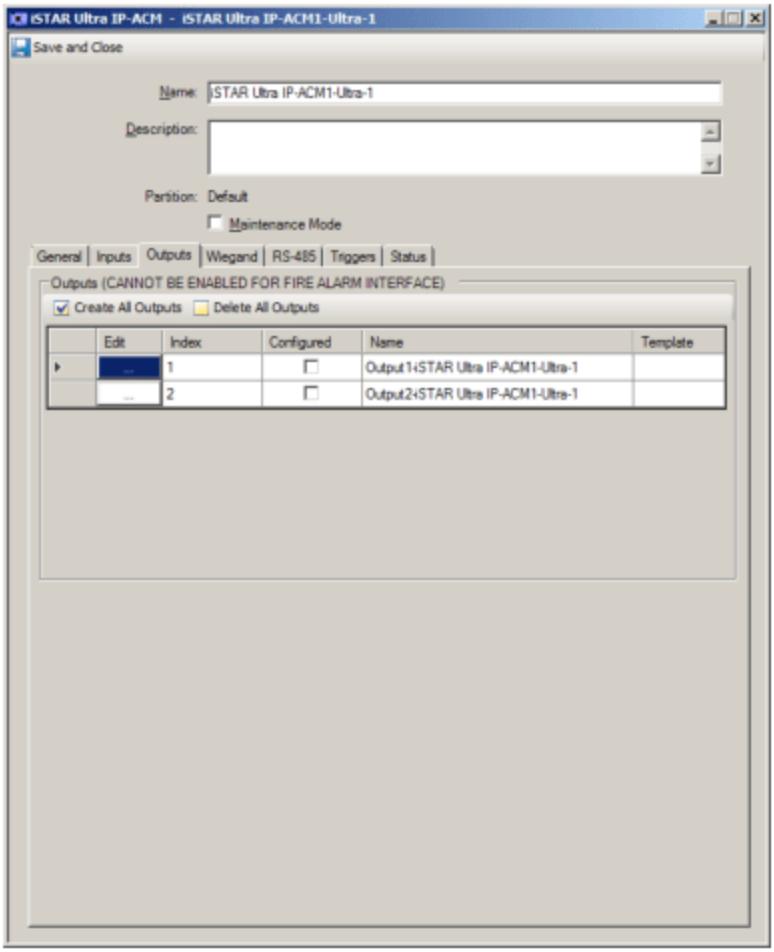


Table 4: iSTAR Ultra IP-ACM Outputs Tab General Tab Definitions

Field/Button	Description
Name	Displays the name for this Output board. The name is system-generated by default, but you can edit this name by clicking this field.
Description	Enter a textual comment about the Output board, such as its location or purpose. This text is for information only.
Partition	This read-only field identifies the Partition in which this Output board resides.
Maintenance Mode	Click to put the iSTAR Outboard Board into Maintenance Mode. See Chapter 2: Maintenance Mode for more information.
Location	
Controller	This read-only field identifies the iSTAR Controller to which this Output is attached.
Board	This read-only field identifies the iSTAR Controller board to which this Output board is attached.

Table 4: iSTAR Ultra IP-ACM Outputs Tab General Tab Definitions (continued)

Field/Button	Description
Board Index	This read-only field identifies the board index (which represents the SW1 address switch setting on the R/8 board) for this Output board.
Outputs	
Create All Outputs	Click to create all Outputs. The check boxes in the **Configured** column are set to ☑.
Delete All Outputs	Click to delete all Outputs. The check boxes in the **Configured** column are set to ☐.
Edit column	Click ... in this column to open the iSTAR Output Editor to edit this Output. NOTE: The **Configured** check box must be selected to open the Output Editor.
Index column	This read-only field identifies the position of each Output (1 - 2) on the IP-ACM board.
Configured column	☑ indicates that the Output has been configured. ☐ indicates that the Output has not been configured. NOTE: The **Configured** check box must be selected to open the Output Editor.
Name column	Displays the system-generated name for this Output. You can edit this name by clicking in the field.
Template column	Displays the Template used for creating this Output. If the Output is not yet configured, you can click in this column, then click to select an Output Template. If the **Configured** column displays ☑, this field cannot be edited.

iSTAR Ultra IP-ACM Wiegand Tab

Use this tab to configure Wiegand readers connected to the IP-ACM board.

Table 5 on Page 289 provides definitions of the fields and buttons on the iSTAR Ultra IP-ACM Wiegand tab.

Figure 4: iSTAR Ultra IP ACM Wiegand Tab

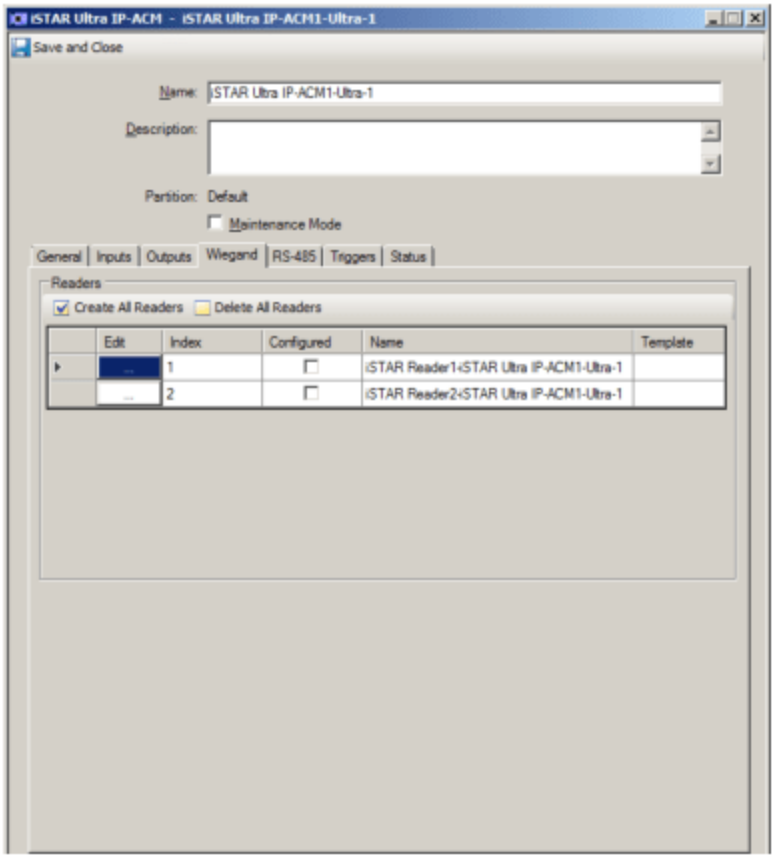


Table 5: iSTAR Ultra IP-ACM Wiegand Tab.Definitions

Box	Description
Create All Readers	Click to create all the Readers. When you click **Create All Readers**, the **Configured** column check boxes are selected, and you can click ... in the **Edit** column to open the iSTAR Reader Editor to configure a direct connect Wiegand Reader.
Delete All Readers	When you click **Delete All Readers**, the check boxes in the **Configured** column are cleared for all Readers, and all these Readers are immediately deleted (any settings you have configured are lost).
Edit column	Click ... in the **Edit** column to open the iSTAR Reader Editor to configure a Reader. See iSTAR Reader Editor on Page 248.
Index column	This column displays the number for each reader. This number is the physical port number for a Direct Connect Wiegand reader.
Configured column	Click in this column to create a reader (make it available to be edited).
Name column	Displays the name for this Reader. The name is system-generated by default, but you can edit this name by clicking in this field.

Table 5: iSTAR Ultra IP-ACM Wiegand Tab.Definitions (continued)

Box	Description
Template column	Click in this column prior to creating the Reader, then click ... to select a Reader template from the list of available Reader templates. The **Template** column shows the template name chosen if you selected a Template prior to creating the Reader.
Readers 1 - 2	Select the check box in the **Configured** column for a Reader and click ... located in the **Edit** column to open the iSTAR Reader Editor General tab to configure the Keypad, Triggers, Groups, Status and State Images that are associated with a Reader. See iSTAR Reader Editor on Page 248 for detailed instructions for configuring iSTAR Readers. The **Name** column displays a name comprised of the Reader Type and the iSTAR Controller name. You can click in this column to edit the Reader name.

iSTAR Ultra IP-ACM RS-485 Tab

Use this tab, shown in Figure 5 on Page 290, to configure RS-485 ports connected to the iSTAR Ultra IP-ACM Board.

Table 6 on Page 291 provides definitions of the fields and buttons on the iSTAR Ultra IP-ACM RS-485 tab.

Figure 5: iSTAR Ultra IP-ACM RS-485 Tab

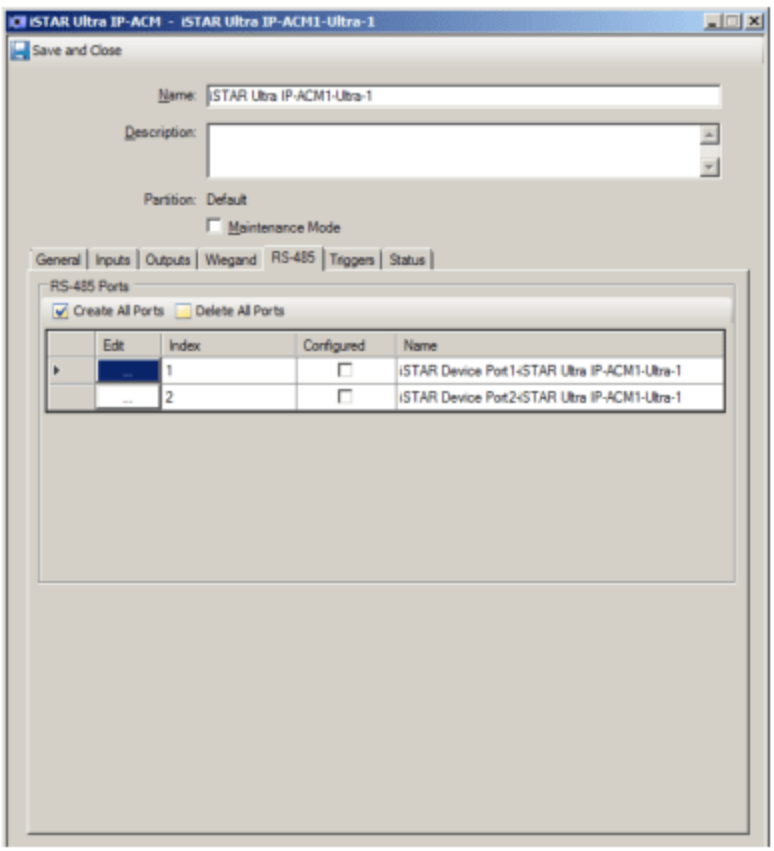


Table 6: iSTAR Ultra IP-ACM Board RS-485 Tab Definitions

Field/Button	Description
Create All Ports	Click to create the RS-485 Ports. When you click **Create All Ports** the Configured column check boxes are selected, and you can click ... in the **Edit** column to open the iSTAR Device Port Editor to configure an RS-485 Port.
Delete All Ports	When you click **Delete All Ports**, the check boxes in the **Configured** column are cleared for all Ports, and all Ports are immediately deleted (any settings you have configured are lost).
Edit column	Click ... in the **Edit** column to open the iSTAR Device Port Editor to configure Device Ports for the IP-ACM. See iSTAR Ultra ACM RS-485 Device Port Editor on Page 188.
Index column	This column displays the number for each Device Port.
Configured column	Click in this column to create a Device Port (make it available to be edited).
Name column	Displays the name for this Device Port. The name is system-generated by default, but you can edit this name by clicking in click in this field.
Device Ports 1 - 2	Select the check box in the **Configured** column for a Device Port and click ... located in the **Edit** column to open the iSTAR Device Port Editor General tab to configure the Readers and ACM extensions that are associated with the Device Port. See iSTAR Reader Editor on Page 248 for detailed instructions for configuring iSTAR Device Ports. The **Name** column displays a name comprised of the Device Port and the iSTAR Controller name. You can click in this column to edit the Device Port name.

iSTAR Ultra IP-ACM Inputs Tab

The Ultra IP-ACM Inputs tab lets you create and configure the Inputs that are attached to this Ultra IP-ACM Board.

You can use an existing Input Template to create one or more of the IP-ACM Board Inputs. Click in the **Template** Column, then click ... . A list of available iSTAR Input Templates appears. Click on the Template you wish to use. See Using Templates for Controller Inputs, Outputs, and Readers on Page 37 for more detailed information about using Templates to create Inputs.

Table 7 on Page 292 provides definitions for the buttons and fields on the iSTAR Ultra IP-ACM Inputs tab.

Figure 6: iSTAR Ultra IP-ACM Inputs Tab

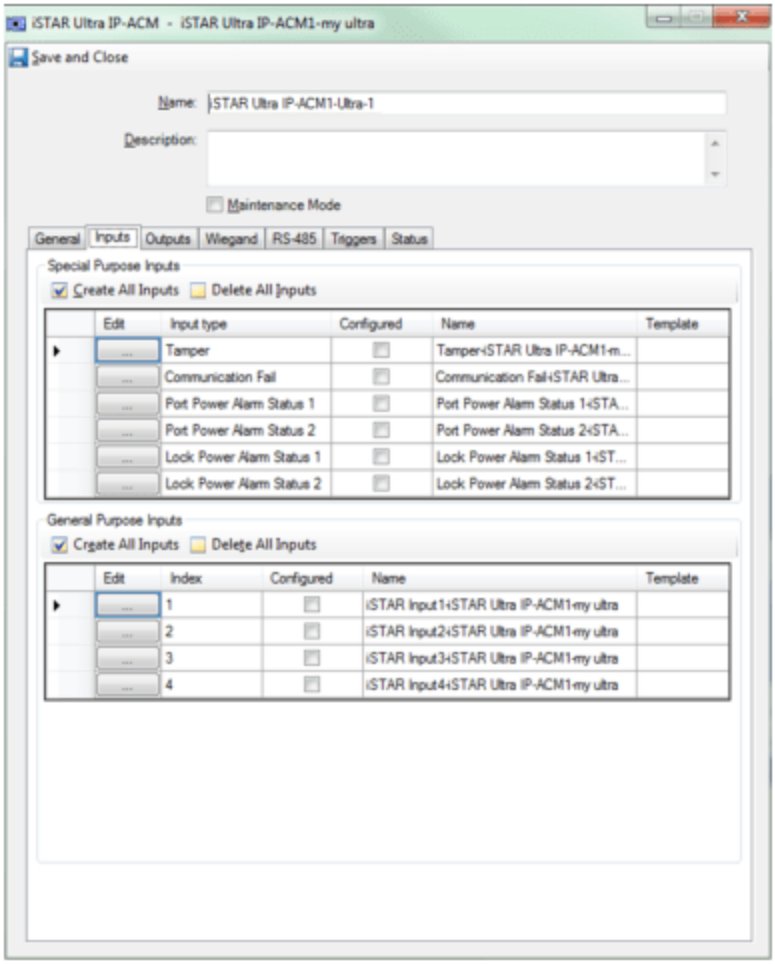


Table 7: iSTAR Ultra IP-ACM Board Inputs Tab Definitions

Field/Button	Description
Special Purpose Inputs	
Tamper	The **Tamper** input activates when the controller cabinet is opened or removed from its mounting surface. NOTE: For UL applications, this field must be enabled. Select the check box in the **Configured** column and click ... located in the **Edit** column to open the iSTAR Input Editor General tab to configure the Tamper input. From the Input Editor you can configure the Options, Triggers, Groups, Status and State Images that are associated with the Tamper Input. The **Template** column shows the template name chosen if you selected a Template prior to creating the Input.
Communication Fail	A logical unsupervised input that reflects the state of the communication between the GCM board and Processor-A on this IP-ACM board.

Table 7: iSTAR Ultra IP-ACM Board Inputs Tab Definitions (continued)

Field/Button	Description
Port Power Alarm Status 1 Port Power Alarm Status 2	Power indicator input for each RM / Weigand port.
Lock Power Alarm Status 1 Lock Power Alarm Status 2	IP-ACM can provide power for the locks directly from the 2 Output connectors (Lock Power 1 & 2). There are automatic over-current shut-off switches on each Lock Power. The Lock Power Alarm Status inputs go Active when the over-current shut-off switches are active (i.e., when Lock Power has been shut off).
General Purpose Inputs	
Inputs 1 through 4	These standard general purpose supervised inputs are available on iSTAR Ultra IP-ACM boards.

iSTAR Ultra IP-ACM Status Tab

The Status tab, shown in Figure 7 on Page 294, provides a read-only listing of information about the operational status of the selected iSTAR Ultra IP-ACM Board.

Figure 7: iSTAR Ultra IP-ACM Status Tab

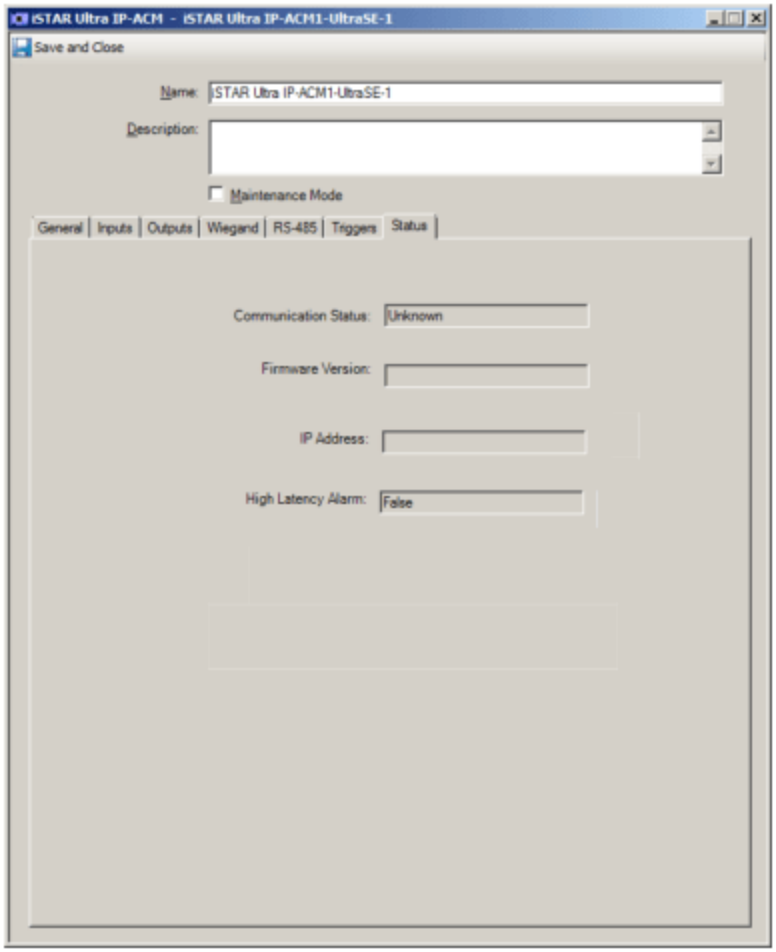


Table 8 on Page 294 provides definitions of the fields and buttons on the iSTAR Ultra IP-ACM Board Status tab.

Table 8: iSTAR Ultra IP-ACM Board Status Tab Definitions

Field/Button	Description
Communication Status	Unknown, Offline, or Online.
Firmware Version	Processor firmware, such as 00.00.36.00008
IP Address	The IP-ACM IP address.
High Latency Alarm	Possible status values are True or False.

7

Chapter 7 Configuring Advanced Processing Controllers (apC)

This chapter explains how to configure the apC, apC/8X, and apC/L software components to work with C•CURE 9000.

In this chapter

apC Panel Overview

The **advanced processing Controller** (apC) panel is an intelligent field device that performs basic access control tasks. The apC, apC/8X, and apC/L are access control field panels that coordinate communication between the C•CURE 9000 server and the system security hardware, such as card readers.

The apC/L is a smaller version of the apC, making it ideal for parking garages and small office buildings. All apC/8Xs and some apC/Ls provide Flash ROM support, which lets you download firmware from the server to the panel. Up to three versions of firmware are available for download. See the *Monitoring Station User's Guide* for information about downloading firmware.

Each apC, apC/8X, or apC/L in the system supports Wiegand, proximity, magnetic stripe, and RFID card technologies. The apC (apC/8X) configuration supports eight card readers wired in a daisy-chain arrangement. The apC/L configuration supports two card readers.

NOTE The apC and apC/L have not been evaluated by UL.

See the following sections for more information:

- Features of apC Panels on Page 296
- Inputs and Alarm Device States on Page 299
- Outputs and Readers on Page 299
- Optional Boards on Page 300
- apC Time Zones on Page 300
- Changing the Time Zone of an apC Controller on Page 303
- apC Time Zone Reports on Page 303
- apC Firmware Update on Page 306
- apC Controller Configuration Summary on Page 308

Features of apC Panels

Several different types of add-on module expansion boards can be used for additional inputs and outputs.The apC firmware offers software-controlled features such as timed activation/deactivation commands, 32-bit card numbers, elevator access and anti-passback control. An apC panel can use multiple card technologies, site codes, and company codes. The apC's full-year real time calendar/clock allows activation and deactivation of cards on specified days. The apC panels can be connected via serial RS-232/485 or networked terminal servers.

apC Panel

The basic apC panel has eight supervised inputs, eight relay outputs and one reader port, capable of handling a maximum of eight readers, which are wired in a multi-drop configuration. Expansion boards can add reader ports, supervised inputs and additional outputs. By using expansion boards, bus modules and RM-4s, an apC can have as many as 128 inputs and 192 outputs. Depending on the amount of available memory, an apC panel can hold up to 40,000 cards in its database. See Table 77 on Page 297 for a listing of the standard apC panel's inputs, outputs and readers. Total indicates that this is the total number of inputs, outputs or readers for the apC panel.

There are three Star Coupler expansion boards that can be used with the apC panel to add inputs, outputs and readers :

- Star Coupler – 8 RM readers, 8 relay outputs, 8 unsupervised inputs (see apC Add-On Board Star Coupler Tab on Page 354 for more information)
- Mini-Star Coupler – 8 RM Readers (this is the same board as Star Coupler but inputs and outputs are not populated)
- WPSC – Wiegand Prox Star Coupler includes 2 boards:
  - Lower board – 4 Wiegand signaling readers and 4 supervised inputs
  - Upper board – 4 Wiegand signaling readers and 4 supervised inputs (the upper board plugs into lower board)

A Star Coupler Reader is an RM reader connected to a Star Coupler. The Mini Star Coupler Reader is an RM reader connected to the Mini Star Coupler and it differs from the Star Coupler only due to its having no inputs or outputs. The readers used by these Star Coupler expansion boards are RM or Wiegand signaling readers that are connected to a Star Coupler.

Table 77: apC Inputs, Outputs and Readers Available

Board	Inputs	Outputs	Readers
Tamper Input	1		
Power Failure Input	1		
Supervised Inputs	8		
Outputs		8	
Readers			8 total
Supervised Reader Inputs	16 total		
Reader Outputs		16 total	
Add-On Boards			
I32 Supervised Input Board	32		
I8 Supervised Input Board	64		
R48 Output Board		96	
R8 Output Board		64	
Star Coupler Readers			8 total
Star Coupler Reader Supervised Inputs	16 total		
Star Coupler Reader Outputs		16 total	
Star Coupler Unsupervised Inputs	8		

Table 77: apC Inputs, Outputs and Readers Available (continued)

Board	Inputs	Outputs	Readers
Star Coupler Outputs		8	
Star Coupler - Ministar Readers			8 total
Star Coupler - Ministar - Reader Supervised Inputs	16 total		
Star Coupler - Ministar - Reader Outputs		16 total	
Wiegand Proximity Star Coupler Readers [Upper and Lower Boards]			8 total
Wiegand Proximity Star Coupler Reader Supervised Inputs [Upper and Lower Boards]	8		

apC/L Panel

A basic apC/L panel has two readers and two relay outputs. An apC/L is expandable up to 36 inputs and 38 outputs using RM-4s and bus modules. Depending on the amount of available memory, an apC/L panel can hold up to 40,000 cards in its database. apC/L panels with Flash EPROMS installed can have firmware upgrades downloaded from the host system.

NOTE The apC/L has not been evaluated by UL.

Table 78: apC/L Standard Inputs, Outputs and Readers Available

Board	Inputs	Outputs	Readers
Tamper Input	1		
Power Failure Input	1		
Outputs		2	
Readers			2
Supervised Reader Inputs	4		
Reader Outputs		4	
Add-On Boards			
I8 Supervised Input Board	32		
R8 Output Board		32	

apC/8X Panel

A basic apC/8X panel has eight supervised inputs, eight relay outputs and one reader port, capable of handling a maximum of eight readers, which are wired in a multi-drop configuration. Expansion boards can add reader ports,

supervised input and additional outputs. Depending on available memory, an apC/8X panel can hold up to 160,000 cards in its database. apC/8X panels with Flash EPROMS installed can have firmware upgrades downloaded from the host system. See Table 77 on Page 297 for a listing of the apC/8X panel's inputs, outputs and readers. Total indicates that this is the total number of inputs, outputs or readers for the apC panel.

Inputs and Alarm Device States

An input is an object that associates an alarm device with an input on the panel or on an input board. There are two kinds of inputs: supervised and unsupervised. All alarm devices can be in one of two states: active or inactive. An **input** reports the state of the alarm device.

A **supervised** input reports on the status of the wiring between the panel and the alarm device when changes in circuit resistance are detected. If wiring is cut, the system reports an open circuit. If someone attempts to create a jumper across the wiring (to prevent the device from reporting), the system reports a shorted circuit. Supervised inputs can report a total of five conditions to the apC: Short, Open Loop, Line Fault, Inactive or Active. The main board on the apC has eight supervised inputs.

An **unsupervised** input does not monitor the wiring. Unsupervised inputs can report two conditions to the panel: Active or Inactive. With the star couplers, the apC has eight unsupervised inputs available. See To Configure apC Controller Inputs on Page 322 for more information.

NOTE Unsupervised inputs have not been evaluated by UL.

Supervised inputs can report five states:

- Short
- Open Loop
- Normal
- Alert
- Line Fault

Outputs and Readers

Outputs

An **output** is an object that associates an alarm device with an output on the panel board or add-on module. The output turns alarm devices, such as closed circuit TV or alarm dialers, on or off. See apC Controller Outputs Tab on Page 323 for more information.

Readers

A **reader** is a hardware device that accepts access requests. To make an access request, a person swipes or presents a card at the reader. The card reader scans the information encoded on the card and sends it to the apC panel, which grants or denies access. See apC Controller Readers Tab on Page 323 for more information.

Optional Boards

apCs and apC/8X panels support these optional (add-on) boards and controller:

- 8 apC I/8 - input modules and 1 apC I/32 input board, and
- 8 apC R/8 - output modules and 2 apC R/48 output boards, and
- 1 Standard Star Coupler, or
- 1 Mini Star Coupler, or
- 1 Wiegand Proximity Star Coupler

Star couplers enable you to wire the apC panel's 8 readers in a star, daisy-chain, or combination configuration. Star couplers also provide unsupervised inputs and additional outputs and readers for the apC and apC/8X.

NOTE apC/L controllers and Mini Star Couplers have not been evaluated by UL.

NOTE The apC/L supports two types of optional boards: four I/8 - input modules and four R/8 - output modules.

See apC Controller Add-On Board Tab on Page 324 for more information.

NOTE Before you configure apC panels, the apC Hardware Interface must be started using the Server Management application - Server Components tab. Right-click the apC Hardware Interface and click **Start Server Component**.

apC Time Zones

You can specify the Time Zone for an apC panel, so that the apC panel can support panel-based operations using the local date/time, and the display of the local date/time at door readers, in controller status screens, in Journal Messages, and in Reports.

Example:

If you specify that an apC panel is in the Pacific Time Zone (GMT- 08:00), and the C•CURE 9000 server is in the Eastern Time Zone (GMT- 05:00), a timed-based action that occurs at the apC panel, such as unlocking a Door, happens at local time (Pacific Time Zone) for the apC panel.

Example:

If you specify that an apC panel is in the Pacific Time Zone (GMT- 08:00), and the C•CURE 9000 server is in the Eastern Time Zone (GMT- 05:00), a server-based Journal message shows the server date/time (EST), while a panel-based Journal Message shows the panel date/time (PST) as highlighted in Figure 91 on Page 300.

Figure 91: Journal Message Showing Local Date/Time

Message Type	Server Date/Time	Message Text	Message Date/Time	Message Local Date/Time
Manual Action	2/28/2012 4:29:32 PM	Manual action by 'su': momentarily activate Output 'Output6-ACM1-1da7 panel'.	2/28/2012 4:29:32 PM	2/28/2012 4:29:32 PM
Object Changed State	2/28/2012 4:29:33 PM	Output 'Output6-ACM1-1da7 panel' is momentarily active.	2/28/2012 4:29:33 PM	2/28/2012 1:29:33 PM

Example:

If you specify that an apC panel is in the Pacific Time Zone (GMT- 08:00), and the C•CURE 9000 server is in the Eastern Time Zone (GMT- 05:00), a Credential with an Expiration Date set as today at 5:00 PM will expire at 5:00 PM Eastern time, rather than Pacific Time, because the expiration occurs at the server, which is in the Eastern Time Zone.

The Time Zone setting is configured on the apC controller General tab by selecting a Time Zone from the **Time Zone** field. See apC Controller General Tab on Page 319 for more information.

You can change the value of the apC controller **Time Zone** field only when the apC Controller is not enabled (**Enabled** field is blank ☐). See Changing the Time Zone of an apC Controller on Page 303 for more information.

apC Time Zones and Schedules

Schedules in C•CURE 9000 are not configured directly with any Time Zone. They are dynamically associated with a local Time Zone when they are used in the C•CURE 9000 Server or are downloaded to a controller. That means that the same schedule can be activated at different times if it is used in different Time Zones.

This is flexible, but also potentially complicated if you have controllers in different Time Zones.

Example:

You create a Schedule to manage Clearances for your night shift. When downloaded to an apC in another Time Zone, the Schedule works as expected. However, if you apply the Schedule to a C•CURE 9000 Server-based Event ("Lock all Doors" using the **All Doors** Group) that affects the Pacific Time Zone apC, the Event's actions would be triggered in the Server's Time Zone, rather than the Time Zone where the apC resides, perhaps causing Doors to be locked at the wrong time.

However, if you create separate Schedules and name them to make it clear which Time Zone (or which controller) they are intended to be used with, you can avoid problems with Time Zone differences.

Example:

You create a Schedule to assign to Door and Elevator Clearances on your apC in the Pacific Time Zone called "Doors & Elevators - Pacific" and only use this Schedule for Pacific Zone. The Door and Elevator Clearances are downloaded to the apC controller

The schedules used in an apC panel for timed actions are primarily associated with Door or Elevator clearances.

When a Schedule becomes active, the Journal Message that is displayed identifies the Time Zone associated with the object (such as an apC panel) to which the Schedule is related.

You can see the active/inactive status of your Schedules with the **Schedule by Time Zones** Dynamic View, accessible from the Configuration pane. See the Schedules chapter in the *C•CURE 9000 Software Configuration Guide* for more information.

Using apC Panel Time Zones with Trigger Schedules

apC Triggers support the ability to designate a Time Zone for a Trigger, so that you can specify that the Schedule for activating the Trigger uses the same Time Zone as the apC panel. If you do not specify a Time Zone for the Trigger, the Trigger Schedule uses the C•CURE 9000 server Time Zone to determine when the Trigger can be activated.

See Defining a Trigger for an apC Device on Page 370 for more information about specifying a Time Zone for an apC Trigger.

Using apC Panel Time Zones with Events

You can add a Time Zone to an Event if you intend to activate a timed Action with that Event. The Event General tab includes a **Time Zone** field that you can use to determine when a Schedule you attach to the Event is Activated. See the Events chapter in the *C•CURE 9000 Software Configuration Guide*.

Time Zone for apC Panel Events

For timed Actions defined in an Event (the Event is armed and/or activated by a Schedule) that the apC driver downloads to an apC panel to execute , the Time Zone for the Action is automatically set to the Time Zone of the apC Panel. You cannot change the Time Zone setting to a different Time Zone.

Example:

The C•CURE 9000 server is in the Eastern Time Zone (GMT - 05:00). The apC Panel is in the Pacific Time Zone (GMT - 08:00). If the Event is activated by a Schedule at 10:00 AM, it will be activated at 10:00 AM Pacific Time (the apC panel's Time Zone), not 10:00 AM Eastern Time.

For an apC time-based action defined in a Event, if a Time Zone is specified in the Event, the apC driver only downloads the action to apC controllers with the same time zone as the Event.

If the apC panel is online when the Event is activated by the Schedule, the apC driver sends the timed Action command to the apC panel.

If the apC Panel is offline when the Event is activated by the Schedule, the apC panel performs the timed Action. However, the apC does not have the capability, after communication is re-established, to display activation and deactivation messages for an Event that occurred while the apC was offline.

Time Zone for apC Host Events

For a host Event (an Event that is initiated at the C•CURE 9000 server, without timed Actions downloaded to the apC Panel), you can specify any Time Zone for the Schedule on the Event General tab. The Time Zone does not need to match the time Zone of the apC panel.

However, if the Time Zone of the Event Schedule and the Time Zone of the apC panel are different, a warning message appears to inform you of the discrepancy, called a Time Zone Mismatch, so that you will be aware that the timed Action will be activated according to the host Time Zone, not the apC panel Time Zone.

Example:

The C•CURE 9000 server is in the Eastern Time Zone (GMT - 05:00). The apC Panel is in the Pacific Time Zone (GMT - 08:00). If the Event is activated by a Schedule at 10:00 AM, it will be activated at 10:00 AM Eastern Time (server time), not 10:00 AM Pacific Time.

If the apC panel is online when the host Event is activated by the Schedule, the apC driver sends the timed Action command to the apC panel.

If the apC Panel is offline when the host Event is activated by the Schedule, the apC panel does not perform the timed Action, because the Event was not downloaded to the apC panel, and the panel is offline from the host.

Changing the Time Zone of an apC Controller

You can change the value of the apC controller **Time Zone** field only when the apC Controller is not enabled (**Enabled** field is blank ☐). To change the Time Zone, you must edit the controller, clear the **Enabled** field, save the controller, then re-open it to change the Time Zone.

If you change the Time Zone of the apC controller, the Time Zone settings of all child objects of that apC controller are changed as well. A warning message appears if you change the Time Zone and any Events have controller-based actions on this apC controller and the Event is configured to use a different Time Zone than this apC controller.

To Change the Time Zone of an apC Controller

1. From the Hardware pane, select the apC controller you wish to change. Right-click and select **Edit**.
2. Clear the **Enabled** field (change ☑ to ☐).
3. Click **Save and Close** to save the change.
4. From the Hardware pane, select the apC controller again. Right-click and select **Edit**.
5. When the apC controller editor opens, the **Time Zone** field can be changed.
6. Click **Save and Close** to save the change.

apC Time Zone Reports

C•CURE 9000 provides several pre-defined Reports (and Queries) that can help you find Time Zone mismatches - where the C•CURE 9000 server and the apC panel are in different Time Zones, such that a host Event will be unable to activate an object on an apC that is offline.) for Events associated with apC panels in different Time Zones than the C•CURE 9000 server.

Table 79: apC Time Zone Reports/Queries

Report	Query
SWH70 - apC Input Groups with Time Zones	
SWH71 - apC Door Groups with Time Zones	
SWH 72 - apC Time Zone Mismatch Actions	SWHrep72 - apC Time Zone Mismatch Actions
SWH 73 - apC Online Only Actions	SWHrep73 - apC Online Only Actions
SWH 74 - Actions with Time Zone Mismatch	SWHrep74 - Actions with Time Zone Mismatch Query

See the Reports chapter of the *C•CURE 9000 Data Views Guide* for more information about these Reports and Queries.

Creating Custom Reports for apC Actions and Time Zones

In addition, you can use the Report Editor to create custom reports on apC controller actions, including Time Zone information. You can use the pre-defined Reports as starting points for your own custom Reports by clicking **Create Copy** and then customizing the copy.

apC Controller Actions Report

You can create a custom Report that lists apC Controller objects and all the actions triggered by the controller and its child objects (like doors, readers and inputs), as well as action items that should be loaded into the apC because they are configured in Event objects.

If a Report Query is not specified, the report lists all the apC Controllers and all the actions, noting each action is **Online Only** - performed only if the apC panel is Online - if the custom fields in the Action Item class are selected.

Specifying a Report Query allows you to select any apC Controller field and any Action Item field, including these custom fields:

- **Online Only** - whether the action can occur only on an online apC)
- **Online Only Reason** - the reason that an action can only occur on an online apC. Possible values are:
  - Time Zone Mismatch - The Time Zone of the timed action is different from the Time Zone of the controller.
  - No Firmware Support - The action is not supported by the controller, so it must be executed on the host.
  - Cross Panel Action - The action is activated by one controller and modifies an object on another controller.
  - Invalid Configuration - The action cannot be activated (for example, a change in Comm Fail status should cause an Event to activate an Output on the same controller, but the Comm Fail prevents the Event from communicating with the Output.)

To Create an apC Controller Actions Report

1. Create a new Report - From the Data Views pane, select **Report** from the drop-down list of objects, then click **New**.
2. Select **apC Controller** as the **Report type** field.
3. Select **apC Controller Actions** as the **Sub type** field.
4. Click on **apC Controller** in the Class Selector.
5. In in the Field Selector, select the fields for the apC Controller class that you want to display in the Report.
6. Click on **Action Item** in the Class Selector.
7. In the Fields Selector, select any fields you want in the report (including the custom fields **Online Only** and **Online Only Reason**) for the Action Item class.
8. Optionally, you can click to select a Report Query as the basis of the report. SWHrep72 and SWHrep73 are available in the **Report Query** drop-down list for this purpose.
9. Click **Save and Close** to save the Report.
10. The Report is added to the Reports Dynamic View. You can double-click the Report to run it.

Action Item Time Zones Report

You can create a custom Report that lists Action Item objects (with the ability to query on any Action Item property) and additionally query on three additional custom fields in the Action Item Time Zone Sub type:

- Source Time Zone - the Time Zone of the Source object of the action item (if any).
- Target Time Zone - the Time Zone of the Target object (if any).

- Time Zone Mismatch - set to TRUE if the Time Zone of the Action Item is not equal to the Time Zone of the Source object and/or not equal to the Time Zone of the Target.

To Create an Action Item Time Zones Report

1. Create a new Report - From the Data Views pane, select **Report** from the drop-down list of objects, then click **New**.
2. Select **Action Items** as the **Report type** field.
3. Select **Action Item Time Zone** in the **Sub type** field.
4. Click on **apC Controller** in the Class Selector.
5. In the Field Selector, select the fields for the apC Controller class that you want to display in the Report.
6. Click on **Action Item Time Zone** in the Class Selector.
7. In the Fields Selector, select any fields you want in the report (including the custom fields **Online Only** and **Online Only Reason**) for the Action Item Time Zone class.
8. Optionally, you can click to select a Report Query as the basis of the report. SWHrep74 is available in the Report Query drop-down list for this purpose.
9. Click **Save and Close** to save the Report.
10. The Report is added to the Reports Dynamic View. You can double-click the Report to run it.

apC Door Group and Input Group Time Zones Report

You can create a custom Report that lists either apC Door Groups or apC Input Groups and their Time Zones by editing the following pre-defined Reports, creating a copy, adding a Query, or customizing the Report Layout:

- SWH70 - apC Input Groups with Time Zones
- SWH71 - apC Door Groups with Time Zones

Both of these pre-defined Reports:

- Start with a Group Report
- Use the Group Member field **Time Zone Name** to output the Time Zone of the objects in the Report.

To Create an apC Door Group or apC Input Group with Time Zones Report

1. From the Data Views pane, select **Report** from the drop-down list of objects, then click  .
2. Select either:
   - SWH70 - apC Input Groups with Time Zones
   - SWH71 - apC Door Groups with Time Zones
3. Right-click and choose **Edit**. The Report editor opens.
4. Click **Create Copy**. A new Report opens in the Report editor, based on the pre-defined Report you chose.
5. Click  in the **Report form** field if you want to select a different Report From.
6. Click  in the **Report query** field if you want to select a Query for the Report.

7. Select **Prompt for Query** ☑ if you want to display a Query Parameter Prompt when the report is run.
8. Click the drop-down list for the **Layout style** if you want to change the Report layout.
9. Change the fields in the **Class selector** and the **Field selector** if you want to change the fields displayed on the Report.
10. Click the Layout Design tab if you want to manually change the Report design.
11. Click the Layout Preview tab to see a preview of how the Report will look.
12. Click **Save and Close** to save the Report.
13. The Report is added to the Reports Dynamic View. You can double-click the Report to run it.

apC Firmware Update

You can update the apC, apC/8X or apC/L firmware on apC panels from either the Admin Client or the Monitoring Station client. You can initiate a firmware update by right-clicking on the apC controller:

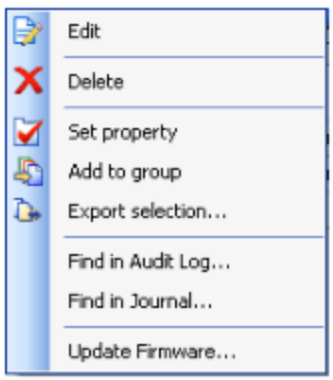
- In the Hardware Tree.
- In a Dynamic View in the Administration Client.
- In the Status List - Controller in the Monitoring Station.

NOTE The UL approved firmware to be used for the apC/8x panel is x.7ZF

To Update Firmware on an apC

1. Right-click on the apC that you want to update.
2. Select Update Firmware from the context menu that appears (see Figure 92 on Page 306).

Figure 92: apC Context Menu



NOTE The Update Firmware selection does not appear if the apC is not Enabled or is off-line.

3. The apC Firmware Download dialog box opens (see Figure 93 on Page 307).

Figure 93: apC Firmware Download Dialog Box

4. Select the firmware version that you want to download from the list in the dialog box.
5. Click **Start firmware download**. A progress bar shows you the when the download is completed.
6. When the download has completed, click **Close** to close this dialog box.

TIP Do not attempt to download firmware to more than one apC panel on a chain at one time, and do not attempt to download firmware if that chain is busy doing a personnel download.

apC Controller Configuration Summary

Configuring an apC is a multiple task process because of the number of options available on the apC.

The following summary gives you an outline of the configuration process, with links to topics that provide the details.

Table 80: apC Configuration Summary

Configuration	See...
1. Create and configure an apC Comm Port.	apC Comm Port Editor on Page 310
2. Create an apC Controller.	To Create an apC Controller on Page 318
3. Use the apC Controller General Tab to configure the Connection Type, Comm Port, RM LCD Message set, apC Type, Time Zone, and apC Address.	apC Controller General Tab on Page 319
4. Use the apC Controller Communications Tab to configure communications parameters for the apC.	apC Controller Communications Tab on Page 321
5. Use the apC Controller Inputs Tab to configure Panel Status Inputs and Supervised Inputs.	apC Controller Inputs Tab on Page 322
Edit each apC Input on the apC Input Editor Triggers tab, and State Images tab, and view the Input's status on the Status tab.	apC Input Editor on Page 332
6. Use the apC Controller Outputs Tab to configure apC Outputs.	apC Controller Outputs Tab on Page 323
Edit each apC Output on the apC Output General Tab and State Images tab, and view the Input's groups and status on the Groups tab and Status tab.	apC Output General Tab on Page 336
7. Use the apC Controller Readers Tab to configure apC Readers and options.	apC Controller Readers Tab on Page 323
Edit each apC Reader on the apC Reader General Tab, I/O tab, Keypad tab, Triggers tab, and State Images tab, and view the Input's status on the Status tab.	apC Reader General Tab on Page 340
8. Use the apC Controller Add-On Board Tab to create and configure an apC add-on board.	apC Controller Add-On Board Tab on Page 324
Edit each apC Add-on Board from the apC Add-on Board Editor, configuring Input Boards, Output boards, and Star Couplers.	apC Add-on Board Editor on Page 347
Edit the apC Input boards from the apC Input Editor, creating I/32 and I/8 Input boards, as needed. Edit each apC Input from the apC Input Editor, configuring Supervised Inputs and Status Inputs.	apC Input Editor on Page 332
If you created a Star Coupler, use the apC Star Coupler Board Editor to create Readers, unsupervised inputs, and outputs.	apC Star Coupler Board Editor on Page 365
If you created a Mini Star Coupler, use the Mini Star Coupler Board Editor to create apC Readers.	Mini Star Coupler Board Editor on Page 373

apC Configuration Summary (continued)

Configuration	See...
If you created a WPSC, use the Wiegand Proximity Star Coupler Editor to create Readers and Inputs.	Wiegand Proximity Star Coupler Editor on Page 376
9. Use the apC Controller Triggers Tab to set up triggers for Actions based on apC controller property states.	apC Controller Triggers Tab on Page 326
10. Use the apC Controller Holiday Groups Tab to add Holiday Lists to the apC.	apC Controller Holiday Groups Tab on Page 327
11. You can view Controller Status from the apC Controller Status Tab.	apC Controller Status Tab on Page 325
12. You can change the state images that appear in the Monitoring Station to represent this controller on the apC Controller State Images Tab.	apC Controller State Images Tab on Page 330
13. You can view the apC Controller groups to which this apC belongs on the Groups Tab for Hardware Devices on.	Groups Tab for Hardware Devices on Page 28

apC Comm Port Editor

You need to create and configure an apC Comm Port object for your apC to establish communications with C•CURE 9000.

An apC panel can communicate with serial port connections, using RS-232 connections to an RS-485 converter, or via an Ethernet-connected network.

For general instructions about the Hardware pane see Using the Hardware Pane on Page 20.

To Configure an apC Comm Port

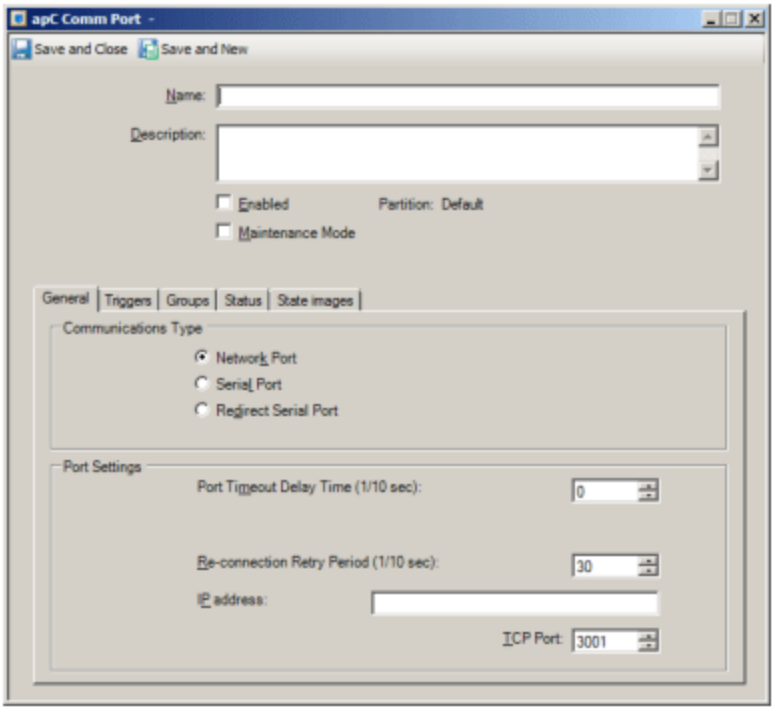
1. To configure an **apC Comm Port**, open the **Hardware Pane**,select the Hardware Folder in which you want the apC Comm Port to reside, and right-click to display the Hardware Folder context menu. Click **apC Comm Port** then click **New**.

Figure 94: Creating an apC Comm Port

The **apC Comm Port** editor appears (see Figure 95 on Page 311). See Table 81 on Page 313 for definitions of the fields on the Comm Port editor General Tab

.

Figure 95: apC Comm Port Editor



You may also choose **New Template**. For further information about creating Templates, see Creating a Template on Page 34.

2. Enter a unique Host Communications Port **Name** (required).
3. Optionally, enter a textual description of the apC Comm Port in the **Description** field.
4. Select the **Enabled** check box if you want the Comm Port online after you have completed the configuration procedure.
5. Select the **Communications Type**.
   - For an apC Controller that uses a network communications path, click **Network Port**. See Configuring an apC Comm Port Network Connection on Page 312.
   - For an apC that uses a serial connection to the C•CURE 9000 server, click **Serial Port**. See Configuring an apC Comm Port Serial Port on Page 312
   - For an apC that uses a redirected serial connection to the C•CURE 9000 server, click **Redirect Serial Port**. See Configuring an apC Comm Port Redirect Serial Port on Page 313.
6. You can set a **Port Timeout Delay Time** in tenths of a second units by typing it within the entry field or by using the selection arrows. The range is 0 through 99; the default entry is 0.
7. When you have completed configuring the apC Comm Port General tab, you can click **Save and Close** to save your changes, or you can click the Triggers tab (see apC Comm Port Triggers Tab on Page 315) to continue configuring the apC Comm port.

Configuring an apC Comm Port Network Connection

To Configure an apC Comm Port Network Connection

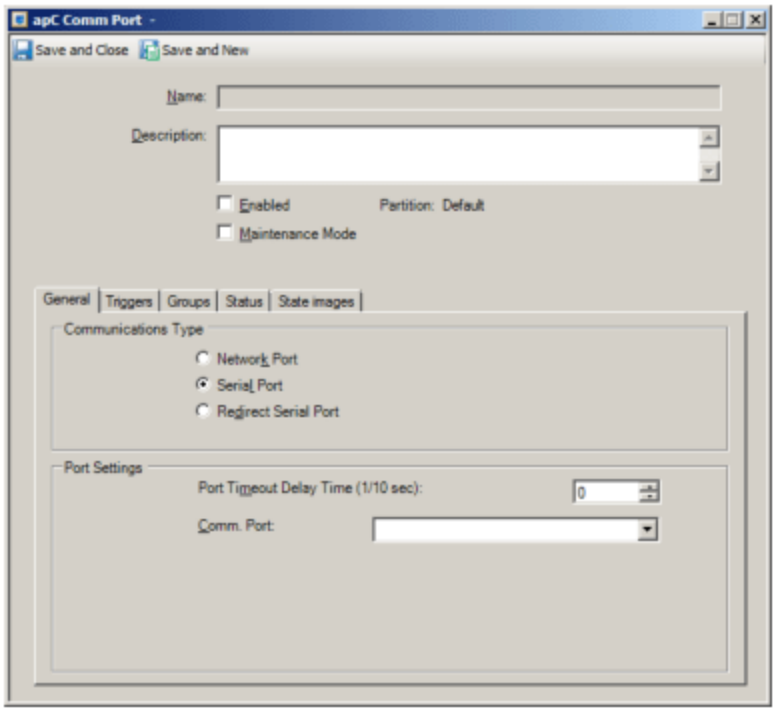
1. Type a unique **IP Address** in the **IP Address** field. This must be the IP Address of the terminal server being used to communicate with the C•CURE 9000 system.
2. Select a **TCP Port**, the address of the node from which the apC Host TCP Port communicates with the C•CURE 9000 system. The values range from 0 through 9999. The default entry is 3001.
3. Select a **Re-connection Retry Period** in tenths of a second units by typing it within the entry field or by using the selection arrows. The values range from 0 through 99. The default entry is 30 (3 seconds).

Configuring an apC Comm Port Serial Port

To Configure an apC Comm Port Serial Port

1. When you choose to configure a **Serial Port**, select the Communications Type **Serial Port** from the drop-down list. The **Name** field will reflect the port number that you select. The range is COM1 through COM256.
2. As in the Network Comm Port, you can set a **Port Timeout Delay Time** in tenths of a second. The range is 0 through 99, the default entry is 0.

Figure 96: apC Comm Port **Editor, Serial Port options**

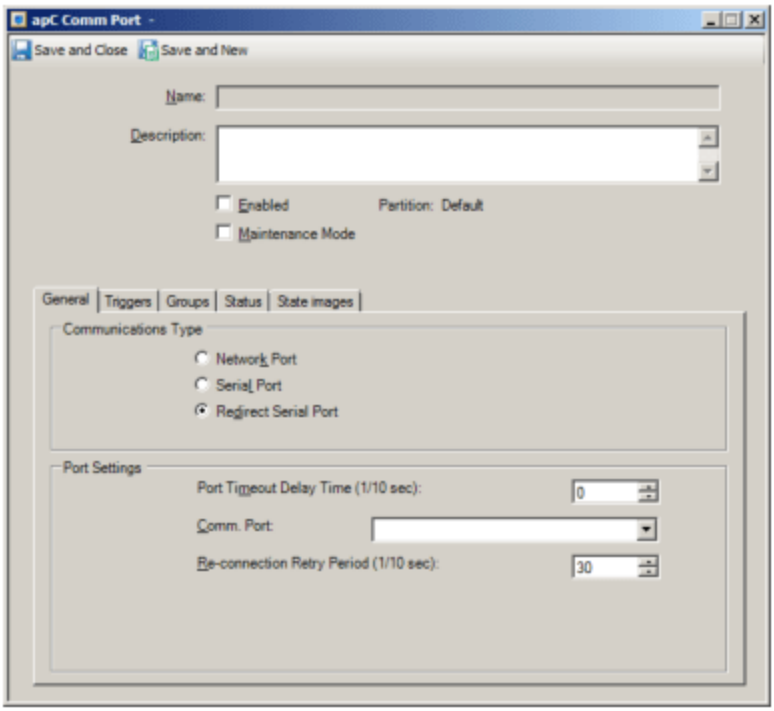


Configuring an apC Comm Port Redirect Serial Port

To Configure a Redirect Serial Port

1. When you choose to configure a **Redirect Serial Port**, select the Communications Type **Redirect Serial Port** button. In the Port Settings box, select a com port from the drop-down list. The **Name** field will reflect the port number that you select. The range is COM1 through COM256.
2. As in the Network Comm Port, you can set a **Port Timeout Delay Time** in tenths of a second. The range is 0 through 99, the default entry is 0.

Figure 97: apC Comm Port Editor, Redirect Serial Port Options



The Fields on the apC Comm Port General tab are described in Table 81 on Page 313.

Table 81: apC Comm Port Field Definitions

Field	Description
Name	Enter a unique name up to 50 characters long for the controller. If you enter the name of an existing object, the system returns an error message indicating there is a conflict.
Description	Enter a textual comment about the controller, such as its location or purpose. This text is for information only.

apC Comm Port Field Definitions (continued)

Field	Description
Enabled	This setting determines whether or not the apC Comm Port is able to provide communication between the apC Controller and the C•CURE 9000 Server. Select **Enabled** to set the Comm Port online. To take the Comm Port offline, you can clear the **Enabled** selection. NOTE: If the apC Comm Port is currently in use by apC controllers, you must disable all of the controllers before you attenpt to take the Comm Port offline. If any apC controllers are enabled when you attempt to take the apC Comm Port offline, an error message is displayed - "Port cannot be disabled with enabled controllers. Please disable controllers first. When the controllers are re-enabled they will do a full personnel download." The message explains that when you re-enable the apC Comm Port, then re-enable the apC controllers, each controller will perform a full personnel download.
Maintenance Mode	Click to put the apC Comm Port into Maintenance Mode. See Chapter 2: Maintenance Mode for more information.
Partition	This read-only field identifies the Partition in which this Controller resides. If you are creating a new Controller, the Partition that is currently the New Object Partition for your Operator account is automatically assigned to each Controller you create. If you want to change the Partition of a Controller, you must move the Cluster in which the Controller resides. See Using Drag and Drop in the Hardware Tree on Page 27.
Communications Type	
Network Port	Select **Network Port** if you are using a terminal server to connect your apC to C•CURE 9000.
Serial Port	Select **Serial Port** if you are using a serial connection for your apC.
Redirect Serial Port	Select **Redirect Serial Port** if you are redirecting the serial connection for an apC to a serial port that is physically on a Terminal Server, but logically on the C•CURE 9000 Server.
Port Settings	
Port Timeout Delay Time (1/10 sec)	The **Port Timeout Delay Time** is the extra interval that the host waits for a response from the apC panel after sending a message to the panel. If the host does not receive a response in the specified time, the host retransmits the message or declares a communications failure. This field allows you to set the timeout delay for all panels that use a specific port.Software House recommends that you set this period to 20 (2 seconds). However, if you require additional delay time because apC panels run on a Digiboard, Equinox board, or over a network, you may need to increase this value. Keep this value as small as possible, or system performance may be affected. If your panel goes into communications failure often, try setting this value between 30 (3 seconds) and 50 (5 seconds).
Re-connection Retry Period (1/10 sec)	**Re-connection Retry Period** is the duration that the host waits to declare an unresponsive panel to be in failure. Software House recommends that you set this period to 300 (30 seconds) which is the default value.
IP Address	The IP address of the terminal server C•CURE 9000 that is being used to communicate with the C•CURE 9000 system.
TCP Port	The address of the node from which the apC Host TCP Port communicates with the C•CURE 9000 system. The values range from 0 through 9999. The default entry is 3001.
Serial Port and Redirect Serial Port Options	

apC Comm Port Field Definitions (continued)

Field	Description
COM Port	Select the Communications Type Serial Port from the drop-down list. The Name field will reflect the port number that you select. The range is COM1 through COM256.

apC Comm Port Triggers Tab

The apC Comm Port Triggers tab allows you to set up Triggers – configured procedures used by C•CURE 9000 to activate specific actions when a particular predefined condition occurs.

This tab provides you with ability to activate an event based on the Comm Status of the apC Comm Port. If the Comm Status property of the apC Comm Port changes, you can specify the event you want to activate.

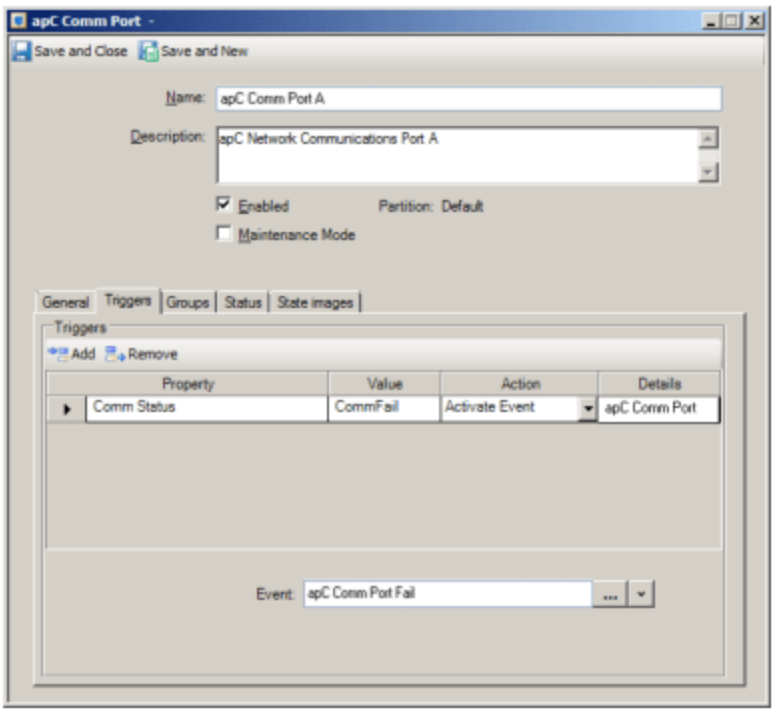
A typical use for a Comm Port trigger would be to warn the Monitoring Station of a communications failure. You can configure an event that would send a message requiring acknowledgment when the apC panels are unable to communicate with the host.

1. Click the apC Comm Port **Triggers** tab to provide a means to link the Comm Port to an event.

   Example:

   A typical use for a Comm Port trigger would be to warn the Monitoring Station of a communications failure. You can configure an event that might send a message requiring acknowledgment when the apC panels are unable to communicate with the host, as shown in Figure 98 on Page 315.

Figure 98: apC Comm Port Triggers Tab



2. Choose a Property for the Trigger from the **Property** drop-down list.

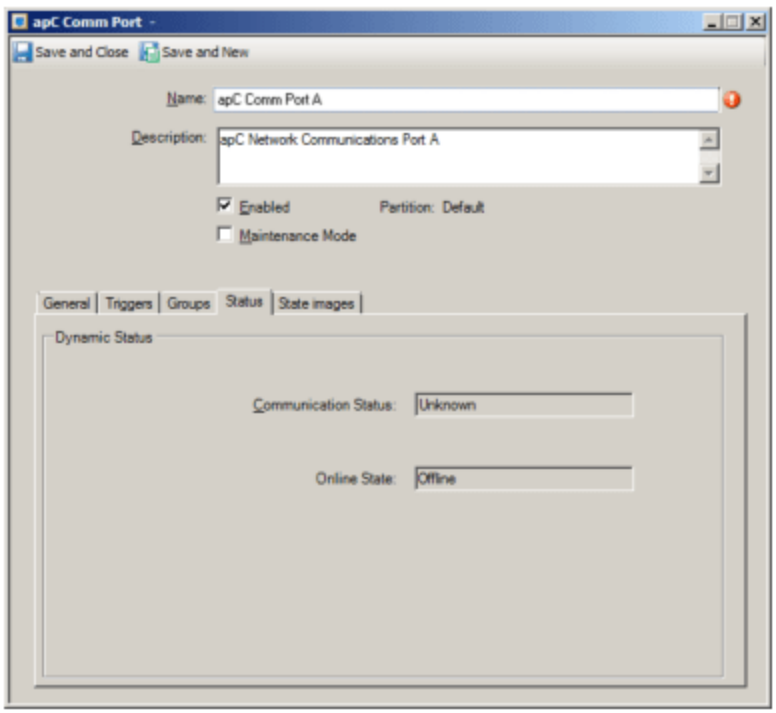
3. Select the value that you want to activate the Trigger from the **Value** drop-down list.
4. Pick the Action you want the Trigger to perform from the Action drop-down list.
5. Depending upon the Action you chose, you may need to select the Action details from the Details field. For example, if you chose to Activate an Event with the Action, you need to select an Event from the Details field. Click [...] and select an Event from the selection box that appears.
6. Click **Save and Close** to save the Trigger settings for the apC Comm Port.

apC Comm Port Status Tab

The Status tab provides a read-only listing of critical information about the operational status of the selected apC Comm Port including:

- **Communications Status** - displays the values Unknown or CommFail.
- **Online Status** - displays the values: Online, Disabled or Offline.

Figure 99: apC Comm Port - Status Tab

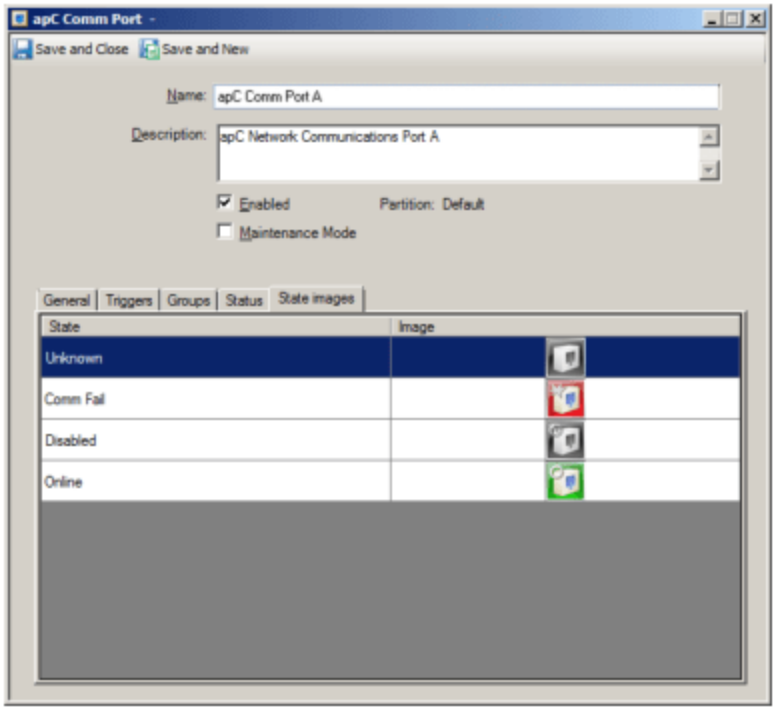


apC Comm Port State Images Tab

The **State Images** tab provides a means to change the default images used to indicate communication port states. These images appear on the Monitoring Station and change according to the state of the object that they represent.

The **apC Comm Port - State Images** tab is shown in Figure 100 on Page 317.

Figure 100: apC Comm Port State Images Tab



To Change a State Image

1. Double-click the existing image. A Windows Open dialog box appears allowing you to browse for a folder in which you have placed replacement images.
2. When you locate the replacement image, select it and click **Open** to add it to the image listing.
3. If you are done editing the apC Comm Port, click **Save and Close** to save the Comm Port's configuration. Alternatively, if you want to save the Comm Port and create a new one, click **Save and New**. The Comm Port Editor remains open to allow you to create a new Comm Port.

To restore the default image, right-click on the new image and select Restore Default.

apC Controller Editor

The apC Controller editor allows you to configure apC, apC/8X, and apC/L panels and their connected Input boards, Output Boards, Readers, Inputs, and Outputs in C•CURE 9000. For more detailed information about the apC panel and its options, see the apC Panel Overview on Page 296.

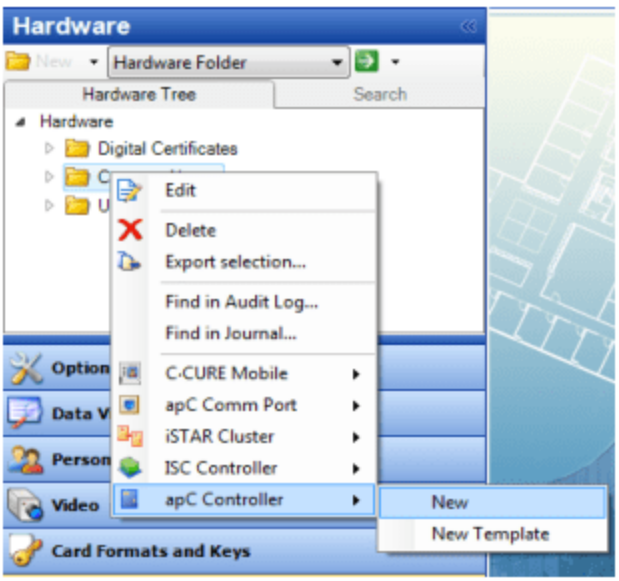
The apC Controller Editor has the following tabs:

- apC Controller General Tab on Page 319
- apC Controller Communications Tab on Page 321
- apC Controller Inputs Tab on Page 322
- apC Controller Outputs Tab on Page 323
- apC Controller Readers Tab on Page 323
- apC Controller Add-On Board Tab on Page 324
- apC Controller Status Tab on Page 325
- apC Controller Triggers Tab on Page 326
- Groups Tab for Hardware Devices on Page 28
- apC Controller Holiday Groups Tab on Page 327
- apC Controller User Defined Fields Tab on Page 329
- apC Controller State Images Tab on Page 330

To Create an apC Controller

1. To configure an apC controller from the C•CURE 9000 Administration **Hardware** pane, select the Hardware folder for which you want to configure an apC Controller and right-click to display the context menu, as shown in Figure 101 on Page 318.

Figure 101: Hardware Pane apC Controller Selection



2. From the **Hardware** context menu, choose **apC Controller** and **New**. The **apC Controller General** tab appears, as shown in Figure 102 on Page 319.

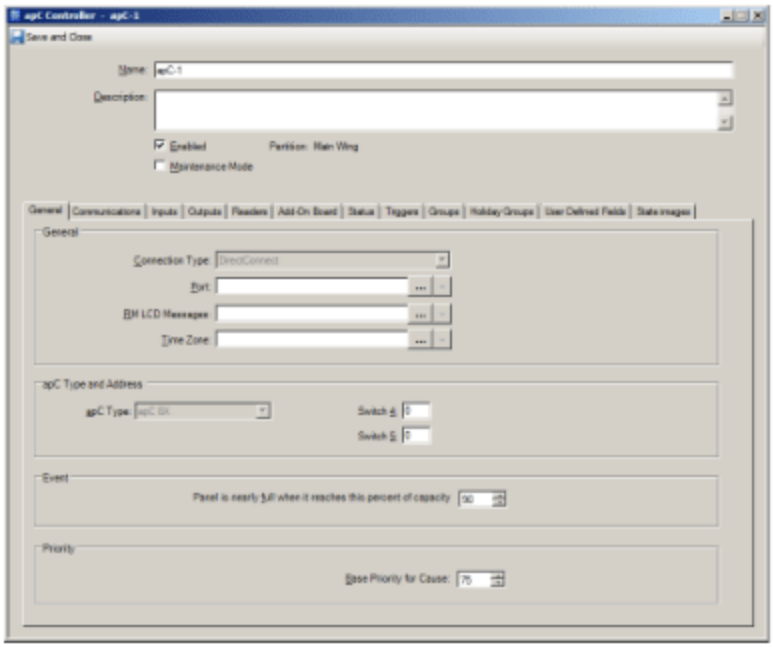
   You may also choose **New Template**. For further information about creating Templates, see Templates on Page 34.

   If the **New** and **New Template** selections are unavailable, you may be trying to create an apC in a Partition that is not your New Object Partition, or you do not have Privileges to create objects in this Partition. Check the C•CURE 9000 Menus to verify that your New Object Partition setting is correct, and check with your C•CURE 9000 administrator that you have the correct Privileges.

apC Controller General Tab

The apC Controller General tab provides a means to select the Communications Port, RM LCD Messages, and to identify the apC panel type.

Figure 102: apC Controller GeneralTab



To Configure the apC Controller General Tab

1. In the **apC Controller** General tab, type a unique controller **Name** and a corresponding **Description** (optional) in the identification fields at the top of the **apC Controller** dialog box.
2. **Maintenance Mode** - Click to put the apC Controller and/or its components into Maintenance Mode. See Chapter 2: Maintenance Mode for more information.
3. Click the **Enabled** check box when you are ready for the apC to establish communications with the C•CURE 9000 server. **You should wait** until you have configured the controller settings and some or all of the Inputs, Outputs, and Readers before enabling the apC.

NOTE The apC Comm Port you choose in Step 5 must also be Enabled; otherwise, the apC cannot remain enabled. If you save the apC controller after assigning a disabled apC Comm Port, the apC will go offline and when you open the apC object again in the apC editor, the **Enabled** check box will no longer be checked.

4. Select **Direct Connect** as the type of connection between the host and the apC. Use the **Port** field in this dialog box to specify a port to which the apC chain is connected.
5. To select a host communications Port for the apC controller, click ... in the **Port** field to select an **apC Comm Port**.

   NOTE Software House strongly recommends that you select an apC comm port that is in the same partition as your apC.

   The example in Figure 102 on Page 319 shows the selection of a Serial Port connection.
6. To select a particular customized set of LCD messages for the RM Readers, click ... to display a Reader LCD Message Set selection list. If you leave this field blank (the default), the Readers use the default messages.
7. Select the **Time Zone** in which your apC panel resides by clicking ... and selecting the Time Zone from the list that appears. If you leave this field blank, the apC panel Time Zone defaults to the C•CURE 9000 server setting. You can only change the value of the apC controller Time Zone when the apC Controller is not enabled (**Enabled** field is blank ☐). See Changing the Time Zone of an apC Controller on Page 303.
8. Select the type of apC panel you are configuring from the **apC Type and Address** box:
   - **apC**
   - **apC/8X**
   - **apC/L**
9. Rotary switch settings can also be set on the apC panels using the two **Switch** entry fields.

   For apC/L panels, the rotary switches are labeled **3-8** and **1**. For all the other apC types, switches **4** and **5** are displayed. The range of settings is 0 through 9 or A through F for all but **Switch 3-8**, which has a range of 0 or 1.

   The values you enter for **Switch 4**, **Switch 5**, **Switch 1**, and **Switch 3-8** should match the switch settings on the physical apC controller.
10. The **Panel is nearly full when it reaches the percent of capacity** field allows you to enter a range from 0% to 99%.
11. The final entry field on the apC Controller - General tab is in the Priority box. Select a numeric value to assign a **Base Priority for Cause**. The range is from 0 to 255.

    When configuring an Event, you can assign an Event Priority. The Event Priority allows you to rank the importance of a particular Event relative to other Events in the system. If Events occur simultaneously, Event Priorities enable the system to execute responses in the proper sequence.
    C•CURE 9000 provides eight priority ranges, each containing 25 priority settings, for a total of 200 possible Event Priorities.
12. Click the **Communications** tab to display it, as shown in Figure 103 on Page 321.

    You can also click **Save and Close** to return to the **Hardware Pane** and finish the **apC Controller** configuration later.

apC Controller Communications Tab

To Configure the apC Panel Communications Tab

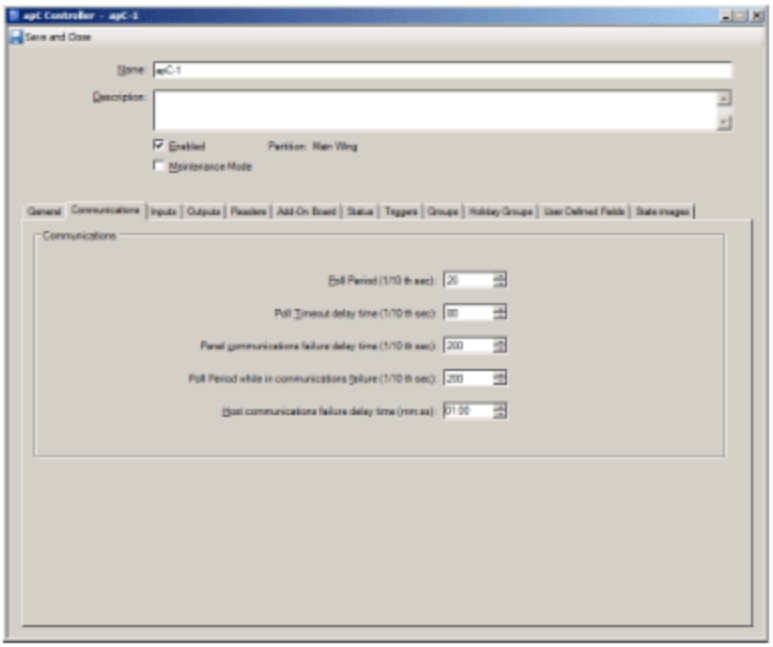
1. In the **Communications** tab, as shown in Figure 103 on Page 321 enter the period in tenths of a second that the panel driver (on the Server) attempts to communicate with this panel in the **Poll Period** field. For example, if you enter 10, the panel driver communicates with this panel a minimum of once per second.

   You can set different poll periods for each panel that you configure. This field is not available when **Dialup** is selected in the **Connection Type** list box.

   Software House recommends that you set the poll period to 20 (2 seconds). Setting this value lower than 20 causes the host to receive activity from the panel more quickly but could cause the driver to interfere with other programs running on the server at larger installations. This is especially true if the panel is on a network port. The range is 0 - 850.

NOTE Setting the poll period to more than 30 will result in up to a 3 or 4 seconds delay between reading the card and opening the door.

Figure 103: apC Controller - Communications Tab



2. Enter the extra interval in tenths of a second that the host waits for a response from this panel after sending a message to the panel in the **Poll Timeout delay time** field. If the host does not receive a response in the specified time, the host retransmits the message or declares a communications failure.

   Software House recommends that you set this period to 80 (8 seconds). However, if you require additional delay time because the panel runs on a Digiboard, Equinox board, or over a network, you may need to increase this value. Keep this value as small as possible, or system performance may be affected. If your panel goes into communications failure often, try setting this value between 80 to 110. The range is 0 - 999.

3. Enter the interval in tenths of a second that the host waits to declare an unresponsive panel to be in failure in the **Panel communications failure delay time**. A message appears on the **Monitoring Station** in the case of a panel failure.

   Software House recommends that you set this period to 200 (20 seconds). The range is 0 - 850.

4. Enter the interval in tenths of a second that the system polls the panel while it is in communications failure in the **Poll period while in communications failure** entry field. Typically, you should set this value higher than the value for the initial poll period to avoid slowing down polling of other units on the chain.

   Software House recommends that you set this period to 200 (20 seconds). The range is 0 - 999.

5. Enter the time period in minutes and seconds (mm:ss format) that the panel waits for a message from the host after receiving the communications failure message from the host in the **Host communications failure delay time** entry field. If the panel does not receive a message in the specified time, the panel declares a communications failure.

   Software House recommends that you set this period to 30 seconds.

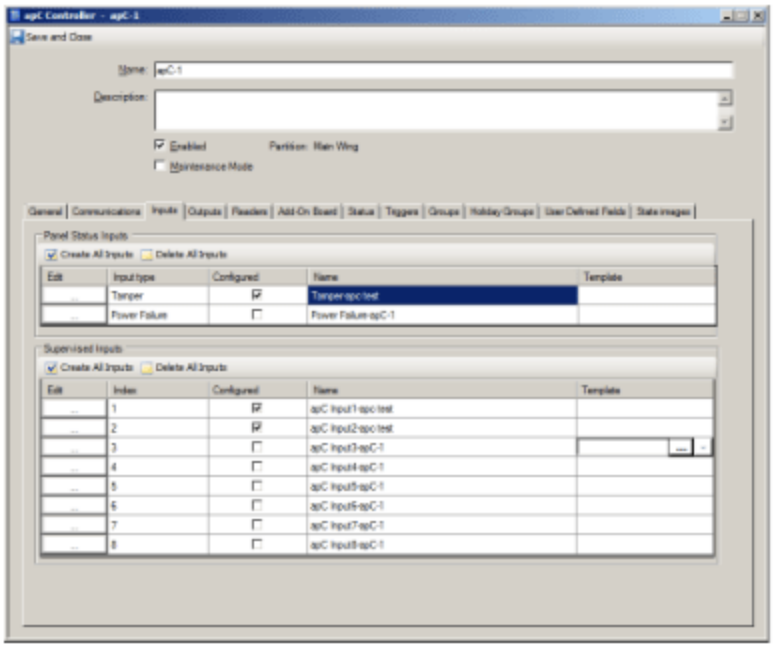
6. Click the **Inputs** tab to display it, as shown in Figure 104 on Page 322.

apC Controller Inputs Tab

To Configure apC Controller Inputs

To configure **Inputs**, select the check box in the **Configured** column (see Figure 104 on Page 322) and click [...] located in the **Edit** column to display the apC Input editor General tab. See the apC Input Editor on Page 332.

Figure 104: apC Controller Inputs Tab



NOTE Click the **Delete All** check box where ever it appears and then click **Save and Close** if you want to eliminate all the Inputs, Outputs, or Readers that you have configured in a given dialog box.

To take an apC panel offline, remove the check from the **Enabled** option check box located below each **Reader**, **Input**, or **Output** board **Description** entry field (located in General tabs).

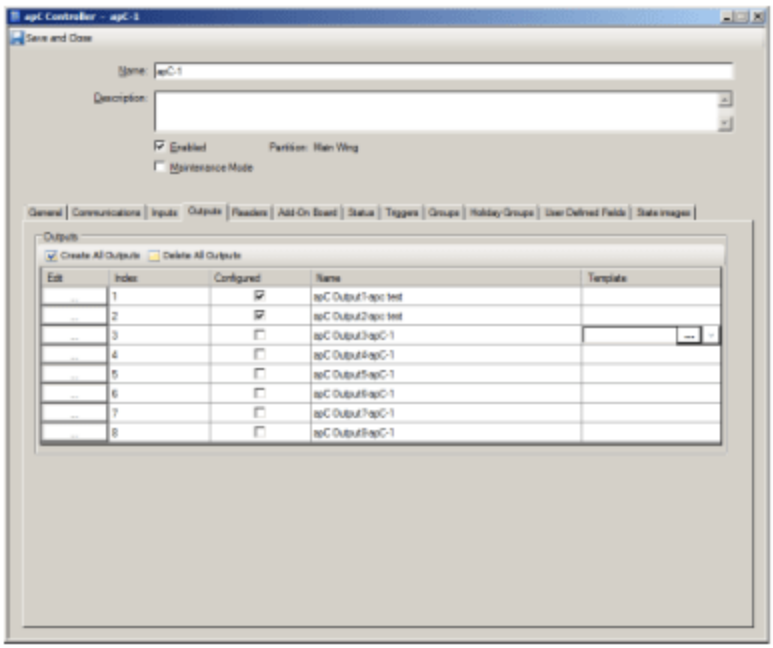
TIP Use the Template column to quickly configure all in a particular set of inputs, outputs or readers.

apC Controller Outputs Tab

To Configure apC Outputs

1. To configure **Outputs**, select the check box in the **Configured** column in the **apC Outputs** tab.
2. Click [...] located in the **Edit** column to display the apC Output Board General tab.
3. Use the apC Output editor to configure the output (See apC Output Editor on Page 336)

Figure 105: apC Controller Outputs Tab



apC Controller Readers Tab

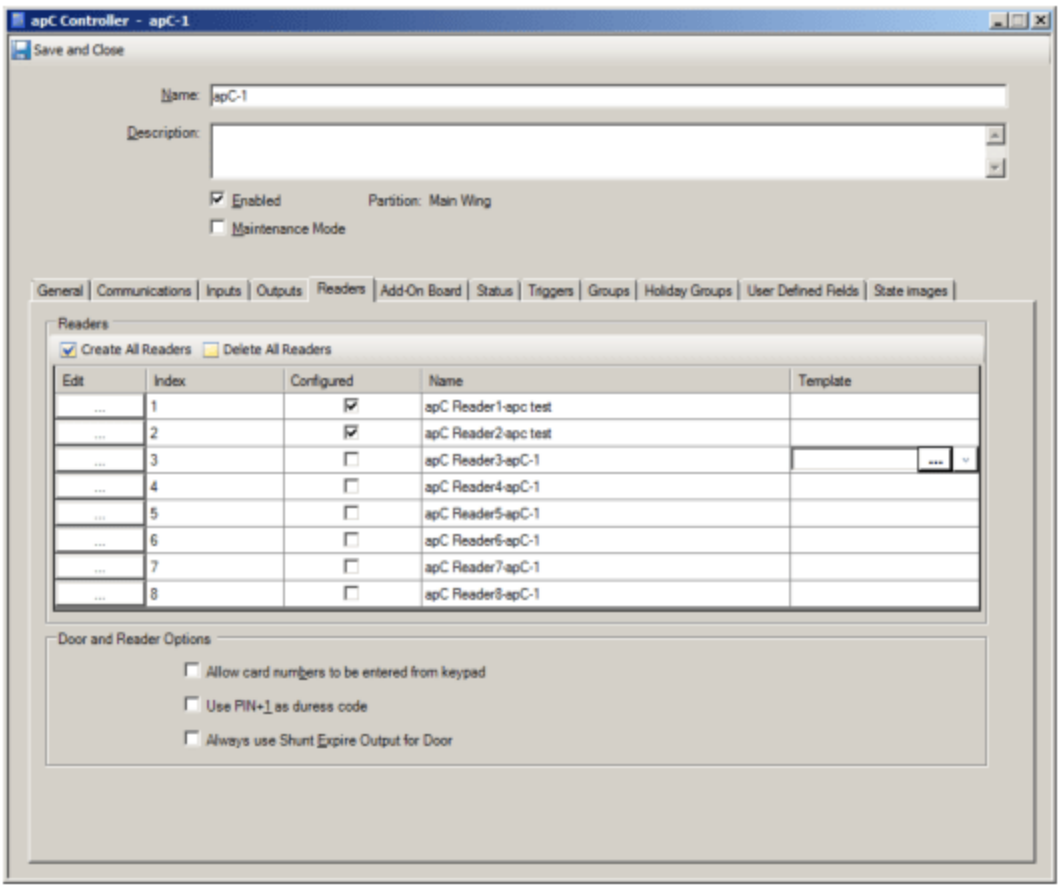
The apC Controller Readers tab, shown in Figure 106 on Page 324, allows you to configure devices that supply Wiegand, magnetic stripe and proximity card signaling.

To Configure an apC Reader

1. Select the check box in the **Configured** column for the **apC Reader** (Index 1 through 8) you want to configure.

2. Click [...] located in the **Edit** column to open the **apC Readers General** tab(see apC Reader General Tab on Page 340).
3. Choose either of the following options for all readers on the Readers tab:
   - **Allow card numbers to be entered from the keypad**.
   - **Use PIN+1 as duress code**.
   - **Always use Shunt Expire Output on Door**

Figure 106: apC Controller ReadersTab



NOTE You may configure an apC Reader from the apC panel Readers tab or from the Add-on Board tab. A reader index configured on one tab will be unavailable on the other tab. The location chosen will affect the possible reader type and reader input/output option selection.

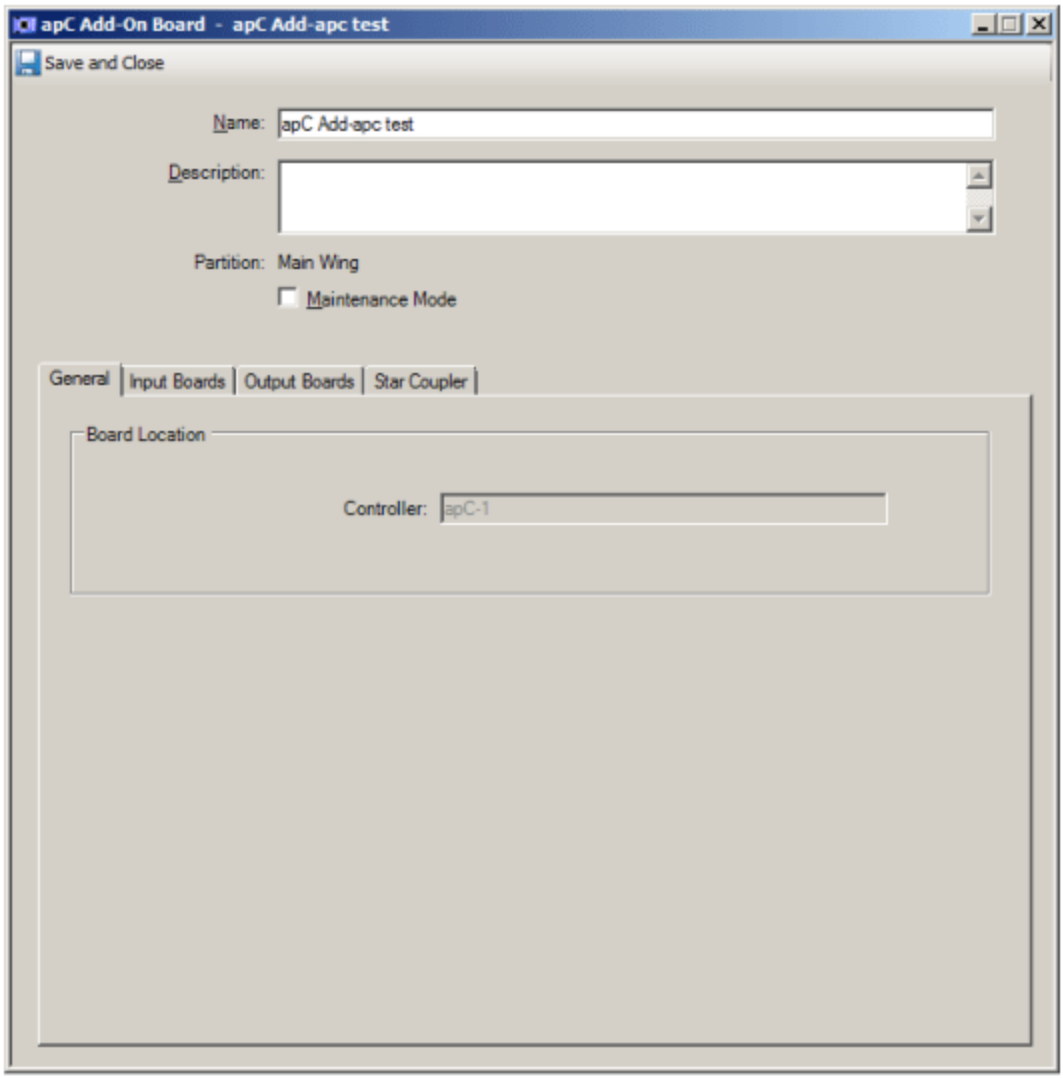
apC Controller Add-On Board Tab

The **Add-On Board** tab, as shown in Figure 107 on Page 325, provides a means to expand the capabilities of the apC panels. Expansion boards can add reader ports, supervised inputs and additional outputs.

To Configure Add-On Boards Using the apC Add-On Board Tab

To start the configuration of **Add-On Boards**, select the check box in the **Configured** column in the **apC Add-On Board** tab and click [...] located in the **Edit** column to display the **apC Add-On BoardGeneral** tab (see apC Add-on Board Editor on Page 347).

Figure 107: apC Controller Add-On Board Tab



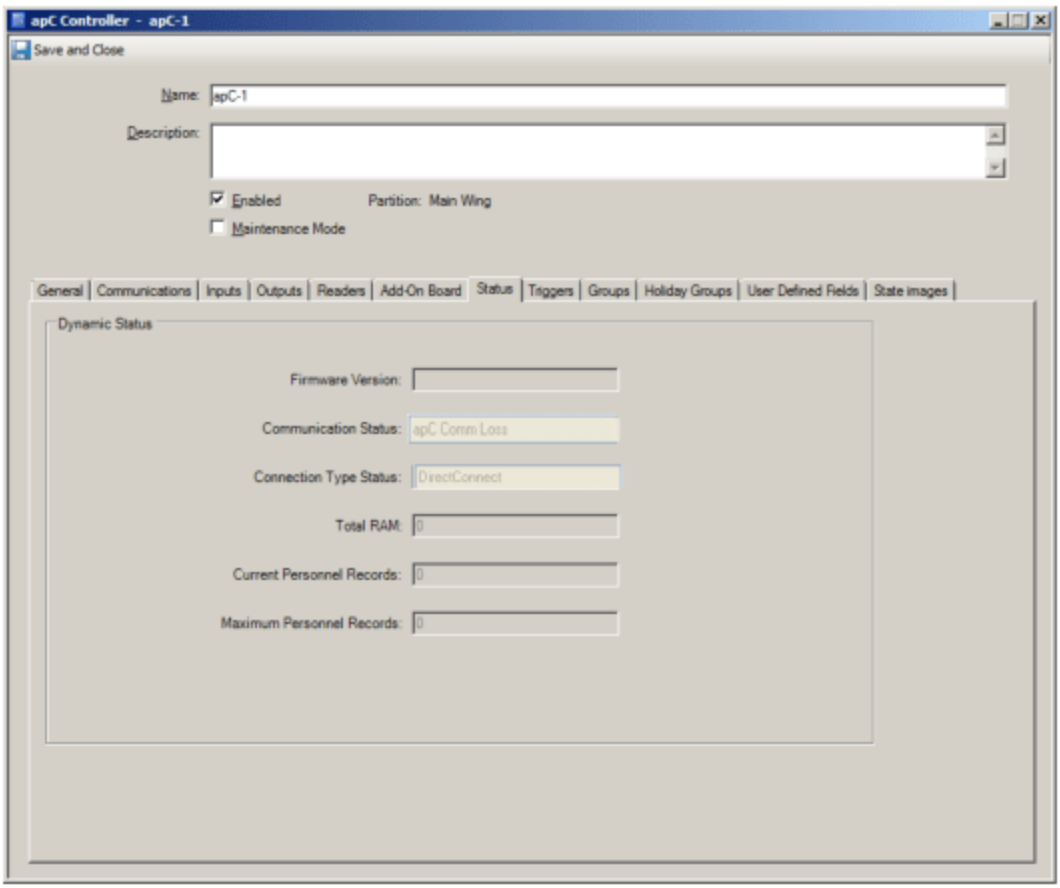
apC Controller Status Tab

The Status tab, as shown in Figure 108 on Page 326, provides a read-only listing of critical information about the operational status of the selected apC Controller including:

- **Online Status** - indicates whether the controller is online and communicating with the system.
- **Firmware Version** - the version of the firmware used by the controller.

- **Communications Status** - displays the values Unknown, CommFail, Comm. Normal, Comm. Loss, Comm. Password Fail, Firmware Download, Card Download, Comm. Tamper, Comm. Power Fail or Comm. Battery Low.
- **Connection Type Status** - displays the values: Unknown, Conn. Normal, Conn. Direct, Conn. Dialup, Conn. Dialing, Conn. Disconnected, or Conn. Connected.
- **Current Personnel Records** - displays the number of records.
- **Panel state status** – displays the values Unknown, Panel Normal, Panel Tamper, Panel Power Failure, Configuration Download, Full Personnel Download, Full Download, Database Backup or Panel Battery Low.

Figure 108: apC Controller Status tab



apC Controller Triggers Tab

See the following for information on apC Triggers:

- Triggers Tab for apC Devices on Page 369.
- Defining a Trigger for an apC Device on Page 370.
- Removing a Trigger on Page 272.

You can click **Save and Close** after configuring apC triggers, or navigate to the Status tab.

apC Controller Holiday Groups Tab

A Holiday is a day or set of days that you configure to allow scheduling access control variations to time-based events and to vary the normal lock and unlock time specifications.

You can include a Holiday in a Holiday Group and assign a Holiday Group to a schedule.

You need to configure the Holiday Groups that should apply to each apC, so that schedules on that apC respect the correct Holidays. If a Holiday Group is not listed on this tab, the Holidays it contains are not applied to this apC.

NOTE Holiday Groups were called Holiday Lists in C•CURE 800/8000.

If a schedule downloaded to the apC has a Holiday Group assigned, and that Holiday Group is listed on this tab, the activation times in the Holiday Group are evaluated. If the schedule is active and one of the Holidays in the Holiday Group is active, the start time and end time assigned with the Holiday Group become the schedule's start time and end time.

For more information about apC Holiday Groups, see the *C•CURE 9000 Software Configuration Guide*.

To use the Holiday Groups tab, see Configuring Holiday Groups for an apC Panel on Page 327 for more information.

Configuring Holiday Groups for an apC Panel

You can download any holiday Group to an apC panel from the **Holiday Group Configuration** dialog box.

A Holiday Group downloaded to an apC panel acts as an override to prevent activation of normally scheduled clearances on the Holidays defined in the Holiday Group. You can configure up to 8 holiday groups for each apC panel.

Only Holiday Groups that are downloaded to an apC panel will affect access control at that panel.

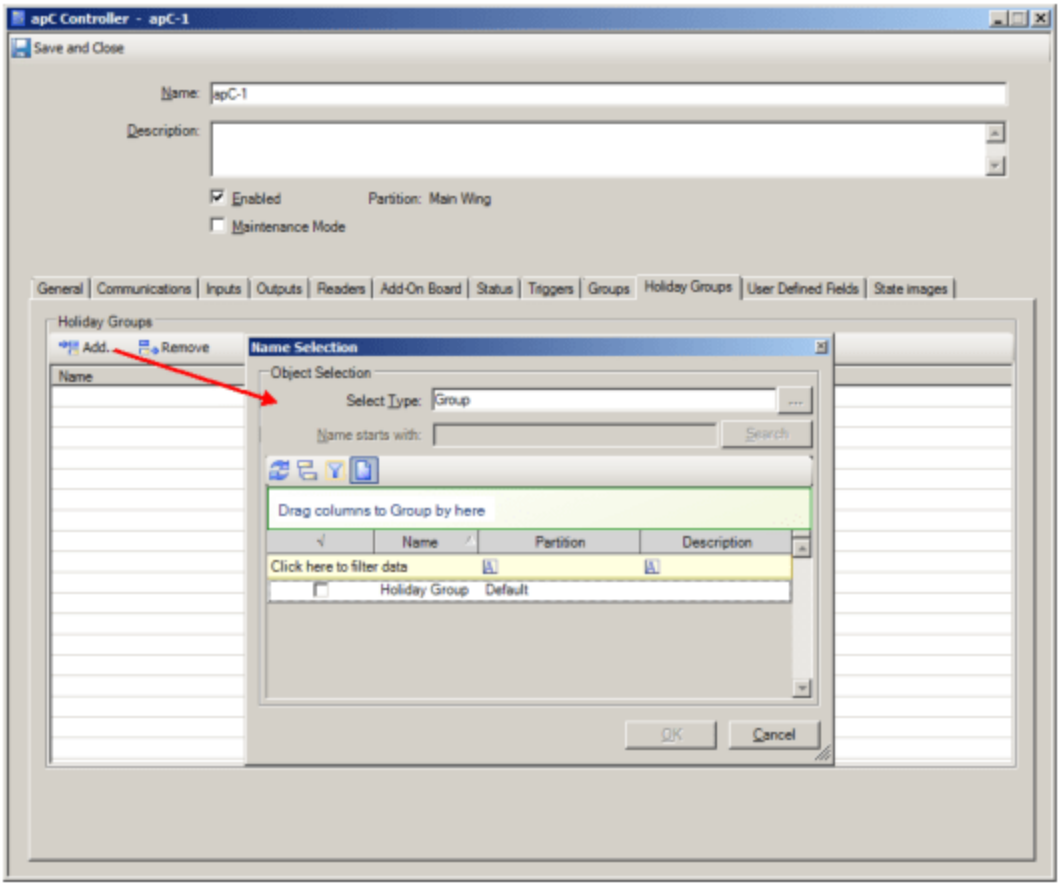
To Select Holiday Groups for the Panel

1. On the **Holiday Groups** tab of the **apC Controller** dialog box, click the **Add** button.

   The **Group** selection box appears allowing you to choose the Holiday Groups that you have configured, as shown in Figure 109 on Page 328.

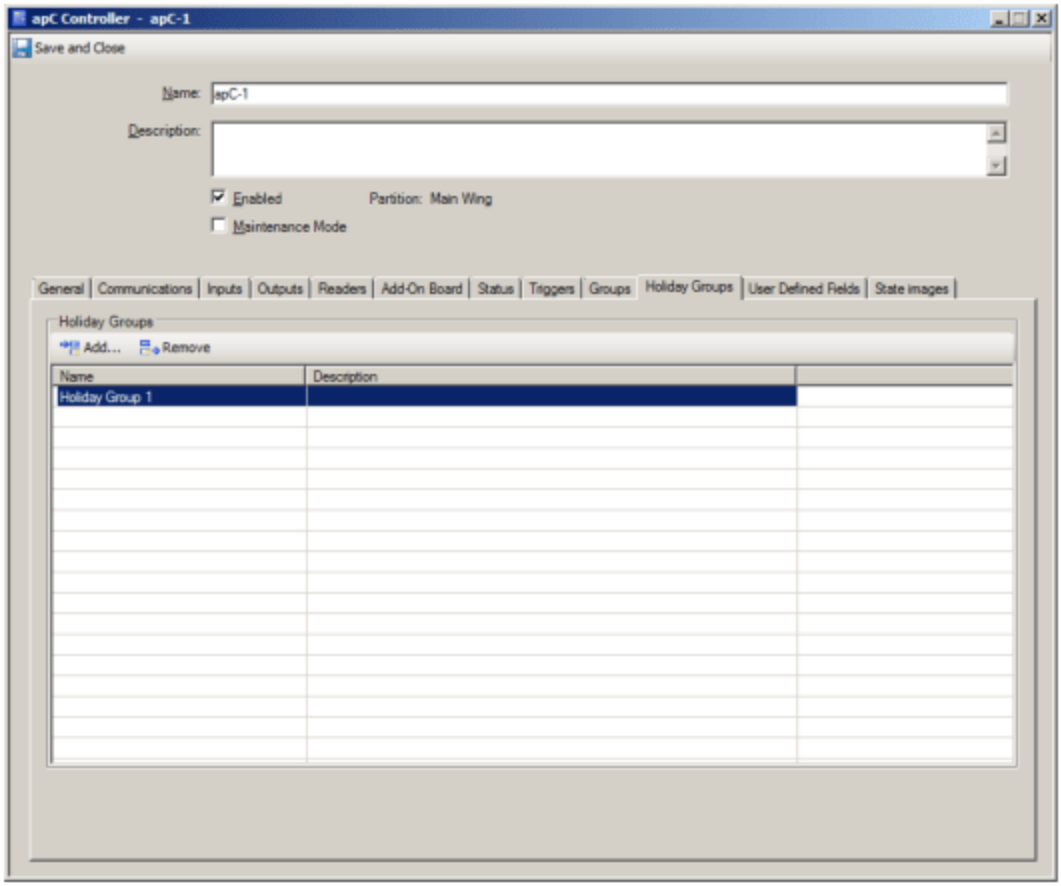
2. For each Group that you want to download to the apC panel, click that Holiday Group in the Group box and click **OK** to add it to the **Holiday Group(s)** box. You can select more than one Holiday Group when you click the Control (Ctrl) key as you select the available Holiday Group.

Figure 109: apC Controller Holiday Groups Tab



3. Click **OK** to save add the selected Holiday Groups.
4. A selected Holiday Group appears in the **Holiday Group(s)** box, as shown in Figure 110 on Page 329.

Figure 110: apC Controller HolidayGroups Tab



5. To remove one or more Holiday Groups, click a Holiday Group to select it (use **CTRL+Left-click** to select multiple Groups), then click **Remove** to remove the selected **Holiday Groups** from the panel.
6. Click the **State Images** tab to display it, as shown in Figure 111 on Page 331.

   - Or -

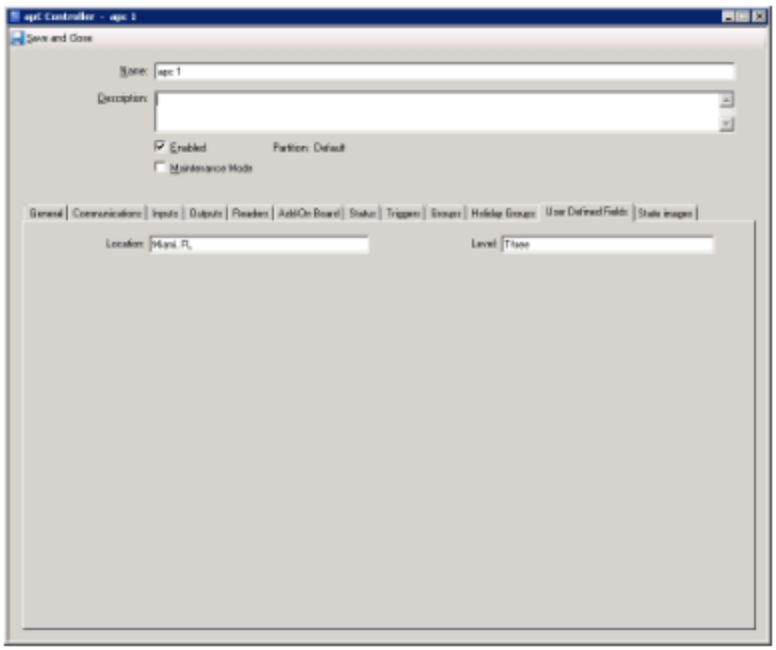
   Click **Save and Close** to return to the **Hardware Pane** to finish the **apC Controller** configuration.

apC Controller User Defined Fields Tab

The User Defined Fields tab, shown in Figure 1 on Page 330, displays user-defined fields in the system for hardware. User-defined fields are configured in the **Configuration** pane. If there are no user-defined fields configured, then the tab is empty.

See the *C•CURE 9000 Software Configuration Guide* for more information.

Figure 1: apC User Defined Tab



apC Controller State Images Tab

The apC Controller **State Images** tab provides a means to change the default images used to indicate controller states (see Figure 111 on Page 331). These images appear on the Monitoring Station and change according to the state of the object that they represent.

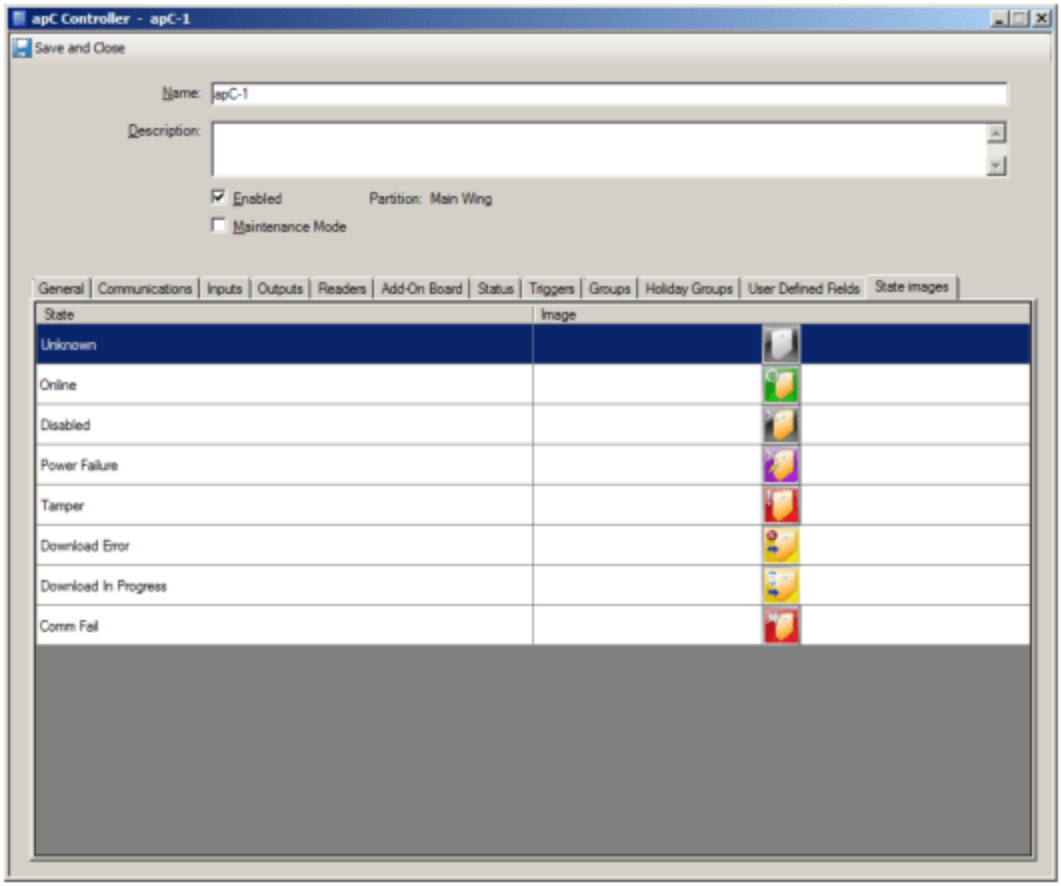
To Change an Image

1. Double-click the existing image.

   A **Windows Open** dialog box appears allowing you to browse for a folder in which you have placed replacement images.

2. When you locate the replacement image, select it to add it to the image listing.
3. To restore the default image, right-click on the new image and select **Restore Default**.
4. Click **Save and Close** to finish the **apC Controller** configuration and return to the **Hardware Pane**.

Figure 111: apC Controller State Images Tab



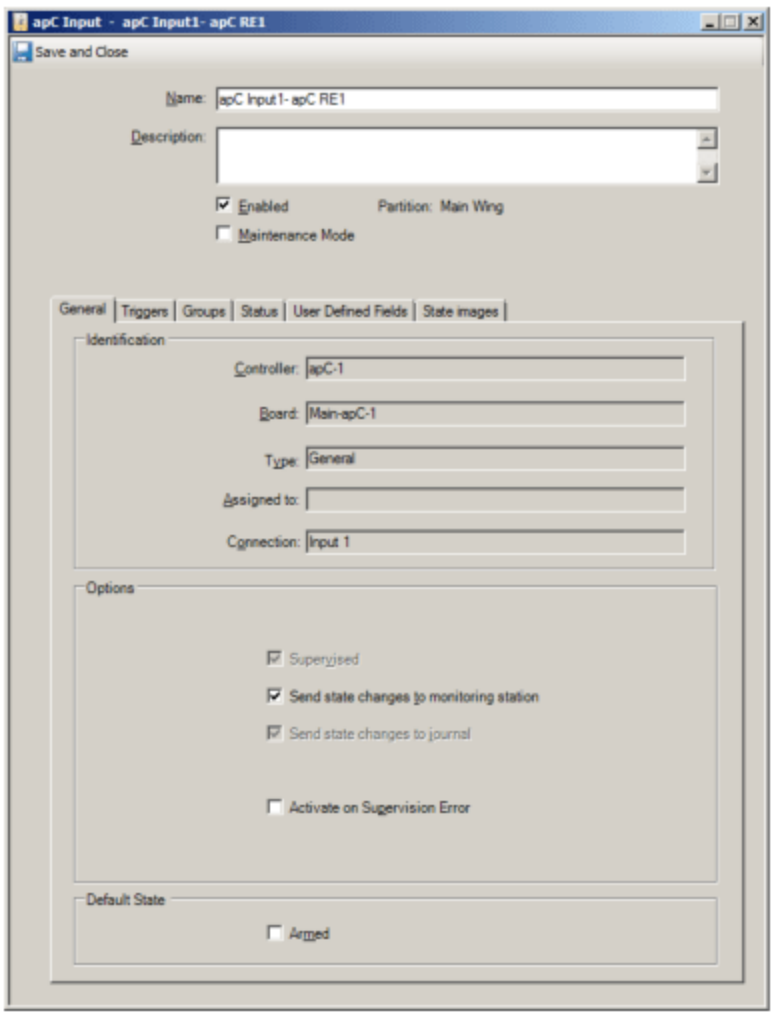
apC Input Editor

The apC Input Editor is used to configure apC Inputs that you have created on the apC Controller Inputs tab.

apC Input General Tab

The apC Input - General Tab, shown in Figure 112 on Page 332, displays five read-only the **Identification** fields. The apC Controller name is shown in the **Controller** field and the Input Board in the **Board** field.

Figure 112: apC Controller Inputs - General Tab



The following Input fields are read-only:

Type - reflects whether the Input has been assigned to a Door or other object or has a special purpose. These include:

- Tamper
- Comm Fail
- General

Assigned To - displays the name of an associated Door or Elevator Button. If the Input is used for a door, then the Name field is read-only displaying the name of the controlled door.

Connection - specifies the input connection point on the Input Board and is assigned when the Board is configured.

To Configure the apC Inputs General Tab

1. When the **Supervised** check box is selected, this read-only field indicates that the panel supports input supervision.

   NOTE The Supervised check box must be selected for Proprietary Burglar Alarm applications.

2. To have a notification of changes in state of the Input sent to the guard station, select the **Send state changes to the monitoring station** check box.

   NOTE The **Send state changes to the monitoring station** option must be selected for Proprietary Burglar Alarm applications.

3. To have a notification of changes in state of the Input sent to the journal, select the **Send state changes to journal** check box. This option will be selected by default.

   NOTE You may limit the transmission of state change messages to the journal exclusively, when you click to de-select the **Send state changes to the monitoring station** option and instead, select the **Send state changes to journal** option. Use of the latter option can decrease the messaging traffic derived from the apC Input during normal operations. To further limit messaging, you may also leave both check boxes unselected.

   You may select multiple Inputs in a dynamic view and use the **Set Property** option to limit the transmission of state changes. See Using Set Property for an iSTAR Controller on Page 130, for more information.

4. **Activate on Supervision Error** – Select this check box if the input is supervised and you want it to activate when a supervision error occurs.
5. Click **Save and Close** or the **Triggers** tab to display it, as shown in on Page 333.

apC Input Board Triggers Tab

The **Triggers** tab, shown in Figure 140 on Page 369, allows you to set up **Triggers**, configured procedures used by C•CURE 9000 to activate specific actions when a particular predefined condition occurs.

See the following for information on apC Triggers:

- Triggers Tab for apC Devices on Page 369.

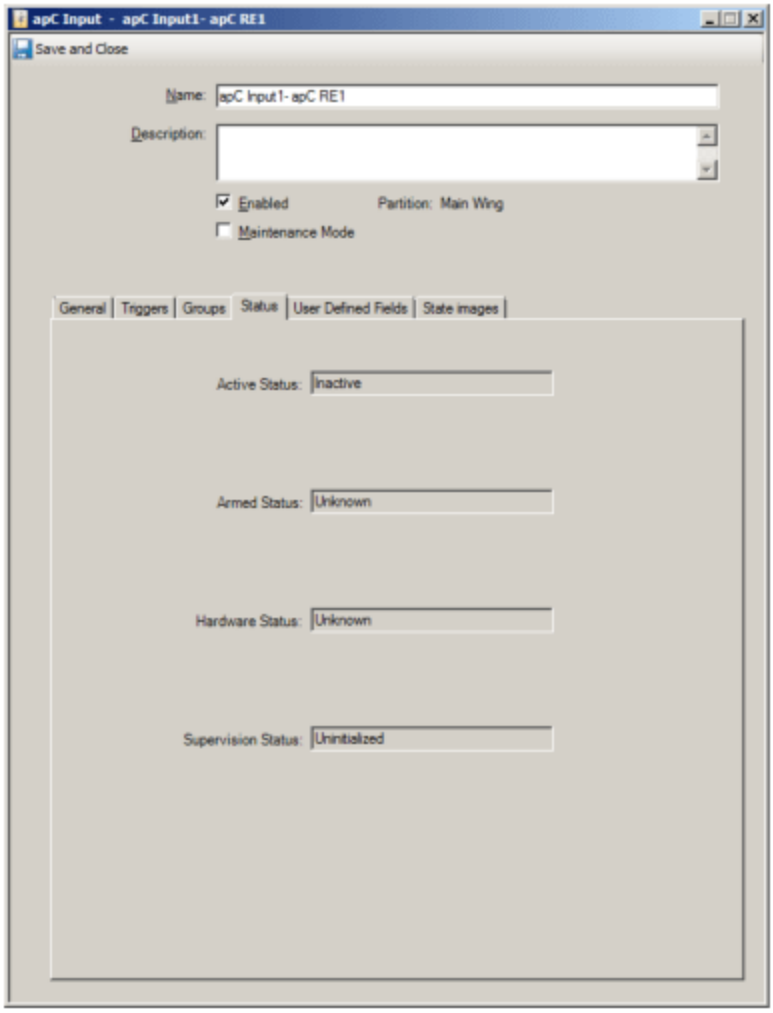
- Defining a Trigger for an apC Device on Page 370.
- Removing a Trigger on Page 272

apC Input Board - Status Tab

The Status tab provides a read-only listing of critical information about the operational status of the selected apC Input including:

- **Active Status** - displays the values Active or Inactive.
- **Armed Status** - displays the values Armed or Disarmed.
- **Hardware Status** - displays the values: Secure, Active, Open Loop, Shorted Loop, or Fault.
- **Supervision Status** - displays the values: Un-initialized (not in supervision error), Open Loop, Shorted Loop, or Fault.

Figure 113: apC Boards Inputs Status Tab



apC Inputs State Images Tab

The apC Inputs **State Images** tab provides a means to change the default images used to indicate input states (see Figure 114 on Page 335). These images appear on the Monitoring Station and change according to the state of the object that they represent.

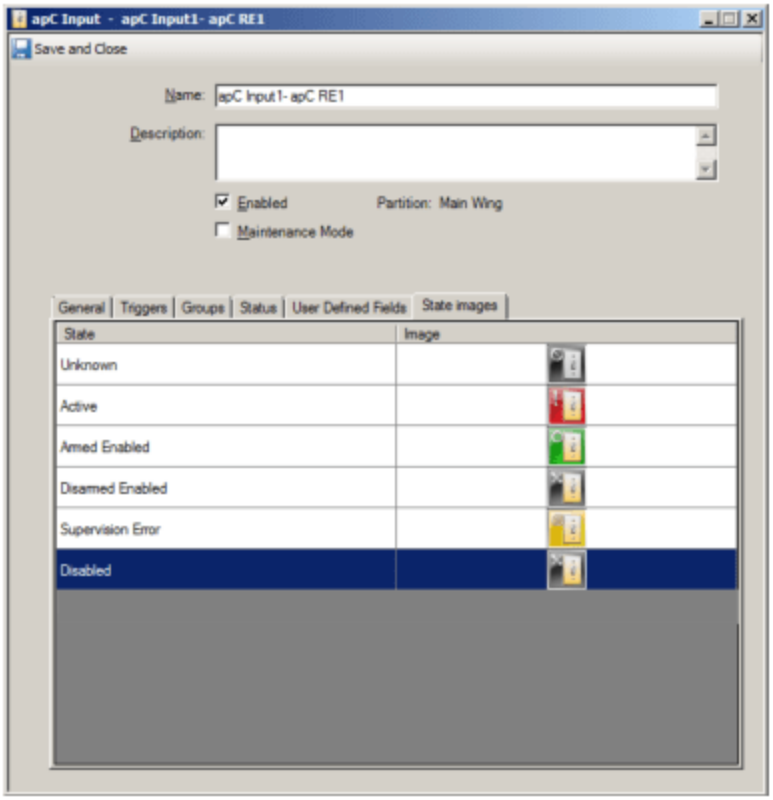
To Change an Image

1. Double-click the existing image.

   A Windows **Open** dialog box appears allowing you to browse for a folder in which you have placed replacement images.

2. When you locate the replacement image, select it to add it to the image listing.
3. To restore the default image, right-click on the new image and select **Restore Default**.

Figure 114: apC Boards Inputs State Images Tab



4. Click **Save and Close**.

apC Output Editor

The apC Output Editor is used to configure apC Outputs that you have created on the apC Controller Outputs tab.

- apC Output General Tab on Page 336
- Groups Tab for Hardware Devices on Page 28
- apC Output Status Tab on Page 337
- apC Output State Images Tab on Page 338

apC Output General Tab

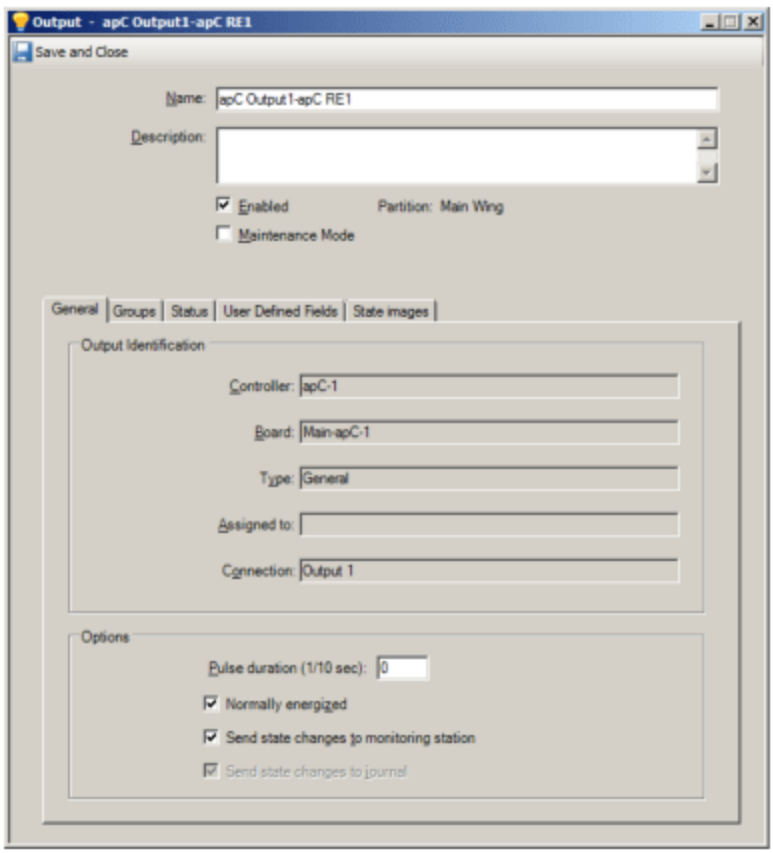
To Configure Outputs Using the apC Output General Tab

The **apC Output General** tab lists the following read-only fields:

Type - reflects whether the Output has been assigned to a Door or other object. For apC panels, General is the un assigned output type.

Assigned To - displays the Elevator or Door object name. For any Output, the **Connection** field indicates the index number on the board.

Figure 115: apC Controller Outputs General Tab



1. The following **Options** are configurable for an Output:

a. **Pulse Duration** – (momentary activation) is entered in tenths of a second intervals with a default of 0 seconds. The range is 0 to 1000.

b. **Normally Energized** – When checked, the output is energized (power is supplied to the relay) when it is inactive. When the output is activated, power is removed.

c. To have a notification of changes in state of the Output sent to the Monitoring station, select the **Send state changes to the monitoring station** check box. This selection is unavailable for an apC Door Output. State changes for a Door Output are not sent to the Monitoring Station.

d. To have a notification of changes in state of the Output sent to the journal, select the **Send state changes to journal** check box. This option is selected by default. This selection is unavailable for an apC Door Output. State changes for a Door Output are not sent to the journal.

NOTE

You may limit the transmission of state change messages to the journal exclusively, when you click to de-select the **Send state changes to the monitoring station** option and instead, select the **Send state changes to journal** option. Use of the latter option can decrease the messaging traffic derived from the apC Output during normal operations. To further limit messaging, you may also leave both check boxes unselected.

You may select multiple Outputs in a dynamic view and use the **Set Property** option to limit the transmission of state changes. See Using Set Property for an iSTAR Controller on Page 130, for more information.

2. Click **Save and Close** or the **apC Outputs - Status** tab to display it, as shown in Figure 116 on Page 338.

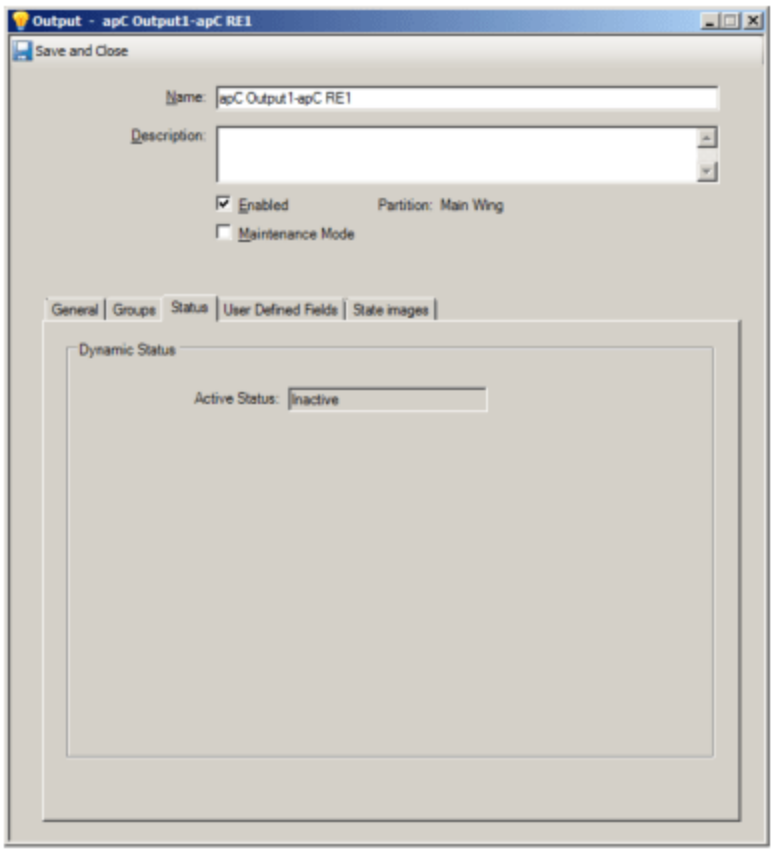
   For further information about the use of the **Groups** tab, see Groups Tab for Hardware Devices on Page 28.

apC Output Status Tab

The Status tab (see Figure 116 on Page 338 provides a read-only listing of critical information about the operational status of the selected apC Board Output including:

- **Active Status** - displays the values Active or Inactive.
- **Active State** - displays Unknown.
- **Mode** - displays Unknown
- **Active Reason** - displays Unknown

Figure 116: apC Outputs Status Tab



apC Output State Images Tab

The **State Images** tab provides a means to change the default images used to indicate output states. These images appear on the Monitoring Station and change according to the state of the object that they represent.

The **apC Output State Images** tab is shown in Figure 117 on Page 339.

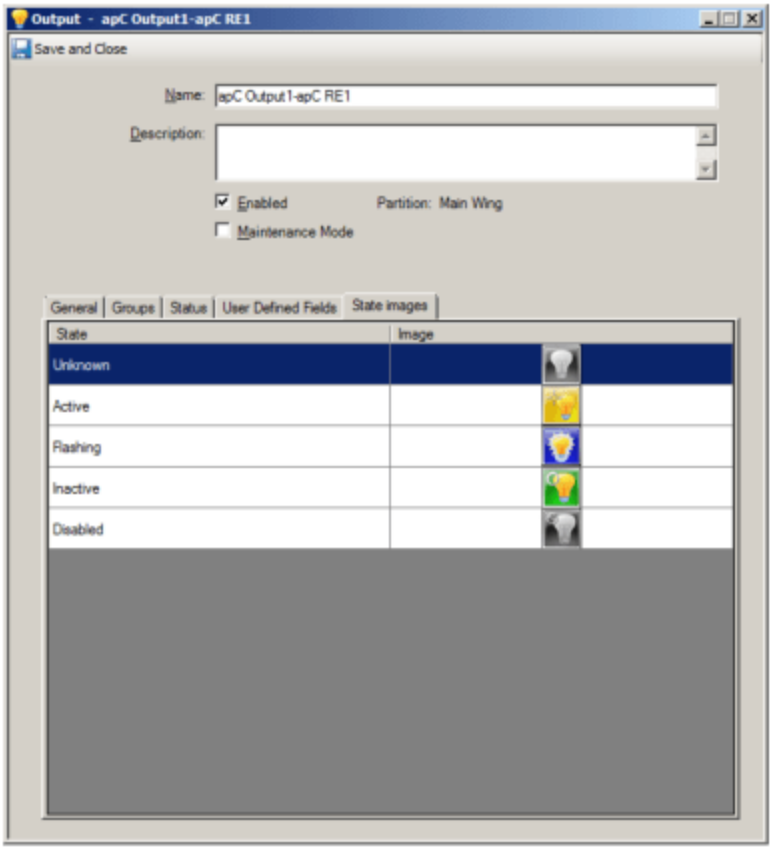
To Change an Image

1. Double-click the existing image.

   A **Windows Open** dialog box appears allowing you to browse for a folder in which you have placed replacement images.

2. When you locate the replacement image, select it to add it to the image listing.
3. To restore the default image, right-click the new image and select **Restore**.

Figure 117: apC Outputs State Images Tab



4. Click **Save and Close**.

apC Reader Editor

The apC Reader Editor is used to configure apC Readers that you have created on the apC Controller Readers tab.

The apC Reader editor has the following tabs:

- apC Reader General Tab on Page 340
- apC Reader Input/Output Tab on Page 341
- apC Reader Keypad Tab on Page 342
- Hardware Groups Tab Definitions on Page 29
- apC Reader Triggers Tab on Page 344
- apC Reader Status Tab on Page 344
- apC Reader State Images Tab on Page 345

You can add or remove Card Formats from multiple Readers via an apC Reader Dynamic View. See Add or Remove Reader Card Formats on Page 25 for more information.

apC Reader General Tab

To Configure a Reader Using the apC Reader General Tab

1. Select a **Reader Type: MRM**, **Direct Connect Wiegand**, or **RM**, as shown in Figure 118 on Page 341.

   The Reader Type selected should match the connected apC panel since the type will affect the inputs and outputs available on the Reader I/O tab.

   Example:

   - The RM has 2 supervised inputs and 2 outputs.
   - the MRM has 2 supervised inputs and 1 output.

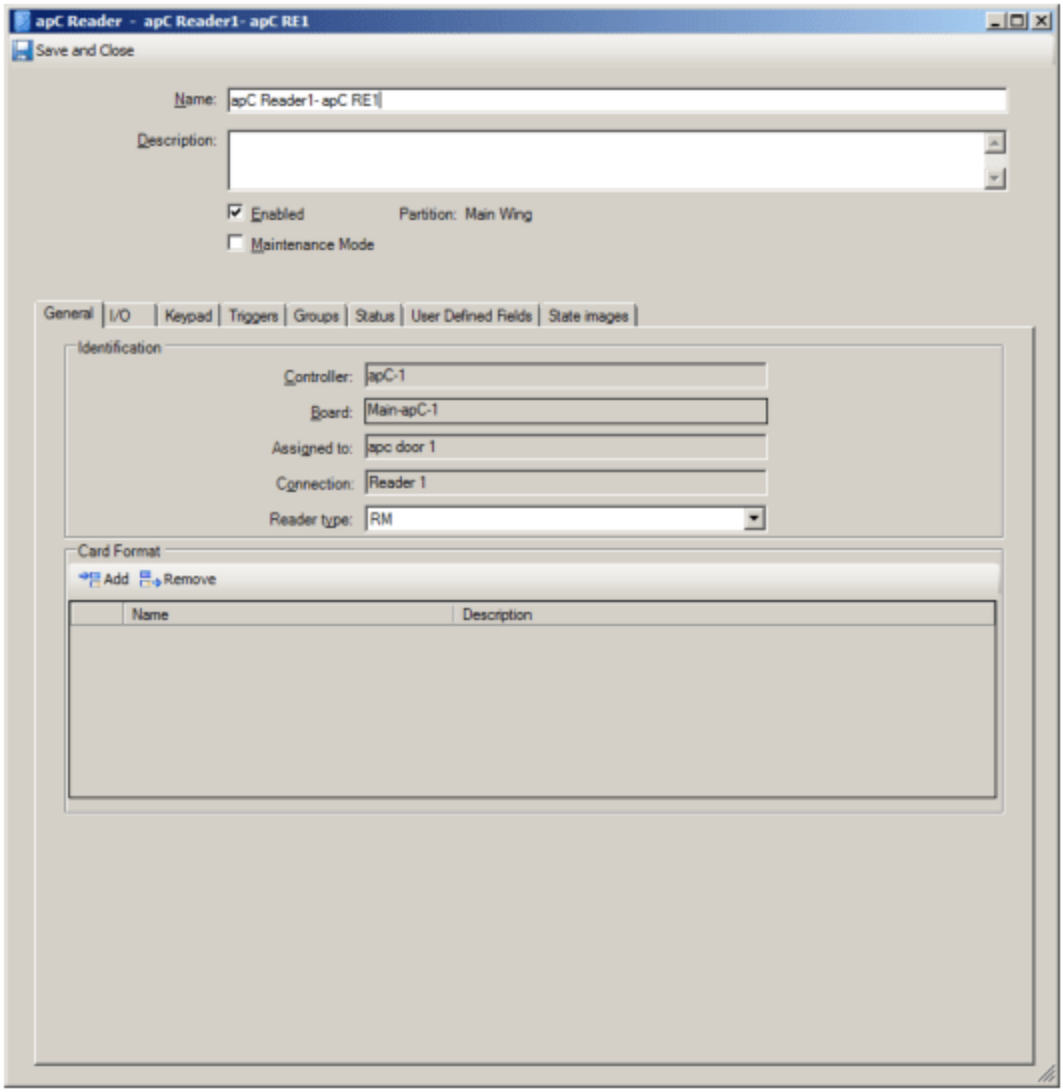
   The **Identification** area in the Readers - **General** tab displays read-only, previously-configured information.

2. To choose a card format for the reader that you have selected, click **Add** in the **Card Format** area. The **Card Format** browser appears, as shown in Figure 118 on Page 341.

NOTE You may configure an apC Reader from the apC panel Readers tab or from the Add-on Board tab. A reader index configured on one tab will be unavailable on the other tab. The location chosen will affect the possible reader type and reader input/output option selection.

See the C•*CURE 9000 Getting Started Guide* - Table 1-5 for a list of UL approved card formats and readers.

Figure 118: apC Controller - Readers - General Tab



3. Click the applicable row in the **Card Format** browser to select **Card Format**. Repeat for multiple formats.
4. Navigate to the **Input/Output** (I/O) tab (see Figure 119 on Page 342).

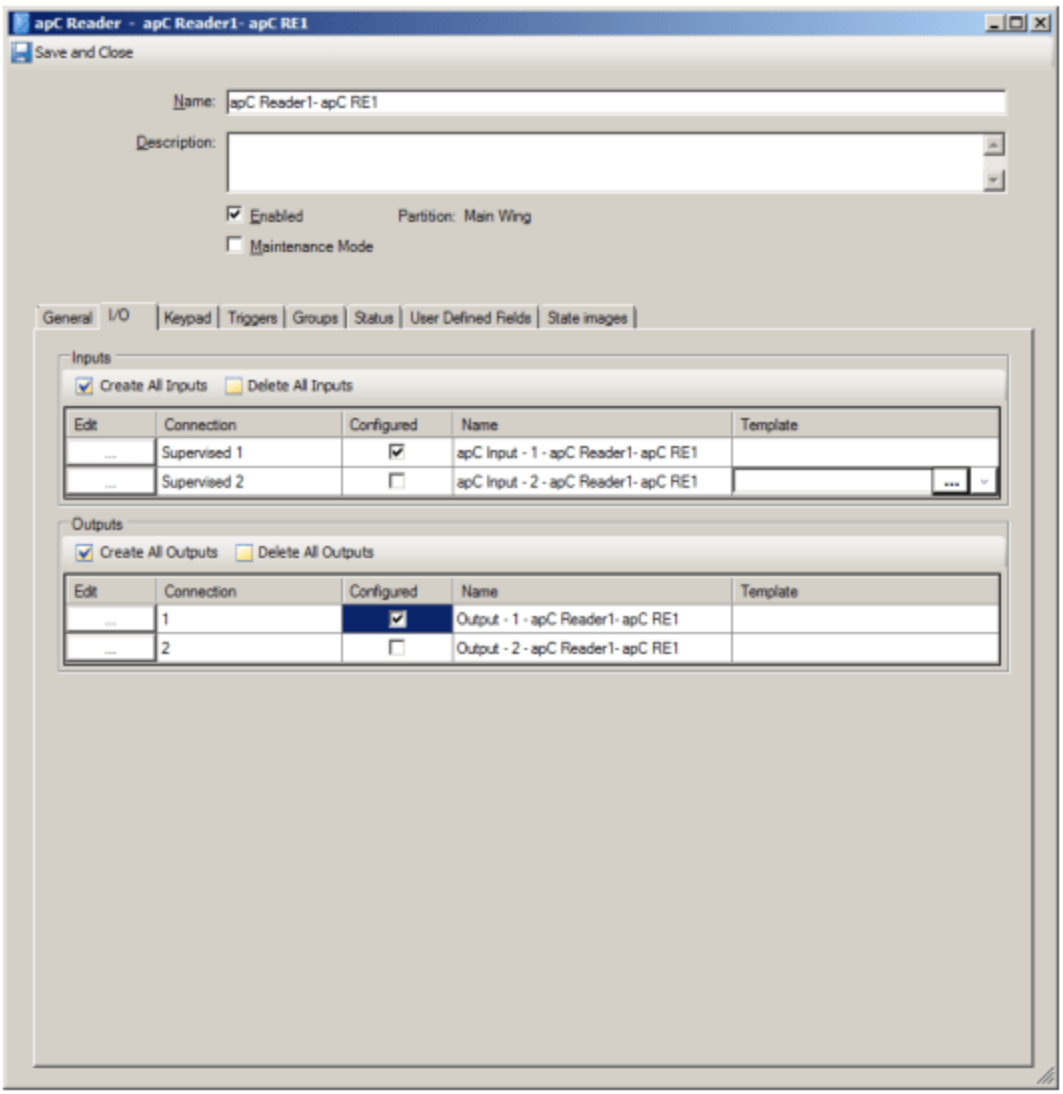
apC Reader Input/Output Tab

Dedicated Supervised Inputs and Outputs vary on the apC Readers I/O tab, depending upon the Reader Type selected in the Reader General tab. The I/O Tab is shown in Figure 119 on Page 342.

To Configure the I/O Tab

1. To configure the **Inputs**, follow the instructions given in To Configure apC Controller Inputs on Page 322.
2. To configure **Outputs**, follow the instructions given in To Configure apC Outputs on Page 323.

Figure 119: apC Controller Reader Input/Output Tab

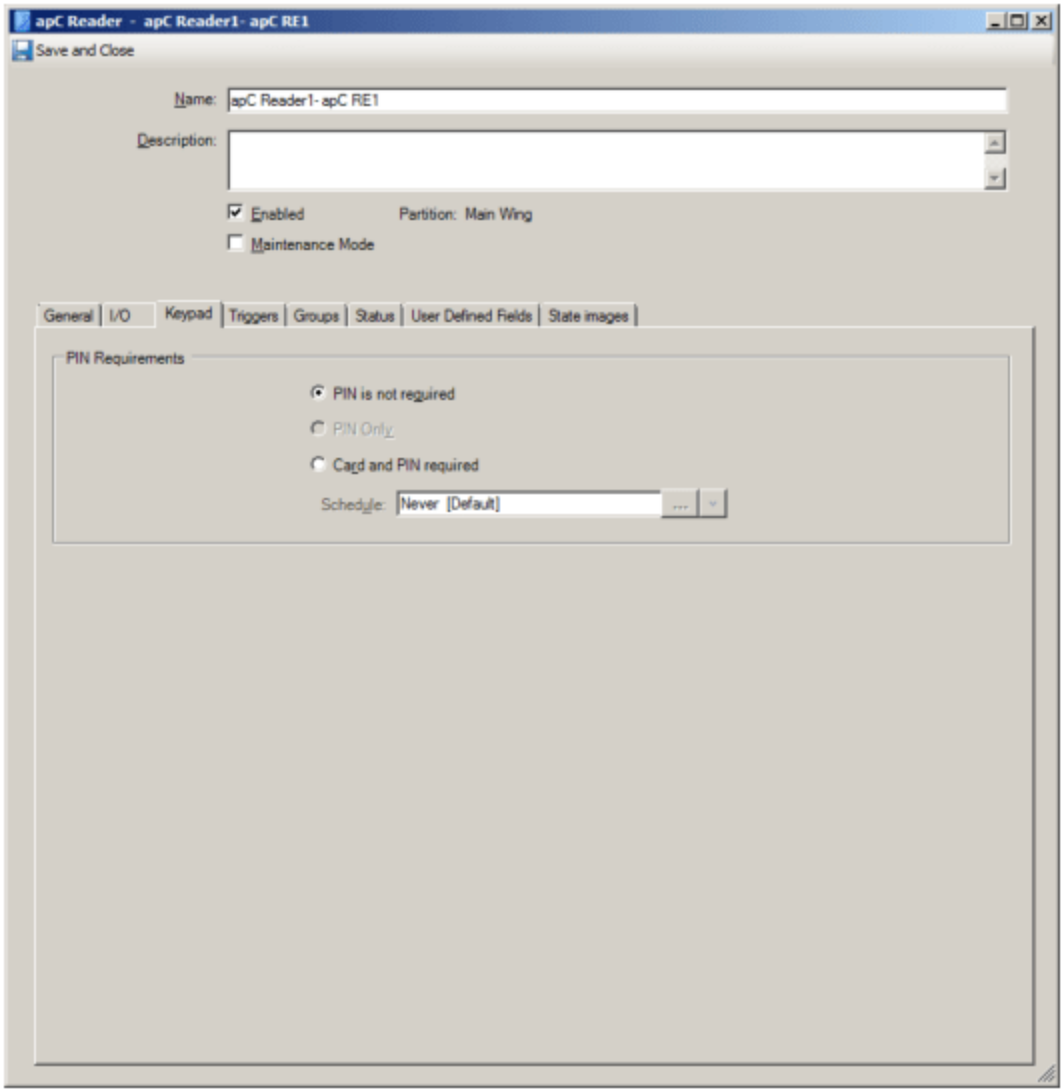


3. Navigate to the **Keypad** tab to configure the PIN requirements for the reader.

apC Reader Keypad Tab

The apC Readers - Keypad tab provides a means to control reader keypads (see Figure 120 on Page 343). Keypad configuration on an apC panel allows specification of **Card and PIN required**. The Schedule is configurable when a PIN is required and restricts the time when the PIN must be entered. The default Schedule is **Always** and is the initial value of the Schedule browser.

Figure 120: apC Controller - Readers - Keypad Tab



To Configure the apC Readers - Keypad Tab

1. Choose one of three options for **PIN Requirements**:
   - **PIN is not required** - to require a card swipe only;
   - PIN Only
   - **Card and PIN required** - to require a both a card swipe or presentation with a PIN entry.
2. Click [...] to select a **Schedule**, which is set up in the **Configuration Pane**.

   If you selected **PIN is not required** or **Card and PIN required** for PIN Requirements, two choices appear in the **Options** area.
3. Choose either of the following options:
   - **Allow card numbers to be entered from the keypad**.
   - **Use PIN+1 as duress code**.

apC Reader Triggers Tab

See the following for information on apC Triggers:

- Triggers Tab for apC Devices on Page 369.
- Defining a Trigger for an apC Device on Page 370.
- Removing a Trigger on Page 272

You can click **Save and Close** after configuring apC Reader triggers, or navigate to the Status tab.

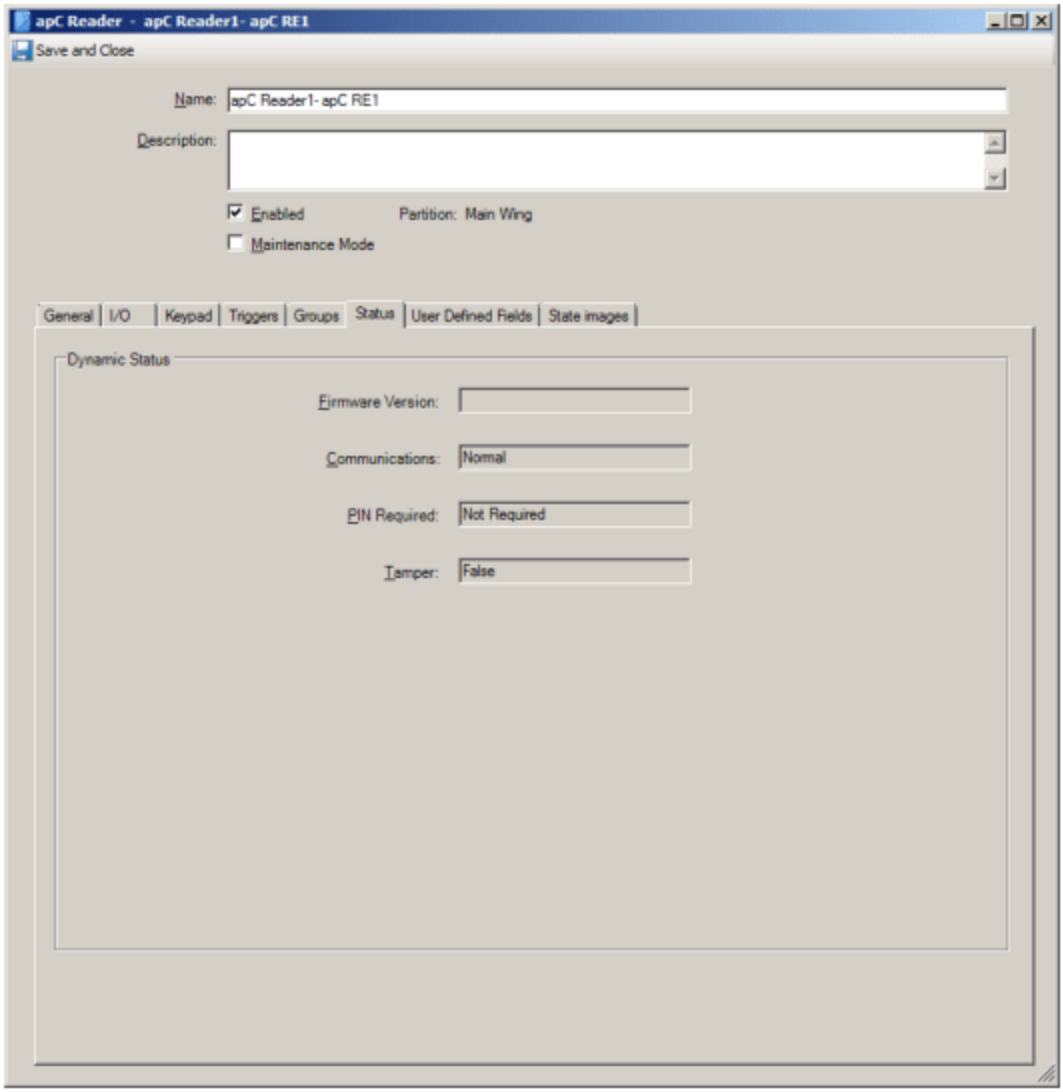
apC Reader Status Tab

The apC Reader **Status** tab provides a read-only listing of critical information about the operational status of the selected apC Readers including:

The apC Reader Status tab is shown in Figure 121 on Page 345

- **Communications** - displays the values Normal or Comm Fail
- **Tamper - displays the values True or False.**
- **PIN Required** - displays the values True or False.

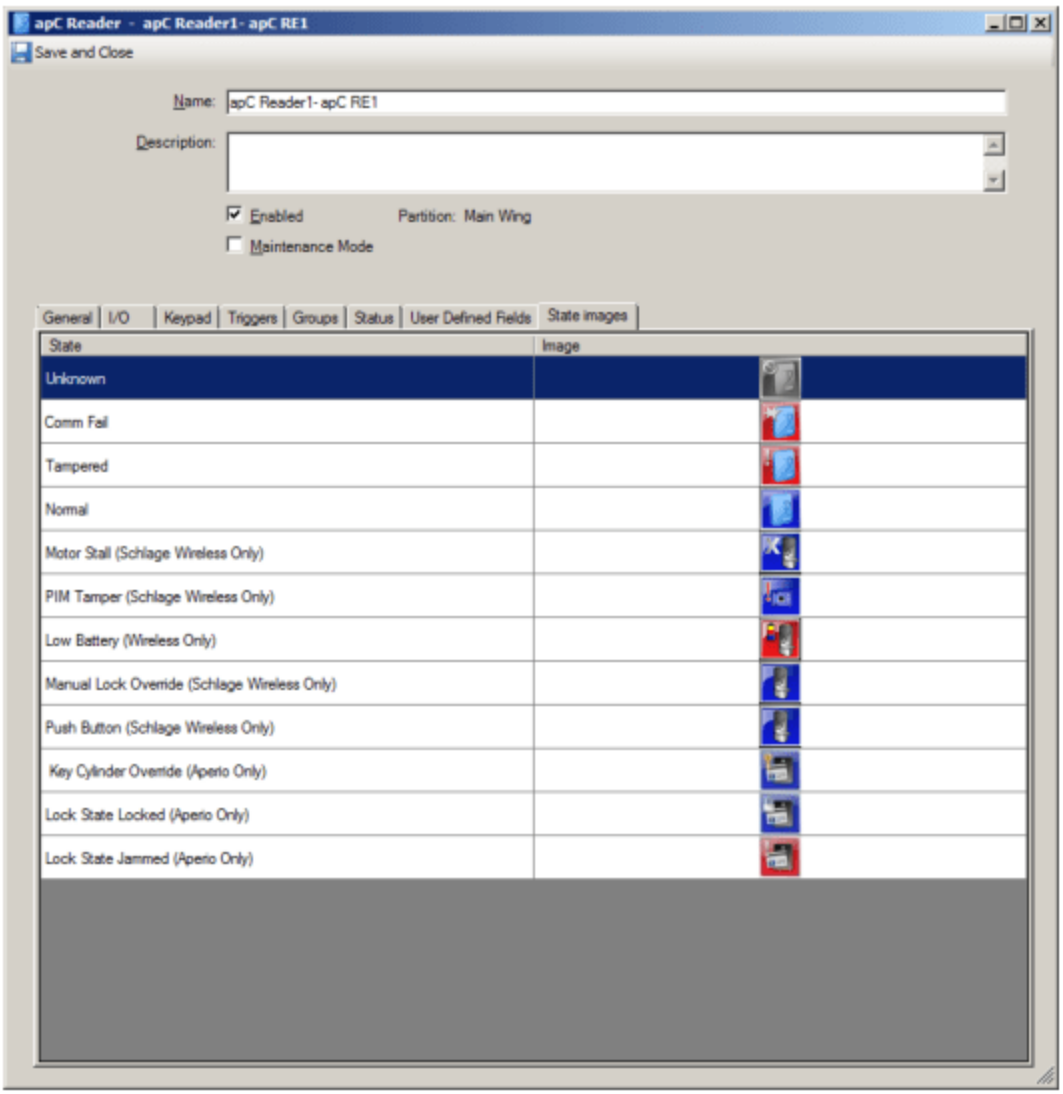
Figure 121: apC Controller - Reader Status Tab



apC Reader State Images Tab

The **State Images** tab provides a means to change the default images used to indicate reader states (see Figure 122 on Page 346). These images appear on the Monitoring Station and change according to the state of the object.

Figure 122: apC Controller - Readers - State Images Tab



To Change an Image

1. Double-click the existing image. A Windows **Open** dialog box appears allowing you to browse for a folder in which you have placed replacement images.
2. When you locate the replacement image, select it to add it to the image listing.
3. To restore the default image, right-click on the new image and select **Restore Default**.
4. Click **Save and Close**.

apC Add-on Board Editor

The apC Add-on Board Editor provides a means to configure boards that expand the capabilities of the apC panels. Expansion boards can add reader ports, supervised inputs and additional outputs.

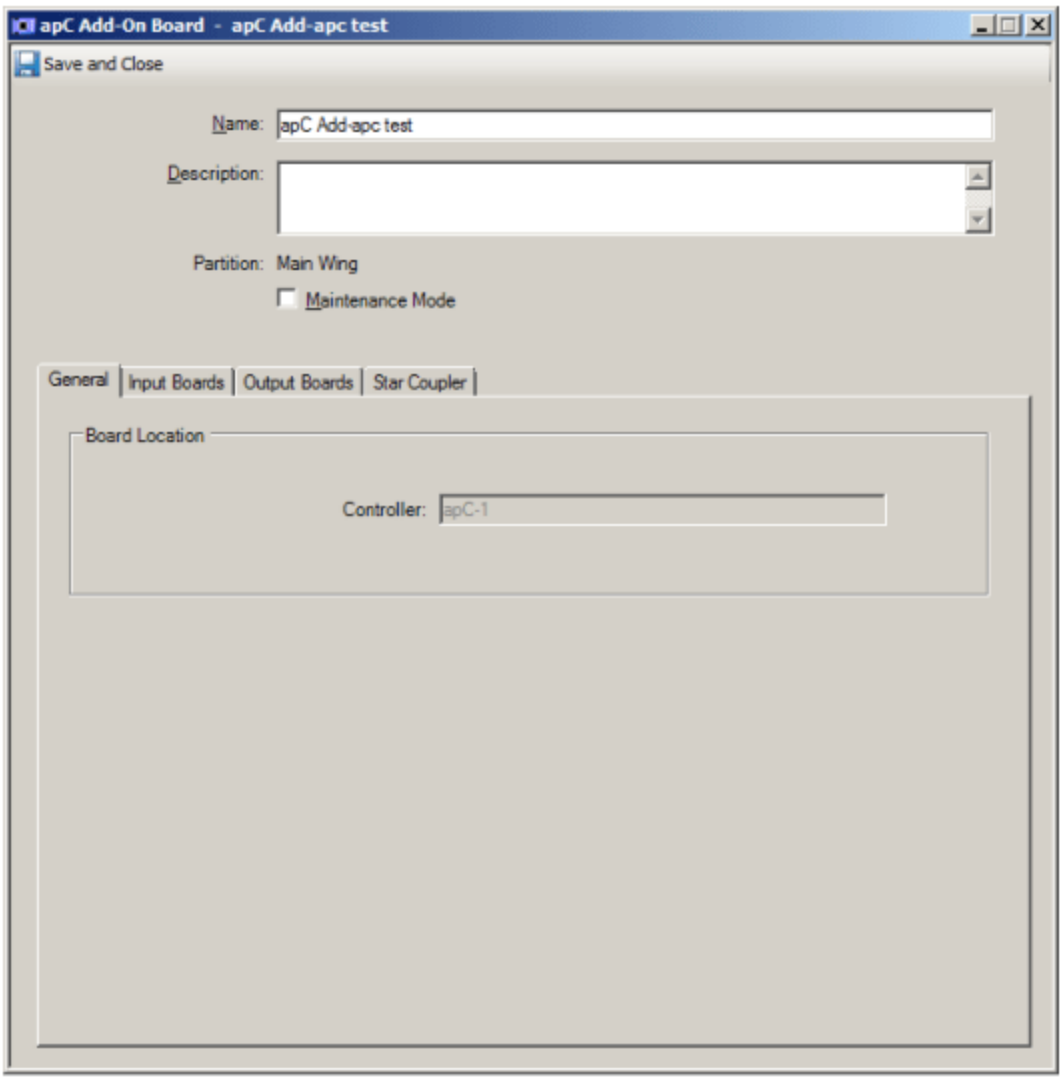
The apC Add-On Board Editor displays the following tabs:

- apC Add-On Board General Tab on Page 347
- apC Add-On Board Input Boards Tab on Page 348
- apC Add-On Board Output Boards Tab on Page 349
- apC Add-On Board Star Coupler Tab on Page 354

apC Add-On Board General Tab

The **apC Add-On Board General** tab displays the Board Location **Controller** field, which is a read-only field that displays the associated apC panel. Navigate to the **Input Boards** tab. See Figure 123 on Page 348.

Figure 123: apC Controller Ad d-On Board General Tab



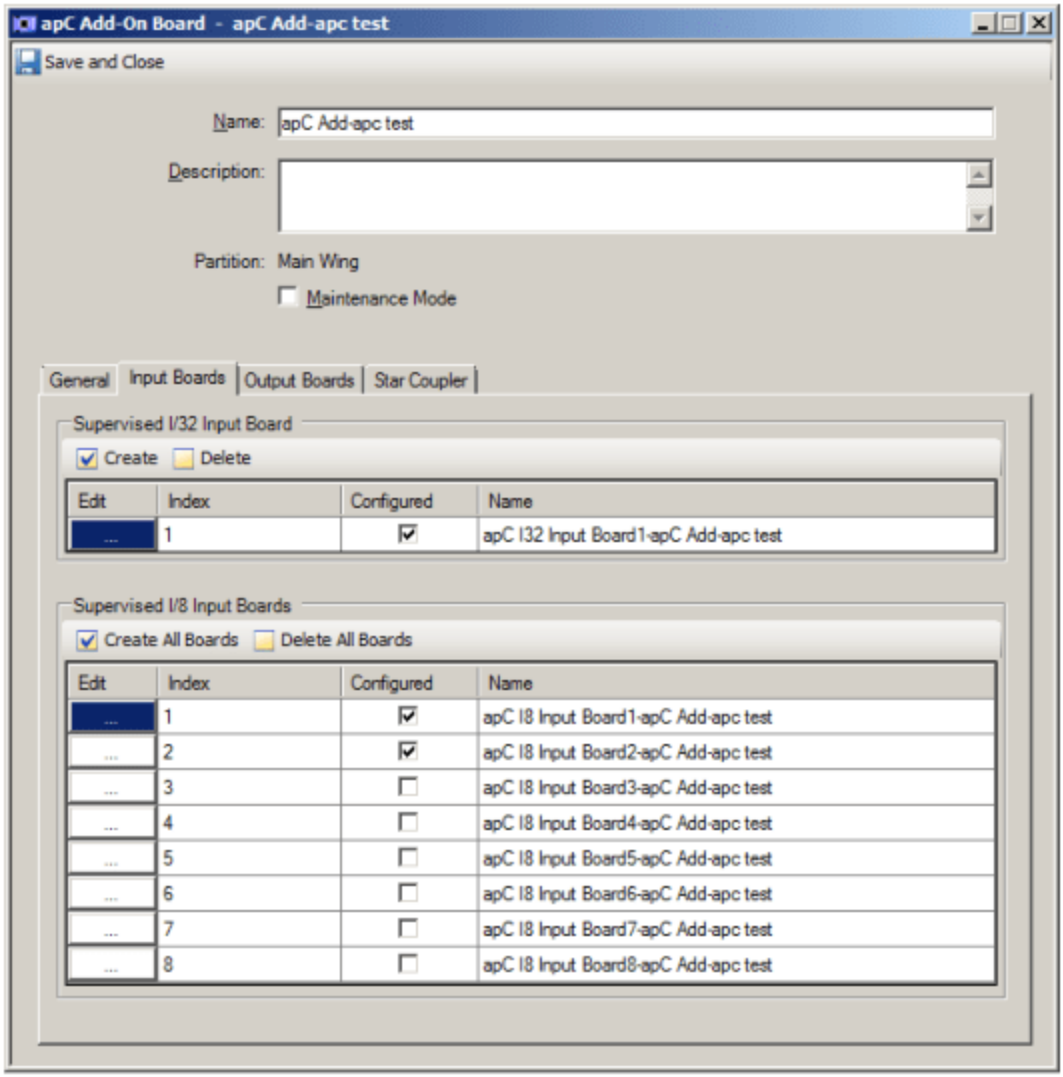
apC Add-On Board Input Boards Tab

The apC Add-On Board Input Boards tab allows you to add a Supervised I32 Input Board (Index 1) and eight Supervised I8 Input Boards (Index 1 through 8).

To Configure the I32 Input Board Using the apC Input Boards Tab

- To configure the **I32 Input Board**, select the check box in the **Configured** column in the **apC Add-On Board - Input Boards** tab and click [...] located in the **Edit** column of the **Supervised I32 Input Board** box to display the **apC I32 Input BoardGeneral** tab (see Figure 124 on Page 349).

Figure 124: apC Controller Add-On Board Input Boards Tab



apC Add-On Board Output Boards Tab

The apC Add-On Board Output Boards tab allows you to add two R48 and eight R8 Output Boards.

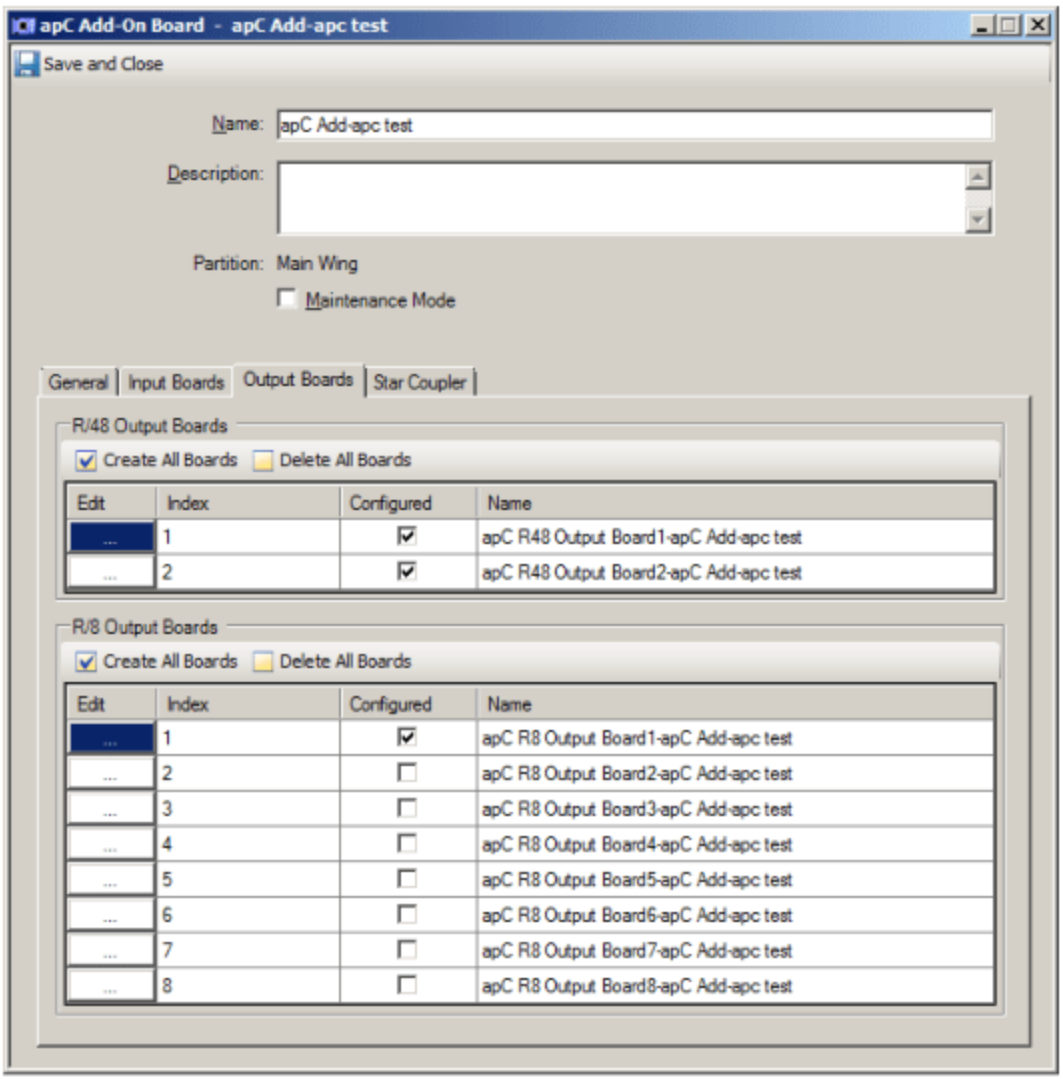
- R48 Output Board on Page 349
- R8 Output Board on Page 352

R48 Output Board

To Configure the R48 Output Board

1. To configure the **R48 Output Board**, select the check box in the **Configured** column in the apC Add-On Board Output Boards tab and click [...] located in the **Edit** column of the **R48 Output Boards** box (see Figure 125 on Page 350) to display the apC R48 Output Board General tab, as shown in Figure 126 on Page 351.

Figure 125: apC Controller Add-On Board Output Boards Tab

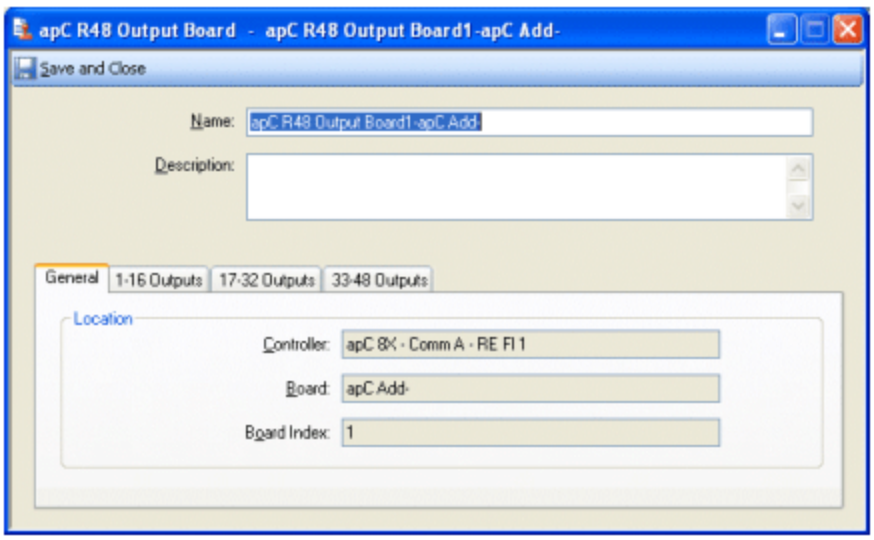


The apC R48 Output Board General tab displays three read-only fields:

- Controller
- Board
- Board Index

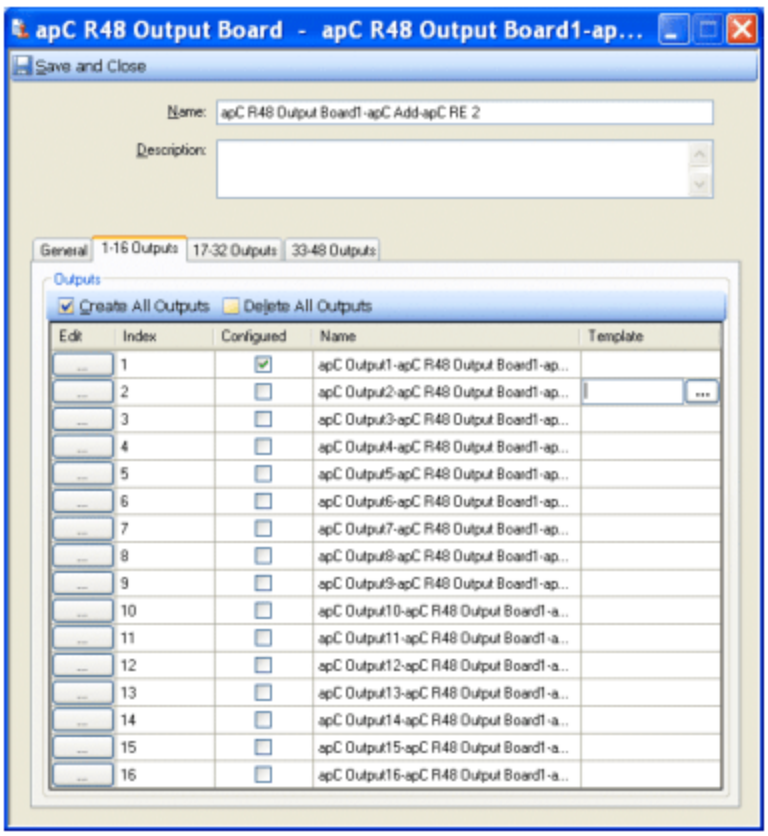
These fields locate the Output that you have chosen to configure. As you configure more Add-On Board Outputs for this controller, the Board Index field reflects the output placement on the R48 output board, ranging from 1 through 2.

Figure 126: apC Controller Add-On Board Output Boards General Tab



2. To configure Outputs, select the apC R48 Output 1-16 Outputs tab, as shown in Figure 127 on Page 351.

Figure 127: apC Controller Add-On Board Output Boards 1-16 Outputs Tab



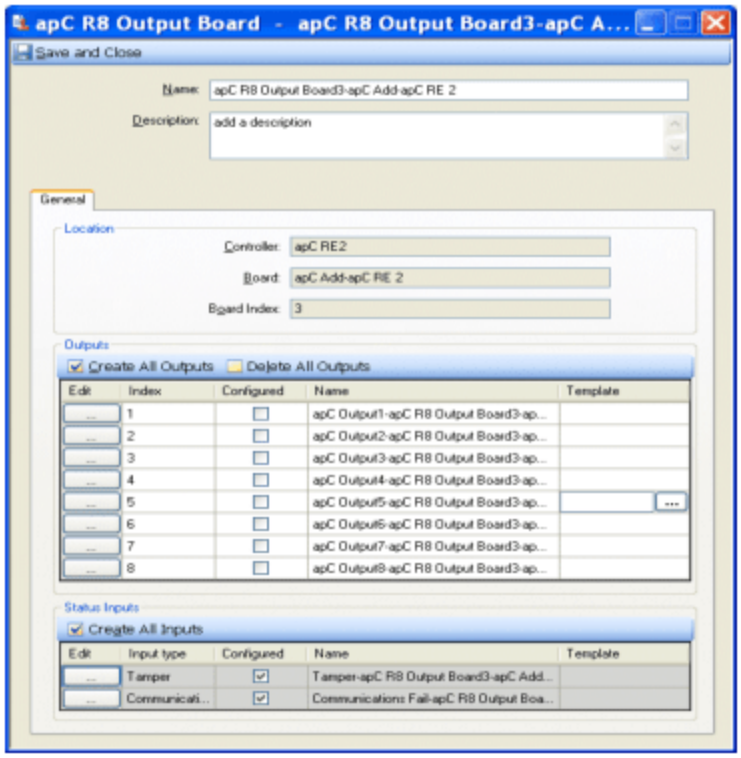
3. To configure the Outputs on the Add-On Board R48 Outputs 1-16 Outputs, 17-32 Outputs and 33-48 Outputs tabs, follow the instructions given in To Configure apC Outputs on Page 323.
4. Once you have finished configuring the R48 Outputs, click **Save and Close** to return to the apC Add-On Board Output Boards tab.

R8 Output Board

To Configure an R8 Output Board

1. To configure the **R8 Output Boards**, select the check box in the **Configured** column in the apC Add-On Board Output Boards tab and click [...] located in the **Edit** column of the R8 Output Boards box (see Figure 125 on Page 350) to display the apC R8 Output Board General tab, as shown in Figure 128 on Page 352.

Figure 128: apC Controller Add-On Board Output Boards General Tab



The apC R8 Output Board General tab displays three read-only fields:

- Controller
- Board
- Board Index

These fields locate the Output that you have chosen to configure. As you configure more Add-On Board Outputs for this controller, the Board Index field will reflect the output placement on the R8 output board, ranging from 1 through 8.

There are also two Status inputs available for the R8 Output Board:

- Board Tampered, which indicates tampering with the Add-On Board
- Communications Fail, which detects a communications failure.

NOTE You will not see comm fail or tamper until at least one of the inputs or outputs is configured.

2. To configure the **R8 Output**, select the check box in the **Configured** column in the apC R8 Output Board General tab and click [...] located in the **Edit** column of the **R8 Outputs** box, as shown in Figure 128 on Page 352.
3. To configure each **R8 Output**, follow the instructions given in To Configure apC Outputs on Page 323.
4. Once you have finished reader the **R8 Outputs**, click **Save and Close** to return to the apC Add-On Board Output Boards tab.
5. Click the **Star Coupler** tab to configure Star Coupler Readers, Inputs and Outputs, Mini Star Readers and WPSC (Wiegand Proximity Star Coupler) Readers and Supervised Inputs.

NOTE Because the apC can only support 8 readers, some of the Reader ports on the Star Coupler may be unavailable to configure on C•CURE 9000 if readers are configured directly on the apC Readers tab. For example, if Readers 1 and 6 are configured on the Readers tab, Readers 1 and 6 will be unavailable on the Star Coupler (Configured check box is read-only). Conversely, if Readers 1 and 6 are configured on the Star Coupler, then Readers 1 and 6 on the Readers tab will be unavailable.

apC Add-On Board Star Coupler Tab

The **apC Add-On Board** Star Coupler tab allows you to add one of the following:

- Star Coupler, with up to 8 Star Coupler Readers, 8 Unsupervised Inputs and 8 Outputs. See the apC Star Coupler Board Editor on Page 365.

  or

- Mini Star with up to 8 Mini Star Readers. See the Mini Star Coupler Board Editor on Page 373.

NOTE The Mini Star Reader has not been evaluated by UL and cannot be used in UL Listed applications.

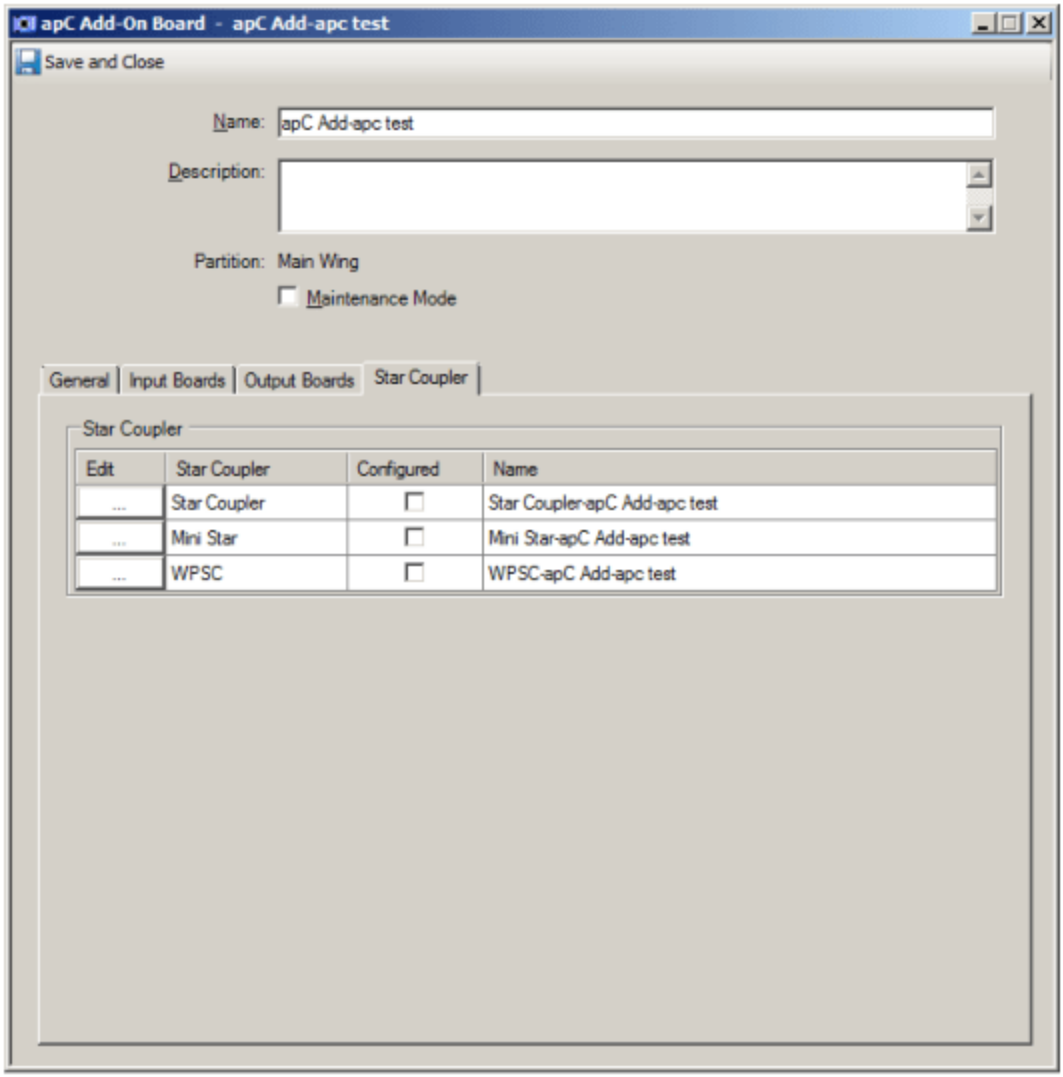
  or

- WPSC (Wiegand Proximity Star Coupler) with up to 8 WPSC Readers and 8 Supervised Inputs on upper and lower boards. See the Wiegand Proximity Star Coupler Editor on Page 376.

NOTE Unsupervised inputs cannot be used in Proprietary Burglar Alarm applications.

Figure 129 on Page 355 shows the apC Add-On Board Star Coupler tab.

Figure 129: apC Add-on Board Star Coupler Tab



Configuring the apC Add-On Board Star Coupler Tab

You use the apC Add-On Board Star Coupler tab to configure the type of Star Coupler board you have connected to your apC controller.

To Configure the apC Add-On Board Star Coupler Tab

1. Open the apC Add-On Board Editor by navigating in the Hardware Tree to the apC controller you want to edit, then navigating in the tree to the apC Add-On Board you want to edit.
2. Double-click on the apC Add-On Board. The apC Add-On Board Editor opens.
3. Click on the Star Coupler tab.
4. For the Star Coupler board type that is attached to your apC, click in the Configured column to enable that board.

   Example:

If you have attached a Mini Star Coupler to your apC, click Configured for the Mini Star in the Star Coupler table.

NOTE If you select a Star Coupler and then try to enable a different one, a message appears asking "Are you sure you want to delete the Star Coupler object ,object-name>?" because you can only have one Star Coupler configured.

Click **Yes** if you want to delete the Star Coupler you configured and replace it with your new choice.

Click **No** if you want to keep the Star Coupler you configured and cancel this action.

apC Add-On Board Star Coupler Tab Definitions

The apC Add-On Board Star Coupler tab has the following file and buttons.

Table 82: apC Add-On Board Star Coupler Tab Definitions

Field/Button	Description
Edit Column	Click ... in the **Edit** column to open the editor for the Star Coupler you have enabled.
Star Coupler Column	This column displays the type of each Star Couplers you can enable and configure.
Configured	Click in this column to enable a Star Coupler, Mini Star, or WPSC (make it available to be edited).
Name	Displays the name for this Star Coupler. The name is system-generated by default, but you can edit this name by clicking in click in this field.
Star Coupler	The Star Coupler is a single expansion board that attaches to the apC/8X or apC to allow the RM readers, I/8 inputs, and R/8 outputs to be wired in a Star topology.
Mini Star	A Mini Star is a single expansion board that attaches to the apC/8X or apC panels to allow the RM readers to be wired in a star topology.
WPSC	The Wiegand/Proximity Star Coupler (WPSC) consists of a two board set that attaches to the apC or apC/8X to allow direct connection of up to 8 read heads using Wiegand signaling.

apC Input Board Editor (I32 and I8)

The apC Input Board editor is used to configure apC Input Boards that you have created on the apC Add-on Boards tab.

The apC Input Board editor has the following tabs:

- apC I32 Input Board General Tab on Page 357
- apC I32 Input Board 1-16 Inputs Tab on Page 358
- apC I32 Input Board 17-32 Inputs Tab on Page 360
- apC I8 Input Board General Tab on Page 362

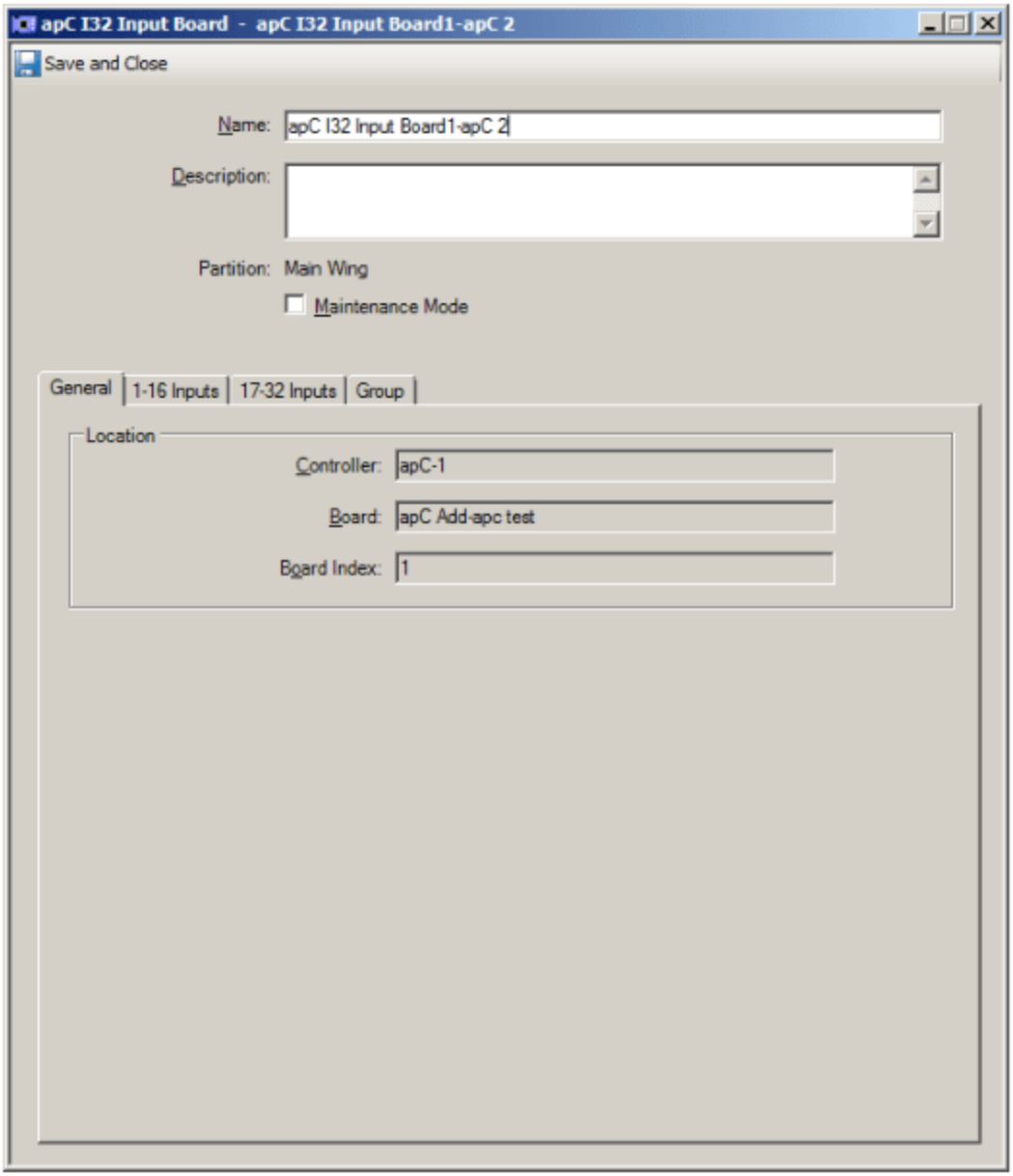
apC I32 Input Board General Tab

The **apC I32 Input Board - General** tab, as shown in Figure 130 on Page 358, displays the Input Location - **Controller**, **Board** and **Board Index** fields. These are read-only fields that display the apC panel, the apC Add-On Board and Index (for the I32 Inputs the Index is 1) associated with the I32 Supervised Inputs.

These fields identify the Input board that you have chosen to configure. The Board Index field reflects the position of the I32 input board on the apC.

Navigate to the **1-16 Inputs** tab.

Figure 130: apC Controller I32 Add-On Board General Tab



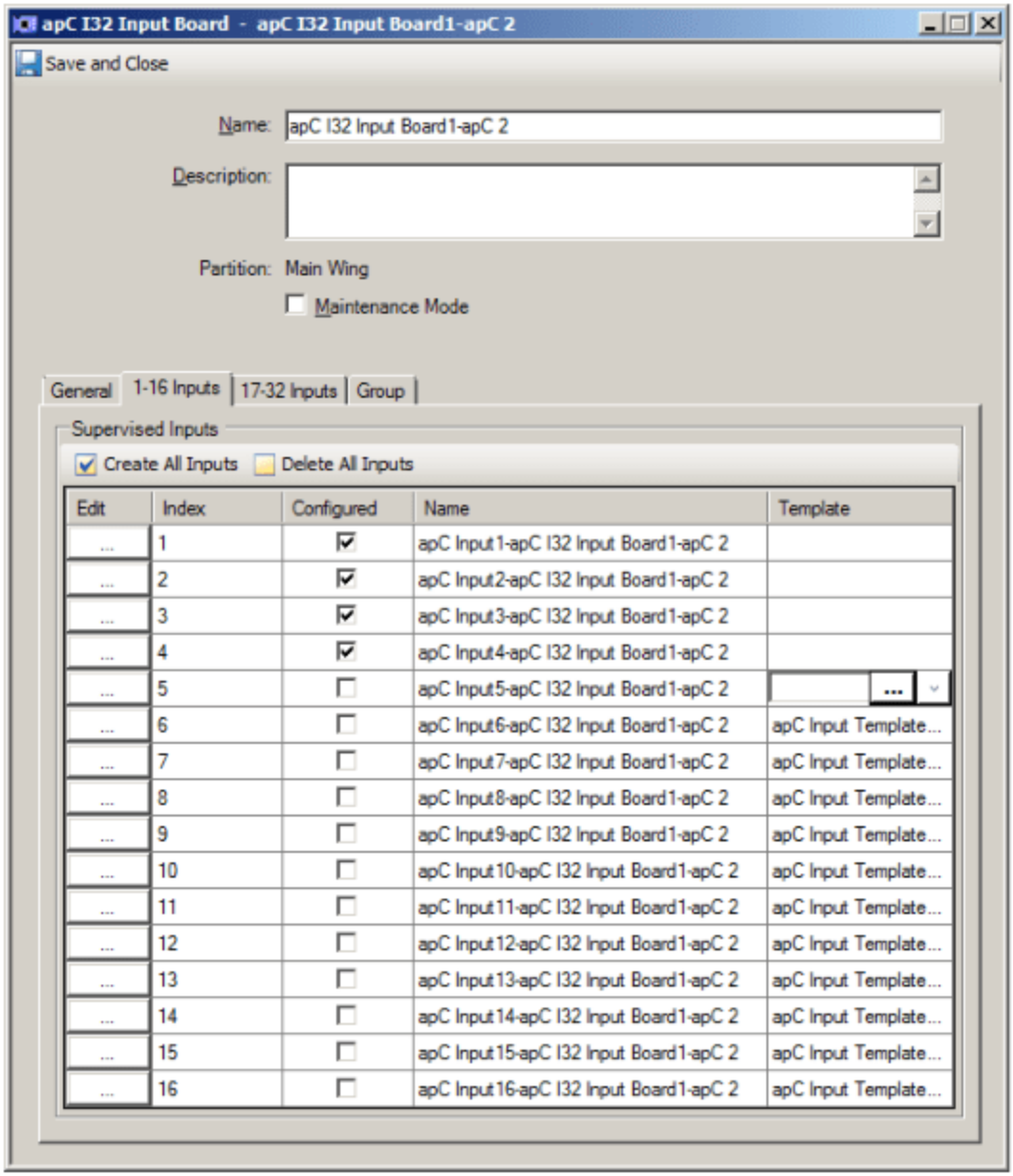
apC I32 Input Board 1-16 Inputs Tab

The **apC I32 Input Board** 1-16 Inputs tab allows you to add 16 Supervised Inputs on the I32 Input Board (Board Index 1).

To Configure the 1-16 Inputs Board

1. To configure the **1-16 Supervised Inputs**, select the check box in the **Configured** column in the **apC Add-On Board - I32 Input Board - 1-16 Inputs** tab (see Figure 131 on Page 359) and click ... located in the **Edit** column of the **Supervised Inputs** box to display the **apC Input** (Index Numbers 1 through 16) **I32 Input Board1 - General** tab (see Figure 132 on Page 360).

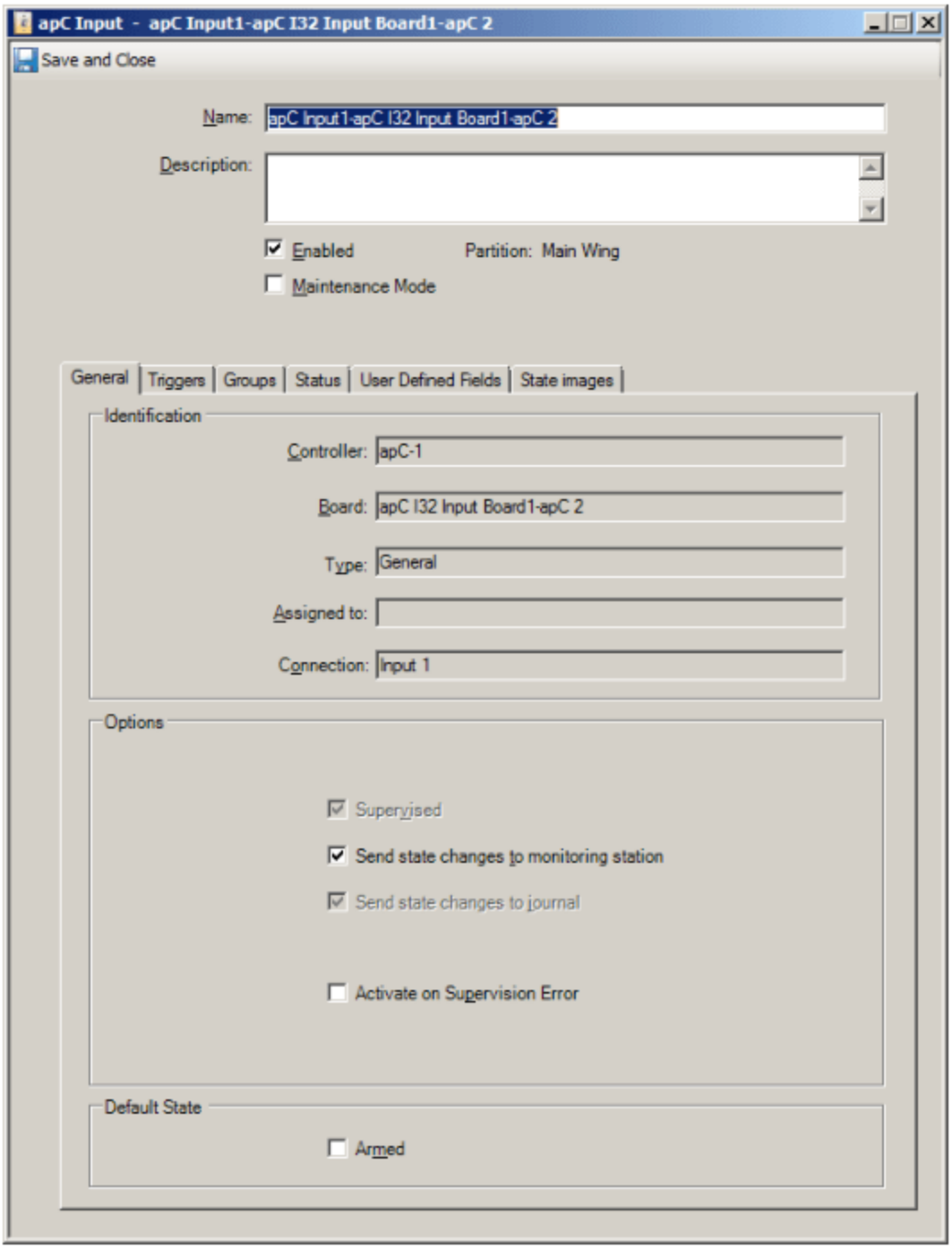
Figure 131: apC Controller I32 Add-On Board 1-16 Inputs Tab



The **apC Input General** tab, as shown in Figure 132 on Page 360, displays the Input Location - **Controller**, **Board** and **Connection** fields. These are read-only fields that display the apC panel, the apC Add-On Board and Input Number associated with an I32 Supervised Input. These fields locate the Input that you have chosen to configure.

2. To configure the **Inputs** on the **I32 Input Board - 1-16 Inputs** tab, follow the instructions given in To Configure apC Controller Inputs on Page 322.
3. Navigate to the **17-32 Inputs** tab.

Figure 132: apC Controller I32 Add-On Board 1-16 Inputs General Tab



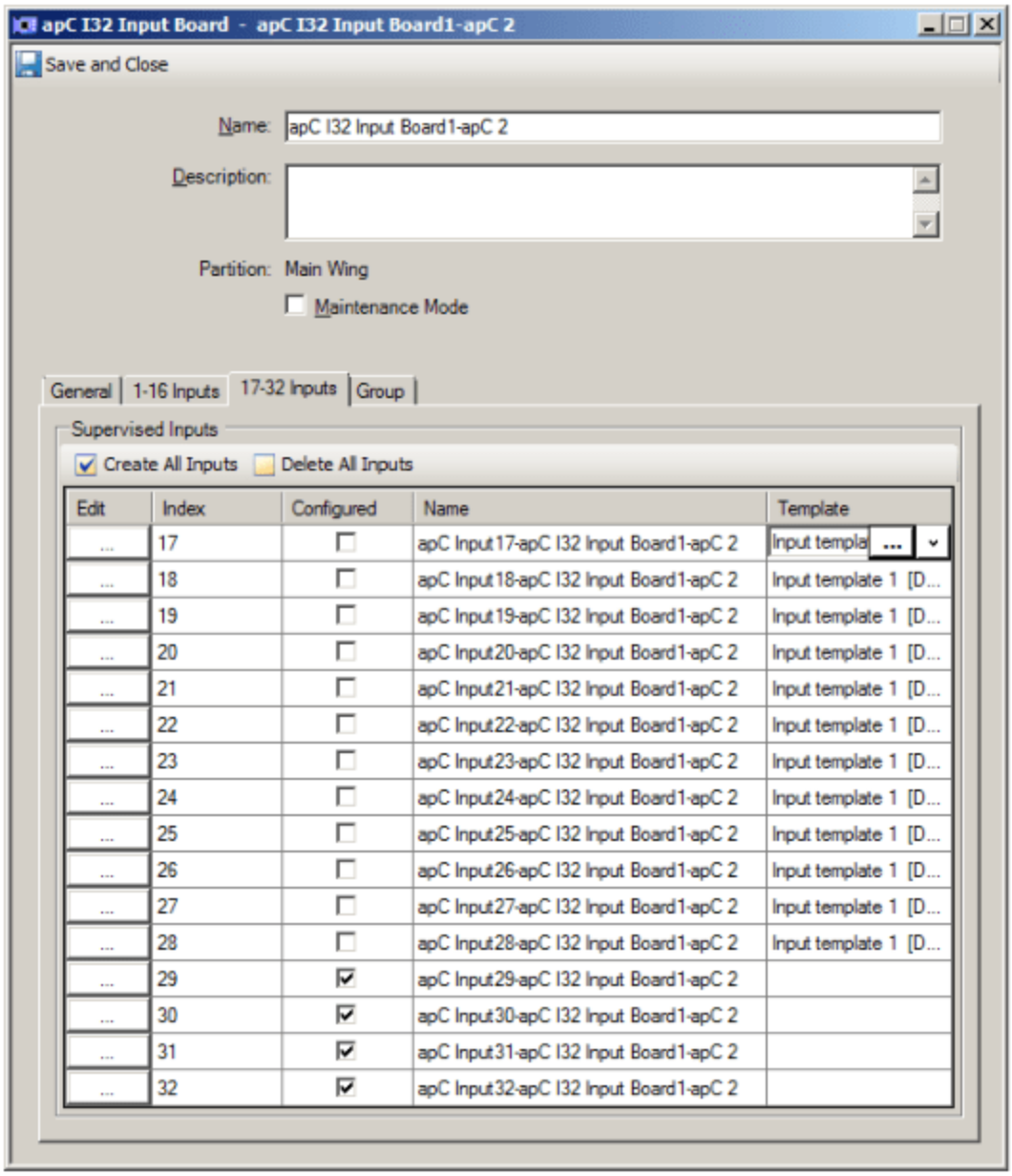
apC I32 Input Board 17-32 Inputs Tab

The **apC I32 Input Board** 17-32 Inputs tab allows you to add 16 Supervised Inputs on the I32 Inputs Board (Board Index 1).

To Configure the 17-32 Inputs Board

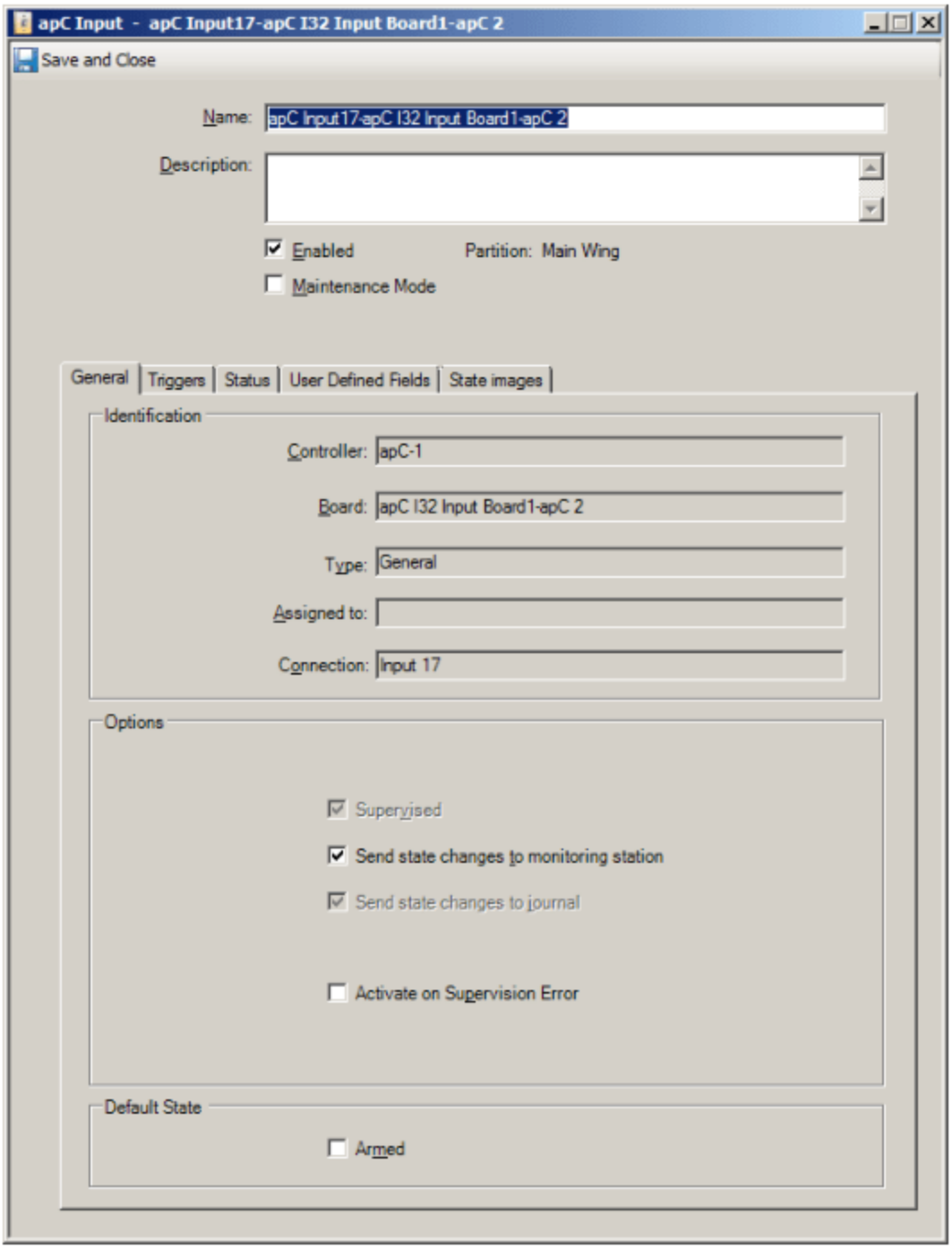
1. To configure the **17-32 Supervised Inputs**, select the check box in the **Configured** column in the **apC Add-On Board - I32 Input Board - 17-32 Inputs** tab (see Figure 133 on Page 361) and click ... located in the **Edit** column of the **Supervised I32 Input Board** box to display the **apC Input** (Index Numbers 17 through 32) **I32 Input Board1 General** tab (see Figure 108 on Page 326).

Figure 133: apC Controller I32 Add-On Board 17-32 Inputs Tab



2. To configure the **Inputs** on the **I32 Add-On Board - 17-32 Inputs** tab, follow the instructions given in To Configure apC Controller Inputs on Page 322.

Figure 134: apC Controller I32 Add-On Board 17-32 Inputs General Tab



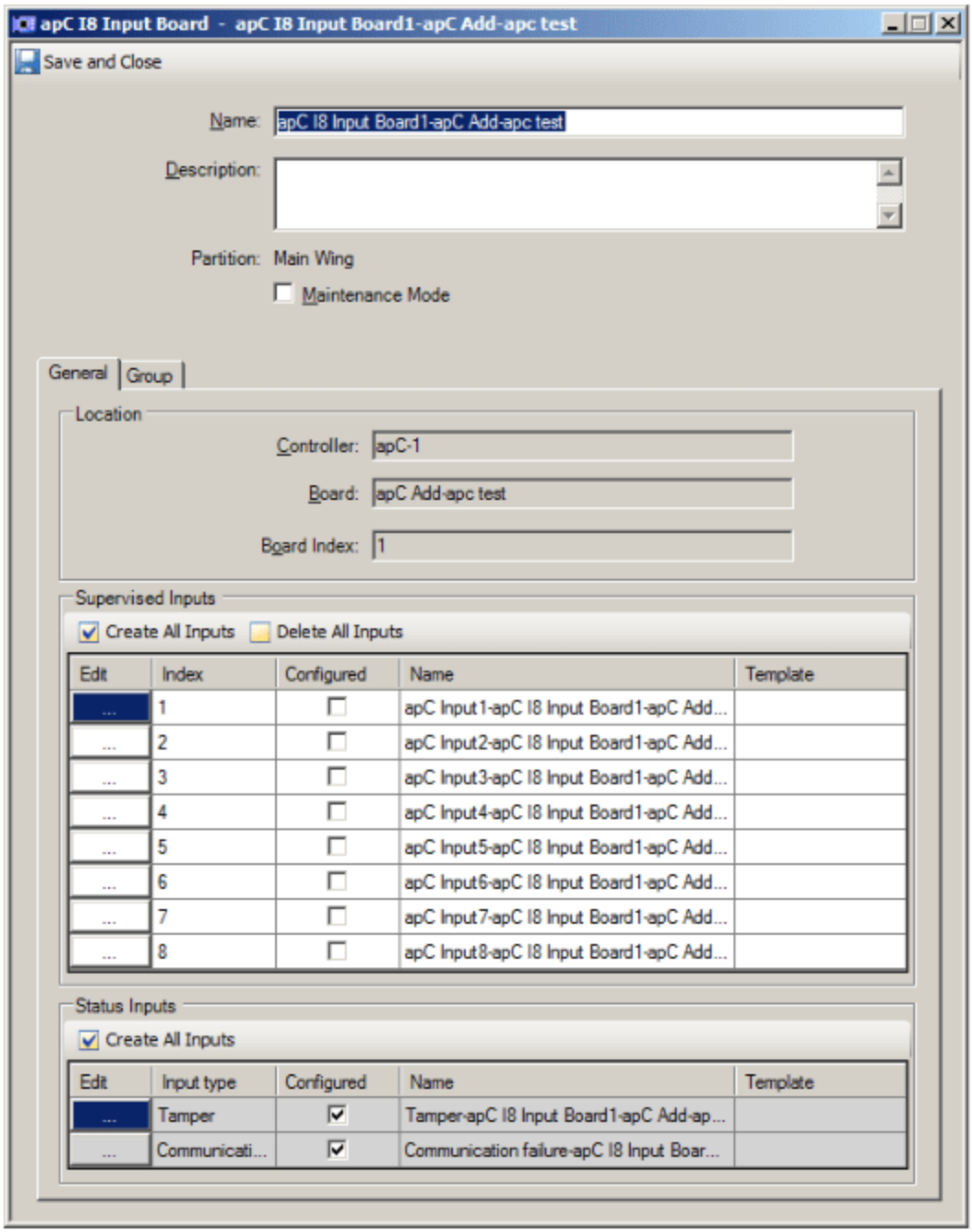
apC I8 Input Board General Tab

You can also add-on up to 64 Supervised Inputs (8 Inputs available on 8 I8 Input Boards) with Triggers available for each input.

To Configure the I8 Input Board

1. To configure an **I8 Input Board**, select the check box in the **Configured** column on the **apC Add-On Board - Input Boards** tab and click ... located in the **Edit** column of the **Supervised I8 Input Board** box to display the **apC I8 Input Board - General** tab (see Figure 135 on Page 363).

Figure 135: apC Controller I8 Add-On Board I8 Inputs General Tab



2. To configure **Inputs**, select the check box in the **Configured** column in the **apC I8 Inputs** tab and click ... located in the **Edit** column to display the **apC Add-On Board - apC I8 Input Board - General** tab.

3. To configure the **Inputs** on the **I8 Add-On Board - I8 Inputs** tab, follow the instructions given in To Configure apC Controller Inputs on Page 322.

   There are also two Status inputs available for the I8 Input Board:

   - Board Tampered, which indicates tampering with the Add-On Board
   - Communications Fail, which detects a communications failure.

4. Once you have finished reader the I8 Inputs, click **Save and Close**.

apC Star Coupler Board Editor

The apC Star Coupler Board Editor is used to configure apC Star Coupler boards.

Star Couplers are single expansion boards that attach to the apC/8X or apC to allow the RM readers, I/8 inputs, and R/8 outputs to be wired in a Star topology. The Star Coupler Board allows addition of:

- 8 MRM/RM Reader ports
- 8 Unsupervised Inputs
- 8 dry contact, form C, relay Outputs

The Star Coupler can be installed on apC and apC/8X panels. For more information, see the *Star Coupler - Mini Star Coupler Quick Start Installation Guide.*

This editor is accessed from the apC Add-on Board Editor Star Coupler tab (see apC Add-On Board Star Coupler Tab on Page 354).

To Configure the Star Coupler Board

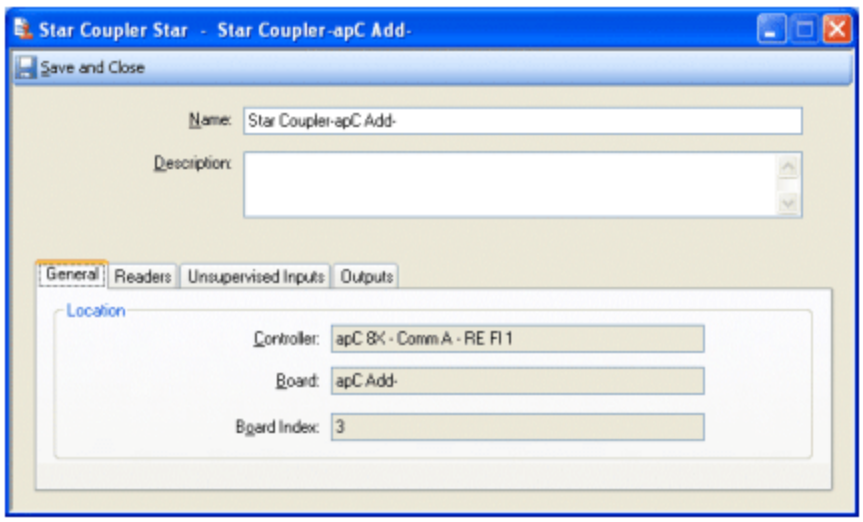
1. To configure the **Star Coupler Board**, select the check box in the **Configured** column in the **apC Add-On Board Star Coupler** tab and click [...] located in the **Edit** column of the **Star Coupler** box (see Figure 129 on Page 355) to display the **Star Coupler General** tab, as shown in Figure 136 on Page 365.

   The **apC Star Coupler Board General** tab displays three read-only fields:

   - Controller
   - Board
   - Board Index

   These fields are located on the Star Coupler that you have chosen to configure. As you configure more Add-On Boards for this controller, the Board Index field will reflect each placement, to differentiate board locations.

Figure 136: apC Star Coupler General Tab



2. Click the **Readers** tab to configure the Star Coupler readers. See Star Coupler Readers Tab on Page 366 for the Star Coupler Readers tab.

3. Click the **Unsupervised Inputs** tab to configure the Star Coupler unsupervised inputs. See Star Coupler Unsupervised Inputs Tab on Page 367 for the Star Coupler Unsupervised Inputs tab.
4. Click the **Outputs** tab to configure the Star Coupler outputs. See Star Coupler Outputs Tab on Page 367 for the Star Coupler Outputs tab.
5. When you have completed configuring the Star Coupler and its attached devices, you can click **Save and Close** to save your changes.

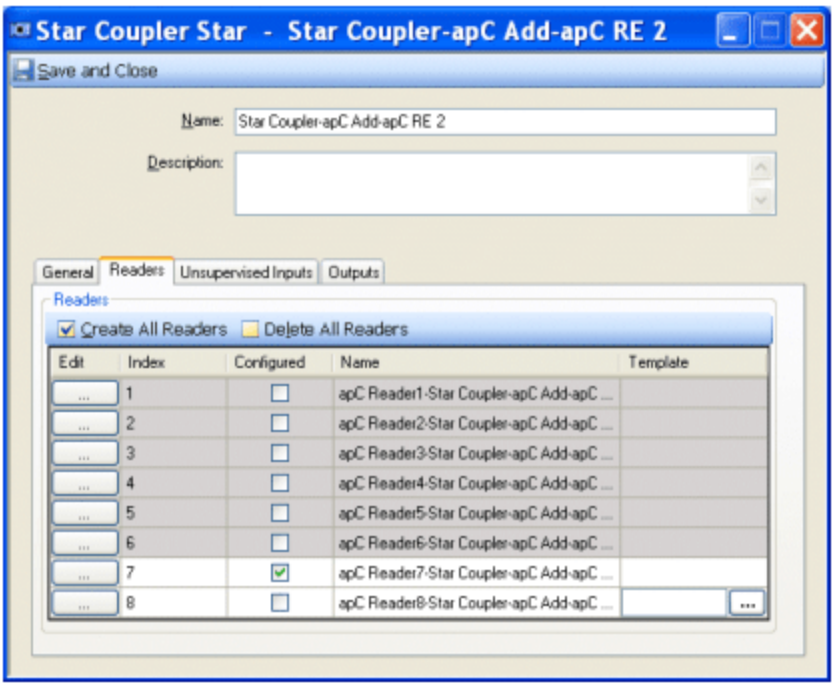
Star Coupler Readers Tab

The Star Coupler Readers tab allows you to configure the readers connected to your Star Coupler.

To Configure Star Coupler Readers

1. Navigate from the apC Controller Add-On Board Tab on Page 324 to the apC Add-On Board Star Coupler Tab on Page 354
2. Click Star Coupler to open the apC Star Coupler Board Editor on Page 365.
3. Click the **Readers** tab to configure readers for the **Star Coupler**. Refer to the Figure 137 on Page 366 for an example of the **Star Coupler Readers** tab.

Figure 137: apC Controller Star Coupler Readers Tab



4. To create all available readers for the Star Coupler, click **Create All Readers**. apC Readers that have previously been created on other board connections are unavailable (shaded gray) to be created here.
5. To create an individual reader, select the check box in the **Configured** column for the **Star Coupler Readers** (Index 1 through 8) and click [...] located in the **Edit** column. The apC Reader Editor opens to allow you to configure this reader. See **apC Reader Editor on Page 340 for details on configuring an apC Reader.**

6. When you have finished creating and configuring readers for the Star Coupler, you can click **Save and Close** to save your changes.

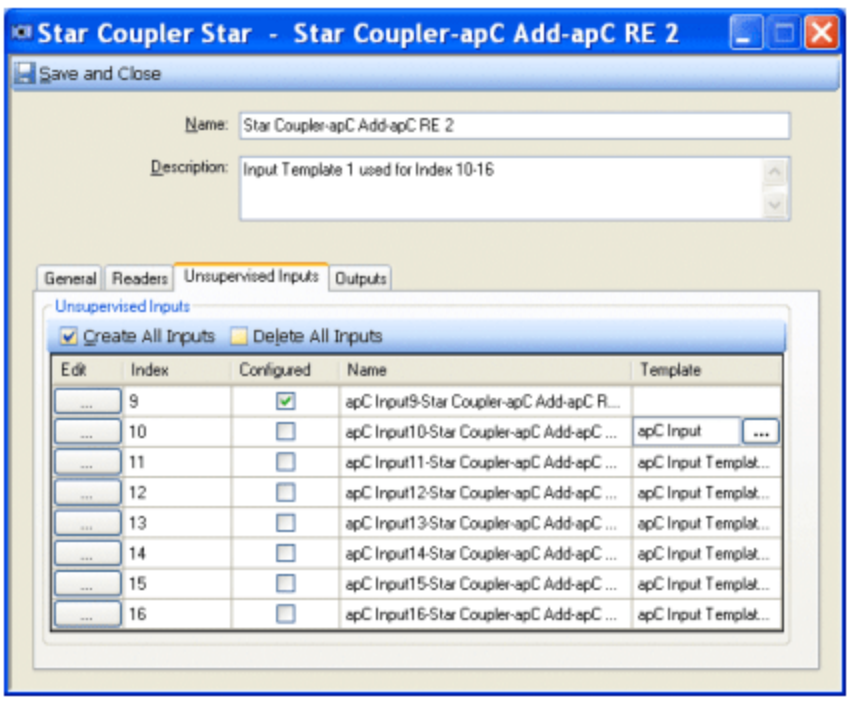
Star Coupler Unsupervised Inputs Tab

The Star Coupler Unsupervised Inputs tab allows you to configure the inputs connected to your Star Coupler.

To Configure Star Coupler Unsupervised Inputs

1. Navigate from the apC Controller Add-On Board Tab on Page 324 to the apC Add-On Board Star Coupler Tab on Page 354, and click Star Coupler to open the apC Star Coupler Board Editor on Page 365.
2. Click the **Unsupervised Inputs** tab to configure Unsupervised Inputs for the Star Coupler (see Figure 138 on Page 367).
3. To create all Unsupervised Inputs for the Star Coupler, click **Create All Inputs**.
4. To create an individual input, select the check box in the **Configured** column for the **Star Coupler Inputs** (Index 9 through 16) and click [...] located in the **Edit** column. The apC Input Editor opens to allow you to configure this input. See **apC Input Editor on Page 332 for details on configuring an apC Input.**

Figure 138: apC Controller Star Coupler Unsupervised Inputs Tab



5. When you have finished creating and configuring inputs for the Star Coupler, you can click **Save and Close** to save your changes.

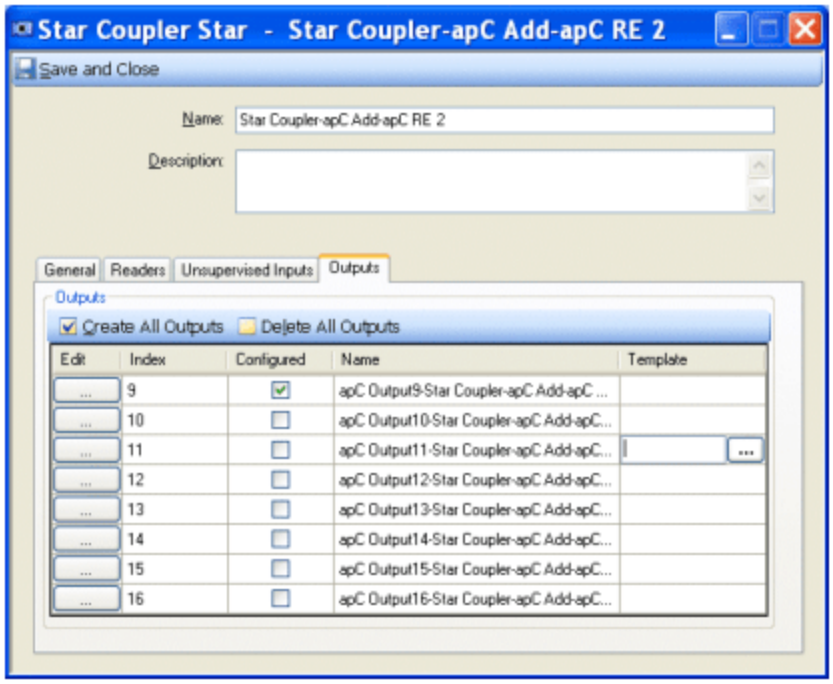
Star Coupler Outputs Tab

The Star Coupler Outputs tab allows you to configure the outputs connected to your Star Coupler.

To Configure Star Coupler Outputs

1. Navigate from the apC Controller Add-On Board Tab on Page 324 to the apC Add-On Board Star Coupler Tab on Page 354
2. Click Star Coupler to open the apC Star Coupler Board Editor on Page 365.
3. Click the **Outputs** tab to configure outputs for the Star Coupler (see Figure 138 on Page 367).

Figure 139: apC Controller Star Coupler Outputs Tab



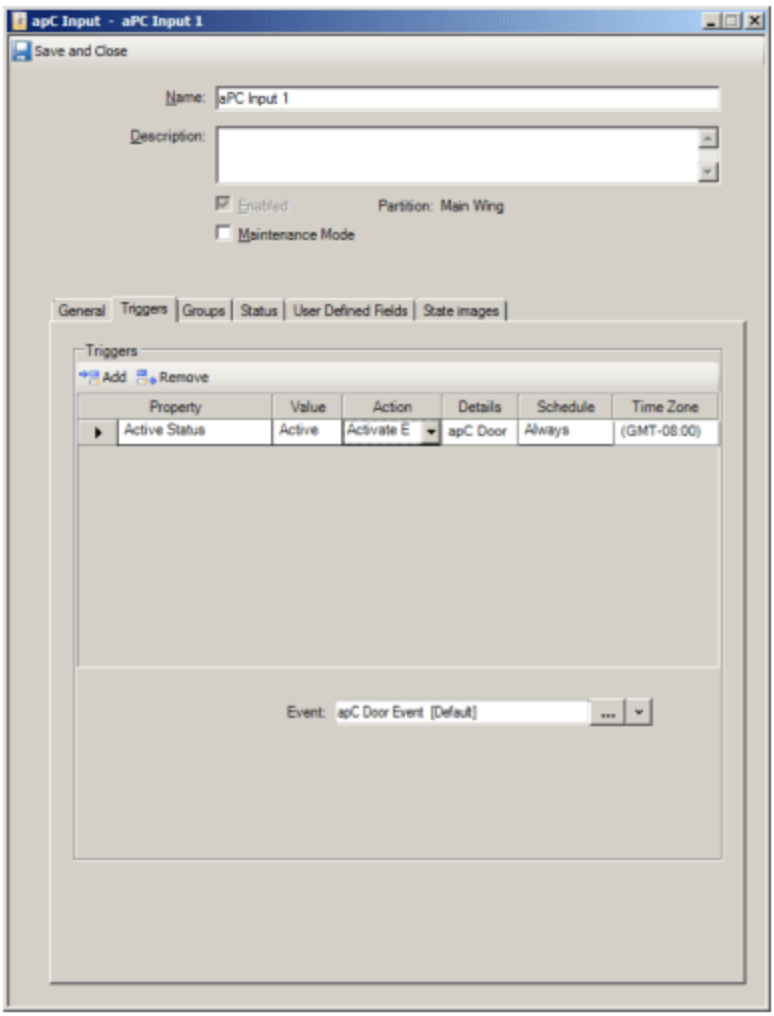
4. To create all outputs for the Star Coupler, click **Create All Outputs**.
5. To create an individual output, select the check box in the **Configured** column for the **Star Coupler Outputs** (Index 9 through 16) and click [...] located in the **Edit** column. The apC Output Editor opens to allow you to configure this output. See **apC Output Editor on Page 336 for details on configuring an apC Output.**
6. When you have finished creating and configuring outputs for the Star Coupler, you can click **Save and Close** to save your changes.

Triggers Tab for apC Devices

C•CURE 9000 uses Triggers, which are configured procedures for activating actions, to activate Events or Outputs for an apC device. A Trigger automatically executes a specified Action when a particular Condition occurs (when the object Property specified in the Trigger reports the Value specified in the Trigger).Navigate to the **Triggers** tab.

Figure 140 on Page 369 shows the Triggers tab for an apC Input, which is typical for an apC device.

Figure 140: Typical apC Triggers Tab



A triggers tab provides you with the ability to define the activation/deactivation, enable/disable, and arm/disarm, etc. of such objects as: events, inputs, outputs, camera actions, door status changes, etc. Triggers can also be used to launch imports and exports, email and reports, viewer and message displays, personnel ID number state changes, controller downloads, sound activation, communication notifications, etc.

Table 83 on Page 370 provides an example of a configured apC Trigger.

Table 83: Triggers Tab Settings Example

The following Triggers Tab settings:					
Property	**Value**	**Action**	**Details**	**Schedule**	**Time Zone**
Active Status	Active	Activate Event	apC Input Event	Always	(Time Zone of apC or C•CURE 9000 Server)
Would create the following Trigger: Any time (Always **Schedule**) the Active Status (**Property**) equals Active (**Value**), activate the event (**Action**) named iSTAR Input Event (**Details**). iSTAR Input Event is an Event that you would need to create using the Event Editor.					

From the Triggers tab of an apC device (such as a Controller, Input, or Reader), you can perform the following tasks.

- Defining a Trigger for an apC Device on Page 370.
- Removing a Trigger on Page 272.

apC Triggers Tab Definitions on Page 371 provides definitions for the fields and buttons on an apC Device Triggers tab.

Defining a Trigger for an apC Device

You can use the Triggers tab to define a Trigger for an apC device. The typical usage for an apC Trigger is to activate an Event or an Output as the result of a state change of an apC device Property.

This tab provides you with the ability to define the activation/deactivation, enable/disable, and arm/disarm, etc. of such objects as: events, inputs, outputs, camera actions, door status changes, etc. Triggers can also be used to launch imports and exports, email and reports, viewer and message displays, personnel ID number state changes, controller downloads, sound activation, communication notifications, etc.

Example:

When an apC Tamper Input changes from the Inactive (normal) to Active (abnormal) state, you wish to activate an Event and activate an audible alarm (an apC Output).

Time Zones for apC Panel Triggers

If you specify a Time Zone in your Trigger definition, you can control when the Schedule for the Trigger is active. You can only select the C•CURE 9000 server Time Zone or the Time Zone of the apC panel you are editing.

Example:

If you have apC panels that are in different Time Zones than your C•CURE 9000 server, you may want to have some Triggers activate according to the apC panel's Time Zone, while other Triggers are activated according to the server Time Zone.

When you specify the Time Zone for a Trigger definition to be the same as the apC Panel Time Zone, the Schedule activation times for the Trigger occur according to the apC Panel Time Zone.

If you have an apC panel in the Pacific Time Zone (GMT - 08:00) and a server in the Eastern Time Zone (GMT - 05:00), a Schedule that is active from Midnight to 6:00 AM is activated from Midnight to 6:00 AM in Pacific Time rather than Eastern time (three hours later).

To Define a Trigger for an apC Device

1. Click on the Triggers tab for your apC device.
2. Click **Add** on the Triggers tab to create a new Trigger.
3. Click [...] within the **Property** column to open the Property dialog box showing the Properties available for the device.
4. Click a Property in the list to select it and add it to the **Property** column.
5. Click [...] within the **Value** column to display a drop-down list of Values associated with the Property that you have selected. Click a **Value** that you want to include as a parameter for the trigger to add it to the column. (If there is no set list of Values, you can type in a Value.)
6. Click [...] within the **Action** column to display a drop-down list of valid actions. Click an Action that you want to include as a parameter for the trigger to add it to the column.
7. When you select an Action, the lower pane in the Triggers box displays an entry field or group of entry fields, specific to the selected Action, so that you can configure the Details for the Action.
8. Once you define the Action details, the **Details** column displays information about how the Action has been configured.

   For example, if an Event field is displayed in **Details**, you can click to select an Event that you want to associate with the Trigger.
9. If the Triggers tab includes a **Schedule** column, click within the **Schedule** column to display a drop-down list of pre-configured schedules. Click [...] to select a **Schedule** that you want to associate with the trigger. Schedules are created in the Configuration Pane. See the *C•CURE 9000 Software Configuration Guide* for more information.
10. If the Triggers tab includes a **Time Zone** column, click within the **Time Zone** column to display a drop-down list of available Time Zones. If the Time Zone column is blank, or you do not select a Time Zone, the Time Zone of the C•CURE 9000 server is used by default.
11. Click **Save and Close** to save the apC trigger.

NOTE Triggers related to apC objects cannot activate an Event that is downloaded to an iSTAR controller.

apC Triggers Tab Definitions

Table 84 on Page 371 provides definitions for the fields and buttons on an apC Triggers tab.

Table 84: apC Triggers Tab Definitions

Field/Button	Description
Add	Click **Add** in the Triggers tab to create a new trigger.
Remove	Click the Row Selector [▸], then click **Remove** in the Triggers tab to delete a trigger.
[▸]	Click the Row Selector to select a row in the Triggers table.

Table 84: apC Triggers Tab Definitions (continued)

Field/Button	Description
Property	Click within the **Property** column, and then click [...]. The Property browser opens presenting properties available for the Comm Port. Click a Property to select it and add it to the column.
Value	Click within the **Value** column to display a drop-down list of Values associated with the Property that you have selected. Click a Value that you want to include as a parameter for the trigger to add it to the column.
Action	Click [...] within the **Action** column to display a drop-down list of valid actions. Click an Action that you want to include as a parameter for the trigger to add it to the column. As you select an Action, a corresponding entry field, or group of entry fields, appear at the bottom of the dialog box. Click to select entries for these fields.
Details	Displays details about how the Action was configured.
Schedule	Click within the **Schedule** column to select a Schedule. Click [...] to select a Schedule that you want to associate with the trigger. Schedules are created in the Configuration Pane. Refer to the *C•CURE 9000 Software Configuration Guide* for more information on creating Schedules.
Time Zone	Click within the **Time Zone** column to select a Time Zone for Schedule activation. Click [...] to select a Time Zone that you want to associate with the trigger Schedule.If you specify a Time Zone, the Schedule start and end times are calculated using that Time Zone. For example, a Schedule that becomes active at 3:00 AM would become active at 3:00 AM in the Pacific Time Zone, if that Time Zone was specified. Refer to the *C•CURE 9000 Software Configuration Guide* for more information on Time Zones.

Mini Star Coupler Board Editor

Mini Star Couplers are single expansion boards that attach to the apC/8X or apC panels to allow the RM readers to be wired in a star topology. For more information, see the *Star Coupler - Mini Star Coupler Quick Start Installation Guide*.

NOTE Mini Star Coupler Boards have not been evaluated by UL and cannot be used in UL Listed applications

To Configure the Mini Star Coupler Board

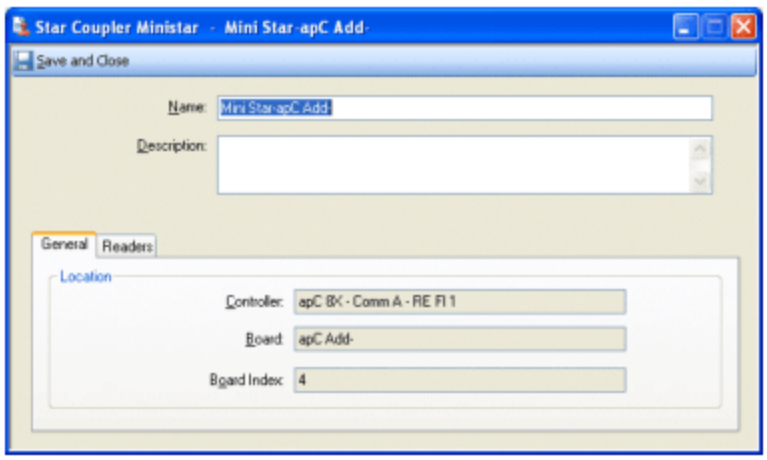
1. To configure the **Mini Star Coupler Board**, select the check box in the **Configured** column in the **apC Add-On Board - Star Coupler** tab and click [...] located in the **Edit** column of the **Star Coupler** box (see Figure 129 on Page 355) to display the **Mini Star Coupler - General** tab, as shown in Figure 141 on Page 373.

   The **Mini Star Coupler Board - General** tab (see Figure 141 on Page 373) displays three read-only fields:

   - Controller
   - Board
   - Board Index

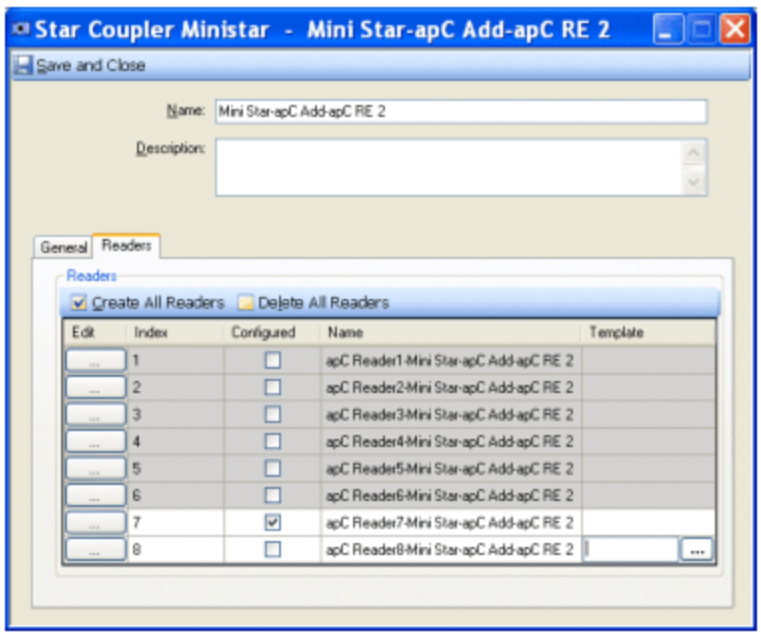
   These fields are located on the Mini Star Coupler that you have chosen to configure. As you configure more Add-On Boards for this controller, the Board Index field will reflect each placement, to differentiate board locations.

Figure 141: apC Controller Add-On Board Mini Star Coupler General Tab



2. Click the **Readers** tab to configure readers for the **Mini Star Coupler**.

Figure 142: apC Controller Add-On Board Mini Star Coupler Readers Tab

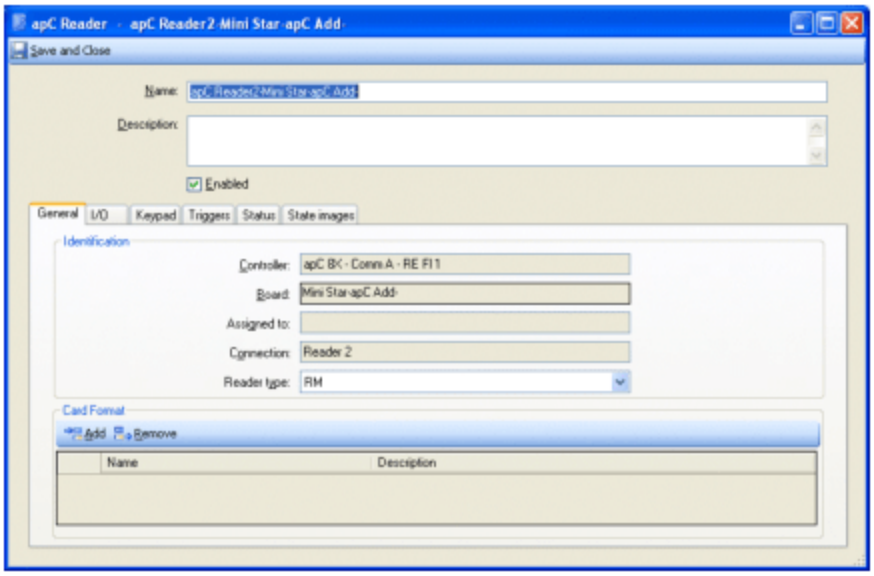


3. Select the check box in the **Configured** column for the **Mini Star Coupler Readers** (Index 1 through 8) and click [...] located in the **Edit** column to display the **Mini Star Coupler Readers - General** tab, shown in Figure 143 on Page 374.

   The 8 available Mini Star Coupler Readers allow up to 2 Supervised Inputs and 2 Outputs. For further instructions for reader readers, see To Configure an apC Reader on Page 323.

NOTE Readers that are unavailable (see Figure 142 on Page 374) have already been configured on the apC panel Readers tab.

Figure 143: apC Controller Add-On Board Mini Star Coupler Readers General Tab



4. Click **Save and Close** to return to the **apC Controller - Add-On Board - Star Coupler** tab.

Be sure that the **Mini Star Coupler Board** is installed correctly on the apC or apC/8X. For more information, see the *Star Coupler - Mini Star Coupler Quick Start Installation Guide*.

5. Click **Save and Close** to return to the **apC Controller - Add-On Board** tab.

Wiegand Proximity Star Coupler Editor

The Wiegand/Proximity Star Coupler (WPSC) consists of a two board set that attaches to the apC or apC/8X to allow direct connection of up to 8 read heads using Wiegand signaling. The WPSC board set consists of a Lower Board and an Upper Board. The Lower Board provides connections for 4 readers indexed 1-4 and 4 inputs indexed 17-23. The Upper Board provides connections for 4 readers indexed 5-8 and 4 inputs indexed 25-31.

When using the WPSC Add-On Board, the standard Star Coupler cannot be used because the WPSC board set attaches to the same bus connector as the Star Coupler.

Each board provides one supervised input for each reader, which should be used in conjunction with one of the 8 supervised inputs on the apC main board to provide a total of two supervised inputs for each reader.

NOTE The supervised inputs on the WPSC remain inactive in the Monitoring Station unless readers are configured in the WPSC editor.

Since the WPSC board set does not provide output relays, it is recommended that the 8 on-board apC relays be used. For more information, see the *WPSC Quick Start Installation Guide*.

To Configure the Wiegand/Proximity Star Coupler Board

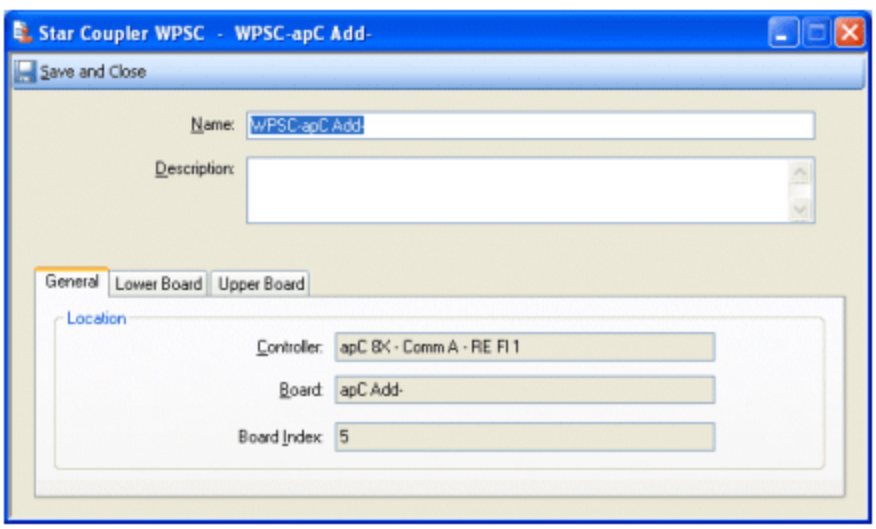
1. To configure the **Wiegand/Proximity Star Coupler (WPSC) Board**, select the **WPSC** check box in the **Configured** column in the **apC Add-On Board - Star Coupler** tab and click [...] located in the WPSC **Edit** column of the **Star Coupler** box.

   The **Wiegand/Proximity Star Coupler Board General** tab displays three read-only fields:

   - Controller
   - Board
   - Board Index

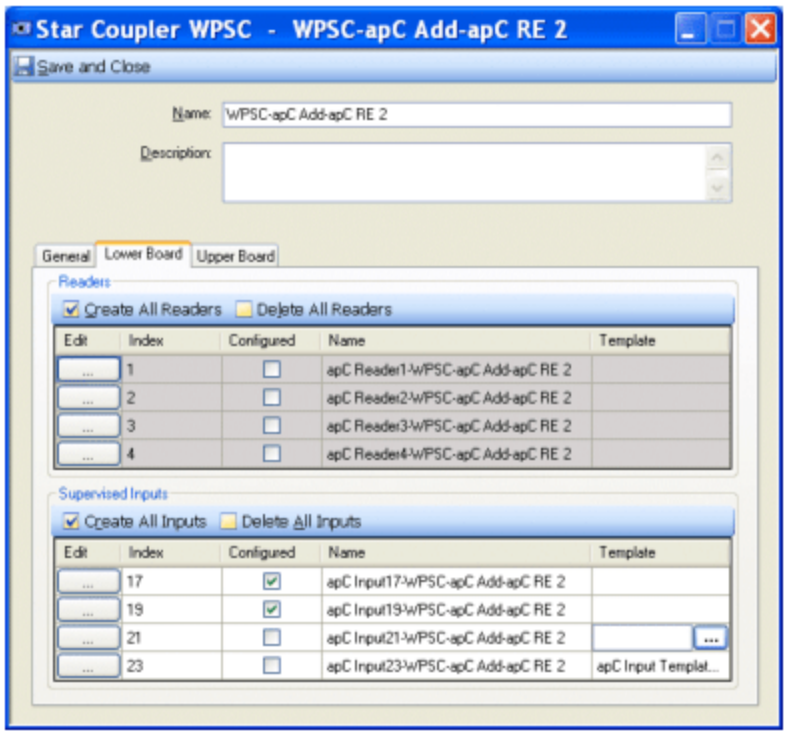
   These fields are located on the Wiegand/Proximity Star Coupler that you have chosen to configure. As you configure more Add-On Boards for this controller, the Board Index field will reflect each placement, to differentiate board locations.

Figure 144: apC Controller Add-On Board Wiegand Proximity Star Coupler General Tab



2. Click the Lower Board tab to display the 4 available WPSC Readers and 4 Unsupervised WPSC Inputs, as shown in Figure 145 on Page 377.

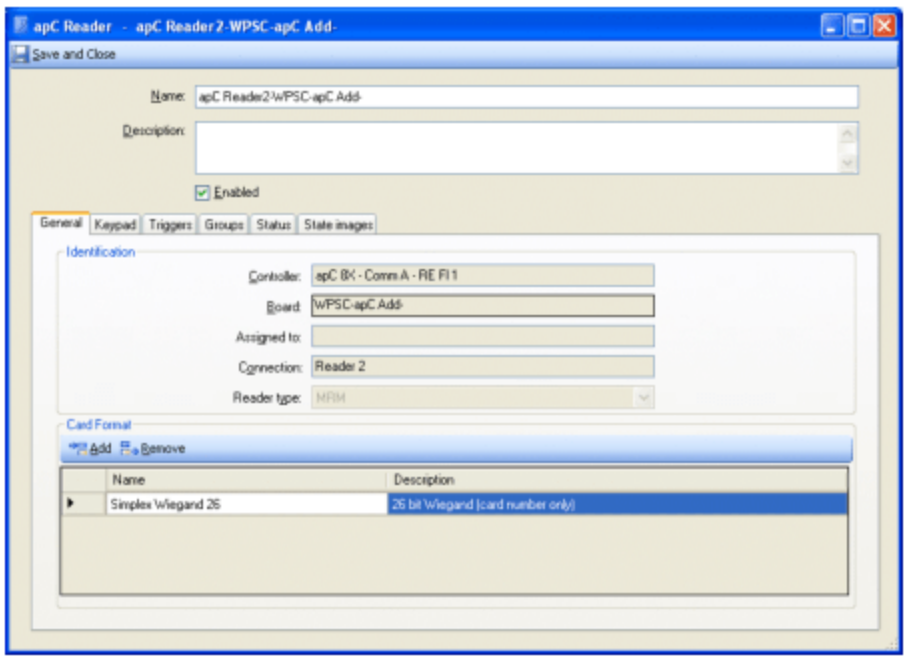
Figure 145: apC Controller Add-On Board WPSC Lower Board Tab



3. Select the check box in the **Configured** column for the **WPSC Readers** (Index 1 through 4) and click ... located in the **Edit** column to display the **apC Readers - General** tab, shown in Figure 146 on Page 378.

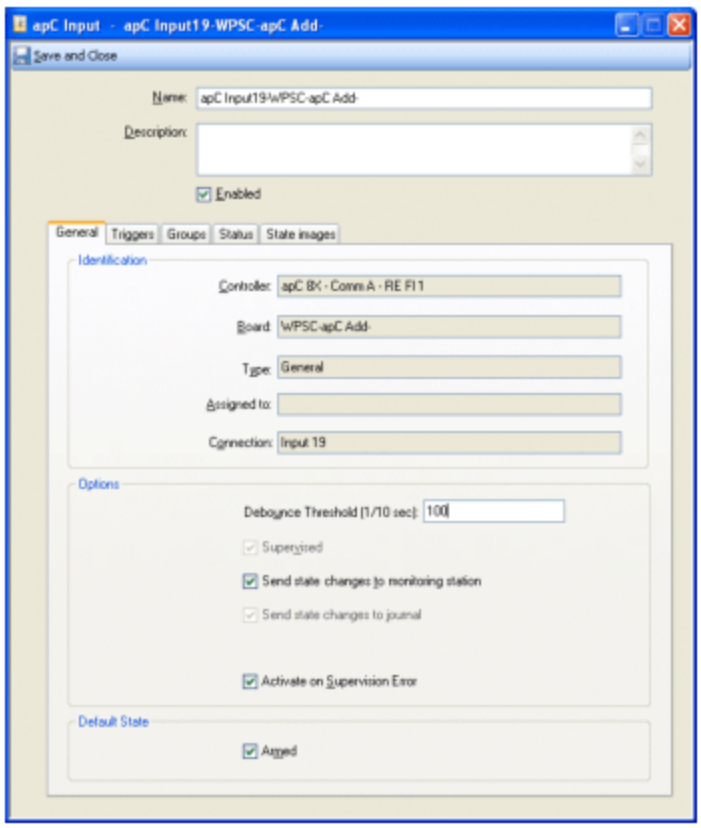
   You can configure the reader keypad and triggers for each of the 4 available WPSC Readers. For further instructions see apC Controller Readers Tab on Page 323.

Figure 146: apC Controller Add-On Board WPSC Lower Board Reader General Tab



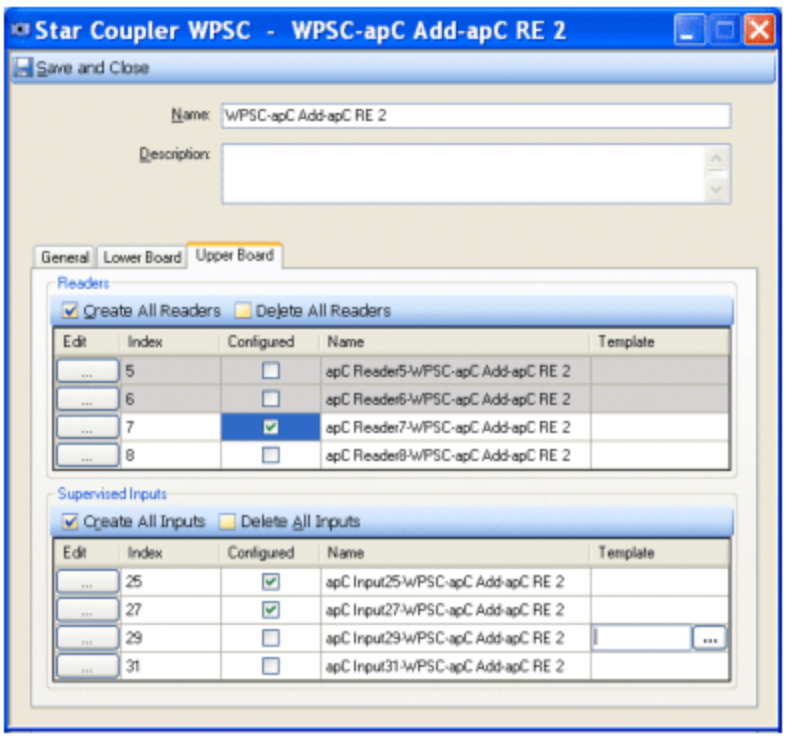
4. To configure **Inputs**, select the check box in the **Configured** column in the **Wiegand/Proximity Star Coupler - Inputs** tab and click [...] located in the **Edit** column to display the **apC Add-On Board - Wiegand/Proximity Star Coupler** Input - **General** tab, as shown in Figure 147 on Page 379.

Figure 147: apC Controller Add-On Board WPSC Lower Board Input General Tab



5. To configure the **Inputs** on the **Wiegand/Proximity Star Coupler Add-On Board - Inputs** tab, follow the instructions given in To Configure apC Controller Inputs on Page 322.

Figure 148: apC Controller Add-On Board WPSC Upper Board Tab



6. Click **Save and Close** to return to the **apC Controller - Add-On Board - Star Coupler** tab.

   Be sure that the **Wiegand/Proximity Star Coupler Board** is installed correctly on the apC or apC/8X. For more information, see the *WPSC Quick Start Installation Guide*.

7. Click **Save and Close** to return to the **apC Controller - Add-On Board** tab.

8. Click the **Status** tab to display it, as shown in Figure 108 on Page 326.

   - Or -

   Click **Save and Close** to return to the **Hardware Pane** and finish the **apC Controller** configuration later.

8

Chapter Configuring RM Reader LCD Messages

This chapter explains how to customize sets of LCD messages, such as "Present Card" or "Access Granted," for your RM readers to meet the specific needs of your facility or site.

In this chapter

Reader LCD Message Set Overview

RM readers display LCD messages, such as "Present Card" or "Access Granted" to indicate different states to cardholders. You can customize sets of these messages to meet the specific needs of your facility or site.

Example:

You could change the "Access Granted" message to "Please Enter Now".

When you assign a set of messages to an iSTAR Controller or an apC Panel, all the RM readers on that controller use those same messages.

The **Reader LCD Message Set Editor** allows you to configure message sets. You can also use the **Reader LCD Message Set Editor** to change the language in which your messages appear. See Changing the Language for the Default RM LCD Messages on Page 393.

NOTE

Only ASCII characters 0 to 125 are supported for display on the RM Reader.

- There are 94 printable characters. (Code 1 to 31 are non-printing, mostly obsolete characters that affect how text is processed.)
- No accented characters are supported.

Reader LCD Message Set Editor

The **Reader LCD Message Set Editor**, shown in Figure 149 on Page 383, lets you create and modify message sets in C•CURE 9000 containing replacement texts for the LCD messages that display on the RM Readers. In addition, the editor lets you set the way that the date and time display on the Reader. The **Reader LCD Message Set Editor** has only one tab—the **General** tab. For more information, see:

- Accessing the Reader LCD Message Set Editor on Page 383
- Reader LCD Message Set Definitions on Page 384
- Creating a Reader LCD Message Set on Page 388

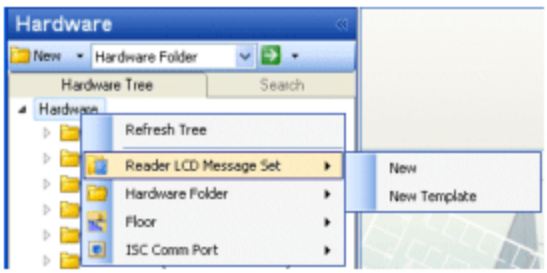
Accessing the Reader LCD Message Set Editor

You access the **Reader LCD Message Set Editor** from the C•CURE 9000 Hardware pane.

To Access the Reader LCD Message Set Editor

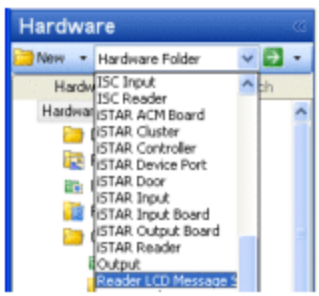
1. Click the **Hardware** button in the Navigation Pane to open the **Hardware** Tree.
2. Right-click the **Hardware** Folder, click **Reader LCD Message Set**, and click **New** on the sub-menu that appears, as shown in Figure 149 on Page 383. (Once you have created a message set, a **Reader LCD Message Set** folder appears in the **Hardware** Tree.)

Figure 149: Hardware Tree Reader LCD Message Sets



- or -

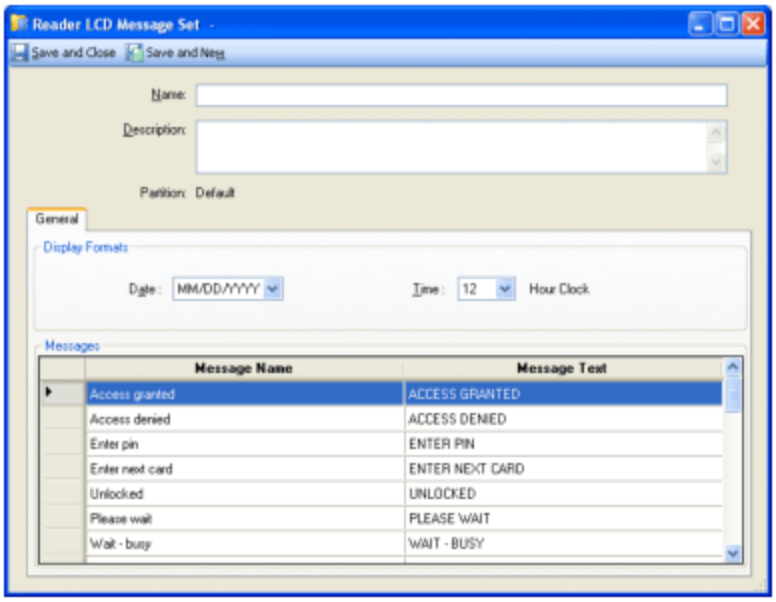
Click the **Hardware** drop-down list and scroll down to select **Reader LCD Message Set**.



Click  to open a Dynamic View showing a list of all existing Reader LCD Message Sets, right-click the Reader LCD Message Set you want to change, and click **Edit** from the context menu that appears.

The **Reader LCD Message Set Editor** opens with the **General** tab displayed, as shown in Figure 150 on Page 384.

Figure 150: Reader LCD Message Set Editor



Reader LCD Message Set Definitions

The **Reader LCD Message Set Editor** has the buttons described in Table 85 on Page 384 and the fields shown in Table 86 on Page 384. Table 87 on Page 385 has detailed information about each of the 34 messages that can be customized for a message set.

Table 85: Reader LCD Message Set Editor Buttons

Button	Description
Save and Close	Click this button when you have completed changes to the Reader LCD Message Set and wish to save those changes. The **Reader LCD Message Set Editor** closes.
Save and New	Click this button when you have completed any changes to the Reader LCD Message Set and wish to save those changes and also create a new Reader LCD Message Set. The message set you were editing is saved, and a new Reader LCD Message Set opens (either blank or including template information if you were using a template to create the message set).
	Click this button when you want to close the **Reader LCD Message Set 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.

Table 86: Reader LCD Message Set Editor - General Tab

Field/Button	Description
Top of Editor	
Name	Enter a name for the Reader LCD Message Set.

Reader LCD Message Set Editor - General Tab (continued)

Field/Button	Description
Description	Enter a brief description for this Reader LCD Message Set.
Partition	This read-only field identifies the Partition to which this Reader LCD Message Set belongs. (This field is visible only if the C•CURE 9000 system is partitioned.)
Display Formats	
Date	Select the format for the date display: **MM/DD/YY** (the default) or **DD/MM/YY**
Time: Hour Clock	Select the format for the time display: **12 hour** (the default) **or 24 hour**.
Messages	
Message Name	Name of the Reader LCD Message string.
Message Text	Default text for the Reader LCD Message.

Table 87: Reader LCD Messages

Message Name	Message Text	Description	iSTAR Uses	apC Uses
Access granted	ACCESS GRANTED	Admit text–general use	Yes	Yes
Access denied	ACCESS DENIED	Reject text–general use	Yes	Yes
Enter PIN	ENTER PIN	Enter PIN prompt–general use	Yes	Yes
Enter next card	ENTER NEXT CARD	Enter next card prompt–used for occupancy and visitor/escort features	Yes	Yes
Unlocked	UNLOCKED	Door unlocked mode text–general use	Yes	Yes
Please wait	PLEASE WAIT	Text displayed while access decision pending–general use	Yes	Yes
Wait - busy	WAIT - BUSY	Text displayed when door busy processing a previous access–general use	Yes	Yes
Enter floor	ENTER FLOOR	apC display for elevator admit–general use	**No**	Yes
Reader not ready	READER NOT READY	Text displayed when reader disabled–general use	Yes	Yes
Present card	PRESENT CARD	Locked Door mode text–general use	Yes	Yes
Enter command	ENTER COMMAND	Intrusion entrance delay text–intrusion zone feature	Yes	**No**

Reader LCD Messages (continued)

Message Name	Message Text	Description	iSTAR Uses	apC Uses
Misread card	MISREAD	Visitor/escort misread card feedback text–visitor/escort feature	Yes	**No**
All secure	ALL SECURE	Intrusion zone all inputs secure text–intrusion zone feature	Yes	**No**
Exit now	EXIT NOW	Intrusion exit delay text–intrusion zone feature	Yes	**No**
Ready to arm	READY TO ARM	Intrusion zone ready to arm status text–intrusion zone feature	Yes	**No**
Not ready to arm	NOT READY TO ARM	Intrusion zone not ready to arm status text–intrusion zone feature	Yes	Yes
Door in alert	DOOR IN ALERT	iSTAR reader tampered text, or apC reader tamper or door held forced open text–general use	Yes	Yes
Area armed	AREA ARMED	Intrusion zone armed mode text–intrusion zone feature	Yes	Yes
Area disarmed	AREA DISARMED	Intrusion zone disarmed mode text–intrusion zone feature	Yes	Yes
Secure pending	SECURE PENDING	Intrusion zone disarm pending text–intrusion zone feature	Yes	**No**
Secure	SECURE	Door secure mode text–general use	Yes	Yes
Keypad Command Issued	CMD ISSUED	Keypad command issued text–keypad commands feature	Yes	**No**
Keypad Command Failed	CMD FAILED	Keypad command failed text–keypad commands feature	Yes	**No**
Keypad Command Prompt 1	ENTER ACCESS	Keypad command prompt 1 text–keypad commands feature	Yes	**No**
Keypad Command Prompt 2	ENTER TARGET	Keypad command prompt 2 text–keypad commands feature	Yes	**No**
Acknowledged	ACKNOWLEDGED	Enter next card acknowledgement text–occupancy and visitor/escort features	Yes	Yes
Enter escort	ENTER ESCORT	Request Escort prompt–occupancy and visitor/escort features	Yes	**No**
Secure violated	SECURE VIOLATED	Intrusion zone armed and violated status text–intrusion zone feature	Yes	**No**
Secure offnormal	SECURE OFFNORMAL	Intrusion zone armed but not ready to re-arm status text–intrusion zone feature	Yes	**No**

Reader LCD Messages (continued)

Message Name	Message Text	Description	iSTAR Uses	apC Uses
Lockout HHH:MM	LOCKOUT & T	Area lockout reject & T will be replaced with remaining lockout time HHH:MM–area lockout feature	Yes	**No**
Reject unattended	REJECT UNATTEND	Occupancy reject indicates that supervisor/escort cannot leave supervisees/visitors unattended–occupancy feature	Yes	Yes
Reject occupancy	REJECT OCCUPANCY	Occupancy general reject text–occupancy feature	Yes	Yes
Door held open	DOOR HELD OPEN	iSTAR door held open status text–STAR only (apC displays Door in Alert instead)	Yes	**No**
Door forced open	DOOR FORCED OPEN	iSTAR door forced open status text–iSTAR only (apC displays Door in Alert instead)	Yes	**No**

Reader LCD Message Set Tasks

You can perform the following tasks to configure Reader LCD Message Sets.

Creating a Reader LCD Message Set

You can create a new Reader LCD Message Set.

To Create a Reader LCD Message Set

1. Click the **Hardware** button in the Navigation Pane to open the **Hardware** Tree.
2. Right-click the **Hardware** Folder, click **Reader LCD Message Set**, and click **New** on the sub-menu that appears.

   - or -

   If Reader LCD Message Sets were already created, right-click the **Reader LCD Message Sets** Folder and click **New** on the sub-menu that appears.
3. The **Reader LCD Message Set Editor** opens, and you can configure the message set.
4. To save your new Reader LCD Message Set, click **Save and Close**.

   - Or -

   Alternatively, if you want to save the Reader LCD Message Set and then create a new one, click **Save and New**. The current Reader LCD Message Set is saved and closed, but the **Reader LCD Message Set Editor** remains open to allow you to create a new Reader LCD Message Set.

Creating a Reader LCD Message Set Template

You can create a new template for a Reader LCD Message Set. A Reader LCD Message Set template saves you time because you can reuse the same configuration repeatedly.

To Create a Reader LCD Message Set Template

1. Click the **Hardware** button in the Navigation Pane to open the **Hardware** Tree.
2. Right-click the **Hardware** Folder, click **Reader LCD Message Set**, and click **New Template** on the sub-menu that appears.

   - or -

   If Reader LCD Message Sets were already created, right-click the **Reader LCD Message Sets** Folder and click **New Template** on the sub-menu that appears.

The **Reader LCD Message Set Editor** where you can configure the Reader LCD Message Set template opens.

3. 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 Reader LCD Message Set from that template, these values are already filled in.
4. In the **Name** field, enter the name you wish to use for the template.

   Example:

   Reader LCD Message Set Template1
5. To save the template, click **Save and Close**.

   The template will be available as an option on the pull-down Template menu.

Configuring/Modifying a Reader LCD Message Set

You can configure a new Reader LCD Message Set or modify an existing one using the **Reader LCD Message Set Editor**.

To Configure/Modify a Reader LCD Message Set

1. Create a new Reader LCD Message Set or modify an existing Reader LCD Message Set.

   The **Reader LCD Message Set Editor** opens for you to edit the Reader LCD Message Set making changes as you wish in the fields on the top of the editor and on the **General** tab.
2. Type a **Name** and **Description** for the Reader LCD Message Set that sufficiently identifies this message set and its purpose.
3. Select your desired date format—by either leaving the default **MM/DD/YY** or clicking the down-arrow to pick **DD/MM/YY**.
4. Select your desired time format—by either leaving the default **12** Hour Clock or clicking the down-arrow to pick the **24** Hour Clock.
5. In the **Messages** box, use the vertical scroll bar to find the message you wish to modify in the **Message Name** column and change its related entry in the **Message Text** column as desired.

   There are 34 messages whose text you can modify for your uses. Many of them are used by (can be downloaded to) both iSTAR and apC controllers; one of the messages is used only by apCs, while about 15 messages are used only by iSTARs. For detailed information about the messages, see Reader LCD Message Set Definitions on Page 384.

Viewing a List of Reader LCD Message Sets

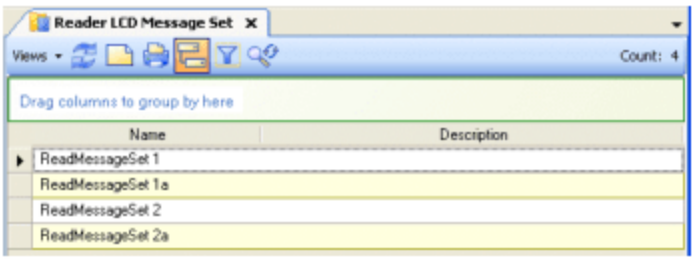
You can display a list of the Reader LCD Message Sets you have created by opening a Dynamic View of Reader LCD Message Sets.

To View a List of Reader LCD Message Sets

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.

2. Select **Reader LCD Message Set** from the **Hardware** drop-down list and click to open a Dynamic View showing a list of all existing Reader LCD Message Sets, as shown in Figure 151 on Page 390. (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 151: Reader LCD Message Set List



- You can sort, filter, and group items in the list.
- You can right-click a Reader LCD Message Set in the list to open the Reader LCD Message Set Context menu (see Table 88 on Page 390) and perform any of the functions on that menu.
- You can right-click any column heading to open a context menu of all possible Reader LCD Message Set fields that can display as columns and add/remove fields to view certain information.

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

Reader LCD Message Set List Context Menu

The context menu that opens when you right-click a Reader LCD Message Set in the Reader LCD Message Set Dynamic View includes the selections described in Table 88 on Page 390.

Table 88: Reader LCD Message Set List Right-Click Context Menu Options

Menu Selection	Description
Edit	Click this menu selection to edit the selected Reader LCD Message Set. The **Reader LCD Message Set Editor** opens. You can rename the message set and change any of its attributes.
Delete	Click this menu selection to delete the selected Reader LCD Message Set. A prompt appears asking you to confirm that you want to delete the Reader LCD Message Set. Click **Yes** to delete the Reader LCD Message Set or **No** to cancel the deletion. NOTE: You cannot delete a Reader LCD Message Set if it is being used by an iSTAR and/or apC Controller.
Set property	Click this menu selection to change the value of the selected properties in the selected Reader LCD Message Set(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 property: • **Description** – You can change the textual description of the Reader LCD Message Set(s) by selecting this property and typing in a new value.
Add to Group	This option is **not** supported for Reader LCD Messages.

Reader LCD Message Set 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 Reader LCD Message Set 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 Reader LCD Message Set. 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 Reader LCD Message Set. When found the results display in a separate Dynamic View.

Deleting a Reader LCD Message Set

You can delete a Reader LCD Message Set if it is **not** currently being used by any iSTAR and/or apC Controller.

To Delete a Reader LCD Message Set

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Select **Reader LCD Message Set** from the **Hardware** pane drop-down list.
3. Click  to open a **Dynamic View** showing all Reader LCD Message Set objects.
4. Right-click the Reader LCD Message Set(s) in the list that you want to delete and select **Delete** from the context menu. A confirmation message appears.
5. Click **Yes** to confirm the deletion of the Reader LCD Message Set or click **No** to cancel the deletion.

   If you click **Yes**, the **Reader LCD Message Set objects** dialog box appears showing the results of the delete operation, with one line per message set. If no controllers are using the message set(s), the line shows that the message set was deleted. If, however, the message set is in use, the message **Unable to delete object - The**

message set is currently in use by iSTAR or apC controllers. Please remove the message set from the controller(s) is displayed.

Using Set Property to Configure Reader LCD Message Sets

You can use **Set Property** to quickly set a property for one or more Reader LCD Message Sets without opening the **Reader LCD Message Set Editor**, thus making it useful for mass updates. See Table 88 on Page 390 for the properties that can be changed.

To Set a Property for a Reader LCD Message Set

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Select **Reader LCD Message Set** from the **Hardware** pane drop-down list.
3. Click  to open a **Dynamic View** showing all **Reader LCD Message Set** objects.
4. Right-click the **Reader LCD Message Set(s)** 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 **Reader LCD Message Set(s)**. 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 Reader LCD Message Set** message box.

Changing the Language for the Default RM LCD Messages

You can use the **Reader LCD Message Set Editor** to easily change the language in which the default messages appear. When you first start the C•CURE 9000, the default messages appear in the system-wide primary language you chose during installation.

Example:

You chose English as the primary system language and configured all the sets of English messages your Boston site needs; you may now want to customize some message sets in French for your Montreal site.

NOTE The C•CURE 9000Multilingual User Interface (MUI) Editor, available as a licensable option when purchasing C•CURE 9000, allows you to localize the C•CURE 9000 user interface for a broad range of languages and cultures. When installed and enabled, the C•CURE 9000 MUI Editor allows anyone with appropriate access permissions to localize individual screens and system messages, including the Reader LCD Message Sets, from within C•CURE 9000 at any time. For information on the MUI Editor see the chapter, "Displaying the C•CURE 9000 in Multiple Languages" in the *C•CURE 9000 System Maintenance Guide*.

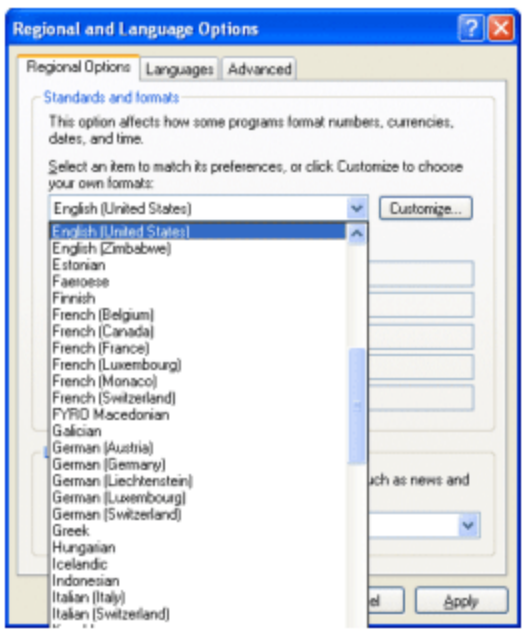
To Change the Language for the Default Message Set

1. Exit the C•CURE 9000 Administration Application.
2. Go to the **Windows Control Panel** and click **Regional and Language Options**.
3. Use the **Regional Options** tab on the **Regional and Language Options** dialog box to change to the language and culture you need by clicking the down- arrow to scroll to your choice and the **Customize** button to specify your own required formats.

   Example:

   French (Canada).

Figure 152: Windows Regional and Language Options Screen



4. Click **Apply** and then **OK**.
5. Restart the Administration Application, click the **Hardware** button in the Navigation Pane.
6. Right-click the **Reader LCD Message Sets** Folder in the **Hardware** tree and click **New** on the sub-menu that appears, as shown in Figure 149 on Page 383.
7. The **Reader LCD Message Set Editor** opens, and you can customize a set of messages in French.

9

Floors

This chapter explains how to configure Floors in C•CURE 9000. Floors are part of Elevator access control. An Elevator associates a Floor with an Input or Output.

In this chapter

Floors Overview

Floors are configured to define Elevator control. Floors are paired with inputs and outputs to control floor access through elevators. Before you can configure elevators, you must configure floors and/or floor groups. See Elevator Configuration Overview on Page 500 for more information.

When a person presents a card at an elevator, the system checks the clearances associated with the card for the elevator and associated floors. If the person's clearances do not allow access, the access attempt is rejected before the person presses an elevator button. If the person has access to a floor, the system grants access to the person and activates the output attached to the button for that floor.

A Floor has only Name, Description and Enabled properties. If the Floor has been assigned to any Elevators, they will appear in a read-only list on the Floor General tab.

NOTE Elevator controls have not been evaluated by UL.

Configuring Floors

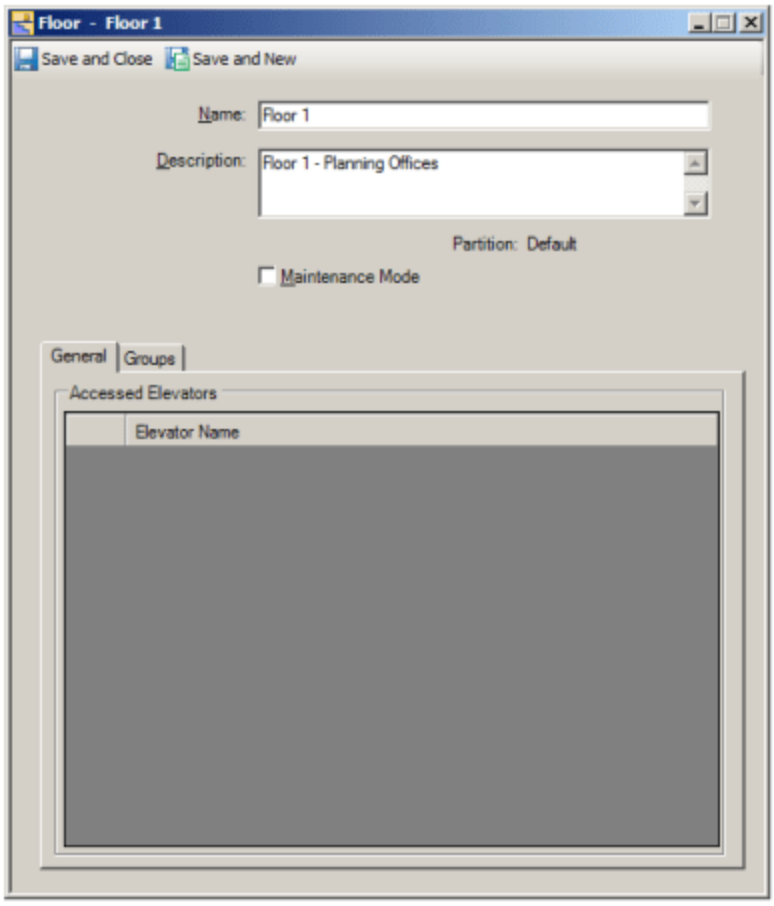
Accessing the Floor Editor

You can access the Floor editor from the C•CURE 9000 Hardware pane.

To Access the Floor Editor

1. Click the **Hardware** pane button.
2. Click the **Hardware** drop-down list and select **Floor**.
3. Click  to open a **Dynamic View** showing all **Floor** objects.
4. Double-click the **Floor** in the list that you want to edit, and the **Floor General** tab opens, as shown in Figure 153 on Page 397.

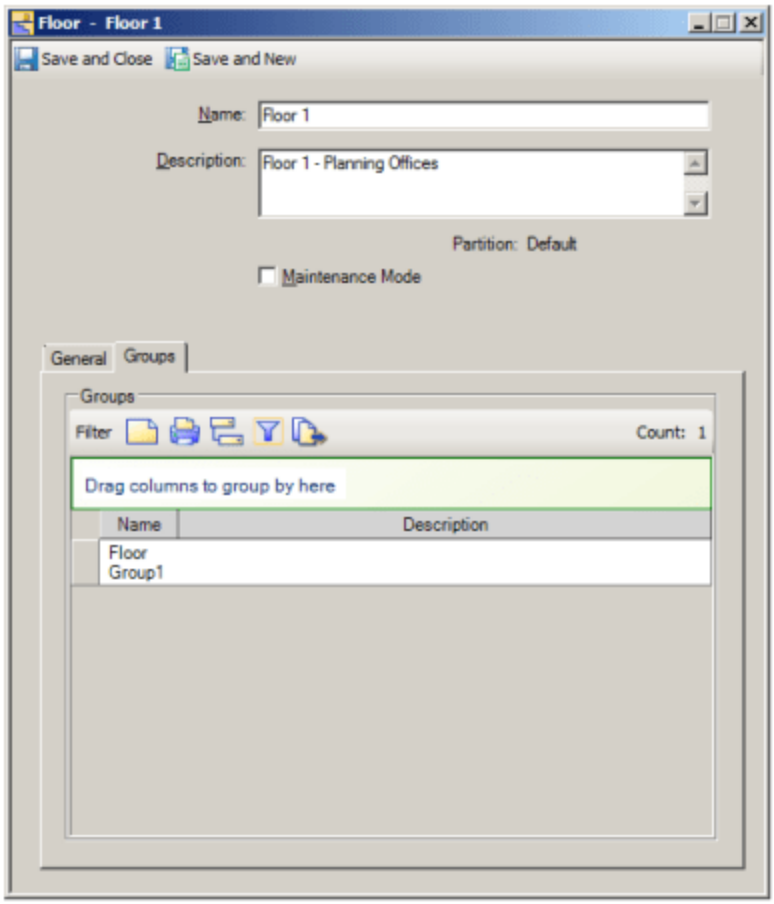
Figure 153: Floor General Tab



5. Type a name for the **Floor** in the **Floor Name** field.
6. Type a description for the **Floor** in the **Description** field.
7. Select **Enable** to indicate that the Floor is available for use. **Elevators** that are assigned to the **Floor** will be shown in the **Accessed Elevators** box.

8. **Maintenance Mode** - Click to put the Floor into Maintenance Mode. See Chapter 2: Maintenance Mode for more information.
9. Click **Save and Close** when you are finished.
10. When you create a Floor group, a Group tab will appear with the Floor General tab, as shown in Figure 154 on Page 398.

Figure 154: Floor Groups Tab



Floor Definitions

The definitions for the fields and buttons on the Floor General tab are listed in Table 89 on Page 398.

Table 89: Floor General Tab

Field/Button	Description
Name	Enter a name for the floor.
Description	Enter a brief description for this floor.
Maintenance Mode	Click to put the floor into Maintenance Mode. See Chapter 2: Maintenance Mode for more information.

Table 89: Floor General Tab (continued)

Field/Button	Description
Enabled	Check this box to put the floor online. When the floor is offline, the C•CURE 9000 System ignores the floor.
Accessed Elevators	Displays a list of elevators with buttons associated with this floor. These associations are set when you configure the Elevators.
Save and Close	Click **Save and Close** to accept your changes to the Floor configuration.

Creating a Floor

You can create a new Floor.

To Create a Floor

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Select **Floor** from the **Hardware** pane drop-down list.
3. Click **New** to create a new **Floor**. The **Floor Editor** opens and you can configure the **Floor**.
4. To save your new **Floor**, click **Save and Close**.

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

Creating a Floor Template

You can create a new template for a Floor. A Floor template saves you time because you can reuse the same configuration repeatedly.

To Create a Floor Template

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Select **Floor** from the **Hardware** pane drop-down list.
3. Click the drop-down arrow next to **New** and select **Template**.
4. The **Floor Template** opens and you can configure the Floor template.
5. To save your new **Floor Template**, click **Save and Close**.

The new Floor template appears under Templates in the Template drop-down list.

To Select a Floor Template

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Select **Floor** from the **Hardware** pane drop-down list.
3. Click the drop-down arrow next to **New** and select **Template**.

4. Select the template you wish to use under Templates.

Deleting a Floor

You can delete a Floor.

To Delete a Floor

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Select **Floor** from the **Hardware** pane drop-down list.
3. Click to open a **Dynamic View** showing all Floor objects.
4. Right-click the Floor in the list that you want to delete and select **Delete** from the context menu.
5. Click **Yes** on the "**Are you sure you want to delete the selected Floor?**" message box.

Modifying a Floor

You can edit a Floor.

To Edit a Floor

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Select **Floor** from the **Hardware** pane drop-down list.
3. Click to open a **Dynamic View** showing all Floor objects.
4. Double-click the **Floor** in the list that you want to modify and select **Edit** from the context menu. The **Floor Editor** opens.

Viewing a List of Floors

You can view a list of Floors.

To View a List of Floors

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Select **Floor** from the **Hardware** pane drop-down list.
3. Click to open a **Dynamic View** showing all **Floor** objects.

Using Set Property to Configure Floors

You can use Set Property to quickly set a property for a Floor without opening a Floor. Set Property allows you to select multiple Floors in the dynamic list, and right-click to use Set Property to set a specific property for all of them. So, for example, if you wanted to change a setting for 20 Floors, you could select all of them and do it in one step.

To Set a Property for a Floor

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Select **Floor** from the **Hardware** pane drop-down list.
3. Click to open a **Dynamic View** showing all **Floor** objects.
4. Right-click the **Floor** 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 **Floor**. 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 Floor** message box.

Add Floors to a Group

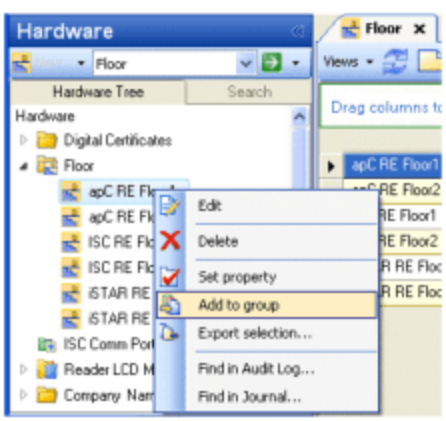
You can use Add To Group for Floors. Add Floors To Group enables you to add the Floor object to the group. When you create a Floor group, a Group tab will appear with the Floor - General tab.

To Add Floors To a Group

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Select **Floor** from the **Hardware** pane drop-down list.
3. Click to open a **Dynamic View** showing all **Floor** objects.
4. Right-click the **Floor** in the list that you want to add to a group and select **Add To Group** from the context menu.

   Figure 155 on Page 401 displays the Hardware pane and the context menu from which you can add a floor object to a Group.

Figure 155: Hardware Pane - Adding a Floor to a Group



10

Doors

A Door in C•CURE 9000 provides access control by specifying the controllers, readers, inputs, and outputs associated with an entrance. From the application's hardware tree, you will configure the specific controller type first, then configure the associated readers, inputs, and outputs, and then configure the Door. This sequence of reader the security components is necessary because each door requires the associated components to operate with their apC or iSTAR controllers.

In this chapter

Door Overview

In general, a door is a logical structure that ties together a controller and its associated readers, inputs, and outputs for access control. In C•CURE 9000, before you configure the door you must first configure the type of controller that is to be used for the readers, input, and outputs. Then you can configure the door associated with the components.

Figure 156 on Page 404 represents the way readers, inputs, outputs, events, and areas are related to Doors in C•CURE 9000, while Table 90 on Page 404 describes typical door components.

Figure 156: Typical Door Configuration

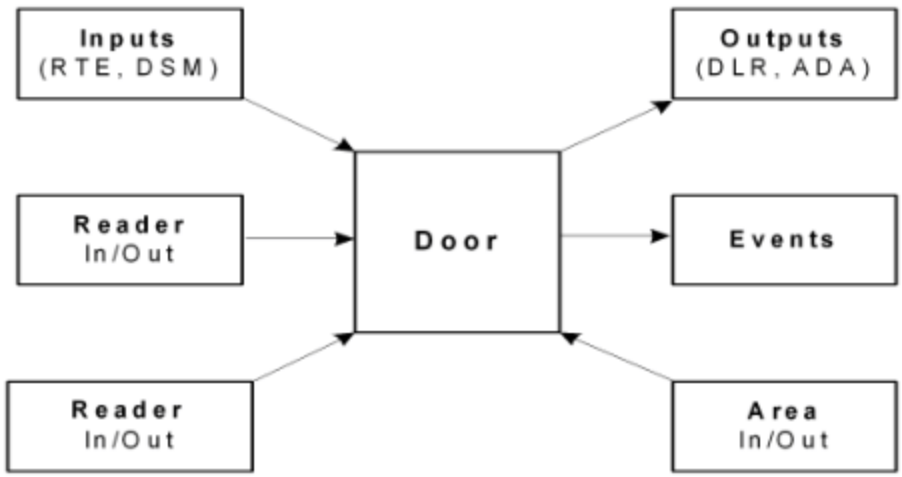


Table 90: Typical Door Components

Component	Description
RTE Input	A Request To Exit (RTE) input sends a signal that lets C•CURE 9000 know that someone is going to open the door to exit. Typically this device is a motion sensor or a press to exit button.
DSM Input	A Door Switch Monitor (DSM) sends a signal that lets C•CURE 9000 know whether the door is open or closed.
DLR Output	A Door Latch Relay (DLR) is used to send a signal from C•CURE 9000 to a door latch to lock or unlock the door.
ADA Output	An output that activates a door assistance mechanism, usually installed for compliance with the Americans with Disabilities Act (ADA).
Reader In/Out	Defines the card readers that control entry or egress through this door.
Events	Door events are usually triggered by state changes in the Door inputs and outputs. You specify the Event you want to activate when a change, such as "Door held open," occurs.
Area In/Out	Defines the Area a cardholder enters and the area a cardholder leaves through this door. **Example:** A cardholder passing through a door named "Sales" is leaving an Area called "Lobby" and entering an Area called "Sales Office."

Door Tasks

You can perform the following general tasks to configure iSTAR and apC Doors.

Creating a Door

A door object must be configured for the type of controller to which it is connected: iSTAR or apC controllers. The process is essentially the same when creating each door object type. First you must create the controller, then configure the controller's General tab and Board tab to configure inputs, outputs and readers. One exception is that with the iSTAR controllers, you are required to first create an iSTAR cluster and then create controllers within that cluster.

Once you have created and configured the door controller, you may create as many doors as that type of controller can accommodate.

To Create a Door

Follow the steps below to create a door for an apC controller. To create an iSTAR door, first refer to the next set of steps for reader the iSTAR Cluster and Controller before reader the iSTAR door.

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. In the Hardware tree, expand the facility folder where you want to create a door. You must create a door by highlighting a controller icon, board icon, or door icon in the hardware tree:
   - **apC** - highlight the **apC controller** icon, right click, and select **apC Door > New**.
   - **iSTAR** - highlight the **iSTAR controller** icon, right click, and select **iSTAR Door > New**.

   You can also create a new door from the door icon in a folder: highlight the door icon, right click, and select **Door > New**. A new Door Dialog box opens. When the **Door Dialog** box opens on the General tab, configure the Door.
3. Enter a **Name** and **Description**.
4. **Maintenance Mode** - Click to put the door into Maintenance Mode. See Chapter 2: Maintenance Mode for more information.
5. Configure the fields on the General tab, as needed. The fields listed below are on the apC and iSTAR Door dialog boxes.
   - **Controller** - This is a read-only field that indicates the controller associated with the door.

- **Door Switch Monitor** - Click ... to display a list of inputs available for the controller. This signal is true when the door is open. It is used to determine Admit Unused, Door Held, and Door Forced. Click an Input to select it and assign it to the Door Switch Monitor field.
- **Door Lock Relay** - Click ... to display a list of outputs available for the controller. T his output is used to open the door. Click an Output to select it and assign it to the Door Lock Relay field.
- **Alternate Shunt Relay** - Click ... to display a list of outputs available for the controller. Alternate Shunt is used for cardholders with disability and sometimes for aircraft loading doors. Click an Output to select it and assign it to the Alternate Shunt Relay field .
- **Shunt Expiration Relay** - Click ... to display a list of outputs available for the controller. This output will indicate the expiration of the shunt. Click an Output to select it and assign it to the Shunt Expiration Relay field.
- **Entrance Reader** - Click ... to display a list of Readers available. Entrance and Exit Readers are required for Area related functions such as Occupancy and Anti-Passback Click a Reader to select it and assign it to the Entrance Reader field.
- **Exit Reader** - Click ... to display a list of Readers available. Entrance and Exit Readers are required for Area related functions such as Occupancy and Anti-Passback Click a Reader to select it and assign it to the Exit Reader field.
- **Readers are continuously active** - Click this check box to enable continuous reader activity. Continuously Active is not normally used. It is typically used for subway gates and other high volume applications.
- **Request to Exit Input** - Click ... to display a list of Inputs available. Click an Input to select it and assign it to the field.
- **Unlock Door on RTE** - Click this check box to unlock the door at a Request to Exit. This is usually checked, but certain high security areas may use the REX as a signal to the Security Officer who verifies the person and opens the door.
- **Shunt DSM while RTE is active** - Click this check box to Shunt Door Switch Monitor While Request to Exit is Active. This is frequently used to correct a race condition between REX and DSM.

6. To save your new Door, click **Save and Close**.

   To save the **Door** and create a new one, click **Save and New**. The current **Door** is saved and closed, but the **Door Editor** remains open to allow you to create a new **Door**.

   The following controller creation provides a sample of the steps involved in the creation of an iSTAR Cluster and Controller. For more detailed information about the creation of iSTAR Clusters, refer to Configuring iSTAR Clusters on Page 87. For more detailed information about the creation of controllers, refer to:

   - Creating an iSTAR Controller on Page 124
   - Configuration Overview for iSTAR Controllers on Page 119
   - apC Panel Overview on Page 296.

Creating a Door Template

You can create a template for a Door. A Door template saves you time because you can reuse the same configuration repeatedly.

To Create a Door Template

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Select either an **apC** or **iSTAR Door** from the **Hardware** pane drop-down list.
3. Click the drop-down arrow next to **New** and select **Template**.
4. The **Door Template** opens and you can configure it.
5. To save your new **Door Template**, click **Save and Close**.

The new Door template appears in the Template drop down list under *Templates*.

To Select a Door Template

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Select either an **apC** or **iSTAR Door** from the **Hardware** pane drop-down list.
3. Click the drop-down arrow next to **New** and select **Template**.
4. Select the template you wish to use under the **Templates** list and configure the door as explained in Creating a Door on Page 405.

Deleting a Door

You can delete a Door from a controller.

To Delete a Door

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Select either an **apC** or **iSTAR Door** from the **Hardware** pane drop-down list.
3. Click to open a **Dynamic View** showing Door objects of the same type.
4. Right-click the Door in the list that you want to delete and select **Delete** from the context menu.
5. Click **Yes** on the "**Are you sure you want to delete the selected Door?**" message box.

Modifying a Door

You can edit a Door.

To Edit a Door

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Select either an **apC** or **iSTAR Door** from the **Hardware** pane drop-down list.
3. Click to open a **Dynamic View** showing Door objects of the same type.
4. Double-click the **Door** in the list that you want to modify, and the **Door Editor** opens. Or, you can select the door in the list, right click, and select **Edit** from the context menu.

Viewing a List of Doors

You can view a list of Doors.

To View a List of Doors

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Select either an **apC** or **iSTAR Door** from the **Hardware** pane drop-down list.
3. Click  to open a **Dynamic View** showing **Door** objects of the same type.

NOTE In the Dynamic View, you can right-click the column header and select new columns from the list to add them to the Dynamic View. (For iSTAR Doors you can add a column that identifies the Intrusion Zone to which the Doors belong.)

If you right-click a row in the Door Dynamic View, a context menu is displayed. This menu contains a number of standard selections, as well as selections that are specific for Doors.

See **Using the Object List Context Menu** in the *C•CURE 9000 Getting Started Guide* for more information about the object context menu.

See Table 91 on Page 408 for context menu selections that are specific to Doors.

There are additional context menu selections for Advanced Door monitoring. See Advanced Door Monitoring Details on Page 495 for more information.

Table 91: Doors Context Menu Selections

Selection	Description
Lock	Opens a Manual action dialog box that lets you lock the selected Door.
Unlock	Opens a Manual action dialog box that lets you unlock the selected Door.
Momentary Unlock	Opens a Manual action dialog box that lets you momentarily unlock the selected Door.
Show Locked Causes	Opens the Cause List viewer for this Door.
Door Monitoring	Opens the Doors Monitoring Screen for the Door you selected. See Door Monitoring Screen on Page 496 for information about the Doors Monitoring screen.
Show Association	Click this menu selection to view a list of Security Objects associated with this iSTAR or apC Door. For more information, see "Showing Associations for an Object" in the *C•CURE 9000 Getting Started Guide*.
Monitor	Click this menu selection to view activity for the selected iSTAR and apC Door(s), and any Input, Output, Reader, 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*.

Using Set Property to Configure Doors

You can use Set Property to quickly set a property for an iSTAR or apC Door without opening an iSTAR or apC Door editor. Set Property allows you to select multiple Doors objects in the dynamic list, and right-click to use Set Property to set a specific property for all of them.

Example:

If you wanted to change an unlock property setting for 20 apC Doors, you could select all of them listed in the dynamic list and do it in one step.

To Set a Property for a Door

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Select either an **apC** or **iSTAR Door** from the **Hardware** pane drop-down list.
3. Click  to open a **Dynamic View** showing all **Door** objects.
4. Right-click the **Door** (or set of doors) in the list for which you want to set a property and select **Set Property** from the context menu.
5. Specify the property for the **Door**. Click the Browse button to see a list of properties.
6. Enter the value for the property and click **OK**.
7. Click **OK** on the **Select a property and value for object** message box.

Add a Hardware Device to Group from a Dynamic View

When you select a Hardware device from a Dynamic View and then right-click for the context menu, **Add to group** appears as a menu selection. This function enables you to add the object(s) to a Group. More more information about the Group function see Groups Tab for Hardware Devices on Page 28.

To Add a Hardware Device To a Group

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the Hardware pane.
2. Select a Hardware device from the Hardware pane drop-down list.
3. Click  to open a **Dynamic View** showing all objects of that type.
4. Right-click on the object that you want to add to a Group and select **Add To Group**. A list of Groups is displayed.
5. Select the Group from the list, and the object is added to that group.
6. Click **OK** to confirm your choice.

apC Door Editor

The apC Door editor has the following tabs:

- apC Door General Tab on Page 411
- apC Door Readers Tab on Page 413
- apC Door Timing Tab on Page 415
- apC Door Triggers Tab on Page 416
- Groups Tab for Hardware Devices on Page 28
- apC Door Status Tab on Page 416
- apC Door Visitor Management Tab on Page 418
- apC Door State Images Tab on Page 417

Configuring an apC Door

To configure a Door associated with an apC controller, first you must configure an apC panel, along with its readers, input, and outputs. For more information see apC Controller Configuration Summary on Page 308. To configure the door, perform the following tasks.

NOTE The apC and apC/L controllers have not been evaluated by UL.

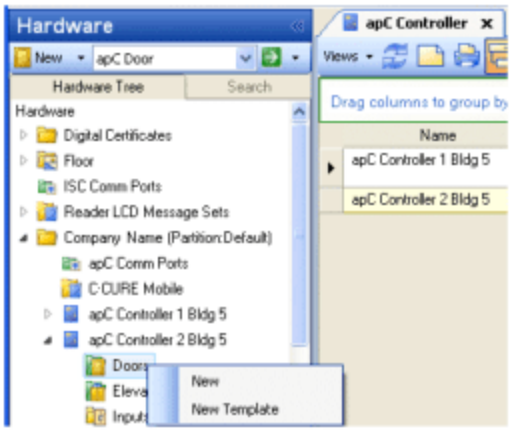
To Configure the apC Door

1. In the C•CURE 9000 **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Configure the apC panel's Readers, Inputs, and Outputs.
3. In the Hardware tree, find the apc **Controller** to which you want to associate the new apC Door, and click the "+" to expand the contents of that directory. A list displays that includes Doors, Elevators, Inputs, Outputs, and Readers. These objects are also directories.

   If you already have some apC doors configured, you can display all existing doors for the controller. Highlight Doors and click  to open a **Dynamic View** showing all **Door** objects of this type (see Figure 157 on Page 411). Edit an existing door by double-clicking the door in the Dynamic View to open the door's editor window.
4. Highlight the **Doors** directory in the Hardware tree, right-click to display the context menu, and select **New**. A new apC Door editor displays. See apC Door - General tab, as shown in Figure 158 on Page 412.

   Another way to create the new apC door is to highlight the Controller in the Hardware tree, right click, and select **apC Door>New**.

Figure 157: Hardware Pane - Create an apC Door



5. Configure the door on the **General** tab and any other tabs, as needed. You will need to have already configured the apC Readers, Inputs, and Outputs to fully configure an apC door.
6. Configure remaining tabs for this door, or click **Save and Close**. The new door displays under the Doors directory in the Hardware tree.

apC Door General Tab

Configure the door on the **General** tab and other tabs, as required. You will need to have configured the apC Readers, Inputs, and Outputs to configure an apC door. Refer to the apC Controller Configuration Summary on Page 308 for further information.

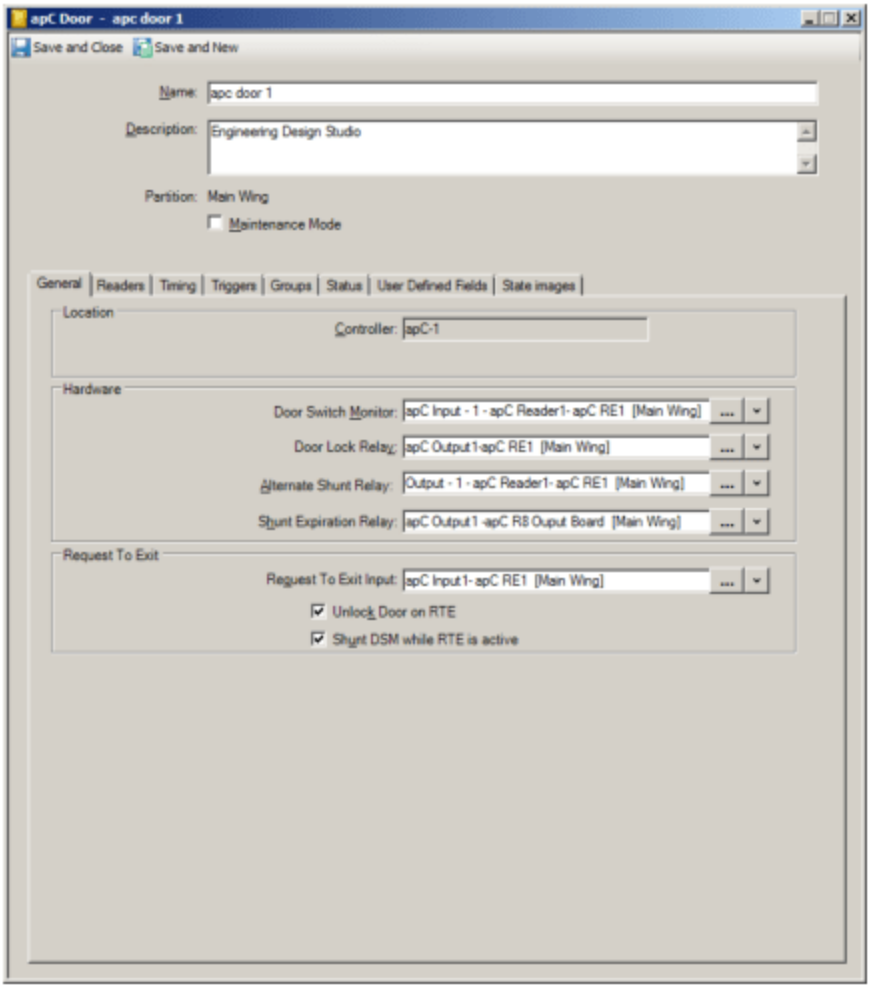
The following section documents the tasks required to configure a basic Door object for apC panel access control. The Door Reader buttons and entry fields on the Door General tab, shown in Figure 158 on Page 412, allow you to specify the card readers associated with this Door, and to configure door-specific settings for these readers.

To Configure the apC Door General Tab

1. Use the Identification box to enter a **Name** and brief **Description** (optional) of the door that you are reader.

   The Controller that you have chosen to operate the door is listed in the read-only Controller field.
2. Click [...] for the **Door Switch Monitor**. When you click this button to select an input to assign to the **Door Switch Monitor**, a browser opens presenting a list of inputs available for the controller. Click an **Input** to select it and add it to the entry field (see Figure 158 on Page 412).

Figure 158: apC Door General Tab



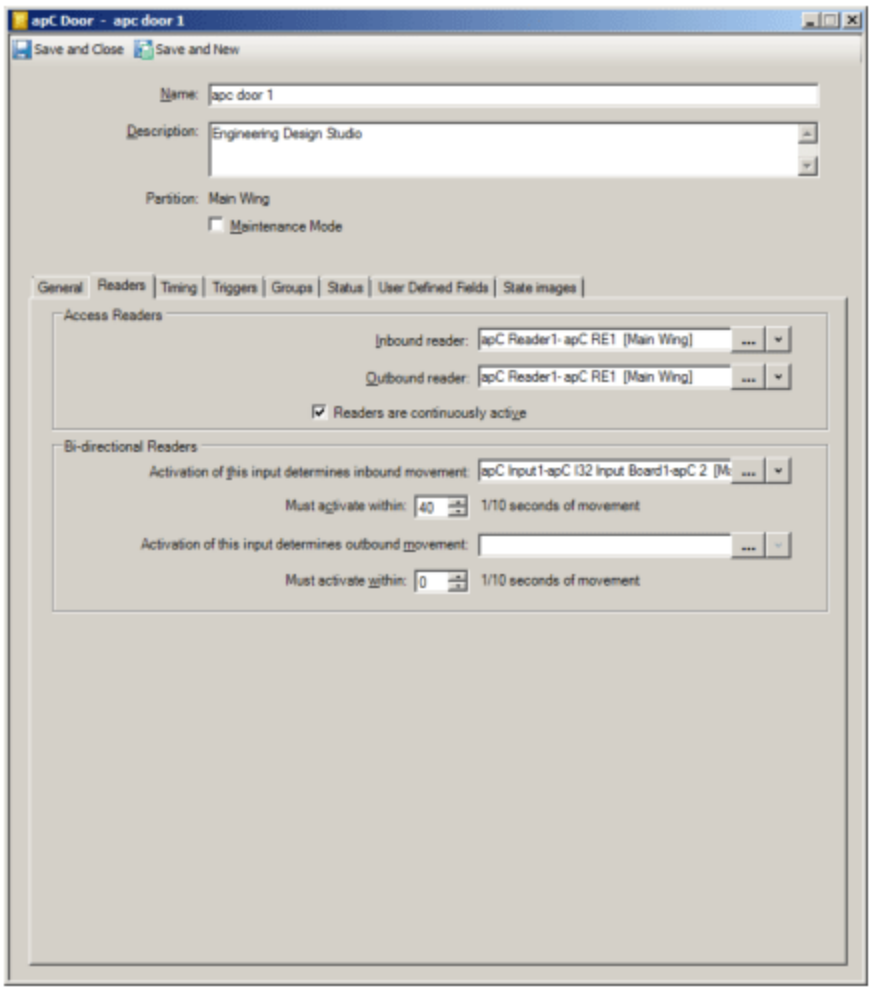
3. Click ... for the **Door Lock Relay**. When you click this button to select an output to assign to the **Door Lock Relay**, a browser opens presenting a list of outputs available for the controller. Click an **Output** to select it and add it to the entry field.
4. Click ... for the **Alternate Shunt Relay**. When you click this button to select an output to assign to the **Alternate Shunt Relay**, a browser opens presenting a list of outputs available for the controller. Click an **Output** to select it and add it to the entry field.
5. Click ... for the **Shunt Expiration Relay**. When you click this button to select an output to assign to the **Shunt Expiration Relay**, a browser opens presenting a list of outputs available for the controller. Click an **Output** to select it and add it to the entry field.
6. Click ... for the **Request to Exit Input**. When you click this button to select an input to assign to the **Request to Exit**, a browser opens presenting a list of inputs available for the controller. Click an RTE **Input** to select it and add it to the entry field.
7. Select the **Unlock Door on RTE** check box to unlock the door at a **Request to Exit**.
8. Select the **Shunt DSM While RTE is Active** check box to **Shunt Door Switch Monitor While Request to Exit is Active**.
9. Navigate to the Readers tab, or click **Save and Close** to return to the Hardware pane.

apC Door Readers Tab

The apC Door - Readers tab allows configuration of inbound and outbound access readers and for bi-directional readers installed at apC controlled doors. All the readers on the door must be located on the same apC panel. See Figure 159 on Page 413.

The Readers tab also lets you configure doors as "ordinary" or turnstile for escorted access for visitors by selecting the **Readers Are Continuously Active** check box.

Figure 159: apC Door Readers Tab



To Configure the apC Door Readers Tab

1. Click [...] for the **Inbound Access Reader**. When you click this button to select a reader to assign to the **Inbound Access Reader**, a browser opens presenting a list of readers available for the panel. Click a **Reader** to select it and add it to the entry field.

   When specifying an access reader, follow these guidelines:

   - Both access readers on the door must be located on the same apC panel.

- If you are using a bi-directional reader, specify the same reader in the inbound and outbound access reader fields.

2. Click [...] for the **Outbound Access Reader**. When you click this button to select a reader to assign to the **Outbound Access Reader**, a browser opens presenting a list of readers available for the controller. Click a **Reader** to select it and add it to the entry field.
3. Select the **Readers are Continuously Active** check box to enable continuous reader activity, enabling readers to read and process cards even when the doors associated with them are unlocked or open because of another card access request. This mode is typically used for turnstiles or other high traffic situations that would result in unacceptable delays if the reader went through its normal sequence of read-open-close for each cardholder.

   Example:

   Suppose a user swipes their card and unlocks a door. Before the door opens and closes, another person swipes his card. If this box is checked, the system treats the second swipe as an access request. If you leave this box unchecked, the system ignores the second swipe. This feature is useful at high volume doors where you don't want to wait for the door to close after every access.

   For escorted access for visitors to work at:

   - "Ordinary" doors — multiple person access on each access cycle — select the Readers Are Continuously Active check box.
   - "Turnstiles" (or Mantraps) — one person access only on each access cycle — clear the Readers Are Continuously Active check box.

4. Click [...] to select an input for the apC Bi-directional Reader in the **Activation of the Input Determines Inbound Movement** entry field. When you click this button to select an input to assign to the inbound input, a browser opens presenting a list of inputs available for the panel. Click an **Input** to select it and add it to the entry field.

   The selected input tests for inbound movement at the apC controlled door. When this input activates within the directional link time, the system determines that the card is moving in the inbound direction. The apC panel uses this information for access control decisions.

   The inbound input must be on the same apC as the bi-directional readers on this door.

5. If the door has an inbound input defined in the **Activation of This Input Determines Inbound Movement** field, enter the time in tenths of seconds that the panel waits between card reads and input state changes to determine that the card is entering the area in the **Must Activate Within** entry field. The range for this field is from 0 to 99.99 seconds in units of 0.1 seconds.

   If the input changes state within the specified time, the panel determines that the card is moving into the inbound area.

6. Click [...] to select an input for the apC Bi-directional Reader in the **Activation of the Input Determines Outbound Movement** entry field. When you click this button to select an input to assign to the outbound input, a browser opens presenting a list of inputs available for the panel. Click an **Input** to select it and add it to the entry field.

   The selected input tests for outbound movement at the apC controlled door. When this input activates within the directional link time, the system determines that the card is moving in the outbound direction. The apC uses this information for access control.

   The outbound input must be on the same apC as the bi-directional readers on this door.

7. If the door has an outbound input defined in the **Activation of This Input Determines Outbound Movement** field, enter the time in tenths of seconds that the panel waits between card reads and input state changes to

determine that the card is entering the area in the **Must Activate Within** entry field. The range for this field is from 0 to 99.99 seconds in units of 0.1 seconds.

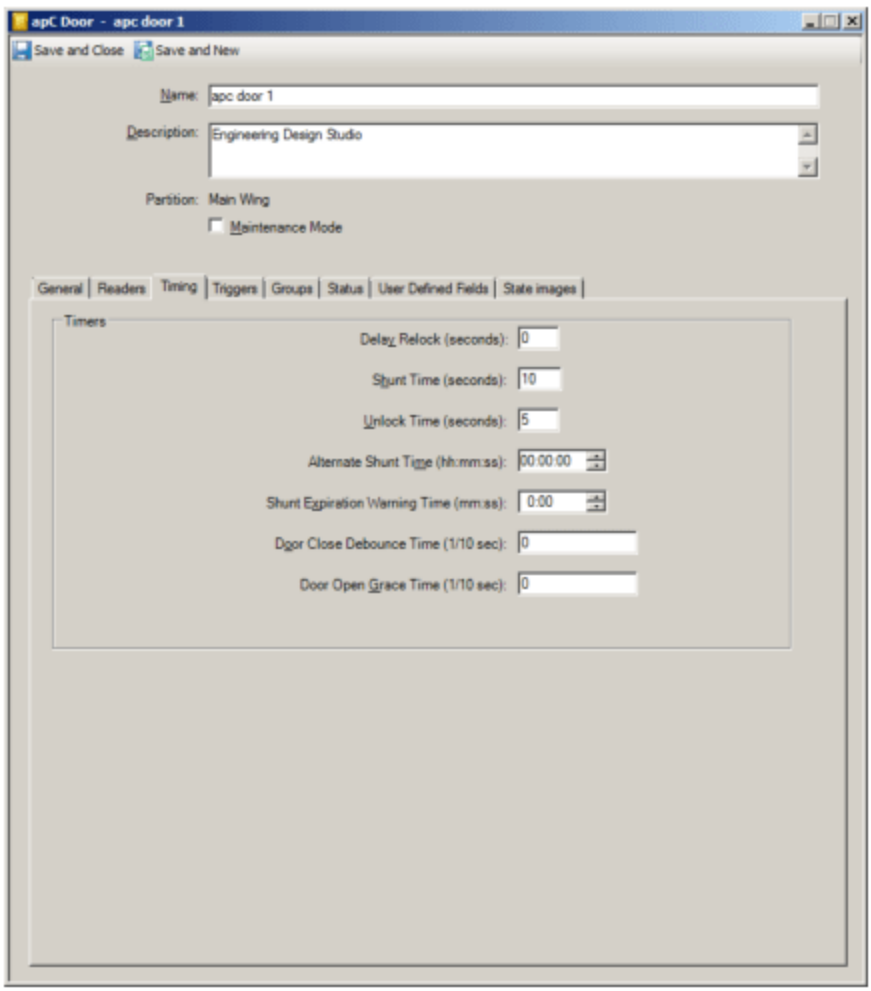
If the input changes state within the specified time, the panel determines that the card is moving into the outbound area.

8. Navigate to the Timing tab, or click **Save and Close** to return to the Hardware pane.

apC Door Timing Tab

A door that is controlled by an apC panel is constrained to a single set of door timing values for each side of the door. Required apC door sequences use the same set of timing values regardless of schedule. Only one alternate set of timer values is used in each door sequence. This corresponds to a personnel record configured to use **Alternate Shunt Time**. See the Timing tab in Figure 160 on Page 415.

Figure 160: apC Door Timing Tab



Setting apC Door Timing

1. **Delay Relock** – Enter the number of seconds to delay door relock after the door is opened (after a request to exit, for example). The range in seconds is 0:0:0 to 0:16:39 (999 seconds); the default is 0:0:0.

2. **Shunt Time** – Enter the number of seconds that the door can remain open before a door held open alert is generated within the range of 0:0:0 to 0:16:39 (999 seconds); the default is 0:0:10 (10 seconds).
3. **Unlock Time** – Enter the number of seconds the Door remains unlocked after a valid card swipe, RTE activation, or momentary unlock within the range of 0:0:0 to 0:4:15 (255 seconds); the default is 0:0:5 (5 seconds).
4. **Alternate Shunt Time** – Enter the number of hours, minutes, and seconds the Door can remain open before a door held open alert is generated after a valid card swipe by a cardholder with the **Alternate Shunt** flag set in their personnel record. This value is used only if it is set to a greater time than the **Shunt time** value within the range of 0:0:0 (default) to 18:0:0 (18 hours).
5. **Shunt Expiration Warning Time** – If set, the Shunt expiration relay is fired regardless of the shunt time used. If set to 0 (the default), the Shunt expiration relay will only be fired if the Alternate shunt time was used. The Shunt Expiration Warning has a range of 0:0:0 to 0:4:0 (4 minutes).
6. **Door Close Debounce Time** - Setting this value to 0 indicates that there is no timer. The range is 0 - 25.5 seconds units of 0.1 seconds.
7. **Door Open Grace Time** – Also known as **Door Open Debounce Time**. Setting this value to 0 indicates that there is no timer; as soon as the door opens, door forced open is reported. The range for this field is from 0 to 25.5 seconds in units of 0.1 seconds.
8. Navigate to the Triggers tab, or click **Save and Close** to return to the Hardware pane.

apC Door Triggers Tab

You can create Triggers for apC Doors using the apC Doors Triggers tab. A Trigger executes a specified **Action** when a particular predefined condition occurs. When a Trigger is defined, the Actions available depend on the property selected

See the following for information on apC Triggers:

- Triggers Tab for apC Devices on Page 369.
- Defining a Trigger for an apC Device on Page 370.
- Removing a Trigger on Page 272

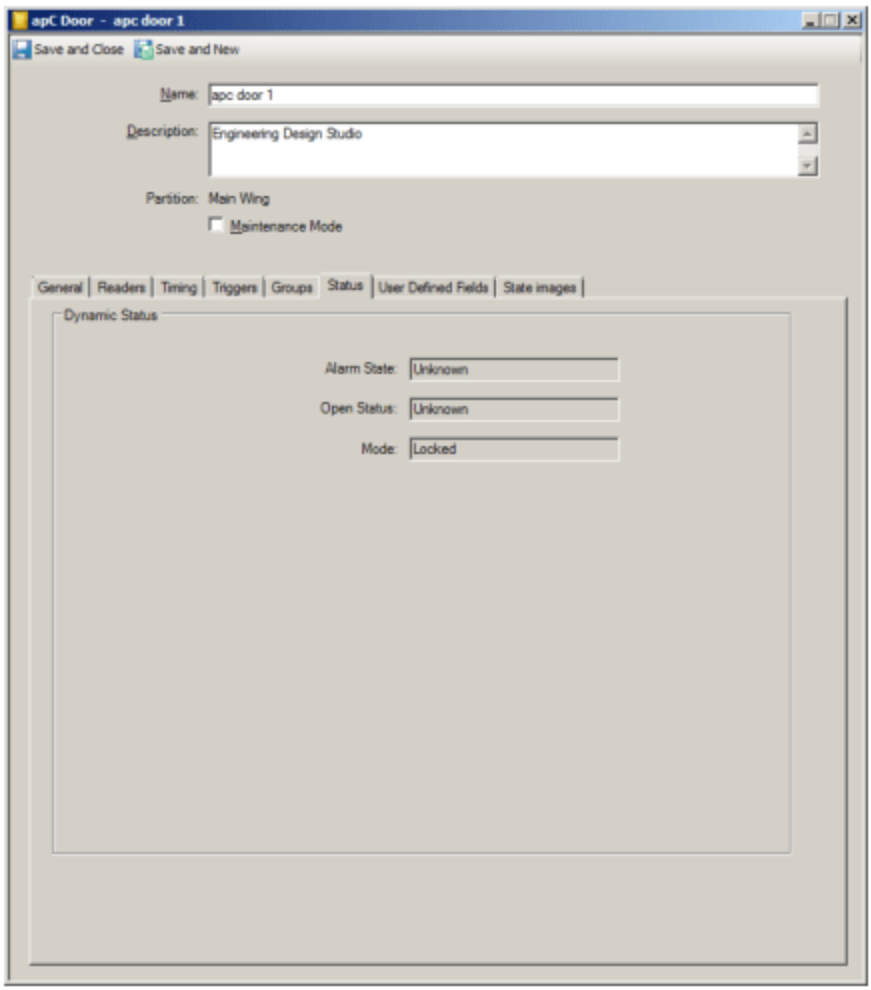
You can click **Save and Close** after configuring apC Door triggers, or navigate to the Status tab.

apC Door Status Tab

The Door Status tab (see Figure 161 on Page 417) provides a read-only listing of critical information about the operational status of the selected Door including:

- **Alarm State** - displays the values Normal, Forced, Held Open, or Unknown.
- **Admit Status** - displays the values Admit, Reject Admit, Duress, Admit Visitor, Reject Visitor, Request To Exit, Reject No Escort, Reject No PIN, Reject Not Time, Reject Unknown, Reject Unknown PIN, or Reject Duress.
- **Open Status** - displays the values Open, Closed, or Unknown.
- **Mode** - displays the values Locked, Unlocked, No Access, or Unknown.

Figure 161: apC Door Status Tab



- Navigate to the **State Images** tab or click **Save and Close**.

apC Door State Images Tab

The **State Images** tab on the Inputs Board (shown in Figure 162 on Page 418) provides a means to change the default images used to indicate controller states.

To Change an Image

1. Double-click the existing image.

   A **Windows Open** dialog box appears allowing you to browse for a folder in which you have placed replacement images.

2. When you locate the replacement image, select it to add it to the image listing.
3. To restore the default image, right-click the new image and select **Restore Default**.

Figure 162: apC Door State Images Tab

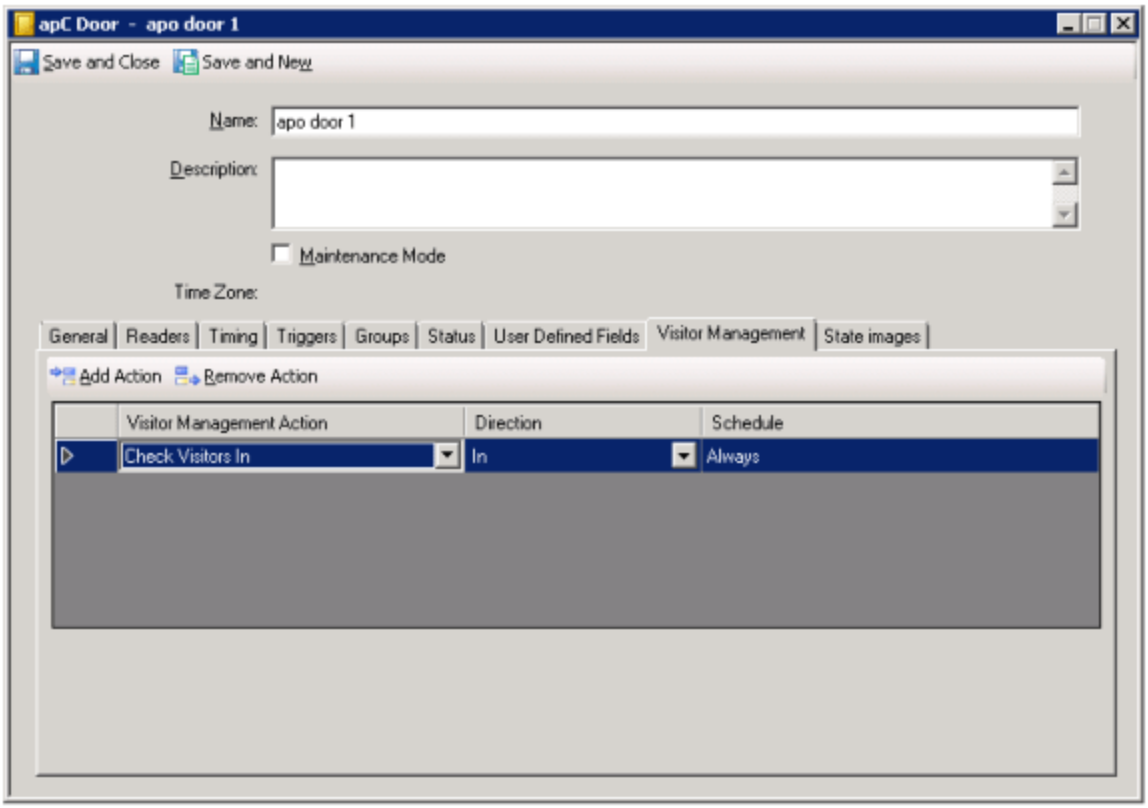
4. Click **Save and Close** to return to the **Hardware** pane.

apC Door Visitor Management Tab

The apC Door Visitor Management tab lets you configure Doors with Visitor Management Actions, so that you can automatically Check-in and Check-out Visitors.

For more information about Check-in and Check-out of Visitor via Visitor Management, see the C•CURE 9000 Visitor Management Guide.

Figure 163: apC Door Visitor Management tab



To Configure a Door Action for Check-In

1. In the C•CURE 9000 Admin Client, navigate to the Door you wish to configure.
2. Click the Visitor Management tab.
3. Click **Add Action**.
4. Chose the Visitor Management Action **Check Visitors In**.
5. Select the Direction for the action to take place.
   - Choose **In** for Visitors to Check-in using an inbound reader.
   - Choose **Out** for Visitors to Check-in using an outbound reader.
   - Choose **In and Out** for Visitors to Check-in using either the inbound or outbound reader.
6. Select a Schedule for the action to be active.
7. Click **Save and Close**

To Configure a Door Action for Check-out

1. In the C•CURE 9000 Admin Client, navigate to the Door you wish to configure.
2. Click the Visitor Management tab.
3. Click **Add Action**.

4. Chose the Visitor Management Action **Check Visitors Out**.
   - Check Out Visitors and Return Badge.
5. Select the Direction for the action to take place.
   - Choose **In** for Visitors to Check-out using an inbound reader.
   - Choose **Out** for Visitors to Check-out using an outbound reader.
   - Choose **In and Out** for Visitors to Check-out using either the inbound or outbound reader.
6. Select a Schedule for the action to be active.
7. Click **Save and Close**

To Configure a Door Action for Check-out

This presumes that a Badge Return mechanism is set up at the Check-out reader.

1. In the C•CURE 9000 Admin Client, navigate to the Door you wish to configure.
2. Click the Visitor Management tab.
3. Click **Add Action**.
4. Chose the Visitor Management Action **Check Visitors Out**.
   - Check Out Visitors and Return Badge.
5. Select the Direction for the action to take place.
   - Choose **In** for Visitors to Check-out and Return the Badge using an inbound reader.
   - Choose **Out** for Visitors to Check-out and Return the Badge using an outbound reader.
   - Choose **In and Out** for Visitors to Check-out and Return the Badge using either the inbound or outbound reader.
6. Select a Schedule for the action to be active.
7. Click **Save and Close**

apC Door Definitions

The definitions of the various fields and buttons on the apC Door editor are given in the following tables.

apC Door General Tab Definitions

Field/Button	Description
Name	Use the Identification box to enter a name (up to 50 characters long) and brief description of the door you are configuring.
Description	A description of the door that you are configuring.
Maintenance Mode	Click to put the apC door into Maintenance Mode. See Chapter 2: Maintenance Mode for more information.
Partition	The Partition label indicates to which partition the door belongs.
Hardware	
Door Switch Monitor	Click ... for the **Door Switch Monitor**. When you click this button to select inputs to assign to the **Door Switch Monitor**, a browser opens presenting a list of inputs available for the controller. Click a **Switch** or other pre-configured **Input** to select it and add it to the entry field.
Door Lock Relay	Click ... for the **Door Lock Relay**. When you click this button to select an output to assign to the **Door Lock Relay**, a browser opens presenting a list of outputs available for the controller. Click a **Lock** or other pre-configured **Output** to select it and add it to the entry field.
Alternate Shunt Relay	Click ... for the **Alternate Shunt Relay**. When you click this button to select an input to assign to the **Alternate Shunt Relay**, a browser opens presenting a list of outputs available for the controller. Click an **Output** to select it and add it to the entry field.
Shunt Expiration Relay	Click ... for the **Shunt Expiration Relay**. When you click this button to select an output to assign to the **Shunt Expiration Relay**, a browser opens presenting a list of outputs available for the controller. Click an **Output** to select it and add it to the entry field.
Request to Exit	
Request to Exit Input	Click ... for the **Request to Exit Input**. When you click this button to select an input to assign to the **Request to Exit Input**, a browser opens presenting a list of inputs available for the controller. Click an **Input** to select it and add it to the entry field.
Unlock Door on RTE	Select the **Unlock Door on RTE** check box to unlock the door at a **Request to Exit**.
Shunt DSM while RTE is active	Select the **Shunt DSM While RTE is Active** check box to **Shunt Door Switch Monitor While Request to Exit is Active**.

apC Door Readers Tab Definitions

Table 92: apC Door Readers Tab Definitions

Field/Button	Description
Access Readers	

apC Door Readers Tab Definitions (continued)

Field/Button	Description
Inbound Access Reader	When you click ... to select an Inbound Access Reader, a browser opens presenting a list of readers available for the panel. Click a Reader to select it and add it to the entry field.
Outbound Access Reader	When you click ... to select an Outbound Access Reader, a browser opens presenting a list of readers available for the panel. Click a Reader to select it and add it to the entry field.
Readers are Continuously Active	Select the **Readers Are Continuously Active** check box if you want readers to read and process cards even when the doors associated with them are unlocked or open because of another card access request.
Bi-directional Readers	
Activation of the Input Determines Inbound Movement	Click ... to select an input for the apC Bi-directional Reader in the Activation of the Input Determines Inbound Movement entry field. When you click this button to select an input to assign to the inbound input, a browser opens presenting a list of inputs available for the panel. Click an **Input** to select it and add it to the entry field. The selected input tests for inbound movement at the apC controlled door. When this input activates within the directional link time, the system determines that the card is moving in the inbound direction. The apC panel uses this information for access control decisions. The inbound input must be on the same apC as the bi-directional readers on this door.
Must Activate Within	If the door has an inbound input defined in the Activation of This Input Determines Inbound Movement field, enter the time in tenths of seconds that the panel waits between card reads and input state changes to determine that the card is entering the area in the Must Activate Within entry field. The range for this field is from 0 to 99.99 seconds in units of 0.1 seconds. If the input changes state within the specified time, the panel determines that the card is moving into the inbound area.
Activation of the Input Determines Outbound Movement	Click ... to select an input for the apC Bi-directional Reader in the Activation of the Input Determines Outbound Movement entry field. When you click this button to select an input to assign to the outbound input, a browser opens presenting a list of inputs available for the panel. Click an **Input** to select it and add it to the entry field. The selected input tests for outbound movement at the apC controlled door. When this input activates within the directional link time, the system determines that the card is moving in the outbound direction. The apC uses this information for access control. The outbound input must be on the same apC as the bi-directional readers on this door.
Must Activate Within	If the door has an outbound input defined in the **Activation of This Input Determines Outbound Movement** field, enter the time in tenths of seconds that the panel waits between card reads and input state changes to determine that the card is entering the area in the **Must Activate Within** entry field. The range for this field is from 0 to 99.99 seconds in units of 0.1 seconds. If the input changes state within the specified time, the panel determines that the card is moving into the outbound area.

apC Door Timing Tab Definitions

Table 93: apC Door Timing Tab Definitions

Field/Button	Description
Timers	

apC Door Timing Tab Definitions (continued)

Field/Button	Description
Delay Relock	Type the number of seconds to delay door relock after the door is opened (after a request to exit, for example). The range in seconds is 0:0:0 to 0:16:39 (999 seconds); the default is 0:0:0.
Shunt Time	**Shunt Time** – type the number of seconds that the door can remain open before a door held open alert is generated within the range of 0:0:0 to 0:16:39 (999 seconds); the default is 0:0:10 (10 seconds).
Unlock Time	**Unlock Time** – type the number of seconds the Door remains unlocked after a valid card swipe, RTE activation, or momentary unlock within the range of 0:0:0 to 0:4:15 (255 seconds); the default is 0:0:5 (5 seconds).
Alternate Shunt Time	**Alternate Shunt Time** – type the number of hours, minutes, and seconds the Door can remain open before a door held open alert is generated after a valid card swipe by a cardholder with the **Alternate Shunt** flag set in their personnel record (This value is used only if it is set to a greater time than the **Shunt time** value) within the range of default/minimum: 0:0:0; maximum:18:0:0 (18 hours).
Shunt Expiration Warning Time	If set, the Shunt expiration relay fires regardless of the shunt time used. If set to 0 (the default), the Shunt expiration relay fires only if the Alternate shunt time is used. The Shunt Expiration Warning has a range of 0:0:0 to 0:4:0 (4 minutes).
Door Close Debounce Time	Specifies the time (in 1/10th of a second intervals) that the C•CURE 9000 ignores DSM inputs, to allow for bouncing doors. Setting this value to 0 indicates that there is no timer. The range for this field is from 0 to 25.5 seconds in units of 0.1 seconds.
Door Open Grace Time	Specifies the time (in 1/10th of a second intervals) that the C•CURE 9000 waits for an RTE, card admit, or momentary unlock signal after receiving the signal from the DSM. Setting this value to 0 indicates that there is no timer; as soon as the door opens, door forced open is reported. The range for this field is from 0 to 25.5 seconds in units of 0.1 seconds.

apC Door Triggers Tab Definitions

Table 94: apC Door Triggers Tab Definitions

Field/Button	Description
Triggers	
Add	Click **Add** in the **Triggers** tab to create a new trigger.
Remove	Click the row selector , then click **Remove** to delete a trigger.
Property	Click within the **Property** column to display [...], When you select this button, the **Property** browser opens presenting properties available for the controller. Click a **Property** to select it and add it to the column.
Value	Click within the **Value** column to display a drop-down list of Values associated with the **Property** that you have selected. Click on a **Value** that you want to include as a parameter for the trigger to add it to the column.

apC Door Triggers Tab Definitions (continued)

Field/Button	Description
Action	Click within the **Action** column to display a drop-down list of valid actions. Click on an **Action** that you want to include as a parameter for the trigger to add it to the column. When a **Trigger** is added, an **Action** must be configured in the Action column. This is the Action that will occur when the object's selected **Property** receives the selected **Value**. As the Action is selected, the lower pane in the Triggers box will show a corresponding entry field, or group of entry fields, specific to the selected Action. Click ... to select entries for these fields. Once the field (or group of fields) is completed, the **Details** column will show information about how the Action has been configured.
Details	Displays details concerning the security objects that are associated with the selected Action.
Schedule	Click within the **Schedule** column to display a drop-down list of pre-configured schedules. Click ... to select a **Schedule** that you want to associate with the trigger. Schedules are created in the Configuration Pane. See the *C•CURE 9000 Software Configuration Guide* for more information.

apC Door Trigger Properties

Table 95: apC Door Trigger Properties

Property	Description
Admit Status Values are: AdmitReject Duress Noticed Admit Noticed Reject	For any one of the Admit Status values (see the Value column list) you can choose one of the following Actions to create a Trigger: **Activate Event** – When this status occurs and the Schedule is Active (you can choose any Schedule). **Activate Event Outside Schedule** – An event is activated when this status occurs while the Schedule is Inactive (choose any Schedule). **Activate Output** – When this status occurs (only works with the Always Schedule). Only these three Actions are supported for Admit Status.
Alarm StateStatus Values are: Forced Held Open	1. Choose a value for the Property from the **Values** column. 2. Select an Action from the **Action** drop-down list: **Activate Event** - Select an Event to activate when this status occurs. **Activate Event Outside Schedule** - Select an Event to activate when this status occurs while the Schedule is inactive. **Activate Output** - Select an Output to activate when this status occurs. Must use the **Always** Schedule. 3. Select a Schedule by clicking in the Schedule column, then click ... to select the Schedule that you want to associate with the trigger. For example, if you chose **Forced** as an Alarm State Status for which you want to define an action, you could then select **Activate Event**. In Details, select the Event you want to activate. Then select a Schedule to determine during what time periods you want the Forced Alarm State Status to activate an Event.

apC Door Groups Tab Definitions

Table 96: apC Door Groups Tab Definitions

Field/Button	Description
Groups	
	For more information about the use of the Toolbar buttons, see Chapter 2, "Dynamic Views" in the *C•CURE 9000 Data Views Guide*
Name	This column displays the name entered for the group when it was configured. The selected door is a member of any group(s) listed in this column.
Description	This column displays the description entered for the group when it was configured.

apC Door Status Tab Definitions

Table 97: apC Door apC Status Tab Definitions

Field/Button	Description
Alarm Status	Displays the values Normal, Forced, Held Open, or Unknown.
Admit Status	Displays the values Admit, Reject Admit, Duress, Admit Visitor, Reject Visitor, Request To Exit, Reject No Escort, Reject No PIN, Reject Not Time, Reject Unknown, Reject Unknown PIN, or Reject Duress.
Open Status	Displays the values Open, Closed, or Unknown.
Mode	Displays the values Locked, Unlocked, No Access, or Unknown.

apC Door State Images Tab Fields and Icons

Table 98: apC Door State Images Tab Definitions

Field/Button	Description		Field/Button	Description
Unknown			Locked	
Forced			Unlocked	
Held Open			No Access	

apC Door State Images Tab Definitions (continued)

Field/Button	Description		Field/Button	Description
Open			Momentary Unlock	

iSTAR Door Editor

You use the iSTAR Door editor to configure iSTAR Doors.

To configure a Door associated with an iSTAR controller, first you must:

- Create an iSTAR cluster
- Create the iSTAR controller in that cluster
- Create the inputs, outputs and readers that are associated with the Door.

For a brief explanation see Creating a Door on Page 405.

For a more detailed explanation of configuring iSTAR controllers see Understanding C•CURE iSTAR Controllers on Page 118.

The iSTAR Door Editor includes the following tabs:

- iSTAR Door General Tab on Page 427
- iSTAR Door Timing Tab on Page 429
- iSTAR Door Areas & Zones Tab on Page 431
- iSTAR Door Double Swipe Tab on Page 432
- iSTAR Door Conditional Access Tab on Page 436
- iSTAR Door Triggers Tab on Page 438
- Groups Tab for Hardware Devices on Page 28
- iSTAR Door Status Tab on Page 440
- iSTAR Door Monitoring Tab on Page 442
- iSTAR Door Visitor Management tab on Page 443
- iSTAR Door State Images Tab on Page 442

iSTAR Door General Tab

Perform the following steps to configure a basic Door object for iSTAR Controller access control. The Door Reader buttons and entry fields on the Door dialog box General tab, shown in Figure 164 on Page 428, allow you to specify the card readers associated with this Door, and to configure door-specific settings for these readers.

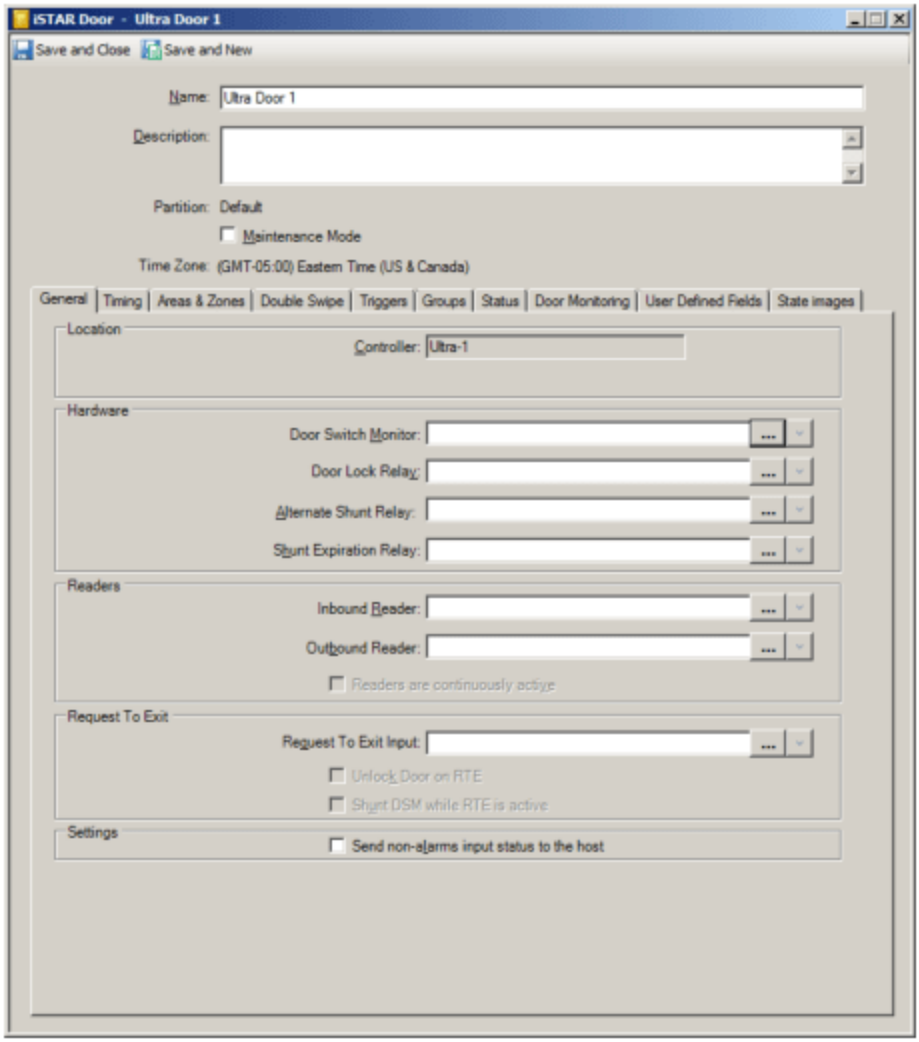
NOTE If the first Input, Output, or Reader you assign is a Shlage Wireless I/O component, a message box appears asking if you wish to auto-fill the remaining objects for the door. If you click **Yes** the remaining objects are selected automatically. This option only appears if all of the options are blank when you assign the first object. See iSTAR PIM-485 Reader I/O Tab on Page 261 for information about Schlage Wireless Reader I/O components.

NOTE An iSTAR Aperio Door does not have the following tabs: Areas & Zones, Double Swipe, and Door Monitoring. Also, for Aperio Doors, some of the General tab settings are unavailable because these Inputs and Outputs are integral to the reader and not user-selectable.

To Configure the iSTAR Door General Tab

1. Use the Identification box to enter a **Name** and brief **Description** (optional) of the door that you are configuring.

Figure 164: iSTAR Door General Tab



The Controller that you have chosen to operate the door is listed in the Controller read-only field.

2. Click ... for the **Door Switch Monitor**. When you click this button to select an input to assign to the **Door Switch Monitor**, a browser opens presenting a list of inputs available for the controller. Click an **Input** to select it and add it to the entry field (see Figure 164 on Page 428).

3. Click ... for the **Door Lock Relay**. When you click this button to select an input to assign to the **Door Lock Relay**, a browser opens presenting a list of outputs available for the controller. Click an **Output** to select it and add it to the entry field.

4. Click ... for the **Alternate Shunt Relay**. When you click this button to select an input to assign to the **Alternate Shunt Relay**, a browser opens presenting a list of outputs available for the controller. Click an **Output** to select it and add it to the entry field.

5. Click ... for the **Shunt Expiration Relay**. When you click this button to select an output to assign to the **Shunt Expiration Relay**, a browser opens presenting a list of outputs available for the controller. Click an **Output** to select it and add it to the entry field.
6. Click ... for the **Entrance Reader**. When you click this button to select a reader to assign to the **Entrance Reader**, a browser opens presenting a list of readers available for the controller. Click a **Reader** to select it and add it to the entry field.
7. Click ... for the **Exit Reader**. When you click this button to select a reader to assign to the **Exit Reader**, a browser opens presenting a list of readers available for the controller. Click a **Reader** to select it and add it to the entry field.
8. Select the **Readers are Continuously Active** check box to enable continuous reader activity, enabling readers to read and process cards even when the doors associated with them are unlocked or open because of another card access request. This mode is typically used for turnstiles or other high traffic situations that would result in unacceptable delays if the reader went through its normal sequence of read-open-close for each cardholder.

   Example:

   Suppose a user swipes their card and unlocks a door. Before the door opens and closes, another person swipes his card. If this box is checked, the system treats the second swipe as an access request. If you leave this box unchecked, the system ignores the second swipe. This feature is useful at high volume doors where you don't want to wait for the door to close after every access.

   - "Ordinary" doors — multiple person access on each access cycle — select the **Readers Are Continuously Active** check box.
   - "Turnstiles" (or Mantraps) — one person access only on each access cycle — clear the **Readers Are Continuously Active** check box.

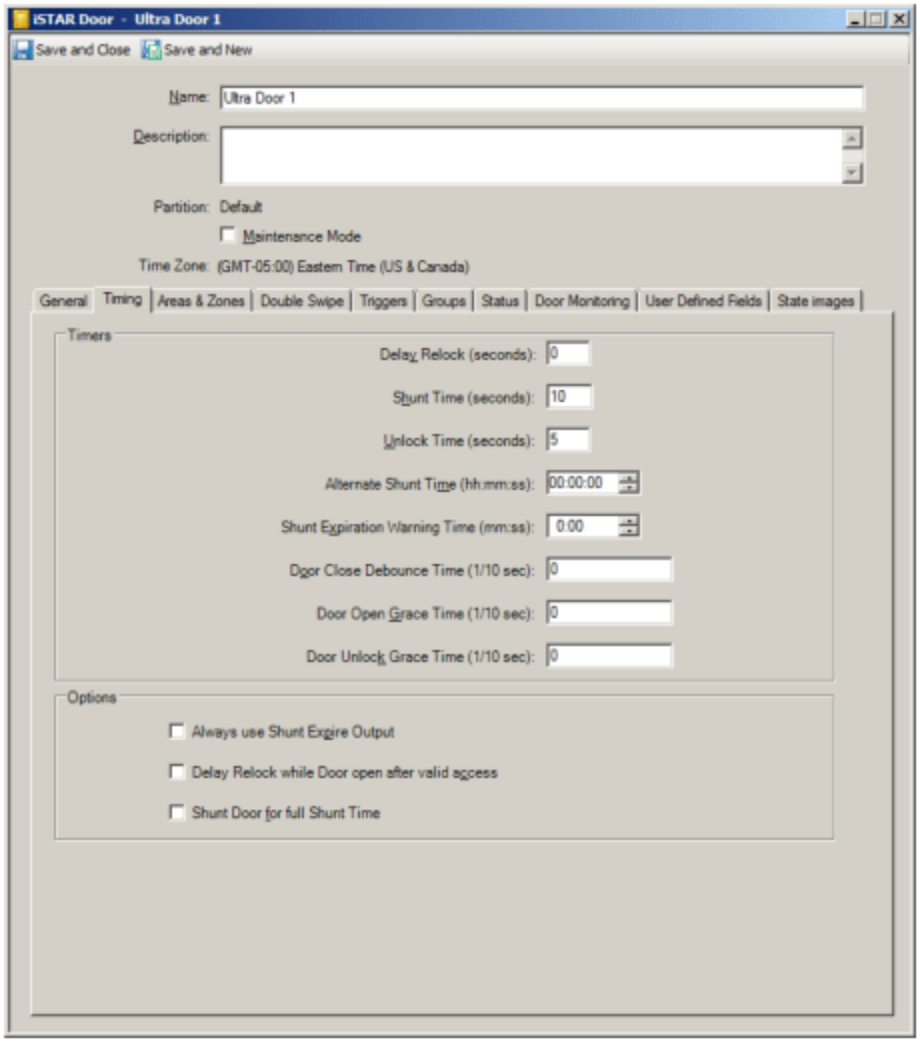
   Selecting this option for a Reader on an iSTAR Area Door permits the Area to be configured for Escorted Access in Companion mode. Leaving this option unselected causes Escorted Access to operate in Remote Escort (or Turnstile) mode.
9. Click ... for the **Request to Exit**. When you click this button to select an input to assign to the **Request to Exit**, abrowser opens presenting a list of inputs available for the controller. Click an **Input** to select it and add it to the ntry field.
10. Select the **Unlock Door on RTE** check box to unlock the door at a **Request to Exit**.
11. Select the **Shunt DSM While RTE is Active** check box to **Shunt Door Switch Monitor While Request to Exit is Active**.
12. Select the **Send non-alarms input status to the host** checkbox to instruct the system to send non-alarm input status to the host.

    Leaving the checkbox unselected (the default setting) instructs the system not to send non-alarm input status to the host. Doing this reduces network traffic demand when expecting large volumes of non-critical activity notifications.
13. Click **Save and Close** or navigate to the **Timing** tab.

iSTAR Door Timing Tab

Like the Door General tab, the layout of this tab depends upon the controller type. For an iSTAR-connected Door, Timings are configured using separate entry fields, as shown in Figure 165 on Page 430.

Figure 165: iSTAR Door Timing Tab



Setting iSTAR Door Timing

The following timers and check boxes appear on the iSTAR Door Timing tab:

1. **Delay Relock** – Type the number of seconds to delay door relock after the door is opened (after a request to exit, for example). The range in seconds is 0 to 999 seconds (0:16:39); the default is 0.
2. **Shunt Time** – Type the number of seconds that the door can remain open before a door held open alert is generated within the range of 0 to 999 seconds (0:16:39); the default is 10 seconds.
3. **Unlock Time** – Type the number of seconds the Door remains unlocked after a valid card swipe, RTE activation, or momentary unlock within the range of 0 to 255 seconds (0:4:15); the default is 5 seconds.

NOTE A value of 0 actually represents a token unlock time (300 microseconds) that can be used, for example, to unlock a turnstile so that one person may pass, but tailgating is not possible.
Also, a setting of 0 disables Momentary Unlock manual actions, so choose a non-zero Unlock Time if you need to use Momentary Unlock with this Door.

4. **Alternate Shunt Time** – Type the number of hours, minutes, and seconds the Door can remain open before a door held open alert is generated after a valid card swipe by a cardholder with the **Alternate Shunt** flag set in their personnel record (see the *C•CURE 9000 Personnel Configuration Guide*) within the range of default/minimum: 0:0:0; maximum:18:0:0 (18 hours). This value is used only if it is set to a greater time than the **Shunt time** value.
5. **Shunt Expiration Warning Time** – If set, the Shunt expiration relay is fired regardless of the shunt time used. If set to 0 (the default), the Shunt expiration relay will only be fired if the Alternate shunt time was used. The Shunt Expiration Warning has a range of 0:0:0 to 0:4:0 (4 minutes).
6. **Door Close Debounce Time** - Setting this value to 0 indicates that there is no timer. The range is from 0 to 25.5 seconds in units of 0.1 seconds.
7. **Door Open Grace Time** – Also known as **Door Open Debounce Time**. Setting this value to 0 indicates that there is no timer; as soon as the door opens, door forced open is reported. The range is from 0 to 25.5 seconds in units of 0.1 seconds.
8. **Door Unlock Grace Time** – Specifies the time that the system waits for a door open signal after the door unlock time has expired. This timing prevents a false door forced message in situations where signals are nearly simultaneous. The range is from 0 to 100 seconds in units of 0.1 seconds.
9. **Always Use Shunt Expire Output** – If this check box is selected, the Shunt expiration relay is fired regardless of the shunt time used. If the **Shunt Expiration Warning Time** is set to 0 (the default), the Shunt expiration relay shall only be fired if the Alternate shunt time was used.
10. **Delay Relock While Door Open After Valid Access** - If access is valid, delays the relock of the door until the door closes, if this check box is selected. This differs from standard relock operations, where relock occurs when the door opens and the relock delay expires. If the door is open, the lock is energized. The C•CURE 9000 system sends an alarm when the shunt time expires.
11. **Shunt Door for full Shunt Time** - If this check box is selected, the door is shunted for the full shunt time. If selected with Delay relock while door open for valid access, the lock is energized and the door unlocked for the full shunt time, regardless of whether the door is open or closed.

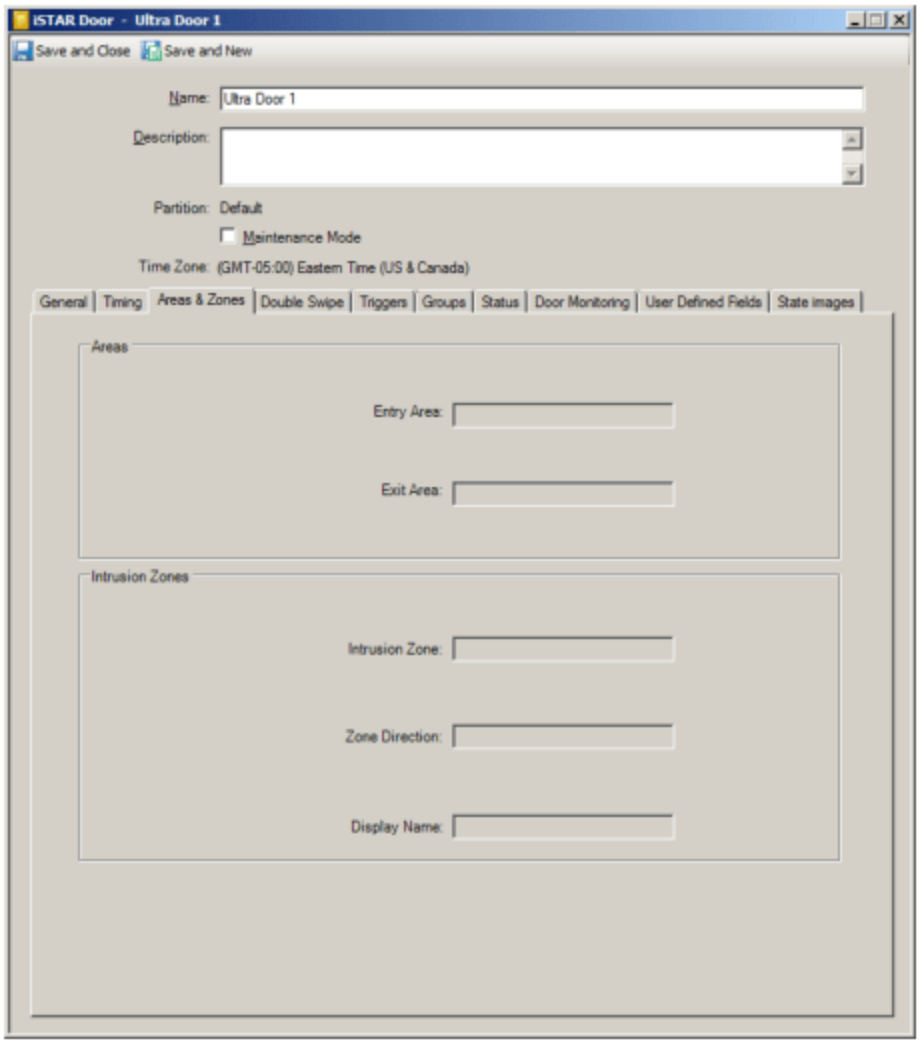
iSTAR Door Areas & Zones Tab

If this Door is assigned to an iSTAR Cluster Area and/or an iSTAR Intrusion Zone, the **Areas & Zones** tab displays read-only assignment information about the Door, as shown in Figure 166 on Page 432.

If the Door is **not** assigned to either an iSTAR Cluster Area or Intrusion Zone, the relevant box is blank.

NOTE The Dynamic View for iSTAR Doors allows you to add a column that identifies the Intrusion Zone to which the Doors belong.

Figure 166: iSTAR Door Areas & Zones Tab



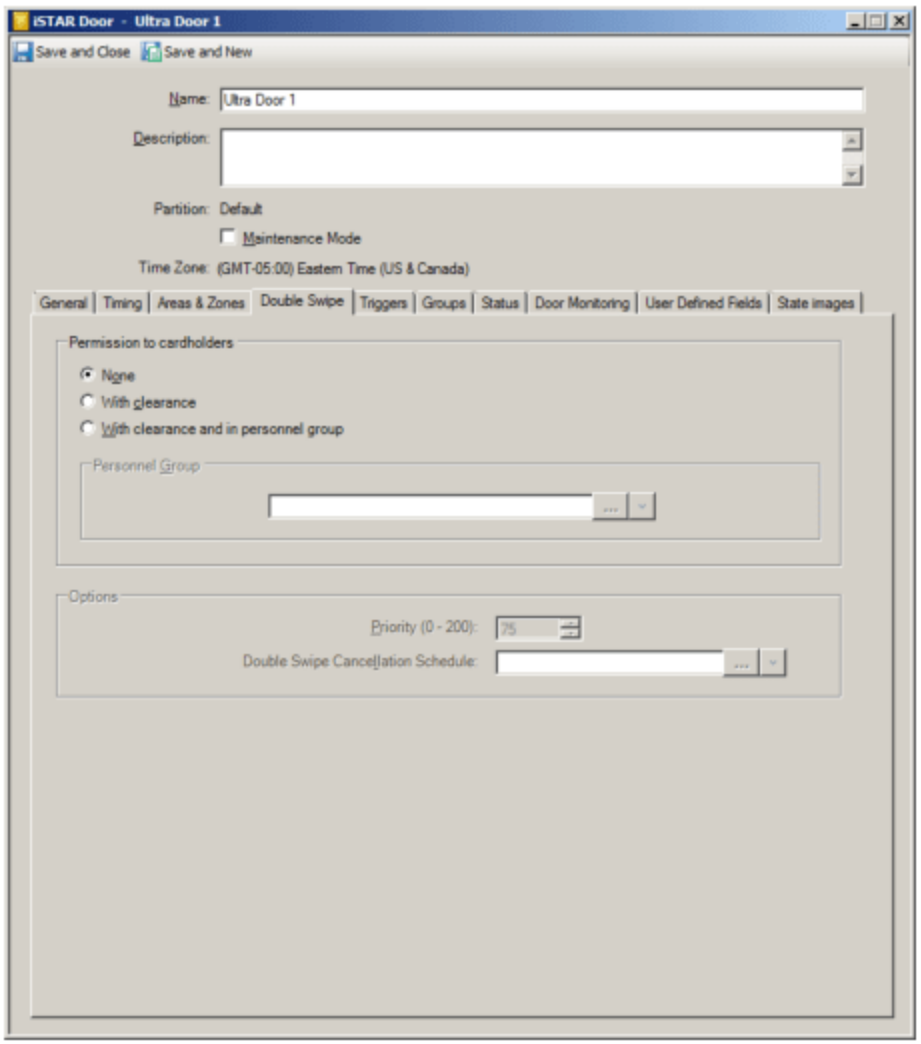
The **Areas & Zones** tab has the read-only fields shown in iSTAR Door Definitions on Page 446.

iSTAR Door Double Swipe Tab

In addition to the typical, single-swipe use of a card at a door's card reader, the **Double Swipe** tab (see Figure 167 on Page 433) allows you to configure a door to enable its reader to interpret a double card swipe as a means to toggle the door's lock state for an indefinite amount of time. Configure the selected door for Double Swipe by setting a combination of privilege, personnel group, priority level, and schedule. As with other security objects in the system, events, manual actions or causes with higher priorities can override a cardholder's double swipe. The double swipe lock/unlock messages display in the journal and in the cause list.

NOTE If the door being configured is assigned a Schlage Wireless Reader, the contents of this tab are disabled because the Schlage readers do not support double swipe.

Figure 167: iSTAR Door Double Swipe Tab



NOTE The **Double Swipe** feature requires iSTAR firmware version 4.3 or later for Classic, Pro, or eX.

NOTE Do not configure **Double Swipe** on a Door that is used with Antipassback, Escort, Conditional Access, Areas, or Intrusion Zone functionality.

To Configure the iSTAR Door Double Swipe Tab

Follow the steps to access the door editor in the Admin application, as described in Creating a Door on Page 405.

The selections below appear on the Door Configuration dialog box - Double Swipe tab (see Figure 167 on Page 433). Make the Double Swipe door configuration selections from these options.

1. **Permission to Cardholders area:**

a. **None** - If None is selected, Double Swipe is not enabled at the door. If Double Swipe is active at the door, you may turn off Double Swipe by selecting None on this tab. Normal card swipe access at the reader is still in effect, if so configured.

b. **With clearance** - Selecting this option enables the door to require that cardholders who use Double Swipe at the reader must have a clearance for access to this particular door configured for them in the Personnel screen, Clearances tab.

c. **With clearance and in personnel group** - Selecting this option will require that cardholders who use Double Swipe at the reader must have a clearance for access to this door configured for them in the Personnel screen, Clearances tab, and they also must be in the personnel group whose members have access to this door.

d. **Personnel Group** - Click [...] to select a personnel group. If a group is selected for Double Swipe, each cardholder who uses Double Swipe at the reader must be a member of the selected Personnel Group. The personnel group may be configured in the Configuration pane, Group dialog box.

2. **Options area:**

a. **Priority (0 - 200)**- Select a Priority for Double Swipe requests at the door. The default is 75.

In the case of a manual action with higher priority than the priority configured for the door, the manual action takes precedence. If the door's priority is higher, the double swipe takes precedence. For two actions with the same priority, the most recent one takes precedence.

NOTE If you change the **Priority** setting on the Double Swipe tab while a double swipe cause is active for the door, that cause will be removed from the cause list, and any the double swipe action is canceled.

b. **Double Swipe Cancellation Schedule** - Click [...] to select a schedule. The cancelling schedule will delete any existing double swipe causes on the door at the start of the schedule. Any double swipe actions currently in effect will be canceled.

3. Click **Save and Close** to save the settings and close the window, or click **Save and New** to save the settings and configure a new door.

A Double Swipe to Lock or Unlock a door also may be configured to trigger an Event. This is configured on the Triggers tab (see Using Double Swipe to Trigger an Event on Page 439).

For the Monitoring Station's Activity Viewer to display Double Swipe lock/unlock messages, the Application Layout must have an Activity Viewer pane configured to display Double Swipe messages. The Activity Viewer pane may be added, if needed, as described below.

To Edit the Application Layout for Double Swipe

1. In the Admin application, select the **Data Views** pane.
2. At the top of the pane, select **Application Layout** from the drop-down menu, and click the green arrow. In the right-hand pane, a new tab displays with a list of application layouts.
3. Select a layout to edit for Double Swipe messages, right click, and select **Edit**. The application layout screen opens.
4. To add an Activity Viewer pane, click **Add Pane**, and a new pane displays.

a. Click and drag the Activity Viewer icon from the left side of the application layout screen to the new pane. The Activity Viewer dialog box displays.

b. Select the Double Swipe check box to display Double Swipe messages at the Monitoring Station. If the box is unchecked, messages will not display at the Monitoring Station. By default, the Activity Viewer displays all these Message Types.

c. Click **Save and Close** .

5. To edit an existing Activity Viewer pane to display Double Swipe messages at the Monitoring Station, click the **Activity Viewer tab** on the pane, right click and select **Properties**. The Activity Viewer dialog box displays.

a. Select the Double Swipe check box to display Double Swipe messages at the Monitoring Station. If the box is unchecked, messages will not display at the Monitoring Station. By default, the Activity Viewer displays all these Message Types.

b. Click **Save and Close** .

Using Double Swipe at the Door

To Use Double Swipe at a Card Reader:

Double Swipe is enabled by:

- the cardholder(s) having a clearance to the specific door

  - or -

- the cardholder(s) having a clearance to the specific door and being a member of the personnel group, if the "With clearance and in personnel group" option is selected on the Double Swipe tab.

The following steps describe how a double swipe at the card reader toggles the door lock, to lock or unlock the door.

To Unlock a Door if the Current State is Lock:

Cardholder swipes the card twice at the reader, within the shunt time.

If the cardholder has the correct clearance set for access to the door or has the correct clearance and is in the correct personnel group, the door toggles to Unlock. The card reader displays the state of the door, and the door remains unlocked until it is locked again by another double swipe, or by other causes such as manual action, scheduled events, and so forth.

If the cardholder swipes only once, a Momentary Unlock occurs for an authorized cardholder.

To Lock a Door if the Current State is Unlock:

Cardholder swipes the card twice at the reader, within the shunt time.

If the cardholder has the correct clearance set for access to the door or has the correct clearance and is in the correct personnel group, the door toggles to Lock. The card reader displays the state of the door, and the door remains locked until it is unlocked by another double swipe, or by other causes such as manual action, scheduled events, and so forth.

For continuous card reader activity, make sure that the **Readers are Continuously Active** check box is selected in the Readers area of the General tab.

To associate Double Swipe with a trigger to cause an event, refer to Using Double Swipe to Trigger an Event on Page 439.

iSTAR Door Conditional Access Tab

The **Conditional Access** tab (see Figure 168 on Page 437) allows you to configure a door so that appropriately authorized Personnel can grant access to Personnel without Clearance for that Door. (This tab is **available** on the iSTAR Doors Editor **only** if the **Include Personnel Without Clearance in Personnel Downloads** option in the **Conditional Access** box is selected on the General tab of the door's iSTAR controller editor.)

NOTE The Conditional Access process can only be started by Personnel Credentials rejected for having no Clearance at the door. Rejections for Lost, Stolen, Not Active, Expired, or Unknown Card or for Antipassback, Occupancy, Lockout, or PIN cause immediate rejection.

This feature is usually used on doors into iSTAR Areas where a person inside can grant entry to the Area to personnel lacking clearance, after validating their identities. (In the latter situation, it can also be used in conjunction with Dynamic Area Manager. See the Areas chapter in the *C•CURE 9000 Areas and Zones Guide*.)

Example:

A bank has a secure area that it uses for counting cash. Two authorized employees with clearance for the entry door (Susan and Tom) have already entered the room and are working. A third employee without clearance (Martin) needs to confer with them and swipes his card at the door. Since the door is configured for Conditional Access, a Conditional Access event is activated and triggers an output inside the room, such as a flashing light or bell, to announce that someone wants to enter. Through the glass pane in the door, Susan sees that it is Martin waiting there. She pushes the button on the wall, activating a 'Conditional Access Response' event whose action opens the door. Martin enters the room. (The iSTAR Area Status tab would show that there were currently a total of three people in the area and that one of them had been admitted conditionally.)

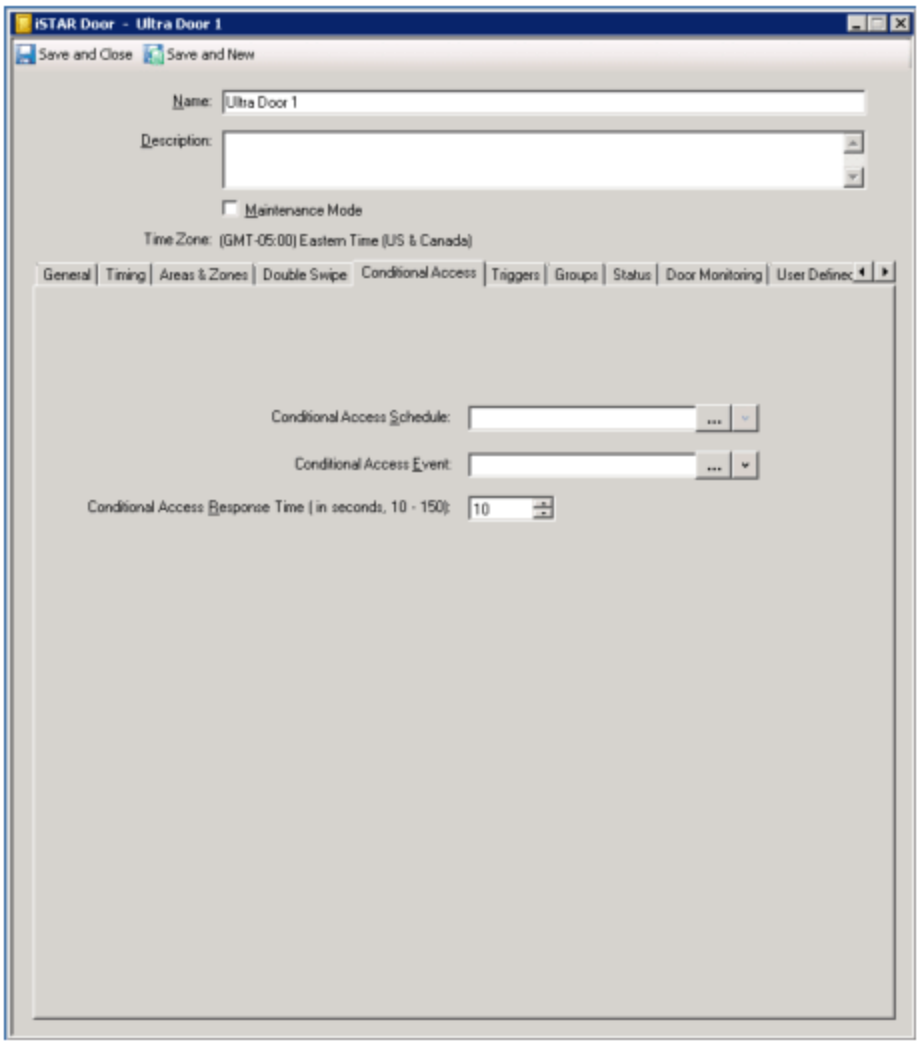
The **iSTAR Area Status** tab keeps track of the number of Personnel currently in the area who were admitted via Conditional Access. See the Areas chapter in the *C•CURE 9000 Areas and Zones Guide*. The **iSTAR Door Status** tab indicates whether or not Conditional Access is configured for an iSTAR door. See iSTAR Door Status Tab on Page 440.

This feature could also be used on any door to allow a guard at a Monitoring Station, with video capability to validate a person's identity, to activate the 'Conditional Access Response' event and let that person through the door.

NOTE

- Conditional Access is **only** supported on doors on iSTAR Pro, eX, Edge, and Ultra Controllers.
- The controller must also have the **Include Personnel Without Clearance in Personnel Downloads** option in the **Conditional Access** box selected on the **General** tab. (Normally credentials for personnel without clearance for any doors on the controller are **not** downloaded to the controller.)
- **Conditional Access** should **not** be configured on a door that is used with Escort or Double Swipe functionality.

Figure 168: iSTAR Door Conditional Access Tab



See iSTAR Door Conditional Access Tab Definitions on Page 449 for definitions of the fields on the Conditional Access tab.

Configuring Conditional Access

To Configure Conditional Access for this iSTAR Door

1. Follow the steps to create/edit the iSTAR Pro, eX, Edge, or Ultra controller that this door will be on, as described in Creating an iSTAR Controller on Page 124 and in Editing an iSTAR Controller on Page 126.
2. On the **General** tab of the iSTAR Controller editor, select the **Include Personnel Without Clearance in Personnel Downloads** option in the **Conditional Access** box, as described in To Configure the iSTAR Controller General Tab on Page 143.
3. Configure the Events needed for the feature:
   a. Configure a panel event for this door's controller that will act as the Conditional Access Event on the iSTAR Door Conditional Access tab—and initiate the 'Conditional Access' process. This event should trigger an

output, such as a buzzer or flashing light, that notifies appropriate personnel that someone without the requisite clearance wants to go through this door.

b. Configure a host or panel event with the action **Allow Conditional Access Cycle** to be activated to open the door conditionally.

For information, see the Events Chapter in the *C•CURE 9000 Software Configuration Guide*.

4. Follow the steps to access the iSTAR Door editor in the Administration application, as described in Creating a Door on Page 405, and then open the **Conditional Access** tab.
5. Click ... for **Conditional Access Schedule** to select the schedule during which Conditional Access is enabled for this door.
6. Click ... for **Conditional Access Event** to select the event that requests Conditional Access at this door for a person without Clearance. (Only panel events within this controller's cluster are available for selection.)
7. In the **Conditional Access Response Time** field, enter the number of seconds that the door will wait for the 'Allow Conditional Access Cycle' event action to open the door after the Conditional Access event entered in the preceding field has been activated. (The range is 1 - 150 seconds with a default of 10 seconds.)
8. Click **Save and Close** to save the settings and close the window, or click **Save and New** to save the settings and configure a new door.

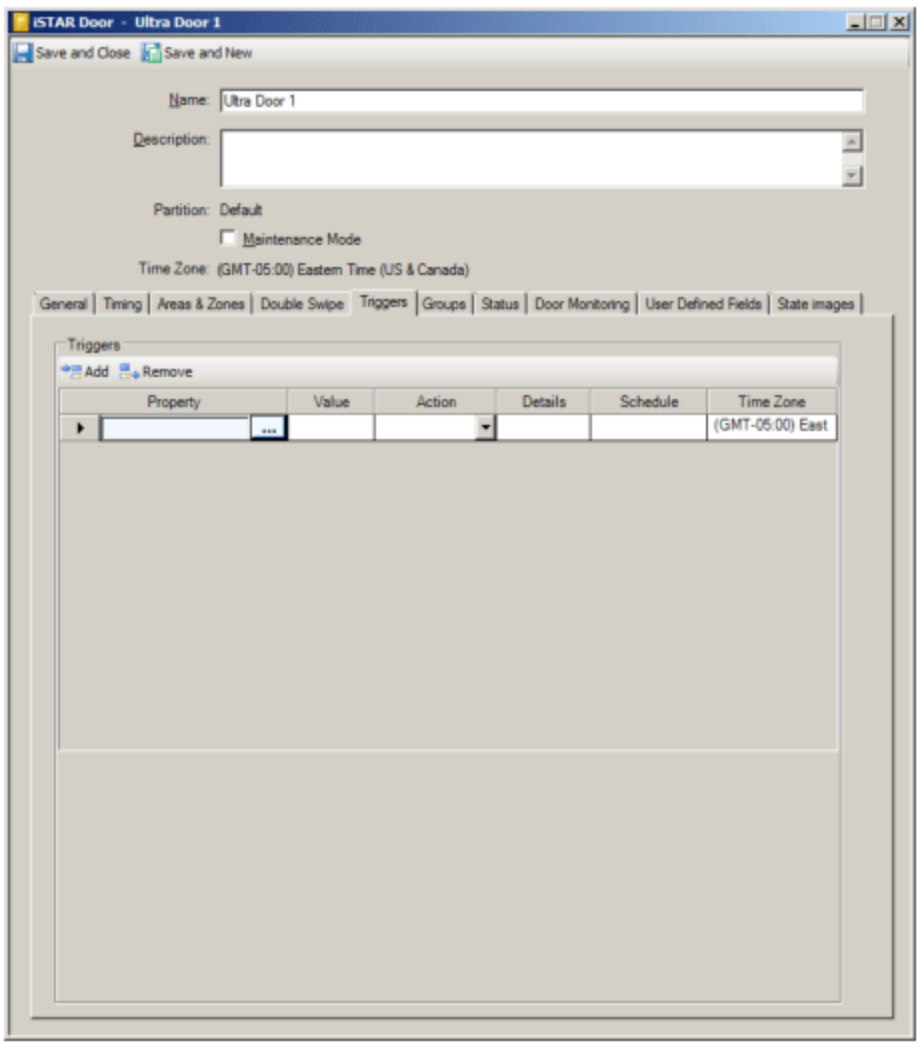
iSTAR Door Triggers Tab

You can create Triggers for iSTAR Doors using the iSTAR Door Triggers tab. A Trigger executes a specified **Action** when a particular predefined condition occurs. When a Trigger is defined, the Actions available depend on the property selected. The Door Triggers tab is shown in Figure 169 on Page 439.

See the following for information on iSTAR Triggers:

- Triggers Tab for iSTAR Devices on Page 270.
- Defining a Trigger for an iSTAR Device on Page 271.
- Removing a Trigger on Page 272

Figure 169: iSTAR Door Triggers Tab



Using Double Swipe to Trigger an Event

You can create a trigger to associate Double Swipe activity with the ability to activate an event on a schedule when the door's reader receives a double-swipe to Lock or Unlock.

To Create the Trigger for an Event

1. Navigate to the **Triggers** tab, as shown in Figure 169 on Page 439.
2. Click **Add** on the **Triggers** tab to create a new trigger.
3. Click within the **Property** column to display the browse button [...]. A window opens, presenting the list of properties for the door.
   a. Select the **Double Swipe** Property to add it to the column.

4. Click in the **Value** column to display the list of Values associated with the Double Swipe Property. Select either **Locked** or **Unlocked** as the value for the trigger and add it to the column. Do not select "Unknown" as a value because it is not a valid option and would be ignored.
5. Click in the **Action** column to display a drop-down list of actions. Select **Activate Event** as the action for the trigger and add it to the column. The other actions in the list are not valid for the double swipe trigger and will be ignored. The lower pane on the Triggers tab will display an event entry field that is specific to the selected Action.

   For the combination of Double Swipe Property and Locked or Unlocked Value, **Activate Event** is currently the only action supported.
6. In the **Event** field, click [...] to display a list of pre-configured Events. Click on an event in the list to add it to the field. This Event will occur when the conditions of the trigger are met.

   Events may be created from the Configuration pane and "Event" in the drop-down menu on the Administration application. See the *C•CURE 9000 Software Configuration Guide* for more information.
7. Click in the **Schedule** column, then click [...] to select a Schedule to associate with the trigger. Notice that when you click in the Schedule column, the details of the Event you selected display in the Details column. If the event has no description entered, the Details cell will remain empty.

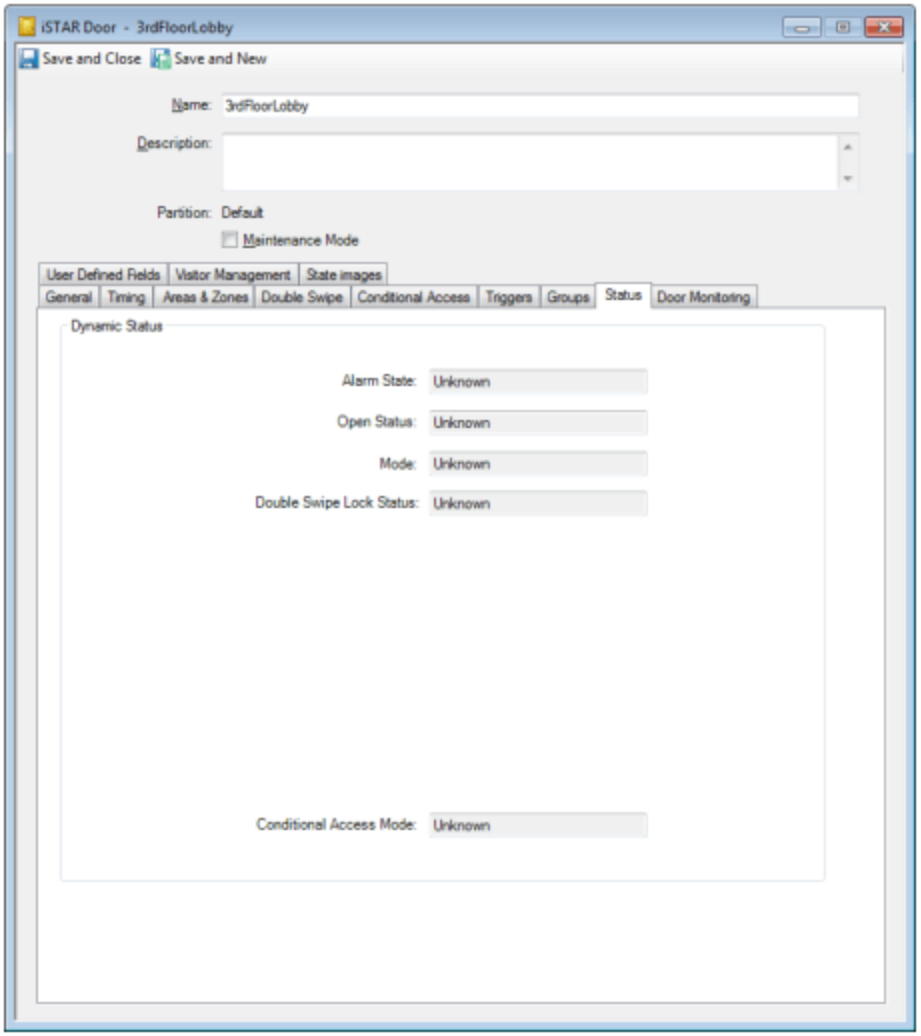
   Schedules may be created from the Configuration pane and "Schedule" in the drop-down menu on the Administration application.
8. Navigate to another tab or click **Save and Close** to save the trigger, or click **Save and New** to open a new door editor.

iSTAR Door Status Tab

The Door Status tab (see Figure 170 on Page 441) provides a read-only listing of critical information about the operational status of the selected Door including:

- **Alarm State** - displays the values Normal, Forced, Held Open, or Unknown.
- **Open Status** - displays the values Open, Closed, or Unknown.
- **Mode** - displays the values Locked, Unlocked, No Access, or Unknown.
- **Double Swipe Lock Status** - displays the values Locked, Unlocked, or Unknown.
- **Conditional Access Mode** - displays the values True, False, or Unknown. (This field displays only if Conditional Access has been enabled by selecting the **Include Personnel Without Clearance in Personnel Downloads** option in the Conditional Access box on the **General** tab of the iSTAR Controller editor.)

Figure 170: iSTAR Door Status Tab

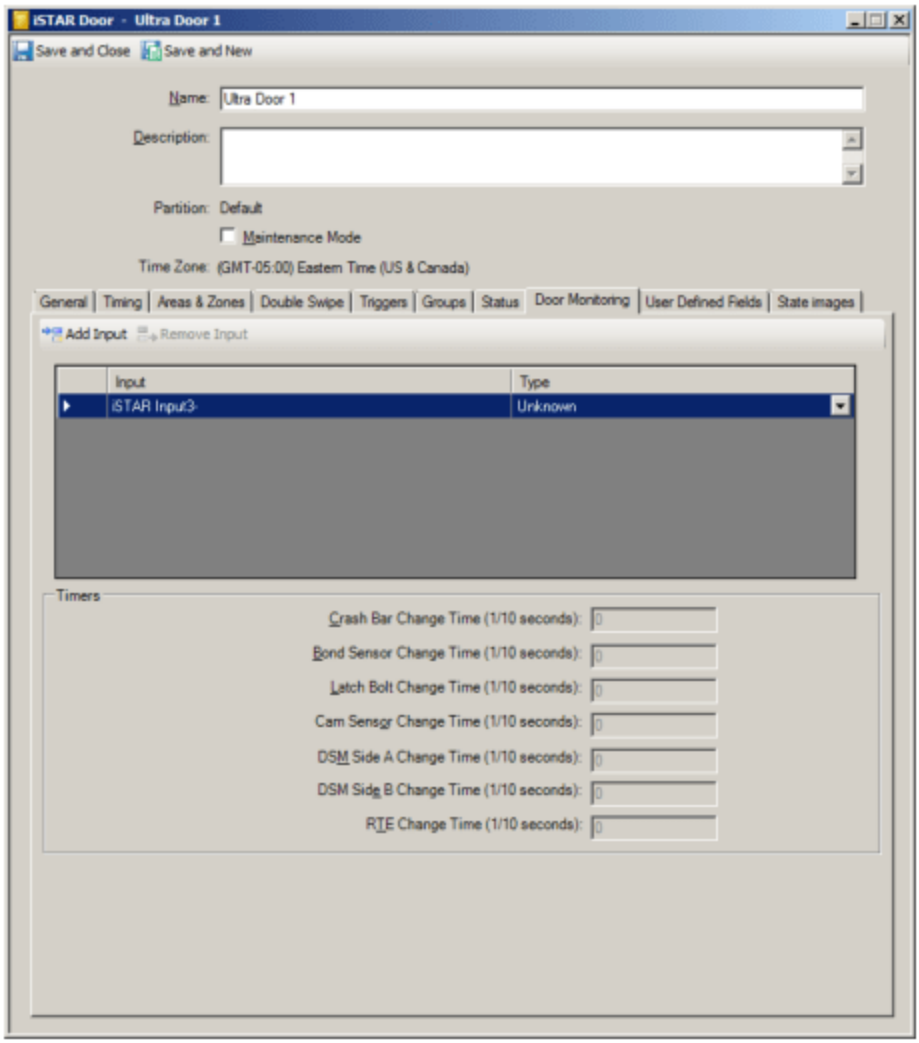


Navigate to the **State Images** tab or click **Save and Close**.

iSTAR Door Monitoring Tab

The iSTAR Door Monitoring tab lets you configure Doors with additional monitoring inputs and lock sensing equipment. You can use this tab to integrate with third-party lock release inputs, such as fire and crash bar devices, that control emergency exit from C•CURE 9000 doors. For more information about Door Monitoring, see Understanding Advanced Door Monitoring on Page 458.

Figure 171: Door Monitoring Tab



See Advanced Door Monitoring Definitions on Page 461 for definitions of the fields on the Door Monitoring tab.

iSTAR Door State Images Tab

The **State Images** tab (shown in Figure 172 on Page 443) provides a means to change the default images used to indicate controller states.

To Change an Image

1. Double-click the existing image.

A **Windows Open** dialog box appears allowing you to browse for a folder in which you have placed replacement images.

2. When you locate the replacement image, select it to add it to the image listing.
3. To restore the default image, right-click the new image and select **Restore Default**.

Figure 172: iSTAR Door State Images Tab

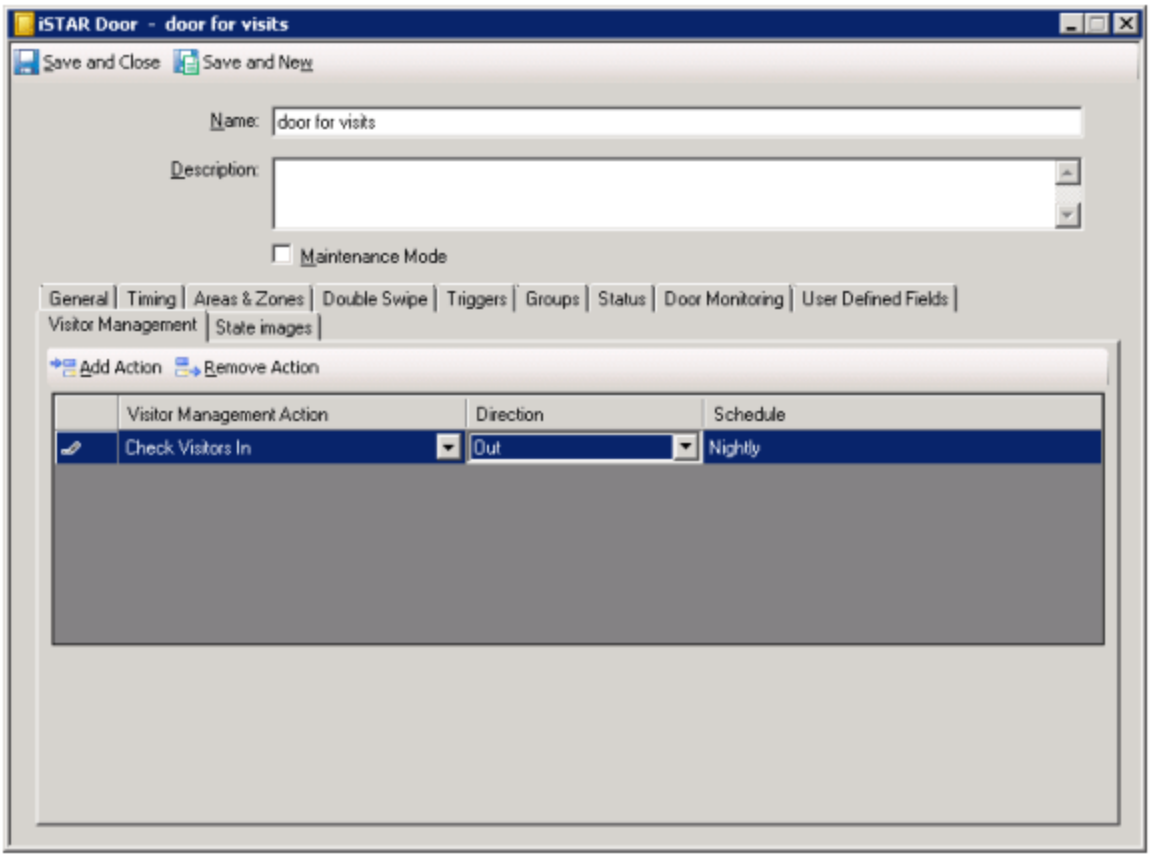
4. Click **Save and Close** to return to the **Hardware** pane.

iSTAR Door Visitor Management tab

The iSTAR Door Visitor Management tab lets you configure Doors with Visitor Management Actions, so that you can automatically Check-in and Check-out Visitors.

For more information about Check-in and Check-out of Visitor via Visitor Management, see the C•CURE 9000 Visitor Management Guide.

Figure 173: iSTAR Door Visitor Management tab



To Configure a Door Action for Check-In

1. In the C•CURE 9000 Admin Client, navigate to the Door you wish to configure.
2. Click the Visitor Management tab.
3. Click **Add Action**.
4. Chose the Visitor Management Action **Check Visitors In**.
5. Select the **Direction** for the action to take place.
   - Choose **In** for Visitors to Check-in using an inbound reader.
   - Choose **Out** for Visitors to Check-in using an outbound reader.
   - Choose **In and Out** for Visitors to Check-in using either the inbound or outbound reader.
6. Select a Schedule for the action to be active.
7. Click **Save and Close**

To Configure a Door Action for Check-out

1. In the C•CURE 9000 Admin Client, navigate to the Door you wish to configure.
2. Click the Visitor Management tab.

3. Click **Add Action**.
4. Chose the Visitor Management Action **Check Visitors Out**.
   - Check Out Visitors and Return Badge.
5. Select the Direction for the action to take place.
   - Choose **In** for Visitors to Check-out using an inbound reader.
   - Choose **Out** for Visitors to Check-out using an outbound reader.
   - Choose **In and Out** for Visitors to Check-out using either the inbound or outbound reader.
6. Select a Schedule for the action to be active.
7. Click **Save and Close**

To Configure a Door Action for Check-out

This presumes that a Badge Return mechanism is set up at the Check-out reader.

1. In the C•CURE 9000 Admin Client, navigate to the Door you wish to configure.
2. Click the Visitor Management tab.
3. Click **Add Action**.
4. Chose the Visitor Management Action **Check Visitors Out**.
   - Check Out Visitors and Return Badge.
5. Select the Direction for the action to take place.
   - Choose **In** for Visitors to Check-out and Return the Badge using an inbound reader.
   - Choose **Out** for Visitors to Check-out and Return the Badge using an outbound reader.
   - Choose **In and Out** for Visitors to Check-out and Return the Badge using either the inbound or outbound reader.
6. Select a Schedule for the action to be active.
7. Click **Save and Close**

iSTAR Door Definitions

The definitions of the various fields and buttons on the Door dialog box for iSTAR doors are given in the tables below.

Table 99: iSTAR Door General Tab Definitions

Field/Button	Description
Name	Use the Identification box to enter a name (up to 100 characters long) and brief description of the door you are configuring.
Description	A description of the door that you are configuring.
Maintenance Mode	Click to put the iSTAR door into Maintenance Mode. See Chapter 2: Maintenance Mode for more information.
Location	
Controller	This read-only field displays the iSTAR Controller that is connected to the Door.
Hardware	
Door Switch Monitor	Click ... for the **Door Switch Monitor**. When you click this button to select an input to assign to the **Door Switch Monitor**, a browser opens presenting a list of inputs available for the controller. Click an **Input** to select it and add it to the entry field.
Door Lock Relay	Click ... for the **Door Lock Relay**. When you click this button to select an input to assign to the **Door Lock Relay**, a browser opens presenting a list of outputs available for the controller. Click an **Output** to select it and add it to the entry field.
Alternate Shunt Relay	Click ... for the **Alternate Shunt Relay**. When you click this button to select an output to assign to the **Alternate Shunt Relay**, a browser opens presenting a list of outputs available for the controller. Click an **Output** to select it and add it to the entry field. Timing for this output is set on the iSTAR Door Timing Tab on Page 429. Cardholders with the Alternate Shunt ADA setting enabled on the Personnel General tab (See the *C•CURE 9000 Personnel Configuration Guide*) are granted the additional Alternate Shunt time before a door held alarm is generated.
Shunt Expiration Relay	Click ... for the **Shunt Expiration Relay**. When you click this button to select an output to assign to the **Shunt Expiration Relay**, a browser opens presenting a list of outputs available for the controller. Click an **Output** to select it and add it to the entry field.
Readers	
Entrance Reader	Click ... for the **Entrance Reader**. When you click this button to select a reader to assign to the **Entrance Reader**, a browser opens presenting a list of readers available for the controller. Click a **Reader** to select it and add it to the entry field.
Exit Reader	Click ... for the **Exit Reader**. When you click this button to select a reader to assign to the **Exit Reader**, a browser opens presenting a list of readers available for the controller. Click a **Reader** to select it and add it to the entry field.
Readers are Continuously Active	Select the **Readers are Continuously Active** check box to enable continuous reader activity. Selecting this option for a Reader on an iSTAR Area Door permits the Area to be configured for **Companion** mode Escorted Access. Leaving this option unselected causes Escorted Access to operate in **Remote Escort** (or **Turnstile**) mode.
Request to Exit	
Request to Exit	Click ... for the **Request to Exit**. When you click this button to select an input to assign to the **Request to Exit**, a browser opens presenting a list of inputs available for the controller. Click an **Input** to select it and add it to the entry field.

Table 99: iSTAR Door General Tab Definitions (continued)

Field/Button	Description
Unlock Door on RTE	Select the **Unlock Door on RTE** check box to unlock the door at a **Request to Exit**.
Shunt DSM While RTE is Active	Select the **Shunt DSM While RTE is Active** check box to **Shunt Door Switch Monitor While Request to Exit is Active**.

iSTAR Door Timing Tab Definitions

Table 100: iSTAR Door Timing Tab Definitions

Field/Button	Description
Timers	
Delay Relock	Type the number of seconds to delay door relock after the door is opened (after a request to exit, for example). The range in seconds is 0:0:0 to 0:16:39 (999 seconds); the default is 0:0:0.
Shunt Time	**Shunt Time** – type the number of seconds that the door can remain open before a door held open alert is generated within the range of 0:0:0 to 0:16:39 (999 seconds); the default is 0:0:10 (10 seconds).
Unlock Time	**Unlock Time** – type the number of seconds the Door remains unlocked after a valid card swipe, RTE activation, or momentary unlock within the range of 0:0:0 to 0:4:15 (255 seconds); the default is 0:0:5 (5 seconds).
Alternate Shunt Time	**Alternate Shunt Time** – type the number of hours, minutes, and seconds the Door can remain open before a door held open alert is generated after a valid card swipe by a cardholder with the **Alternate Shunt** flag set in their personnel record (This value is used only if it is set to a greater time than the **Shunt time** value) within the range of default/minimum: 0:0:0; maximum:18:0:0 (18 hours).
Shunt Expiration Warning Time	If set, the Shunt expiration relay fires regardless of the shunt time used. If set to 0 (the default), the Shunt expiration relay fires only if the Alternate shunt time is used. The Shunt Expiration Warning has a range of 0:0:0 to 0:4:0 (4 minutes).
Door Close Debounce Time	Specifies the time (in 1/10th of a second intervals) that the C•CURE 9000 ignores DSM inputs, to allow for bouncing doors. Setting this value to 0 indicates that there is no timer. The range is 0 - 25.5 seconds.
Door Open Grace Time	Specifies the time (in 1/10th of a second intervals) that the C•CURE 9000 waits for an RTE, card admit, or momentary unlock signal after receiving the signal from the DSM. Setting this value to 0 indicates that there is no timer; as soon as the door opens, door forced open is reported. The range is 0 - 25.5 seconds.
Door Unlock Grace Time	Specifies the time (in 1/10th of a second intervals) that the C•CURE 9000 waits for a door open signal after the door unlock time has expired. This timing prevents a false door forced message in situations where signals are nearly simultaneous. The range is 0 - 100 seconds.
Options	
Always Use Shunt Expire Output	if this option is selected, the Shunt expiration relay is fired regardless of the shunt time used. If the **Shunt Expiration Warning Time** is set to 0 (the default), the Shunt expiration relay shall only be fired if the Alternate shunt time was used.

Table 100: iSTAR Door Timing Tab Definitions (continued)

Field/Button	Description
Delay Relock While Door Open After Valid Access	If access is valid, delays the relock of the door until the door closes, if this check box is selected. This differs from standard relock operations, where relock occurs when the door opens and the relock delay expires If the door is open, the lock is energized. The C•CURE 9000 sends an alarm when the shunt time expires.
Shunt Door for full Shunt Time	If this option is selected, the door is shunted for the full shunt time. If selected with Delay relock while door open for valid access, the lock is energized and the door unlocked for the full shunt time, regardless of whether the door is open or closed.

iSTAR Door Areas and ZonesTab Definitions

Table 101: iSTAR Door Areas & Zones Tab Fields

Box/Fields	Description
Areas	
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.
Intrusion Zones	
Intrusion Zone	Name of iSTAR Intrusion Zone this Door is assigned to
Zone Direction	**I n** 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.

iSTAR Door Double Swipe Tab Definitions

Table 102: iSTAR Door Double Swipe tab definitions

Field/Button	Description
Permission to Cardholders	
None	If this option is selected, Double Swipe is not enabled at the door. If Double Swipe is active at the door, you may turn off Double Swipe by selecting None on this tab. Normal card swipe access at the reader is still in effect, if so configured.
With clearance	Selecting this option will enable the door to require that a cardholder who uses Double Swipe also has Double Swipe clearance configured for them in the Personnel screen, Clearances tab.

Table 102: iSTAR Door Double Swipe tab definitions (continued)

Field/Button	Description
With clearance and in personnel group	Selecting this option will require that a cardholder who uses Double Swipe at the reader have a Double Swipe clearance set and also be in the personnel group that may be selected in the next fields
Personnel group	Click ... to select a personnel group whose members may be admitted on Double Swipe as long as each member has the proper clearance set for them in the Personnel screen, Clearances tab.
Options	
Priority	Select a priority (from 0 - 200) for Double Swipe requests at the door. In the case of a manual action with higher priority than the priority configured for the door, the manual action takes precedence. If the door's priority is higher, the double swipe takes precedence. For two actions with the same priority, the most recent one takes precedence.
Double Swipe Cancellation Schedule	Click ... to select a schedule. The cancelling schedule will delete any existing double swipe causes on the door at the start of the time spec. Any double swipe actions currently in effect will be cancelled.

iSTAR Door Conditional Access Tab Definitions

Table 103: iSTAR Conditional Access Tab Definitions

Field/Button	Description
Conditional Access Schedule	Click ... to select the schedule during which the door is 'Conditional Access-enabled'. This can be any schedule in the same time zone as the controller. The **iSTAR Door Status** tab will indicate whether Conditional Access is enabled or not.
Conditional Access Event	Click ... to select the event that requests 'Conditional Access' at this door for a person without Clearance. Only panel events within this controller's cluster are available for selection. This event **cannot** be the same one that targets this door with the 'Allow Conditional Access Cycle' action—lets the person through the door.
Conditional Access Response Time	Specifies the time (in seconds) that the door waits for an 'Allow Conditional Access Cycle' event action in response to the activation of the Conditional Access event. The range is 1 - 150 seconds with a default of 10 seconds.
NOTE: You can choose to display columns on the **iSTAR Door Dynamic View** that indicate for a given door: • Whether or not Conditional Access is enabled. • The selected Conditional Access schedule, event, and response (delay) time.	

iSTAR Door Triggers Tab Definitions

Table 104: iSTAR Door Triggers Tab Definitions

Field/Button	Description
Triggers	
Add	Click **Add** in the **Triggers** tab to create a new trigger.
Remove	Click the row selector , then click **Remove** to delete a trigger.
Property	Click within the **Property** column to display ..., When you select this button, the **Property** browser opens presenting properties available for the controller. Click a **Property** to select it and add it to the column.
Value	Click within the **Value** column to display a drop-down list of Values associated with the **Property** that you have selected. Click on a **Value** that you want to include as a parameter for the trigger to add it to the column.
Action	Click within the **Action** column to display a drop-down list of valid actions. Click on an **Action** that you want to include as a parameter for the trigger to add it to the column. When a **Trigger** is added, an **Action** must be configured in the Action column. This is the Action that will occur when the object's selected **Property** receives the selected **Value**. As the Action is selected, the lower pane in the Triggers box will show a corresponding entry field, or group of entry fields, specific to the selected Action.Click ... to select entries for these fields. Once the field (or group of fields) is completed, the **Details** column will show information about how the Action has been configured.
Details	Displays details concerning the security objects that are associated with the selected Action.
Schedule	Click within the **Schedule** column, then click ... to select a **Schedule** that you want to associate with the trigger. Schedules are created in the Configuration Pane. See the *C•CURE 9000 Software Configuration Guide* for more information.

iSTAR Triggers Properties

Table 105: iSTAR Triggers Properties

Property	Description
Admit Status Admit Admit Visitor Reject Visitor Reject Duress Noticed Admit Noticed Reject Pre-Admit	For any one of the **Admit Status**, **Mode Status**, or **Open Status** values (see the Value column drop-down list) you can choose one of the following Actions to create a Trigger: **Activate Event** – When this status occurs and the Schedule is Active (you can choose any Schedule). You must set a **Minimum Activation Time** in the Event or the actions in the Event will not activate. **Activate Event Outside Schedule** – An event is activated when this status occurs while the Schedule is Inactive (choose any Schedule). **Activate Output** – Activate an Output when this status occurs (only works with the **Always** Schedule). **Pre-Admit** status is a special case used to activate a panel Event on a card swipe before the door is opened. It is used with the Activate Event action to activate an Event that can, for example, change the state of an output on the iSTAR panel.
Mode Status Unlocked Locked No Access Momentary Unlock	
Open Status Open Closed	
Double Swipe Status Locked Unlocked	For any one of the **Double-Swipe Status** values (see the Value column drop-down list) you can choose one of the following Actions to create a Trigger: **Activate Event** – When this status occurs and the Schedule is Active (you can choose any Schedule). You must set a **Minimum Activation Time** in the Event or the actions in the Event will not activate. **Activate Event Outside Schedule** – An event is activated when this status occurs while the Schedule is Inactive (choose any Schedule).
Alarm State Status Normal Forced Held Open	1. Choose a value for the Property from the Values column. 2. Select an Action from the Action drop-down list. See iSTAR Trigger Actions in Table 106 on Page 452. 3. Select a Schedule by clicking in the Schedule column, then click to select the Schedule that you want to associate with the trigger. For example, if you chose **Forced** as an Alarm State Status for which you want to define an action, you could then select **CCTV Action** if you wanted to send a command to a CCTV Switch, then in Details, select the Switch and the Command (such as **Call Up Camera**) that you wanted to activate when a Forced status occurred.

iSTAR Triggers Actions

Table 106: iSTAR Triggers Actions

Action	Description
Activate Event	Select an Event to activate when this status occurs
Activate Event Outside Schedule	Select an Event to activate when this status occurs while the Schedule is inactive.
Activate Output	Select an Output to activate when this status occurs. Must use the **Always** Schedule.
Arm Event	Select an Event to arm. An armed Event can be activated; a disarmed Event cannot be activated.
Arm Input	Select an Input to arm. An armed Input can be activated. A disarmed Input cannot be activated.
CCTV Action	Select a CCTV Action to perform by choosing a CCTV Switch and Command from the Details area, and filling in one or more Values for the Command's parameters.
Control Access	Select an Elevator Button which you want the Action to set for controlled access, turning on security restrictions on the use of this button.
Deactivate Event	Select an Event to be deactivated. If the Event is Active when this action occurs, the action deactivates the Event.
Deactivate Output	Select an Output to be deactivated. If the Output is Active when this action occurs, the action deactivates the Output.
Disable Keypad Commands	Disable Keypad Commands on the iSTAR Reader you select in **Details**.
Disable PIN	Set the Reader you select to no longer require that a cardholder perform a card swipe, then enter a PIN to be granted access.
Disarm Event	Select an Event to disarm. A disarmed Event cannot be activated; an Event must be armed to be activated.
Disarm Input	Select an Input to disarm. A disarmed Input cannot be activated; an Input must be armed to be activated.
Enable Keypad Commands	Set the Reader you select to accept Keypad Commands on the reader.
Enable PIN	Set the Reader you select to require that a cardholder perform a card swipe, then enter a PIN to be granted access.
Lock Door	Select a Door to Lock from the Door field in the Details area.

Table 106: iSTAR Triggers Actions (continued)

Action	Description
Momentary Unlock Door	Select a Door to Momentarily Unlock from the Door field in the Details area.
Pulse Output	Select an Output to activate for the duration specified in the Output's Pulse Duration field.
Secure Door	Select a Door that you want to secure. A secure Door cannot be unlocked; this action disarms the reader associated with the Door.
Send Email	Send an email message to the email address specified in the Details area Recipient **Email Address** field. You can designate an Event to activate if the email attempt fails. You can click the Message tab to type the text of the message and optionally choose to send the date, time, and name of the Event triggered. For Send Email to work, you must configure the **Email Server** and the **Sender Email Address** in **Options & Tools>System Variables** in the Customer Support area.
Uncontrol Access	Select an Elevator Button which you want the Action to set for uncontrolled access, turning off security restrictions on the use of this button.
Unlock Door	Select a Door to unlock from the Door field in the Details area.
Video Camera Action	Select a Video Camera Action to perform by choosing a Video Server and Camera from the Details area Camera tab, and choosing one of the following Action Types. • **Record Camera** lets you set a Pre Alarm Time and Post Alarm Time for retrieving recorded video. • **Camera Preset Command** allows you to designate a Camera Preset to activate when this action is triggered. • **Camera Pattern Command** lets you designate a Camera Pattern to activate when this action is triggered.

iSTAR Door Groups Tab Definitions

Table 107: iSTAR Door Groups Tab Definitions

Field/Button	Description
Groups	
	For more information about the use of the Toolbar buttons, see Chapter 2, "Dynamic Views" in the *C•CURE 9000 Data Views Guide*
Name	This column displays the name entered for the group when it was configured. The selected door is a member of any group(s) listed in this column.
Description	This column displays the description entered for the group when it was configured.

iSTAR Door Status Tab Definitions:

Table 108: iSTAR Door Status Tab Definitions

Field/Button	Description
Alarm State	Displays the values Normal, Forced, Held Open, or Unknown.
Open Status	Displays the values Open, Closed, or Unknown.
Mode	Displays the values Locked, Unlocked, No Access, or Unknown.
Double Swipe Lock Status	Indicates the current status of a door configured for Double Swipe access: Locked, Unlocked, or Unknown. If the door is not configured for double swipe access, the field displays Unknown.
Conditional Access Mode	Displays the values True, False, or Unknown.

iSTAR Door State Images Tab Definitions:

Table 109: iSTAR Door State Images Tab Definitions

Field/Button	Description		Field/Button	Description
Unknown			Locked	
Forced			Unlocked	
Held Open			No Access	
Open			Momentary Unlock	

iSTAR Aperio Door Editor

You use the iSTAR Aperio Door editor to configure iSTAR Aperio Doors.

iSTAR Aperio Doors are created automatically when you configure and enable an iSTAR Aperio Reader (see iSTAR Aperio Reader Editor on Page 264). You cannot manually create an iSTAR Aperio Door.

If you delete an iSTAR Aperio Door, the iSTAR Aperio Reader associated with the door is also deleted.

NOTE iSTAR Aperio Doors do not support manual actions for Lock, Unlock, and Momentary Unlock.

You cannot create Door Groups that combine iSTAR Aperio Doors with other types of iSTAR Doors.

The iSTAR Aperio Door Editor includes the following tabs:

- iSTAR Door General Tab on Page 427
- iSTAR Door Timing Tab on Page 429
- iSTAR Door Triggers Tab on Page 438
- Groups Tab for Hardware Devices on Page 28
- iSTAR Door Status Tab on Page 440
- iSTAR Door Visitor Management tab on Page 443
- iSTAR Door State Images Tab on Page 442

11

Chapter 11 Configuring Advanced Door Monitoring

This chapter explains the concepts of Advanced Door monitoring, and also includes the procedures that are used to create various types of monitored doors.

In this chapter

Understanding Advanced Door Monitoring

Advanced Doors are C•CURE 9000 doors that provide increased security for sites with complex requirements, like airports or hospitals. Standard Doors use the Door State Monitor (DSM) to monitor for Admit Used, Admit Unused, Door Forced and Door Held.

Advanced Doors support additional monitoring inputs and lock sensing equipment. Advanced Doors also integrate with third-party lock release inputs, such as fire and crash bar devices, that control emergency exit from C•CURE 9000 doors.

Features

Use Advanced Door Monitoring to configure:

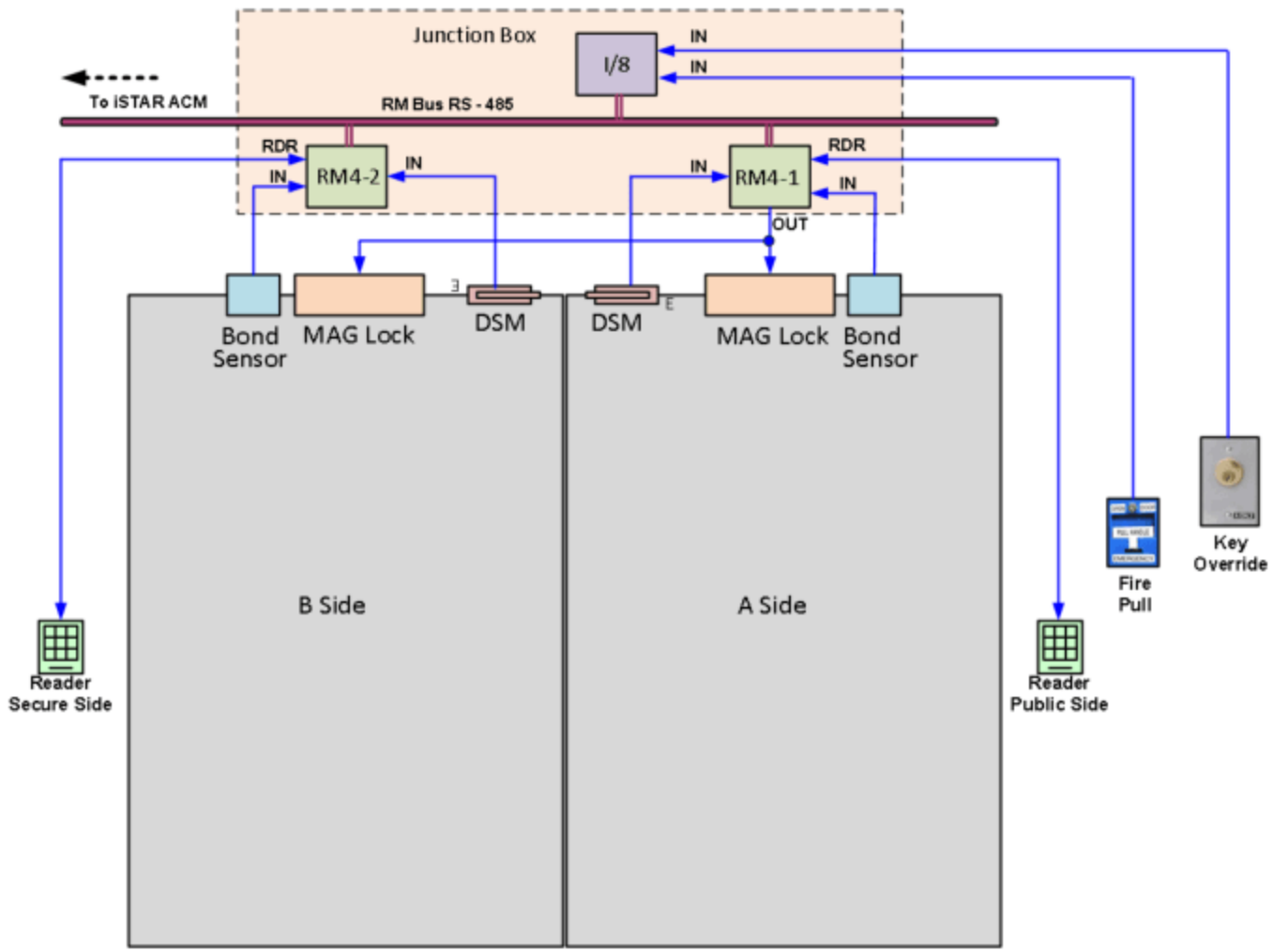
- Multiple inputs – Advanced Doors provide up to 16 inputs, 14 more than on a standard door configuration.
- More complex door configurations – including single- and double-leaf doors with multiple DSM or Request To Exit (RTE) inputs.
- Lock sensing devices – to monitor locking on magnetic bonds, bolts, and cams.
- Integrated lock releases – to integrate door unlocking with fire, crash bar, power fail, and key switch inputs.
- Special events and actions – to create keypad commands that lock, unlock, and secure doors for a specific time period.
- Alarm Suppression and RTE control on a per door basis.
- Enhanced Shunt control.
- Grace and change timing options – to fine tune C•CURE 9000 timing to avoid the effects of 'door bounce' and to correct other door timing situations at the site.
- Journal reports and Monitor Station activities – to manage the system and monitor door activity.
- Additional Event Actions related to Advanced Doors.

Example:

Figure 174 on Page 459 shows a double-leaf Advanced Door, configured into A and B sides. Each side contains a maglock, bond sensor, and DSM input that connects to RM4 modules in a nearby junction box. Access on the public side of the door is controlled using the public-side read head. This read head is also configured to accept keypad commands that allow personnel to lock and unlock the door for specific time intervals. Exit from the secure side of the door is controlled by the secure-side read head.

Locks can be released for fire alarm, crash bar, power failure, or manual key switch. Inputs from the fire pull and key switch over-ride are shown connected to an I/8 board in the local junction box.

Figure 174: Typical Advanced Door Configuration



Hardware Requirements

The following guidelines apply to Advanced Doors:

- Advanced Door monitoring is available only on iSTAR configurations.
- Advanced Door inputs can be any mix of lock sensors, lock releases, or DSM or RTE connections.
- Each Advanced Door supports up to 16 input connections. However, the number of available inputs per door is limited by the number of doors in the configuration and the input capacity of the fully loaded iSTAR controller.
- All Door components, Readers, Inputs, and Outputs, must reside on the same Controller. The table below shows that some controllers may not have enough Inputs for the maximum configuration. In actual practice, these limits will rarely, if ever, be reached.,

Table 110: Maximum Inputs per iSTAR

Controller	Max Doors	Max Advanced Door Inputs	Max Inputs on Controller	Result
iSTAR Ultra	16	16 x 16 = 256	336	Adequate Inputs
iSTAR Pro	16	16 x 16 = 256	192	- 64 Inputs
iSTAR eX 8 Door	8	8 x 16 = 128	96	- 32 Inputs
iSTAR eX 4 Door	4	4 x 16 = 64	88	Adequate Inputs
iSTAR Edge 4 Door	4	4 x 16 = 64	64	Adequate Inputs
iSTAR Edge 2 Door	2	2 x 16 = 32	32	Adequate Inputs
iSTAR Edge 1 Door	1	1 x 16 = 16	4	- 12 Inputs

- Advanced Doors support the same number and types of outputs as standard doors—which are as follows:
  - Door Latch Relay (1)
  - Alternate Shunt (ADA) Relay (1)
  - Shunt Expiration warning Relay (1)

Advanced Door Monitoring Definitions

New Definitions, Acronyms, and Abbreviations

- **Lock Sensor** - An input that monitors the state of the lock on a door. This is not the same as the Door Switch Monitor (DSM) that monitors whether the door is physically open or closed.
  - **Bond Sensor** - A type of lock sensor input that monitors the condition of a magnetic lock on door. A normal bond sensor input will be active when the door is unlocked (meaning that the door latch relay is active), regardless of whether the door is open or closed, but will also be active when the door is open, regardless of whether the door is unlocked or not unlocked. In other words, it should be active when the door is unlocked and/or when the door is open. The bond sensor should not be active when the door is closed and locked.
  - **Cam Detector** - A type of lock sensor input that monitors the condition of the cam on an electric strike on a door. A normal cam detector input will be active when the door is unlocked. The Cam detector should not be active when the door is locked.
  - **Latch Bolt Detector** - A type of lock sensor input that monitors the condition of a latch bolt on an electric strike on a door. A normal latch bolt will be active or inactive while the door is unlocked, and will be active when the door is open. The latch bolt should not be active when the door is closed and locked.
- **Lock Release Device** - A external device that may unlock a door that is also controlled by the access control system. Indication that the lock release device is active will be supplied through an input.
  - **Fire Alarm Lock Release** - An input that indicates that the fire alarm system has unlocked the door.
  - **Crash Bar Lock Release** - An input that indicates that the door has been unlocked by local crash bar / panic hardware.
  - **Key Switch Lock Release** - An input that indicates that the door has been unlocked by local key switch override.
  - **Power Fail Lock Release** - An input that indicates that the door has been unlocked by a lock release device because of power fail.

Lock Sensor States

Table 111 on Page 461 indicates operational differences in the Lock Sensors.

0 = False or Not Active

1 = True or Active

Table 111: Lock Sensor States

Door and Lock State	DSM	Bond Sensor	Cam Detector	Latch Bolt Detector
1. Door Closed and Locked	0	0	0	0
2. Door Closed and Unlocked	0	1	1	1
3. Door Open and Unlocked	1	1	1	1
4. Door Open and Locked	1	1	0	1

1. When the door is Closed and Locked, none of the sensors are active.

2. When the door is Closed and Unlocked, all of the sensors are active except for the DSM because the Door is still closed.
3. When the door is Open and Unlocked, all of the sensors are active including the DSM because the Door is now open.
4. When the door is Open and Locked, all of the sensors are active except for the Cam Detector because the Door is Locked.

   In this case, the Latch Bolt Detector is active because the door is Locked. When the Latch Bolt Detector is active, along with the door being open, there is a possibility of damaging the door frame. The Latch Bolt lock is like a dead bolt in that the bolt is extended when the door is locked.

Advanced Door Monitoring Components

In addition to standard door components, Advanced Doors support:

- Lock sensor devices
- Lock release devices
- Alarms based on lock sensor, lock release, and multiple DSM inputs to the C•CURE 9000
- Expanded Door Triggers
- Expanded Event Actions

Lock Sensor Devices

A **lock sensing device** monitors the state of a door lock.

Table 112 on Page 463 shows the types of lock sensing devices that can be configured on an Advanced Door.

Table 112: Lock Sensing Devices

Lock Sensing Device	Function
Bond sensor	Monitors the condition of a magnetic lock on a door.
Cam detector	Monitors the condition of the cam on an electric strike on a door.
Latch bolt detector	Monitors the condition of a latch bolt on an electric strike on a door.

Lock Release Devices

A **lock release device** is a third-party device that controls door unlock activities. Lock release devices operate independently from C•CURE 9000 and function even if the C•CURE system is not running.

To inter-operate, the lock release device has an output, called a lock release input, that is input to the C•CURE 9000. The C•CURE 9000 uses the lock release input to:

- Monitor the lock release activities on a door
- Monitor lock sensor activity
- Decide if an open door is reported as door forced open, door open, or door open by one of the lock release inputs.

Table 113 on Page 463 and Figure 175 on Page 464 show the types of lock release devices that can be configured on an Advanced Door.

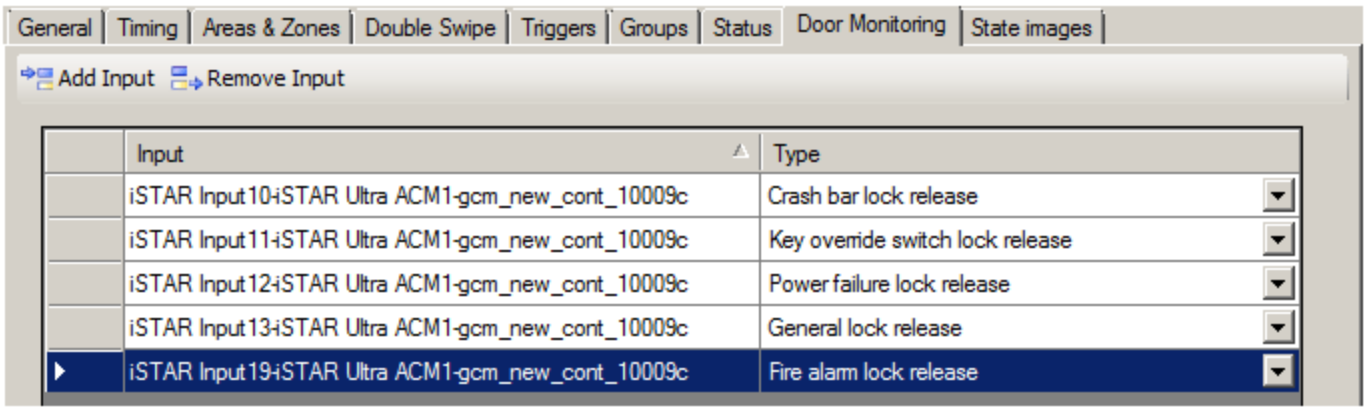
Table 113: Lock Release Devices

Lock Release Device	Function
Crash bar lock release	Input to C•CURE 9000 from crash bar or panic hardware

Lock Release Devices (continued)

Lock Release Device	Function
Key override switch lock release	Input to C•CURE 9000 from a key override switch
Power failure lock release	Input to C•CURE 9000 from power fail hardware
General Lock Release	Input to C•CURE 9000 from a Fire Alarm System or iSTAR.
Fire alarm lock release	Input to C•CURE 9000 from a Fire Alarm System

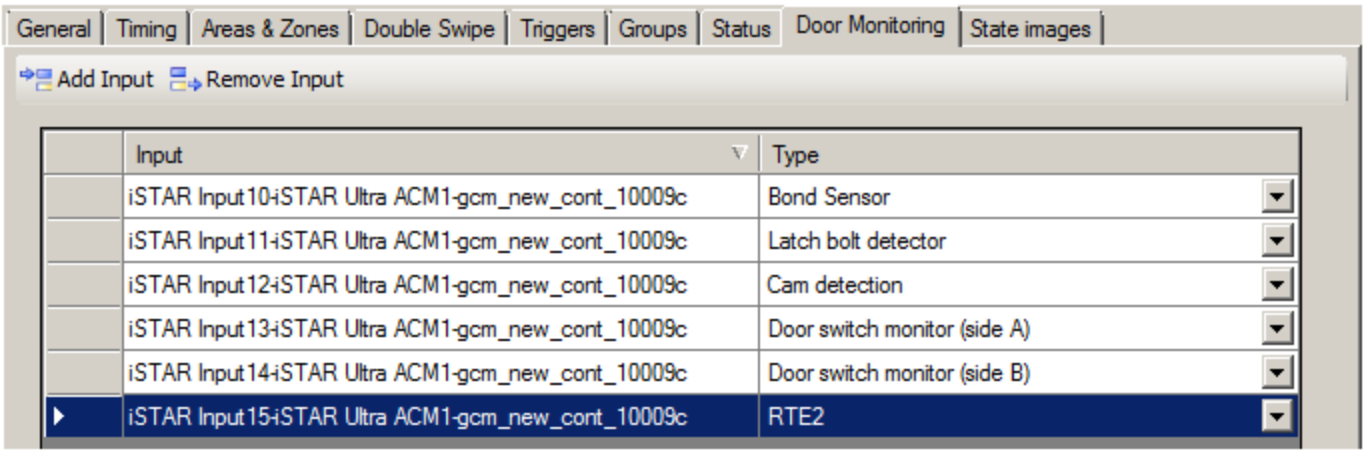
Figure 175: Lock Release Devices in the Door Monitoring Tab



Expanded Door Inputs

In addition to the Lock Sensors, there are also additional inputs for multiple DSMs and RTEs as shown in Figure 176 on Page 464.

Figure 176: Expanded Door Inputs in the Door Monitoring Tab



Advanced Door Alarms

Table 114 on Page 465 and Figure 177 on Page 465 show the alarm operations available for Advanced Doors. Each alarm reports the name of the input (lock sensor, lock release device, DSM) that caused the alarm.

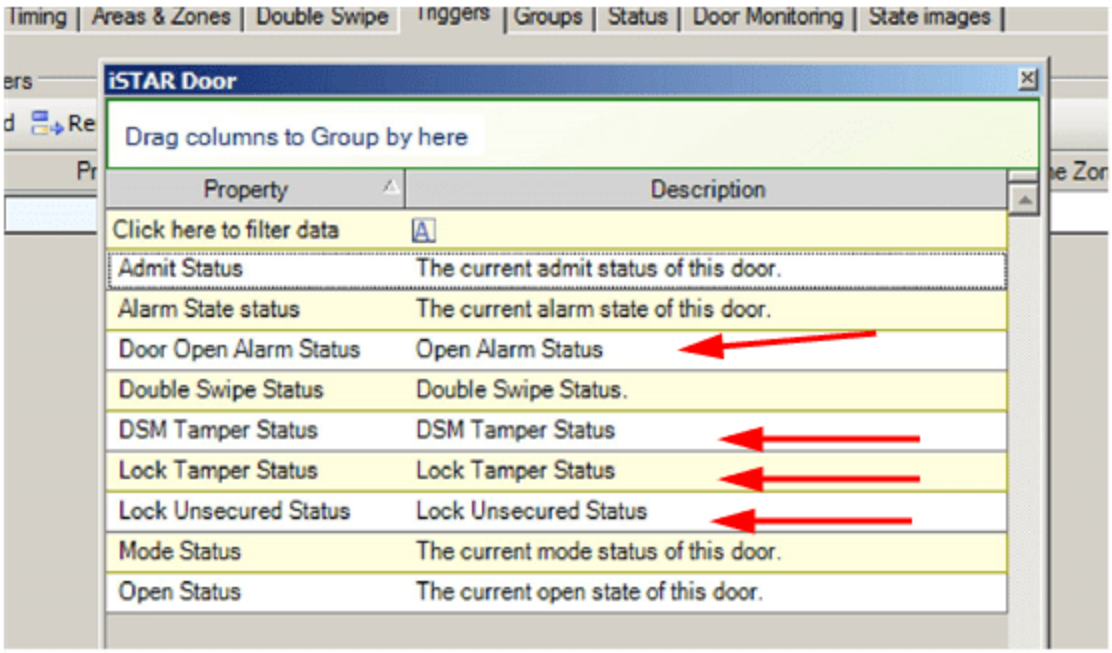
Table 114: Advanced Door Alarms

Alarm	Description
Door Open	Door opens without valid card or RTE, and one of the lock release devices is active.
Lock Unsecured	A lock sensor activates when it should be inactive. Indicates that the hardware failed to return to the locked position after a valid lock release.
Lock Tamper	A lock sensor is inactive when it should be active. Indicates lock tampering while the door is open, or failure of lock hardware.
DSM Tamper	For doors with multiple DSM devices on a single side. Indicates that one DSM changed state, and that the corresponding change did not occur to other DSMs devices on the same side of the door.

Expanded Door Triggers

There are four additional Door Triggers for Advanced Doors Alarms in the triggers Tab.

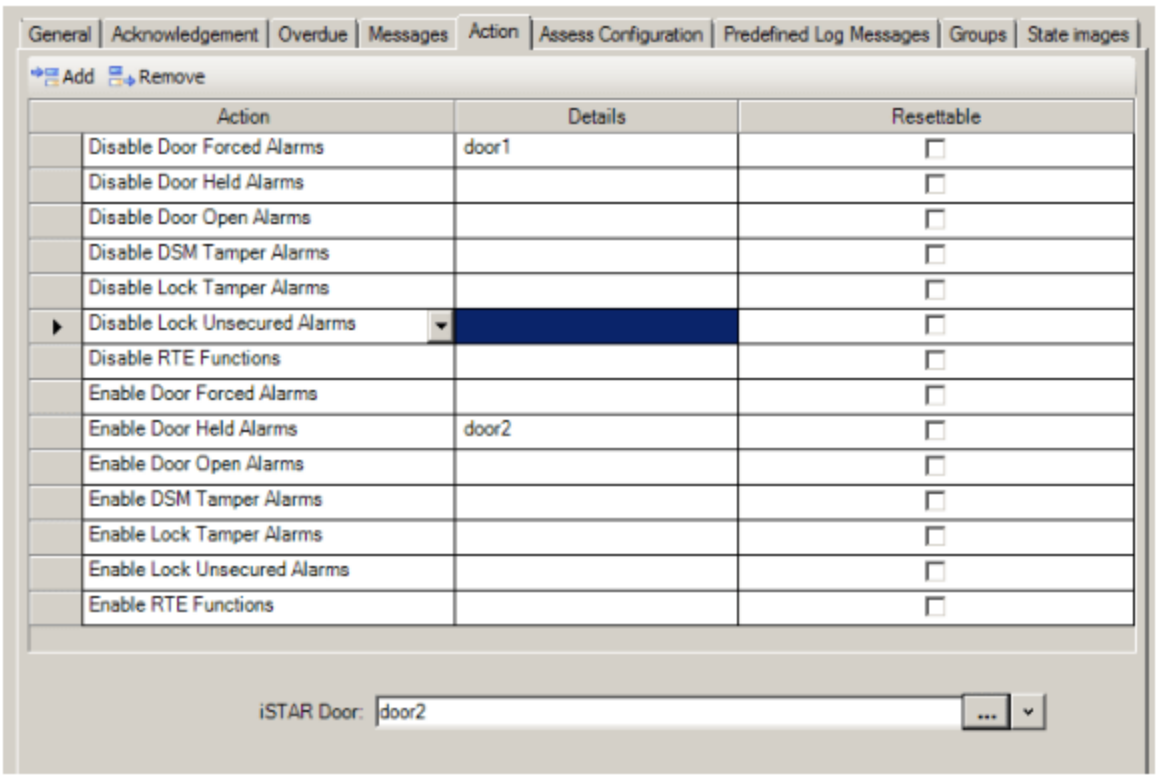
Figure 177: Additional Door Triggers



Expanded Event Actions

In addition to the Triggers on the Door, there are seven pairs of actions that toggle the allowance of the various alarms, including Door Held, Door Forced, and RTE Functions. Associate an iSTAR door with each entry. Door Groups are not supported.

Figure 178: Expanded Event Actions



Advanced Door Monitoring Configurations

Advanced Doors support configurations that include multiple RTE and DSM inputs. These are described in the following sections.

Multiple RTE Configurations

Multiple RTE devices are typically configured to:

- Provide tight security screens
- Increase coverage over wide areas

Configuration Guidelines

You must specify the first RTE in the **Request to Exit** field of the **Configure Door** dialog box. This activates other request to exit options on the **Configure Door** dialog box. Specify additional RTEs by adding them on the **Configure Advanced Door Monitoring** dialog box.

To Display the Configure Door Dialog Box

- Select Hardware Pane >Cluster>iSTAR>Doors>Door Name

To Display the Configure Advanced Door Monitoring Dialog Box

- Select Hardware Pane >Cluster>iSTAR>Doors>Door Name>Door Monitoring

NOTE If a door has multiple RTEs and is configured to shunt the DSM while RTE is active, the C•CURE 9000 will shunt the DSM when any RTE on the door is active.

Figure 179: Door Editor - Door Monitoring Tab

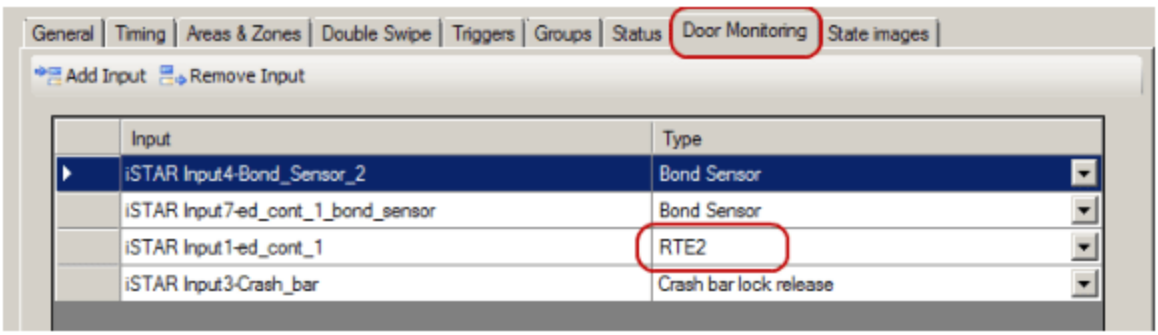
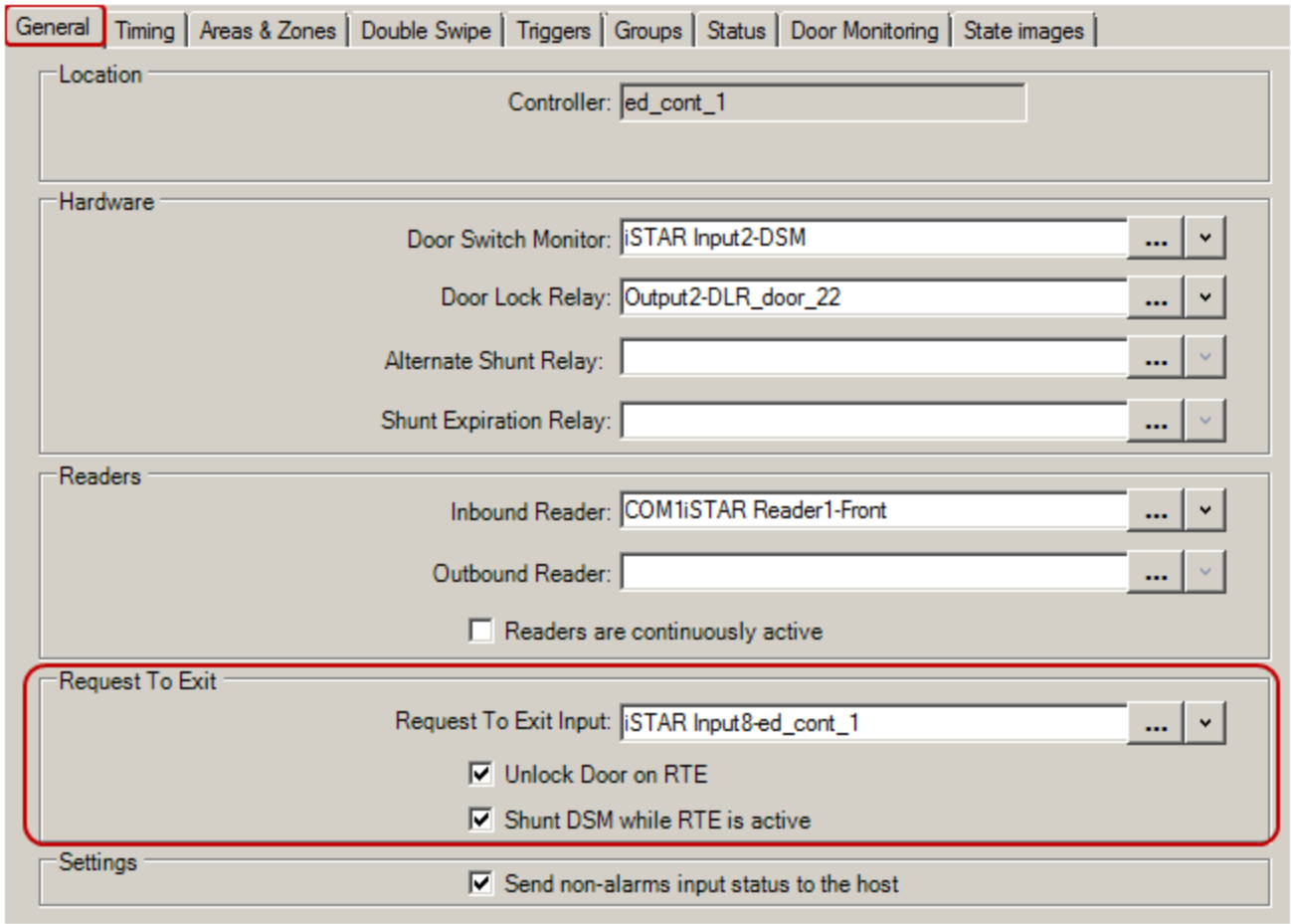


Figure 180: Door Editor General Tab



Multiple DSM Configurations

Multiple DSM configurations are used for double-leaf doors (side by side), and also to provide a tighter security screen (top and bottom). The following sections describe typical multiple DSM configurations.

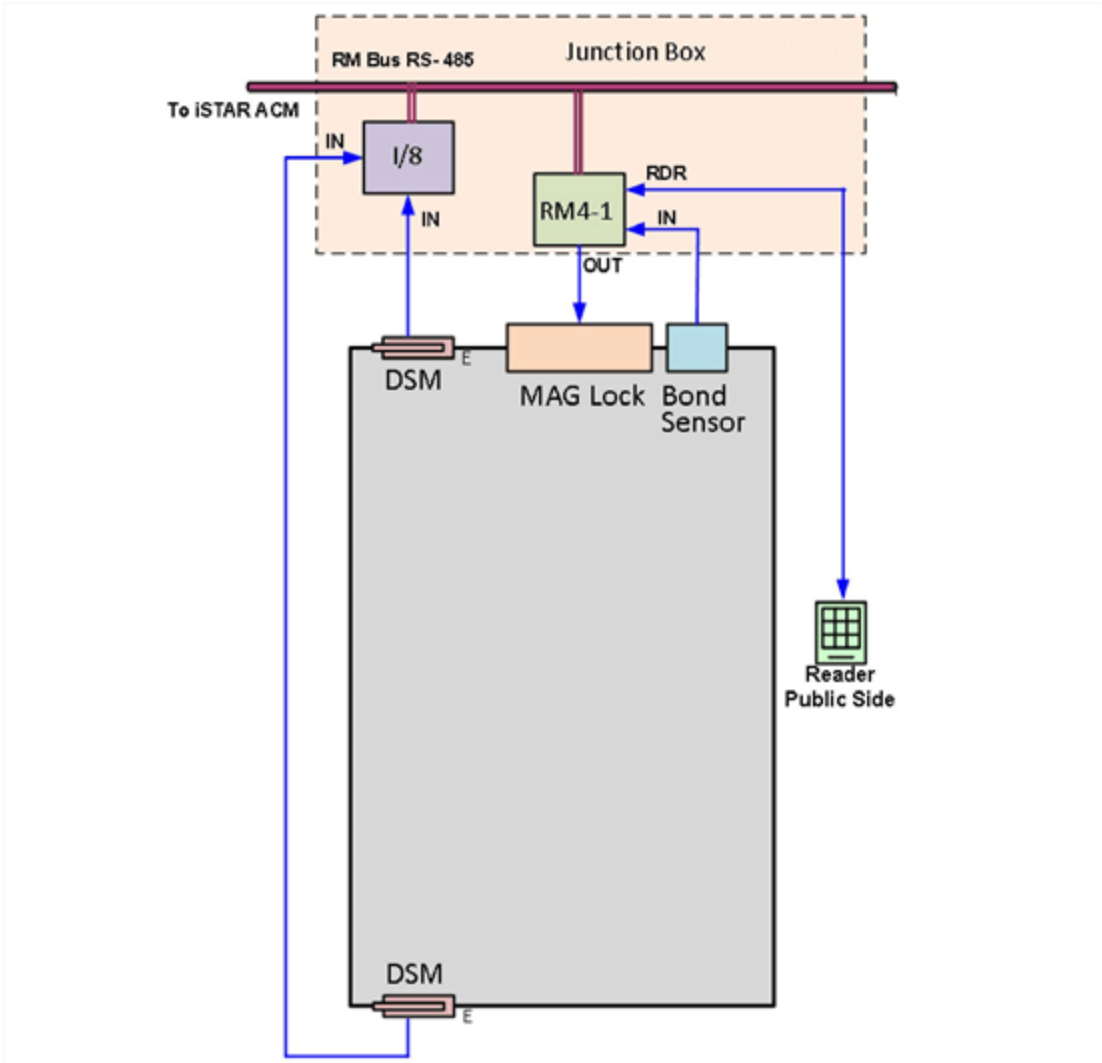
Single-leaf Doors (DSM top and bottom)

Figure 181 on Page 469 shows a single-leaf door with a DSM at the top and bottom. C•CURE 9000 uses the following to determine door state:

- If the door is closed, with both DSMs inactive, and then a DSM activates, the door state is open.
- If the door is open, with both DSMs active, and then a DSM de-activates, the door state is closed.

All DSMs on a single side must activate and deactivate together. If the DSMs do not activate together, C•CURE 9000 issues a DSM Tamper alarm and identifies the DSM that did not change state.

Figure 181: Single-leaf Door with DSM Top and Bottom



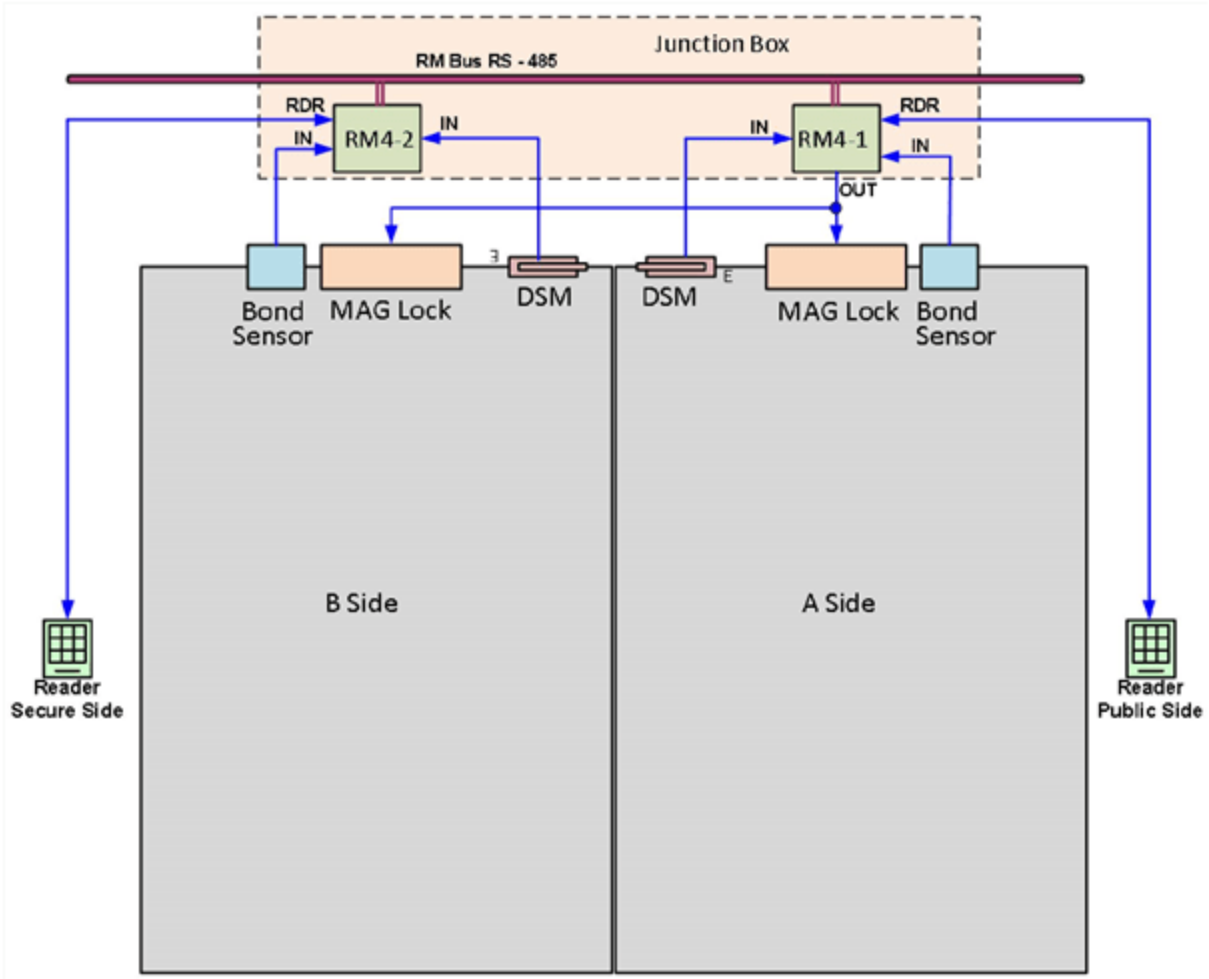
Double- Leaf Doors (DSM each side)

Figure 182 on Page 470 shows a double-leaf door with a DSM on side A and another on side B. C•CURE 9000 uses the following to determine door state:

- If either DSM is active, the door state is open
- If both DSMs are inactive, the door state is closed.

Because double-leaf door configurations with one DSM per side are designed to operate with one leaf open and the other leaf closed, C•CURE 9000 does not issue DSM tamper alarms for this configuration.

Figure 182: Double-leaf Door with DSM on Each Side



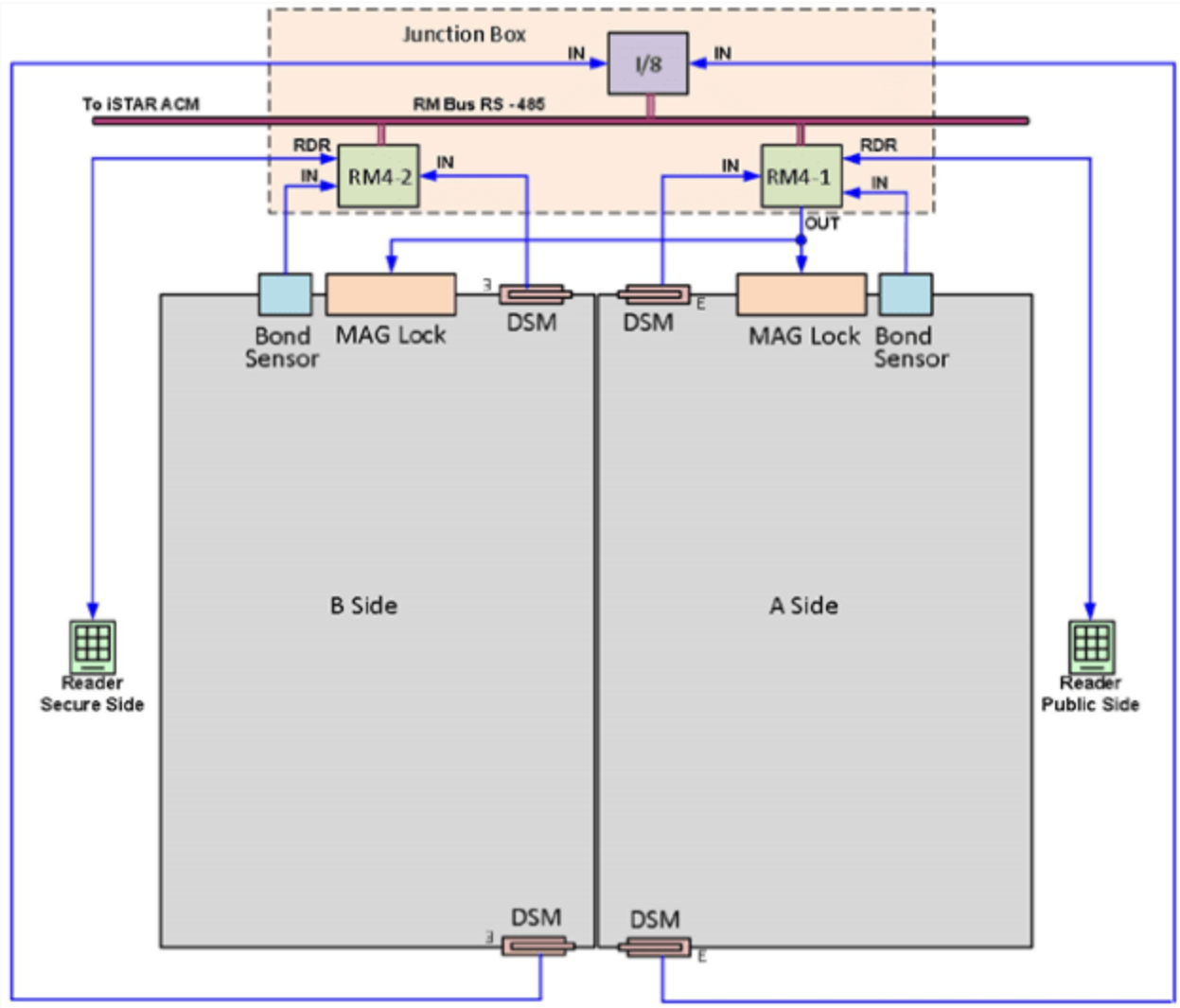
Double-leaf Doors (DSM top and bottom)

Figure 183 on Page 471 shows a double-leaf door with a DSM at the top and bottom of both side A and side B. C•CURE 9000 uses the following to determine door state:

- If the side is closed, and a DSM activates, the side is open
- If the side is open, and a DSM de-activates, the side is closed
- If either side is open, the door is open
- If both sides are closed, the door is closed

All DSMs on a single side must activate and deactivate together. If the DSMs do not activate together, the C•CURE 9000 issues a DSM Tamper alarm and identifies the DSM that did not change state.

Figure 183: Double-leaf Door with DSM Top and Bottom of Each Side



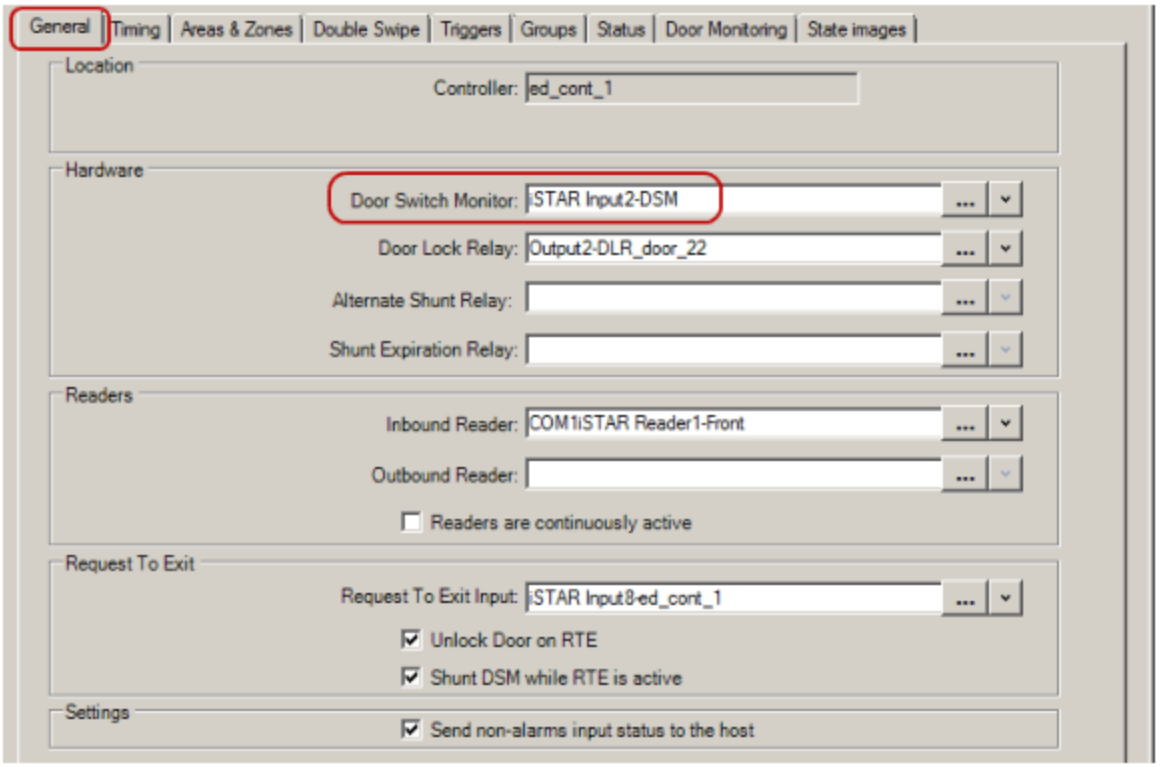
DSM Configuration Guidelines

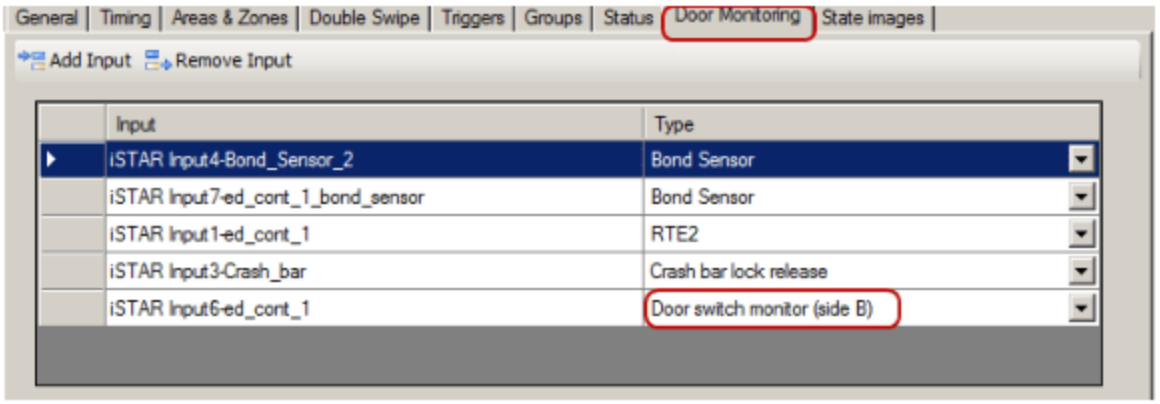
You can configure DSM inputs in the **Door Switch Monitor** field on the **Configure Door** dialog box, or by adding them on the configure **Door Monitoring** dialog box.

If you specify a DSM in the **Door Switch Monitor** field of the **Configure Door** dialog box, C•CURE 9000 uses that input as the DSM for side A of the door. DSM inputs that are added using the configure **Door Monitoring** dialog box can be either A or B side.

Unlike multiple RTEs, you do not have to use the General Tab for DSM 1. Although the examples show two DSMs and two RTEs, it is possible to have more than two of each.

Figure 184: Multiple DSM Configuration





Configuration Overview

Although Advanced Door configuration procedures vary based on site requirements, most configurations involve the tasks and activities described in Table 115.

Table 115: General Configuration Procedure

Task	Configuration Dialog Box	Description	Additional Information
1. Configure Monitoring Inputs, Readers, and Outputs.	**Hardware Pane > Cluster > Controller > Boards > 1st ACM/2nd ACM**	Configure inputs, readers, and outputs on the iSTAR controller using standard procedures and dialog boxes.	See Configuring RM4-1 and RM4-2 Reader, Inputs, and Output on Page 474
2. Configure Lock Releases	**Hardware Pane > Cluster > Controller > Boards > 1st ACM/2nd ACM**	Configure lock release components on the iSTAR controller using standard controller configuration procedures and dialog boxes. Specify how C•CURE 9000 annunciates the lock release inputs.	See Configuring Lock Releases on the I/8 on Page 477 See Annunciating Lock Releases Inputs on Page 477
3. Configure the Advanced Door	**Hardware Pane > Cluster > Controller > Doors > Door Name** **Hardware Pane > Cluster > Controller > Doors > Door Name > Door Monitoring**	Configure the first RTE and the door latch relay using the standard **Door** dialog box (required). You can also use the Door dialog box to configure the DSM for side A. Add additional components using the **Configure Advanced Door Monitoring** dialog box.	See Configuring the Advanced Door on Page 478
4. Configure Grace and Change Time parameters	**Hardware Pane > Cluster > Controller > Doors > Door Name > Door Monitoring**	Specify timing requirements for unlock grace timers. Also specify the change time options for individual door components, and for door shunts.	See Understanding Timing on Page 481

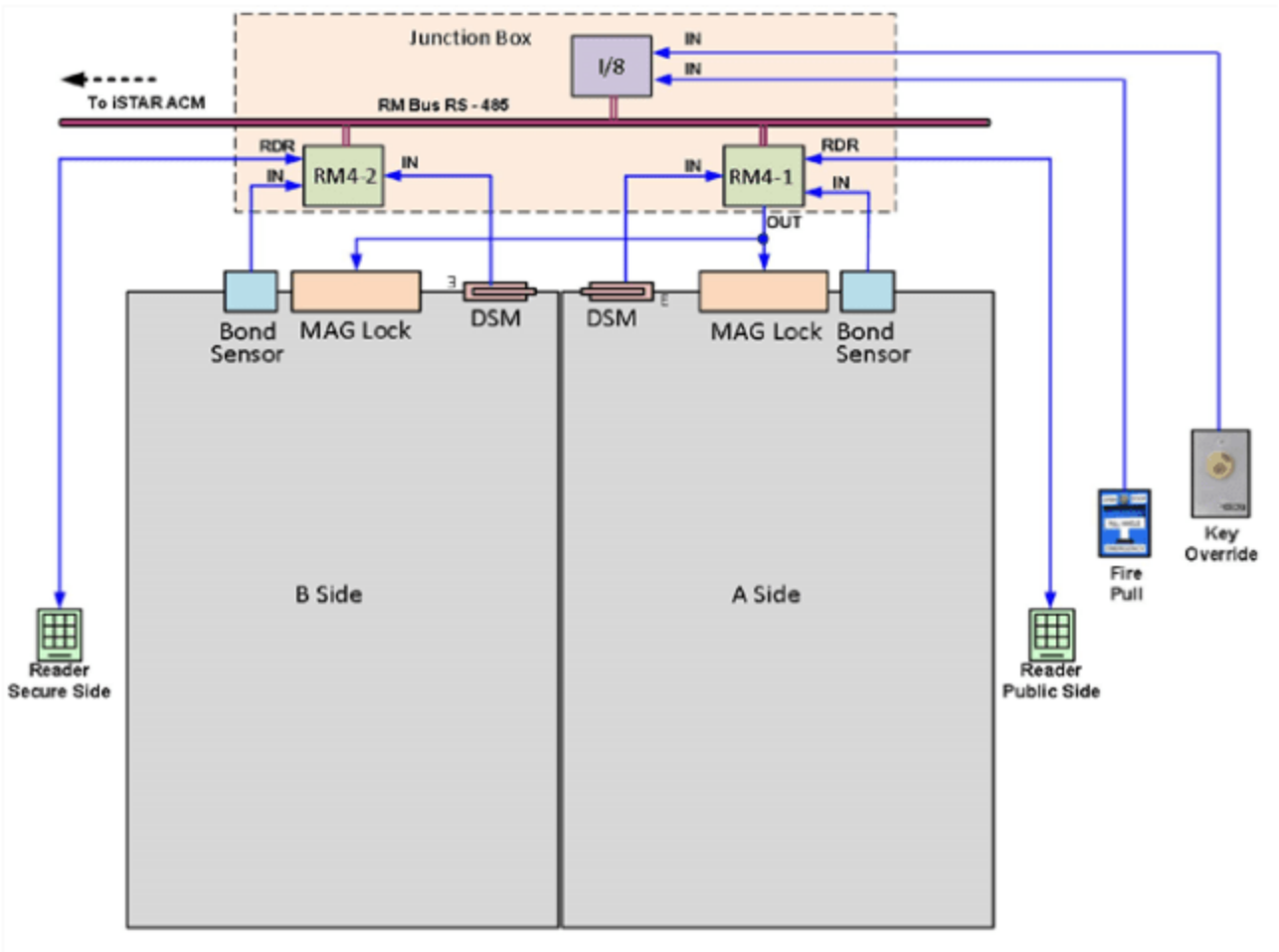
Configuring an Advanced Door

This section provides step-by-step configuration information for a sample Advanced Door configuration.

Sample Door

The configuration for this example, shown in Figure 185 on Page 474, is a double-leaf door with multiple read heads, lock sensors, DSMs, and lock release inputs.

Figure 185: Door Configuration Example



Configuring RM4-1 and RM4-2 Reader, Inputs, and Output

Configuring RM4 inputs for the door in Figure 185 on Page 474 involves using standard controller configuration procedures to configure the monitoring inputs, door latch relays, and read heads for A and B sides of the door. This is detailed in the following procedure.

To Configure RM4 (RS-485) Inputs for the Sample Configuration

1. From the main menu, select **Hardware Pane** > Cluster > **Controller**. From the **iSTAR Controller Selection** browser, select the name of the iSTAR that includes Advanced Door components, and select **Edit**.
2. Select the tab that includes the inputs to be configured. This will vary, depending on the iSTAR model. In some cases you will have to first select the ACMn board and a Port.

   The RM Readers are configured under the following Tabs:

   - iSTAR Ultra - Boards > ACM 1 or 2> RS-485 Port> Reader Port > Readers
   - iSTAR Pro - Boards > ACM 1 or 2> Readers
   - iSTAR Edge - COM1 or COM2 or COM3 > Readers
   - iSTAR eX - COM1 or COM2 > Readers

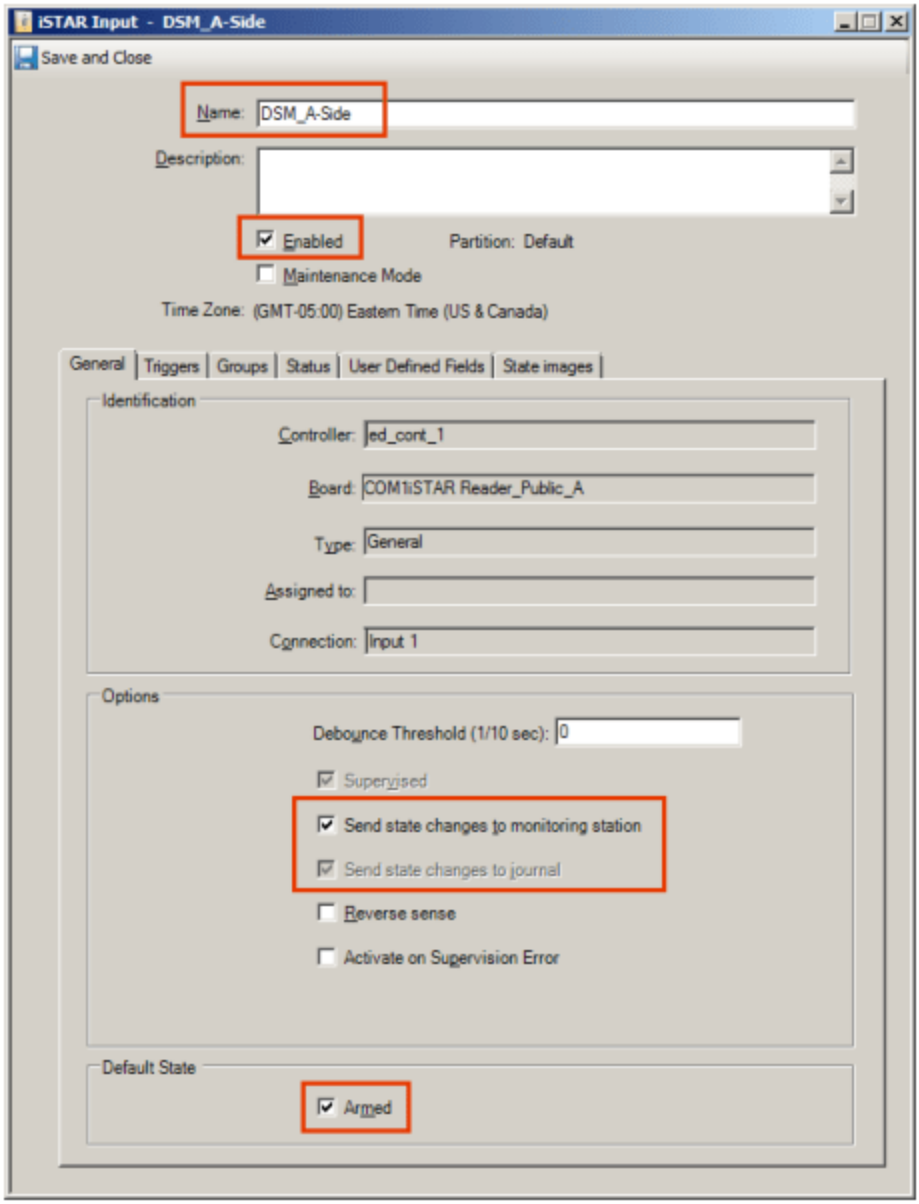
   To configure the inputs for side A in Figure 185 on Page 474 (on RM 1), create an RM Reader.

NOTE Software House recommends that the **Communication failure** option be configured for all security devices that connect to the iSTAR. Select the I/O Tab from the Reader Editor, to configure this option.

3. In the General tab of the **Reader** Editor enter the following:
   - **Name** - the name of the reader
   - **Enabled** - activated
4. Go to the I/O Tab
5. In the **Inputs** box, select an input and configure it. Enter at least the following:
   - **Name** - the name of the input
   - **Enabled** - check box checked
   - **Send State changes to Monitoring Station** (and Journal)
   - **Armed** - check box checked. It's good practice to Arm Inputs, but if the Input is a door component, it will be automatically armed.

   To configure the inputs for the example in Figure 185 on Page 474, enter information for DSM side A and the Magnetic Bond Sensor.

Figure 186: iSTAR Input DSM side A



6. Click **OK** and **Close**.
7. Repeat step 5 to configure the Bond Sensor Input.

NOTE

For consistency, Advanced Doors that include more than one instance of the same input (two DSMs, for example) should use a naming convention that indicates the area of the door that the device monitors.

Example:

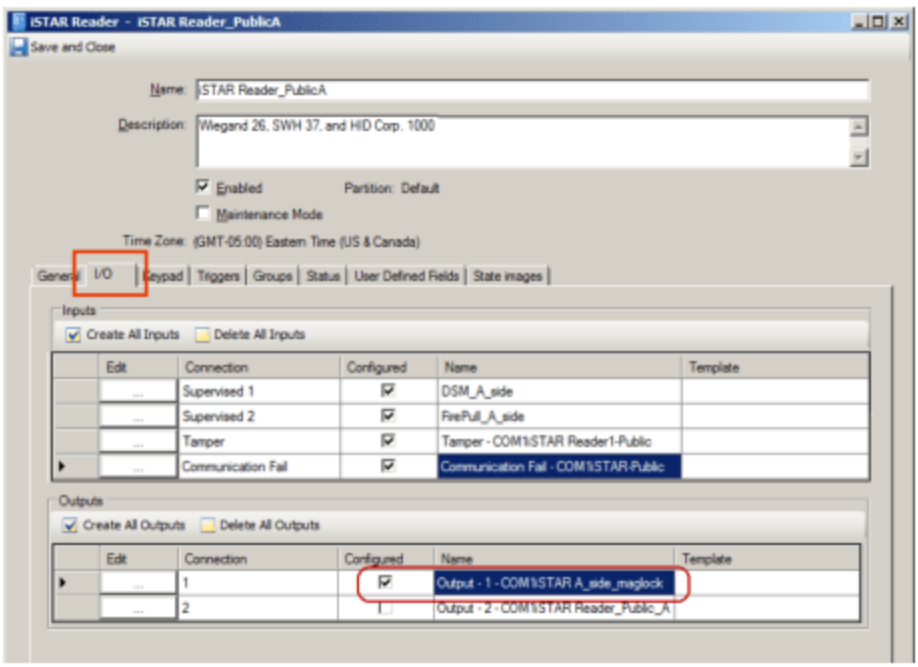
DSM-Lobby-sideA.

8. In the **Outputs** box, select an output and configure it. Enter at least the following:
   - **Name** - the name of the output

- **Enabled** - check box checked
- **Normally energized** - activated or de-activated, depending on site requirements. Magnetic Locks are usually Normally Energized.

To configure the outputs for the example in Figure 185 on Page 474, enter information for the magnetic lock output.

Figure 187: Reader I/O Tab



9. Click **Save and Close** until you return to the Controller editor.
10. Repeat steps 1 through 7 to configure the RM4-2 for the B side of the door.

Configuring Lock Releases on the I/8

Configuring lock releases for the door in Figure 185 on Page 474 involves using standard controller configuration procedures.

You must also specify how C•CURE 9000 annunciates the lock release inputs. For configuration guidelines, see the next section.

Annunciating Lock Releases Inputs

If the lock release input is configured to annunciate, C•CURE 9000 reports input activation and de-activation. Annunciation of inputs has no impact on door actions or lock release operations.

To reduce message traffic, most configurations will choose to annunciate lock release inputs to test or troubleshoot the system, but will not annunciate them for normal door operations.

To Configure Lock Releases for the Sample Configuration

1. From the main menu, select **Hardware>Cluster>Controller**. Right-click the iSTAR that includes lock release components and then **Edit** from the context menu.
2. Select the tab that includes the I/8 to be configured. This will vary, depending on the iSTAR model. In some cases you will have to first select the ACM board and a Port.

   The I/8 boards are configured under the following Tabs:

   - **iSTAR Ultra** - Boards > ACM 1 or 2> RS-485 Port> ACM Ext > I/8 >Input
   - **iSTAR Pro** - Boards > ACM 1 or 2> ACM Ext > I/8 >Input
   - **iSTAR Edge** - COM1 or COM2 or COM3 > I/8 >Input
   - **iSTAR eX** - COM1 or COM2 > I/8 >Input
3. On the I/8 Editor, select an input and click **Edit**.
4. On the Input Editor, enter at least the following:
   - **Name** - the name of the input
   - **Enabled** - check box checked
   - **Armed** - check box checked
   - **Send state changes to monitoring station** - activated (includes sending to the journal) or deactivated, according to the site requirements
   - **Send state changes to journal** - Read only. Will be activated if Send state changes to Monitoring station is true.
5. Click **Save and Close**. Repeat steps 3 to 5 to configure additional inputs.

Figure 188: I/8 Inputs for Sample Door

6. Click **Save and Close** until you return to the main menu.

Configuring the Advanced Door

Configuring the Advanced Door involves adding door components using both the standard Door editor and the Door Monitoring Tab editor.

To Configure the Advanced Door in the Sample Configuration:

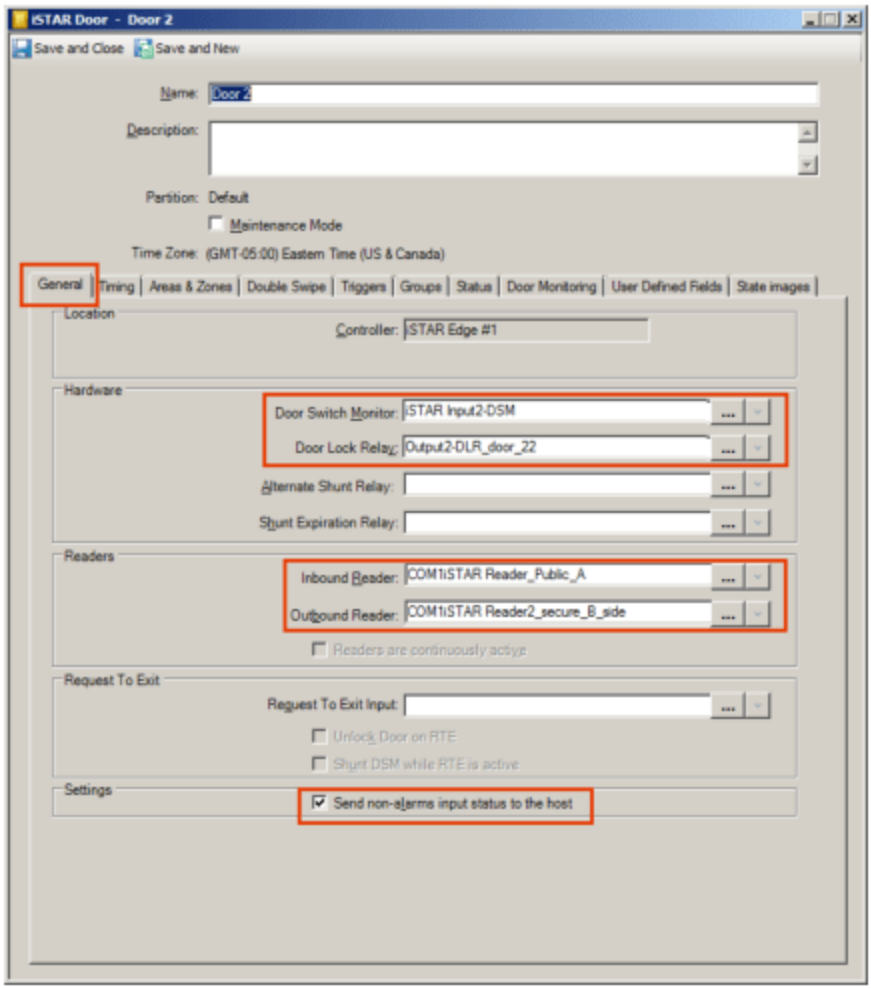
1. From the **Hardware Pane**, right click on iSTAR to **Configure>Door** and select **New**. Or select an existing door in the controller to edit.
2. On the **iSTAR Door** Editor, click the **General Tab** and enter at least the following:
   - **Door has RTE** - the name of RTE input (if required by the door)
   - **Door switch monitor** - the name of the side A DSM input
   - **Door latch relay** - the name of the door latch relay output

- Optional - Send non-alarm input status to the host. Similar to input annunciation, this will increase traffic but it is a good mode to understand Advanced Doors.

3. Enter the Readers for the Inbound and Outbound reader fields.
4. Click **Save and Close** until you return to the main menu.

To configure the door in Figure 189 on Page 479, enter the name of the side A DSM and the door latch relay. The sample door uses a read head instead of an RTE. However, doors that use one or more RTE devices must configure the first RTE on the Door Editor.

Figure 189: Sample Door



5. Select the **Door Monitoring** tab.
6. To add door components:

   a. Select **Add Input** and pick the appropriate input to add to the Input list.

7. To specify component type:

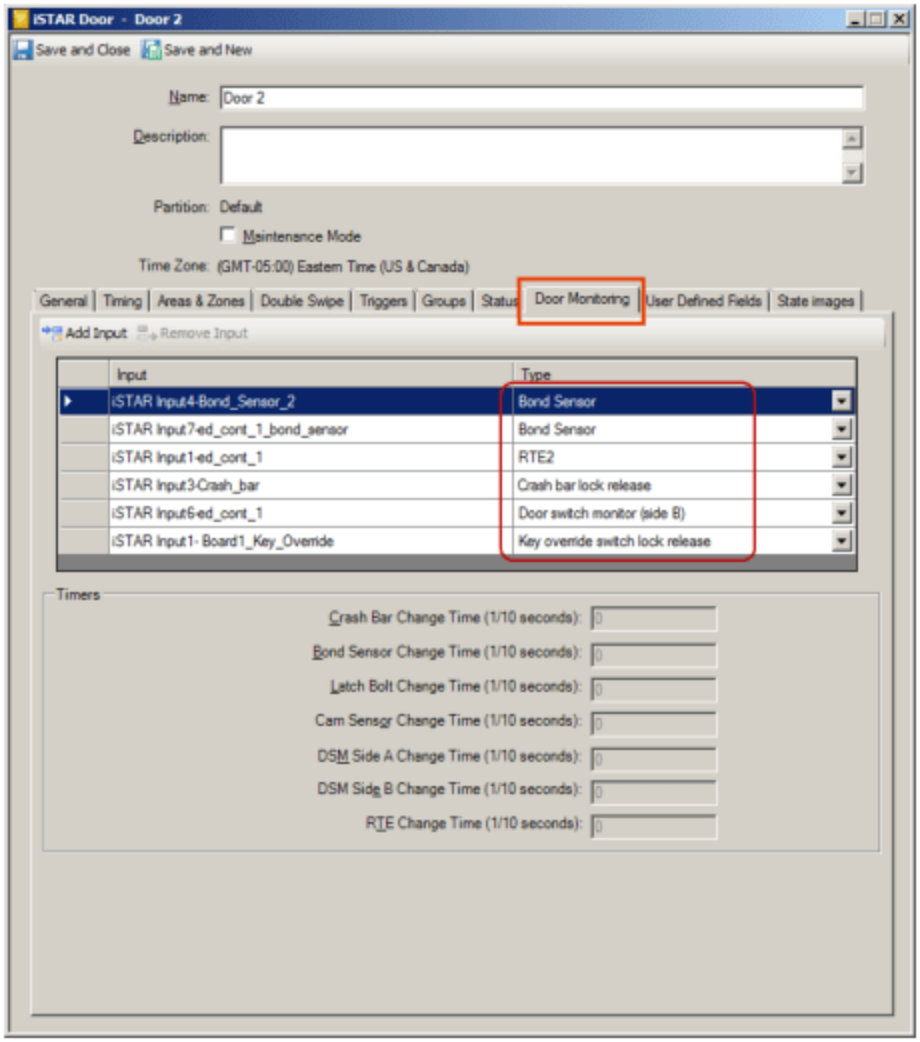
   a. In the **Input** list box, select an input.

   b. Click on the **Type field** and use the drop-down list to select the component's type.

To configure components and types in Figure 190 on Page 480, add inputs for the key override, fire pull, A and B side bond sensors, and B side DSM. Specify the component type for each of the corresponding inputs. **This field is required**.

8. Click **Save and Close**.

Figure 190: Door Monitoring



Understanding Timing

Time Delays

Use timing options to prevent false alerts caused by nearly simultaneous inputs to C•CURE 9000, and also to fine tune timing to meet specialized door and site requirements.

In addition to the normal door de-bounce and grace times, on the Timing Tab, there are seven other timing tweaks that are used to avoid race conditions. The Timers default to zero but it is good practice to set them all at 0.2 or 0.3, and then adjust, as necessary. See Figure 191 on Page 481.

Since input changes cannot occur simultaneously, and if almost simultaneous may be read by our hardware in any order, some input change time values are provided. This change time will be used whenever one of the inputs changes, to allow the system to wait and see if any of the normally accompanying inputs is also going to change.

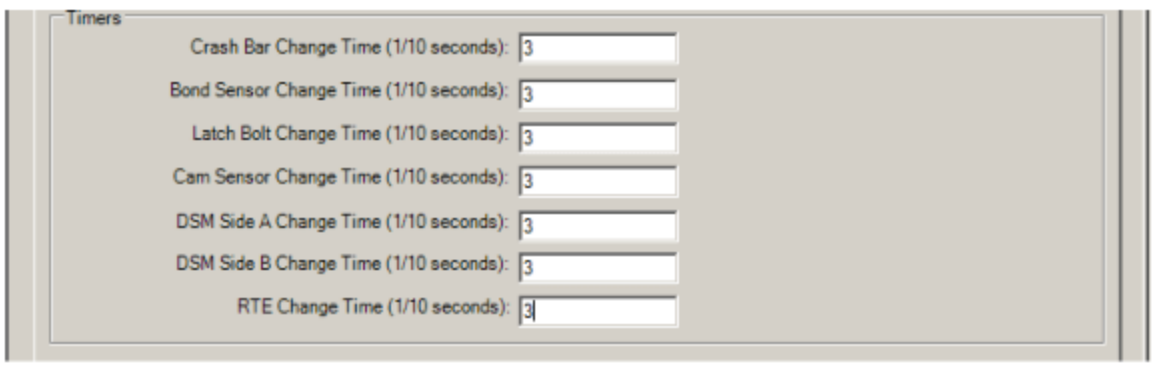
For example, every time the door is open (meaning the DSM input is active), the latch bolt or bond sensor input should also be active. Therefore, every time the door opens, if the input is not already active, a timer will be started with the value of the lock sensor change value. If the timer times out without the lock sensor input activating, then a Lock Tamper alarm will be reported. Then when the door closes and locks, this time value will be the time we allow the lock sensor input to change from active to secure before reporting Lock Unsecured.

Use the **Timers** box on the **Configure Advanced Door Monitoring** dialog box to fine tune timing delays for Advanced Door components.

To Display the Configure Advanced Door Monitoring Dialog Box

- Select **Door>Door Monitoring** tab.

Figure 191: Timers



Kinds of Timing Options

C•CURE 9000 includes timing options that provide:

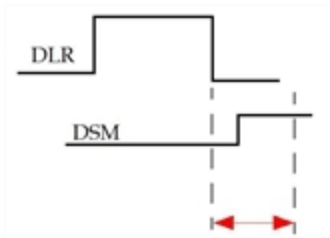
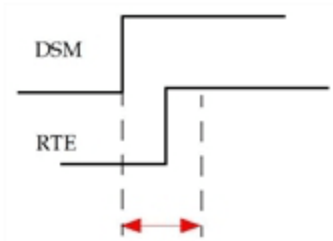
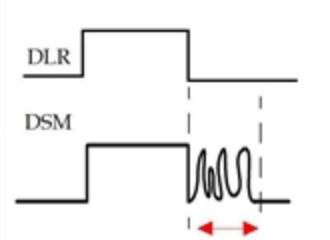
- **Grace times** - a wait period that prevents false alerts caused by door open, door unlock, and door bouncing inputs.
- **Change times** - a wait period that defines the amount of time allowed for changes in input states. Change times are used with timing values from other door inputs to define how long C•CURE 9000 waits before issuing lock tamper or lock unsecure alarms.

- **Shunt /Delay Relock times** - a wait period that defines the number of seconds the door can remain open before relock or before an alert is sounded.

Grace Time Options

Table 116 on Page 482 describes grace time options.

Table 116: Grace Timing Options

Option	Description	Example
Unlock Grace Time 	Specifies the time that C•CURE 9000 waits for a door open signal after the door unlock timer has expired. Prevents a false "door forced" message in situations where the signals are nearly simultaneous.	Personnel who are granted card access delay opening a door until unlock time is nearly expired, thereby causing nearly simultaneous DSM and unlock timer expiration inputs to C•CURE 9000. If configured, C•CURE 9000 waits the number of seconds you specify for a door open input, thereby preventing a false "door forced open" message.
Door Open Grace Time 	Specifies the time that C•CURE 9000 waits for an RTE, card admit, or momentary unlock signal after receiving the signal from the DSM. Prevents a false "door forced open" message in situations where signals are nearly simultaneous. For additional information, see Special Timing Considerations on Page 484.	Personnel lean on a door release mechanism while pressing the RTE switch, causing nearly simultaneous door open and RTE inputs to C•CURE 9000. If configured, C•CURE 9000 waits the number of seconds you specify for the RTE, card admit, or momentary unlock signal, thereby preventing a false "door forced open" message.
Door Close De-bounce Time 	Specifies the time that C•CURE 9000 ignores DSM inputs, to allow for bouncing doors.	Unintended door movement (bouncing) can activate a DSM input to C•CURE 9000 and cause false "door forced open" messages. If configured, the Door close de-bounce time option ignores DSM inputs for the time specified after the door closes to allow for bouncing doors.

Change Time Options

C•CURE 9000 determines change time based on the door components you have configured (DSM, RTE, lock releases, for example) and the door operation (card access, RTE access, door forced, for example).

NOTE

Change time is specified in units of 1/10 second. Enter 1 to specify 1/10 second, 5 to specify 5/10 (1/2) second and so forth.

Software House recommends that you set all change times to at least 5/10 second and make adjustments only as necessary.

Table 117 on Page 483 describes how change time options work for lock releases, lock sensors, and DSM and RTE devices.

Table 117: Change Timing Options

Option	Function	Associated Inputs	Activation Criteria
Crash bar change time	Specifies the amount of time C•CURE 9000 allows, after a crash bar state change, for a lock sensor change	C•CURE 9000 uses the crash bar change time to determine changes to corresponding: • Bond sensors • Latch bolts • Cam sensors	Activated by the bond sensor, latch bolt, or cam sensor.
Bond sensor change time	Specifies the amount of time C•CURE 9000 allows for a bond sensor state change. C•CURE 9000 uses this time, and the time of the other door inputs, to determine the wait before issuing a "lock tamper" or "lock unsecure" alarm.	C•CURE 9000 uses the greatest value of the following: • Door open grace time • Door close de-bounce time • Crash bar change time • Bond sensor change time • RTE change time	The bond sensor should be active if: • Door is open • Door latch relay is active • Lock release input(s) are active The bond sensor should be inactive when: • Latch relay is inactive, the door is closed, and the lock release inputs are inactive
Latch bolt change time	Specifies the amount of time C•CURE 9000 allows for a latch bolt state change. C•CURE 9000 uses this time, along with the time of the other door inputs, to determine the wait before issuing a "lock tamper" or "lock unsecure" alarm.	C•CURE 9000 uses the greatest value of the following: • Door open grace time • Door close de-bounce time • Crash bar change time • Latch bolt change time • RTE change time	The latch bolt should be active if the door is open. The latch bolt should be inactive if: • Door is closed • Door latch relay is inactive • Lock release inputs are inactive The latch bolt can be active or inactive if: • Door latch relay is active • Lock release input(s) are active
Cam sensor change time	Specifies the amount of time C•CURE 9000 allows for a cam sensor state change. C•CURE 9000 uses this time, along with the time of the other door inputs, to determine the wait before issuing a "lock tamper" or "lock unsecured" alarm.	C•CURE 9000 uses the greatest value of the following: • Crash bar change time • Cam sensor change time • RTE change time	The cam sensor should be active if: • Door latch relay is active • Lock release input(s) are active The cam sensor should be inactive if the door latch relay is inactive and all lock releases are inactive

Table 117: Change Timing Options (continued)

Option	Function	Associated Inputs	Activation Criteria
DSM side A change time - or - DSM side B change time	Specifies the amount of time C•CURE 9000 allows for a DSM state change. C•CURE 9000 uses this value to determine the wait period before activating a DSM tamper for multiple DSM devices on one side of the door.	Additional DSM inputs on the same door side	DSM change time is active when the first DSM in a group changes state. (DSMs must be located on the same side of the door).
RTE change time	Specifies the amount of time C•CURE 9000 allows, before or after an RTE state change, for a lock sensor change. For additional information, see See "Special Timing Considerations" on page 484	C•CURE 9000 uses the RTE change time to determine changes to corresponding: • Bond sensors • Latch bolts • Cam sensors	Activated by the bond sensor, latch bolt, or cam sensor.

Shunt Time Options

Table 118 on Page 484 describes options that control shunt time.

Table 118: Shunt Time Options

Option	Description
Delay relock while door open after valid access	If access is valid, delays the relock of the door until the door closes. This differs from standard relock operations where relock occurs when the: • Door opens. • Door opens and the relock delay expires. If the door is open, the lock is energized. C•CURE 9000 sends an alarm when the shunt time expires.
Shunt door for full shunt time	Activates the shunt for the full time specified. If selected with **Delay relock while door open after valid access**, the lock is energized and the door unlocked for the full shunt time, regardless of whether the door is open or closed.

Special Timing Considerations

Sites that use an RTE motion detector angled over a door can cause C•CURE 9000 to report a valid RTE that is caused by door motion, instead of a forced open alarm. This situation occurs because of a race condition in which the RTE caused by forced motion on the door reports to C•CURE 9000 before the DSM, thereby causing C•CURE 9000 to execute a valid exit instead of a door forced alarm.

You can correct the situation by:

- **Repositioning door hardware** – adjust the position of any RTE motion detectors angled over doors. You should also replace any slow DSM components that may be contributing to the problem.

- **Adjusting the timing of door components** – use the **RTE change time** option to specify timing for incoming traffic and also to change the function of the **Door open grace time** option.

The **RTE change time** option specifies the amount of time that C•CURE 9000 ignores RTE inputs after the door is closed. Use this value to prevent false door forced reports caused by door components (slow bolts or sensors, bouncing door, for example) for outgoing traffic.

The **RTE change time** option also changes the function of the **Door open grace time** option. If you specify a value for **RTE change time**, the **Door open grace time** option now specifies the time C•CURE 9000 ignores RTE changes before the door open occurs. This prevents RTE signals from the motion detector that are caused by door mechanics rather than human access. If C•CURE 9000 sees an RTE on a closed door, and then sees the door open within the period you specify, it cancels the RTE and issues a door forced alarm.

Monitoring Door Activity

You can monitor Advanced Door activities using:

- Door, alarm, and show cause features on the **Monitoring Station**
- Journal reports from the **Administration application**

Using Monitoring Station Commands

To Display Information about Alarms, Alarm Causes, and Door Component Status

1. Select **Doors** from the **Non-Hardware Pane** on the Monitoring Station Explorer Bar.
2. Right click on a Door and select Door Monitoring.
3. Use Door Monitoring to Show Locked Causes and various Alarm States.
4. Door Monitor Inputs are also shown at the top of the Door Monitoring Editor. Right click on an input for further context menu options.

Using Journal Reports

To Display Journal Messages about Advanced Doors

1. From the Administration application, select Options & Tools.
2. Select Journal
3. Enter a range for Start date/time and End date/time.
4. Use the Journal Query Assistant to select:
   - Object Changed State Message Type
   - iSTAR Doors Object Type
   - Door Name(s)
   - You can also use Journal Triggers to get detailed information.

Understanding Door Alarms

Alarms

This section describes how C•CURE 9000 manages alarm traffic and contradictory component reports that can sometimes accompany Advanced Door configurations.

Door Open Alarm - this alarm occurs whenever the door opens without benefit of card or request to exit access, and one of the lock release devices is active. This alarm indicates that some kind of emergency unlock is occurring. The alarm message includes the name of the lock release device as the reason for the door open alarm. In the case that none of the lock release devices is active, this is a normal door forced open alarm.

Lock Unsecured Alarm - this alarm occurs whenever a lock sensor is active when it should be inactive. This indicates that the lock hardware failed to return to locked position after being unlocked by one of the lock release devices or by regular door control. The alarm message includes the name of the lock sensor input that caused the alarm.

Lock Tamper Alarm - this alarm occurs whenever one of the lock sensors is inactive when it should be active. This is whenever one of the lock release devices is active or the door latch relay has been activated by the door or the DSM indicates that the door is open. This may indicate that someone is tampering with the lock sensor while the door is opening or that the lock hardware has failed. The alarm message includes the name of the lock sensor input that caused the alarm.

DSM Tamper Alarm - this alarm is reported if multiple DSM inputs monitor the same door and one of them does not become active when it should. The alarm message includes the name of the input that is not active.

New Activity / Journal Reports

New door activity reports will be added:

- **Lock Tamper Alarm** (reported with input name indicating which input caused the lock tamper alarm condition)
- **Lock Unsecured Alarm** (reported with input name indicating which input caused the lock unsecured alarm condition)
- **Door Open Alarm** (reported with input name indicating which input caused the door open alarm condition)
- **DSM Tamper Alarm** (reported with input name indicating which input caused the DSM tamper alarm condition)

Managing Message Traffic

To reduce the redundant door open, lock tamper, DSM tamper, and lock unsecured alarms generated by multiple inputs on Advanced Doors, C•CURE 9000 reports Monitoring Station and journal activity **only** when the alarm changes from an inactive to an active state. Additional inputs to the same alarm are **not** reported. C•CURE 9000 also clears the alarm only when all inputs deactivate.

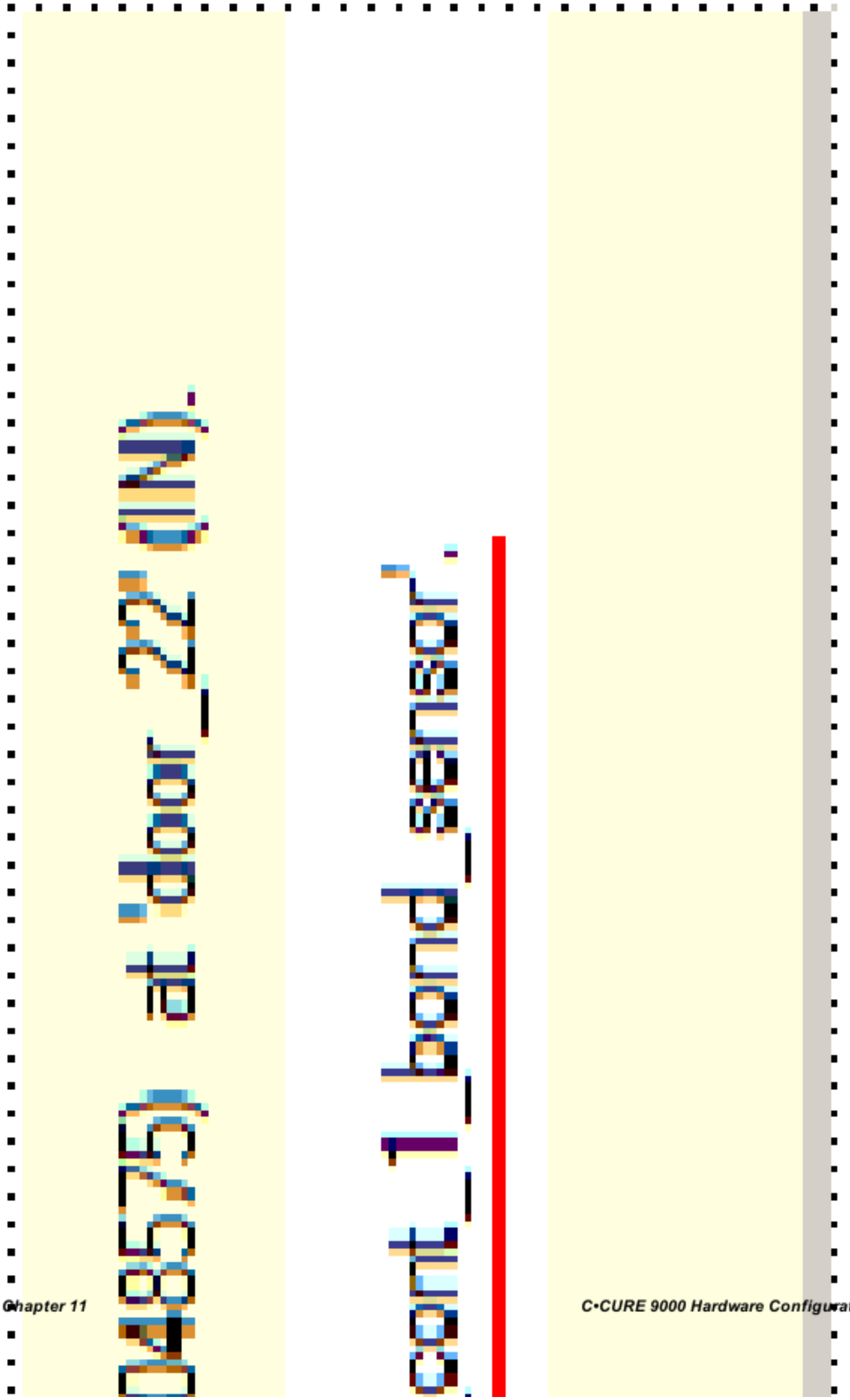
The example in Figure 192 on Page 489 shows the General Activity Monitor for a simplified door that includes two bond sensor inputs and a DSM. The following actions occurred:

1. Door closed (no inputs inactive).
2. Card admitted, door open (DSM activates, bond sensor 1 activates as expected, bond sensor 2 does not activate).

3. Door Lock unsecured reported (bond sensor 1).
4. Bond sensor 1 deactivates while the door is open, causing a second input to the lock tamper alarm.

   C•CURE 9000 does not display an additional alarm report for bond sensor 2 on the General Activity window.
5. Door closed (DSM deactivates).

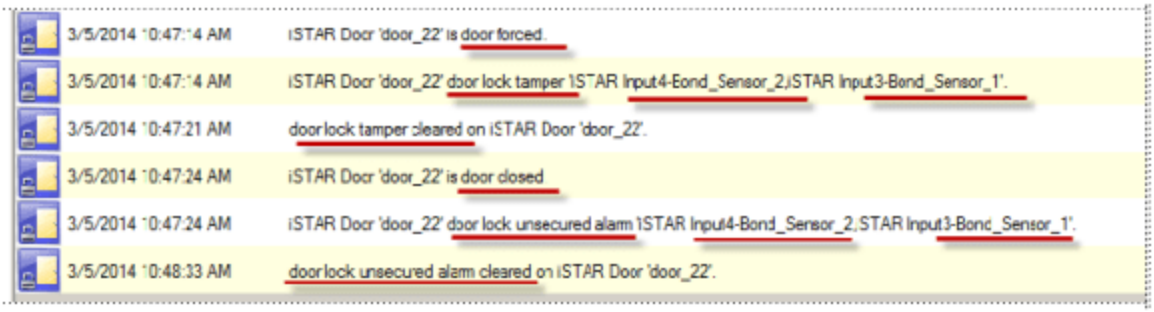
Figure 192: General Activity Alarm Reports Example



EFTA01226421

Figure 193 on Page 491 shows the Monitoring Status for the example door activities. C•CURE 9000 reports the first lock tamper (bond sensor 2) and does not clear the alarm. The second lock tamper (bond sensor 1) on the same door does not display on the General Activity Monitor.

Figure 193: General Activity Alarms Reports Example



Clearing Alarms

Advanced Door alarms may occasionally appear "stuck" because C•CURE 9000 waits for the input to change state before clearing the alarm. This is to reduce unnecessary alarm traffic. If all inputs are functioning properly, you can clear all door and input alarms by performing a normal door access cycle (opening and closing the door).

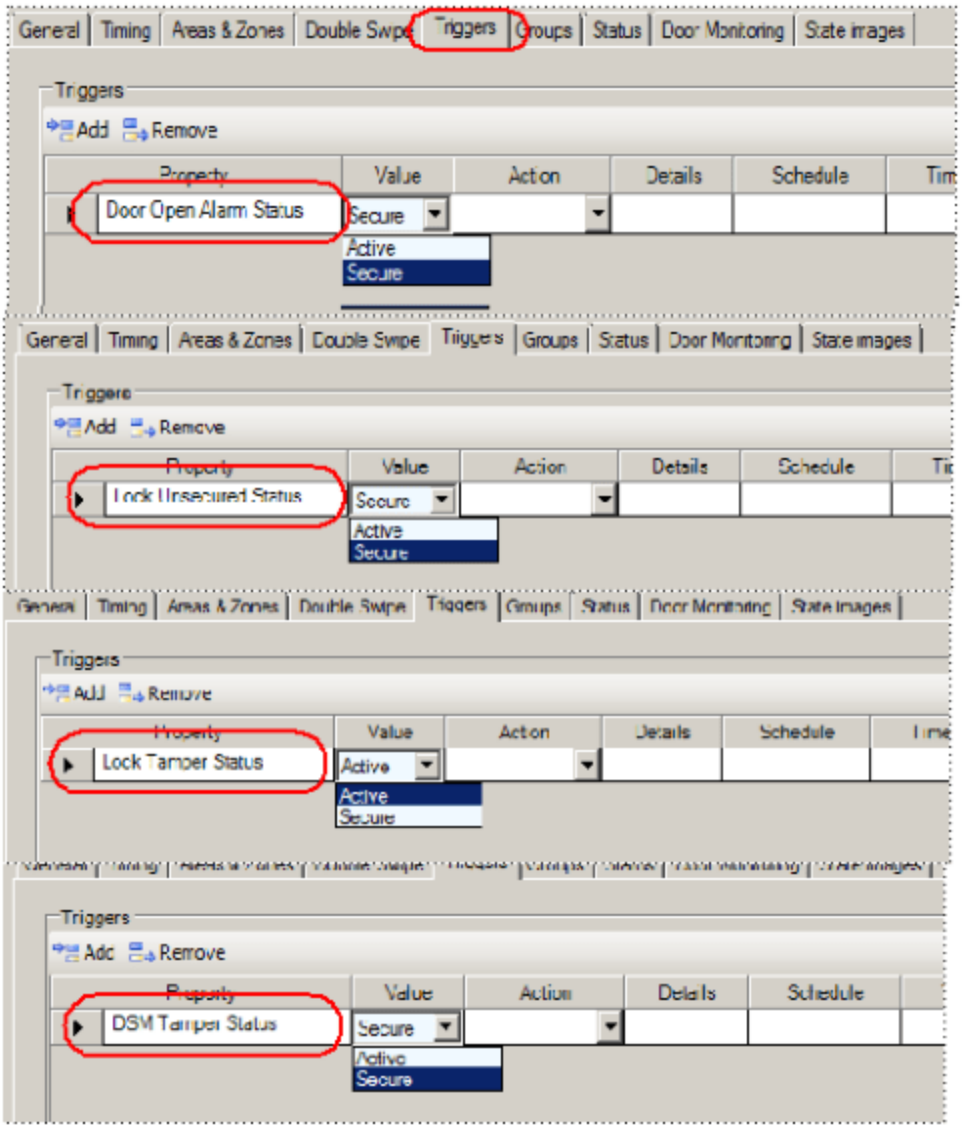
Door Triggers

In addition to the usual five Door Triggers:

- **Admit Status** - Admit, Reject, Noticed Admit, Noticed Reject, Duress
- **Double Swipe Status** - Locked, Unlocked
- **Mode Status** - Unlocked, Locked, No Access
- **Open Status** - Open, Closed
- **Alarm State Status** - Normal, Forced, Held Open

There are four additional Advanced Door Triggers shown in Figure 194 on Page 492.

Figure 194: Advanced Door Triggers



Privilege Modifications

iSTAR Door Permission list

- Enable Door forced alarms
- Disable Door forced alarms
- Enable Door held alarms
- Disable Door held alarms
- Enable RTE functions
- Disable RTE functions

- Enable Lock Tamper alarms
- Disable Lock Tamper alarms
- Enable Lock Unsecured alarms
- Disable Lock Unsecured alarms
- Enable Door Open Tamper alarms
- Disable Door Open Tamper alarms
- Enable DSM Tamper alarms
- Disable DSM Tamper alarms
- Door Monitoring Details

Reports

A standard iSTAR Door Report can be used to list all of the Advanced Door components.

Figure 195: iSTAR Door Report

C-CURE 9000 report_door_mon

ISTAR DOOR

Advanced Door Monitoring Inputs

Input Name	Link Type
iSTAR Input4-iSTAR Ultra ACM1-gcm_new_cont_10009c	Bond Sensor
iSTAR Input5-iSTAR Ultra ACM1-gcm_new_cont_10009c	Bond Sensor
iSTAR Input1-iSTAR Ultra ACM1-gcm_new_cont_10009c	Latch bolt detector

Advanced Door Monitoring Inputs

Input Name	Link Type
iSTAR Input8-iSTAR Ultra ACM1-gcm_new_cont_10009c	Cam detection
iSTAR Input9-iSTAR Ultra ACM1-gcm_new_cont_10009c	RTE2
iSTAR Input18-iSTAR Ultra ACM1-gcm_new_cont_10009c	General lock release
iSTAR Input17-iSTAR Ultra ACM1-gcm_new_cont_10009c	Fire alarm lock release

Advanced Door Monitoring Inputs

Input Name	Link Type
iSTAR Input3-Crash_bar	Crash bar lock release
iSTAR Input4-Bond_Sensor_2	Bond Sensor
iSTAR Input7-ed_cont_1	Bond Sensor

Advanced Door Monitoring Details

If you have Advanced Door Monitoring, additional selections are displayed on the Door context menu from a Dynamic View or a Monitoring Station Status List of Doors.

Each of these selections let you initiate a Manual Action to enable or disable the selected function.

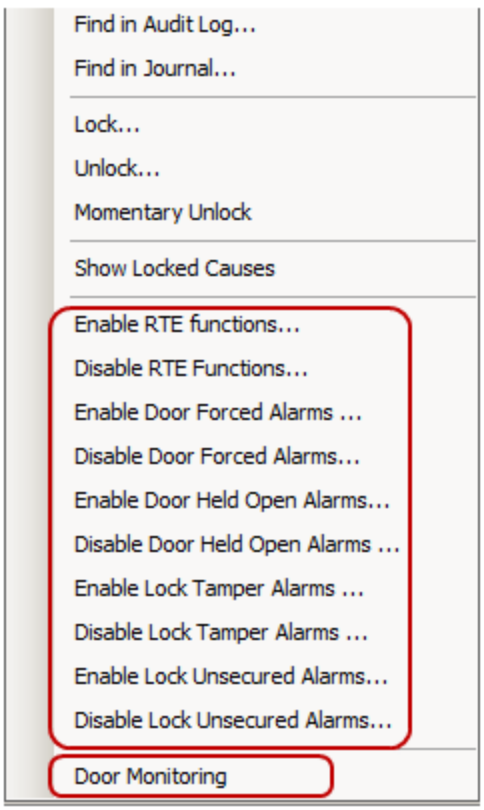
See Viewing a List of Doors on Page 408 for more information about the context menu for Doors.

Advanced Door Monitoring has 7 Cause List type states, and 14 possible manual actions that may be associated with these:

- RTE enable/disable,
- door forced alarm enable/disable,
- door held open alarm enable/disable,
- door open alarm enable/disable,
- lock tamper alarm enable/disable,
- lock unsecured alarm enable/disable,
- DSM tamper alarm enable/disable.

Enter the **Door Monitoring** Status screen for iSTAR doors by right clicking on the Door and selecting Door Monitoring from the context menu. You can also execute the Manual Actions listed above, from this context menu.

Figure 196: Door Context Menu



See Door Monitoring Screen on Page 496 for more information about the **Door Monitoring** screen.

Door Monitoring Screen

The Door Monitoring screen shows all inputs monitored by a door, their state, and any door alarm condition derived from them as well as the Cause Lists.

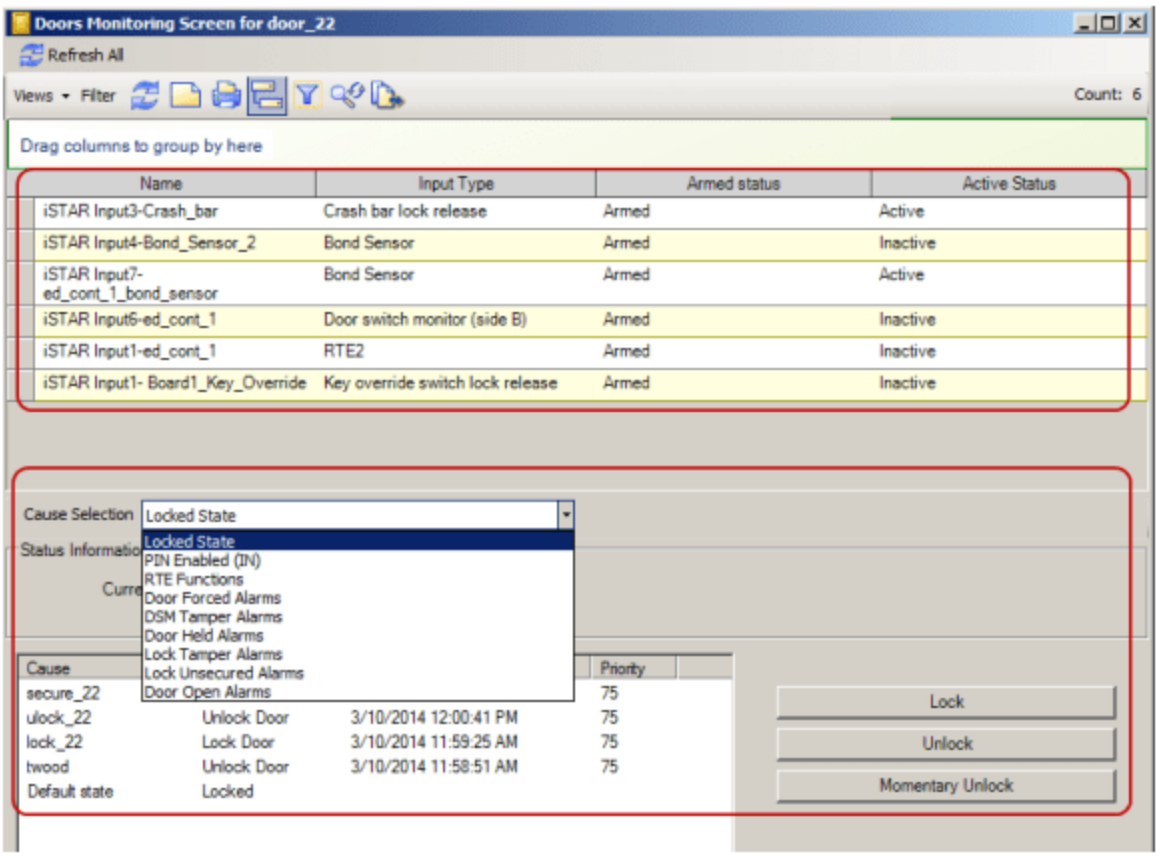
The upper dynamic view displays Door Monitoring Inputs status. The bottom part displays cause lists and all 'cause list' standard functionality is available (right mouse click on selected row will activate "Details/Cancel" context menu).

Figure 197 on Page 496 shows an example of the Door Monitoring Screen.

Table 119 on Page 497 provides definitions for the fields and selections on the screen.

Also see Table 114 on Page 465 for an explanation of the Alarms.

Figure 197: Door Monitoring Screen



The availability of manual actions depends on input assignments. The rules to show/hide manual action on the Door Monitoring Screen and show/hide executors on iSTAR Door Dynamic Views are:

- If there is an RTE input then show Enable/Disable RTE;
- If there is a DSM input then show Enable/Disable Door Forced Alarms, Enable/Disable Door Held alarms, if there is also any DSM side A inputs, then Enable/Disable DSM Tamper
- If there is a Bond Sensor input then show Enable/Disable Lock Tamper alarms, Enable/Disable Lock unsecured alarms;

- If there is a Latch Bolt Detector input then show Enable/Disable Lock Tamper alarms, Enable/Disable Lock unsecured alarms;
- If there is a CAM detection input then show Enable/Disable Lock Tamper alarms, Enable/Disable Lock unsecured alarms;
- If there is a DSM Side A input then show Enable/Disable Door Forced Alarms, Enable/Disable Door Held alarms, if there is also a main DSM, or another DSM side A, then Enable/Disable DSM Tamper;
- If there is a DSM Side B input then show Enable/Disable Door Forced Alarms, Enable/Disable Door Held alarms, if there is more than one DSM side B, then Enable/Disable DSM Tamper;
- If there is an RTE2 input then show Enable/Disable RTE.

Table 119: Doors Monitoring Screen Definitions

Field/Button	Description
 Refresh All	Click this button to refresh the values of all Inputs on the screen.
	This toolbar lets you perform Dynamic View functions on the list of Door Inputs, such as filtering, printing, and switching to Card View.
Name	This column displays the name of the Input.
Input type	This column displays the function that the Input serves in Door Monitoring.
Armed Status	This column displays the Armed Status of the Input. Inputs associated with Doors are automatically Armed and are reported as unknown.
Active Status	This column displays the Active Status of the Input.
Cause Selection	This drop-down list lets you choose the Cause type to display in the Status Information and Cause List section of the screen.
Status Information	This read-only field displays the current state of the selected Input.
Cause	This read-only field displays the Cause State for the Input.
Action	This read-only field displays the Lock and Unlock actions that are in effect on the door.
DateTime	This read-only field displays the Date and Time the cause occurred.
Priority	This read-only field displays the Event Priority of the cause.
Lock	Click this button to initiate a manual action to lock the Door.
Unlock	Click this button to initiate a manual action to unlock the Door for a defined period.
Momentary Unlock	Click this button to momentarily unlock the Door for the Door Unlock period (usually 5 seconds).
Enable _____	The **Enable** button changes to match the selected **Cause Selection** in the drop-down list. Click this button to enable the selected Cause type. **Example:** If the Cause Selection is **Door Forced Alarms**, then the button reads **Enable Door Forced Alarms**.

Table 119: Doors Monitoring Screen Definitions (continued)

Field/Button	Description
Disable _____	The **Disable** button changes to match the selected **Cause Selection** in the drop-down list. Click this button to disable the selected Cause type. **Example:** If the Cause Selection is **Door Forced Alarms**, then the button reads **Disable Door Forced Alarms**.

12

Configuring Elevators

This chapter explains how to configure elevators in C•CURE 9000.

In this chapter

Elevator Configuration Overview

Access to floors is managed through Elevator control. Elevators are similar to doors, but have many exit points which are determined by the floor objects. Floors are created independently from controllers, and are integrated into Elevators through the definition of elevator buttons (see Creating a Floor on Page 399). Elevator control requires readers, inputs, outputs, and Personnel Clearances.

A reader is used to control access to the elevator by authenticating cardholders.

A cardholder is given access to an elevator by assigning a Personnel Clearance that includes the Elevator to the cardholder.

Outputs are used to control the elevator buttons. When the Output is energized, the button for a floor in the Elevator becomes available for use.

Inputs can be configured to determine at which floor the cardholder exited. When the Elevator door opens at a Floor, an Input state change indicates that the door has opened.

Elevators or elevator groups are configured through the use of buttons that represent floors with inputs and outputs. You can then add elevators to clearances that are used to control which cardholders can access the elevators and floors and at what times.

You can configure Elevators for iSTAR and apC controllers.

- iSTAR Elevators on Page 505
- apC Elevators on Page 519

NOTE Elevators are associated with the time zone that is used by the elevator's inputs, outputs, and readers.

NOTE Elevator controls and Clearances for Elevators have not been evaluated by UL, and cannot be used in UL Listed applications.

Elevator Tasks

You can perform the following general tasks to configure iSTAR and apC Elevators.

Creating an Elevator

You can create a new Elevator.

To Create an Elevator

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the Hardware pane.
2. Select **Elevator** from the Hardware pane drop-down list.
3. Right-click the Elevator folder and select **New** to create a new **Elevator**. The Elevator Editor opens and you can configure the **Elevator**.
4. Type an identification for the Elevator in the **Name** and **Description** entry fields.
5. To save your new Elevator, click **Save and Close**.

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

Creating an Elevator Template

You can create a new template for an Elevator. An Elevator template saves you time because you specify some of the Elevator configuration settings in the Template. When you use the Template to create new Elevators, you do not have to enter those configuration settings again.

To Create an Elevator Template

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the Hardware pane.
2. Select **Elevator** from the Hardware pane drop-down list.
3. Click the drop-down arrow next to **New** and select **New Template**.
4. The Elevator Template opens and you can configure the Elevator template.
5. To save your new Elevator Template, **click Save and Close**.

   The new Elevator template appears under *----Templates* in the New Template drop-down list.

To Create an Elevator from an Elevator Template

1. In the **Navigation Pane** of the **Administration Workstation**, click Hardware to open the Hardware pane.
2. Select **Elevator** from the Hardware pane drop-down list.
3. Click the drop-down arrow next to **New** and click a Template name from the list under *----Templates*. The Elevator editor opens.
4. Configure the Elevator.
5. To save your new Elevator, click **Save and Close**.

Deleting an Elevator

You can delete an existing Elevator.

To Delete an Elevator

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Select **Elevator** from the **Hardware** pane drop-down list.
3. Click  to open a **Dynamic View** showing all Elevator objects.
4. Right-click the Elevator in the list that you want to delete and select **Delete** from the context menu.
5. Click **Yes** on the "**Are you sure you want to delete the selected Elevator?**" message box.

Modifying an Elevator

You can edit an Elevator to modify its buttons (Floors and Outputs) and state images.

To Edit an Elevator

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Select **Elevator** from the **Hardware** pane drop-down list.
3. Click  to open a **Dynamic View** showing all Elevator objects.
4. Double-click the **Elevator** in the list that you want to modify, or right-click and select **Edit** from the context menu. The **Elevator Editor** opens.

Viewing a List of Elevators

You can a open Dynamic View listing your Elevators.

To View a List of Elevators

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the Hardware pane.
2. Select **Elevator** from the Hardware pane drop-down list.

3. Click  to open a **Dynamic View** showing all **Elevator** objects.

NOTE You can right-click the column header to add columns—Enabled, Controller, Comm Status, and so forth.

If you right-click a row in the Elevator Dynamic View, a context menu is displayed. This menu contains a number of standard selections, as well as selections that are specific for elevators.

See **Using the Object List Context Menu** in the *C•CURE 9000 Getting Started Guide* for more information about the object context menu.

Using Set Property for Elevators

You can use Set Property to set properties for Elevators to quickly set a property for an Elevator without opening an Elevator. You can select multiple Elevators in a Dynamic View list, and right-click to use Set Property to set a specific property for all of them.

Example:

To change the setting for **Send to Monitoring Station** for 10 specific Elevators, display a Dynamic View of Elevators (see Viewing a List of Elevators on Page 502), the use multiple selection (typically SHIFT+LEFT-CLICK to select a range or CTRL+LEFT-CLICK to select multiple items) to select the 10 Elevators, then right-click to display the context menu. Choose **Set Property** from the context menu, then click  to see a list of Elevator properties. Select **Send to Monitoring Station**, then select  or  for the **Value** setting. When you click **OK** the property will be set for these elevators.

To Set a Property for an Elevator

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the Hardware pane.
2. Select **Elevator** from the Hardware pane drop-down list.
3. Click  to open a Dynamic View showing all Elevator objects.
4. Right-click the **Elevator** in the list that you want to set the property for and select **Set Property** from the context menu.
5. Specify the property for the **Elevator**. Click  to choose from a list of properties.
6. Enter the **Value** for the property and click **OK**.

Adding Elevators to a Group

You can use **Add To Group** for Elevators to add one or more Elevators to a group.

To Add Elevators To Group

1. In the **Navigation Pane** of the **Administration Workstation**, click Hardware to open the Hardware pane.
2. Select **Elevator** from the Hardware pane drop-down list.
3. Click  to open a Dynamic View showing all Elevator objects.

4. Right-click the **Elevator** in the list that you want to add to the group and select **Add To Group** from the context menu.
5. Select a **Group** from the list that appears.
6. Click **OK** to confirm that the Elevators were added to the Group. Alternatively, you can click:
   - **Print** to print the message.
   - **Email** to send the message to the email address you have configured in the Customer Support section of the C•CURE 9000 System Variables.

iSTAR Elevators

A cluster of iSTAR controllers can be used to manage elevator access. A cluster consists of a system of one or more iSTAR controllers which determine communications between individual controllers. Each cluster is configured for either iSTAR Classic/Pro or iSTAR eX controllers. For more information see Configuring iSTAR Clusters on Page 87.

NOTE Elevator controls have not been evaluated by UL.

After configuring the parent objects, iSTAR Clusters and Controllers, iSTAR Elevators require floors, iSTAR Readers, Inputs, Outputs and Doors. The iSTAR Inputs are used to determine at which floor the cardholder exited and the iSTAR Outputs are used to control the elevator buttons, which are set in the Buttons tab. These dependent objects must be set up before you can configure an iSTAR Elevator. For more information, see the references listed below.

1. Cluster and Controller - for more information see:
   - iSTAR Cluster Editor on Page 91
   - iSTAR Controller Editor on Page 137
2. Floor - for more information see:
   - Floors Overview on Page 396
   - Configuring a Floor for an iSTAR Elevator on Page 505
3. Boards with Readers, Inputs, Outputs - for more information see:
   - iSTAR Controller Boards Tab (iSTAR Classic/Pro) on Page 156
   - iSTAR eX and iSTAR Edge Configuration Summary on Page 121

Once these parent and dependent objects are created, you can continue the elevator configuration process:

1. Elevator name (for more information see iSTAR Elevator General Tab on Page 506).
2. Elevator Buttons (for more information see iSTAR Elevator Buttons Tab on Page 510).
3. Elevator Triggers (see iSTAR Elevator Triggers Tab on Page 512
4. Groups tab (see Groups Tab for Hardware Devices on Page 28).

Configuring a Floor for an iSTAR Elevator

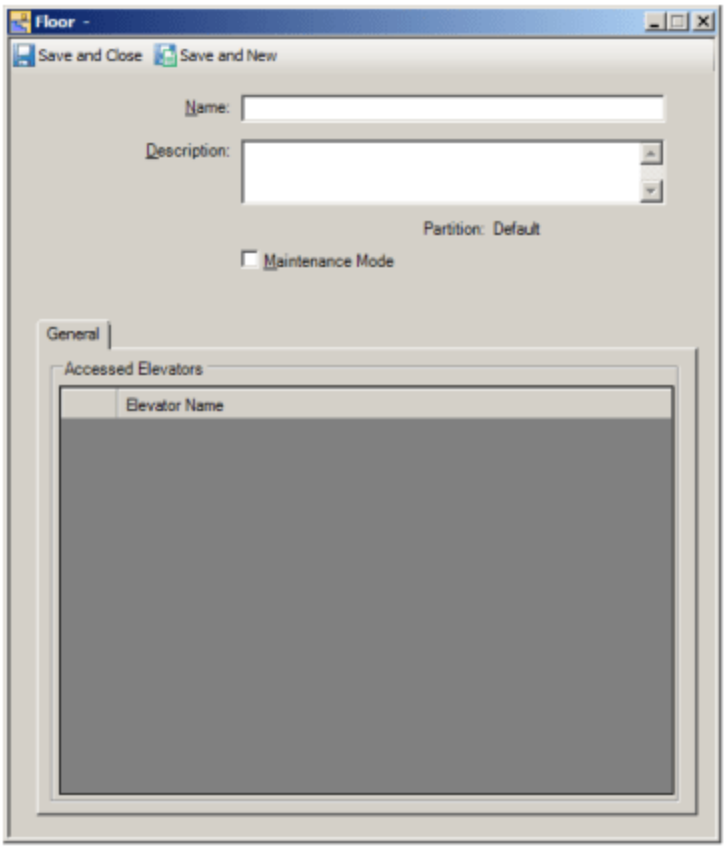
You may create new floors or configure existing floors using the Floor folder displayed in the Hardware tree. After you create the iSTAR cluster and controller(s), you can configure inputs, outputs, readers, elevators, and buttons and associate the these objects with specific floors or elevators for access by authorized cardholders. For more information see Using the Hardware Pane on Page 20.

When you add a floor to a group, the Groups tab will be displayed with the Floor - General tab.

Configuring a Floor for an iSTAR Elevator

1. From the default **Floor** directory of the **Hardware** tree, create a new floor, or edit the name or description of an existing floor.
2. Highlight the **Floor** folder, right-click, and select **New**. A Floor dialog box opens.
3. Enter a **Name** and **Description** for the new floor and click the **Enabled** box if you want to set the floor online.

Figure 198: Floor Dialog Box - General Tab



4. Click **Save and Close**. The new floor name displays below the Floors folder in the Hardware tree.

   Continue this creation process until your facility's floors, which you want to access via an elevator, have been assigned to a C•CURE 9000 Floor object.

   The next task that must be completed before you can configure an iSTAR Elevator is to complete the configuration of an iSTAR Cluster, Controller(s), Readers, Inputs, Outputs and Doors. For more information, see the references listed above.

iSTAR Elevator General Tab

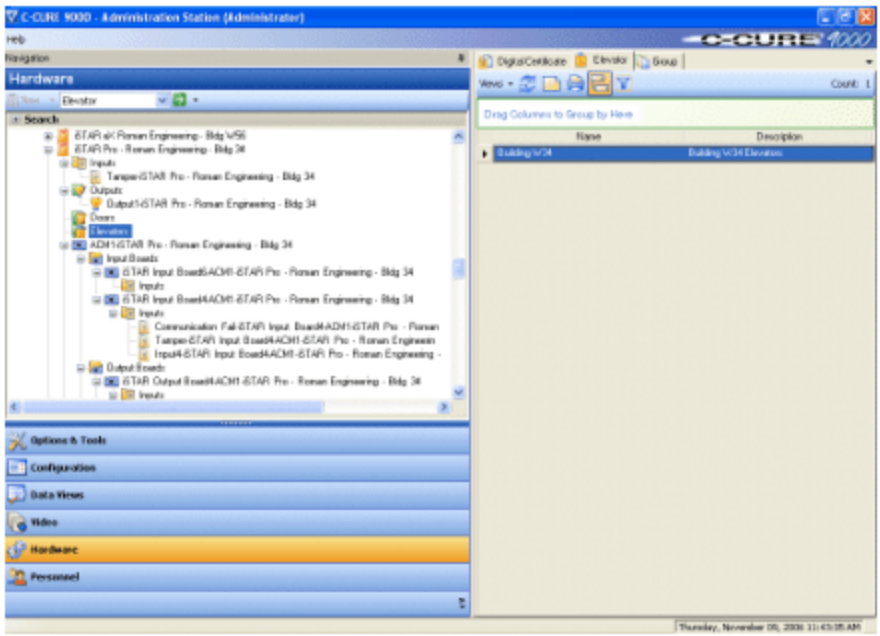
You can access the Elevator editor from a configured iSTAR Elevator object in the C•CURE 9000 Hardware pane. See iSTAR Elevator General Tab Definitions on Page 514 for descriptions of the fields on this tab.

To Access the iSTAR Elevator Editor

1. In the C•CURE 9000 **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Click the iSTAR Controller drop-down list and select **Elevator**.
3. Right-click the Elevator listing and click **New** or **New Template**.

4. If you have configured Elevators, double-click the Elevator listing for the selected controller to open a **Dynamic View** showing all existing **Elevator** objects (see Figure 199 on Page 507).
5. Double-click the **Elevator** in the list that you want to edit, and the **Elevator - General** tab opens, shown in Figure 200 on Page 508.

Figure 199: Hardware Pane Elevator Selection

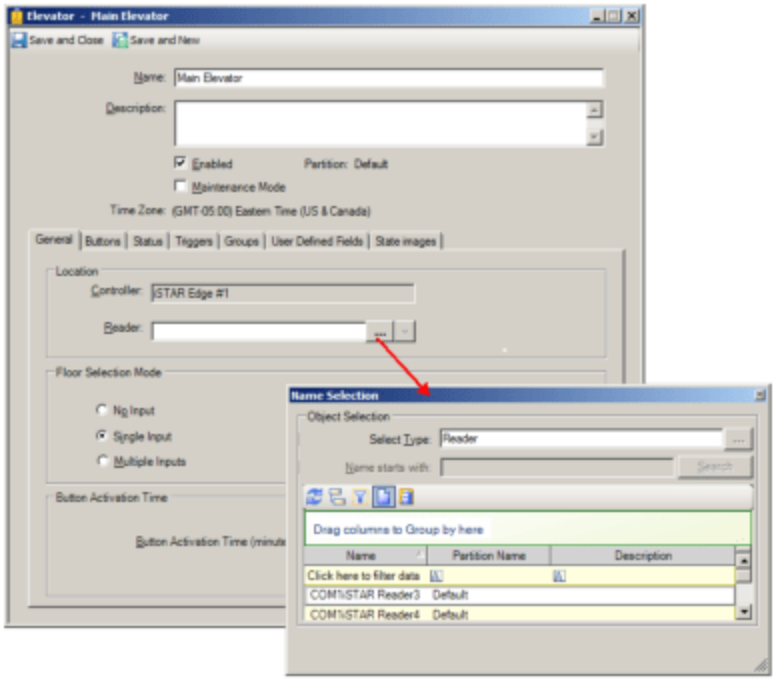


To Configure Elevators

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Right-click the **Elevators** folder in the **Hardware** tree and select **New** to create a new **Elevator**. The **Elevator - General** tab, shown in Figure 200 on Page 508 opens.
3. Enter a **Name** and description (for example, its location or function) for the elevator.
4. Select **Enabled** to put the **Elevator** online once you click **Save and Close**.

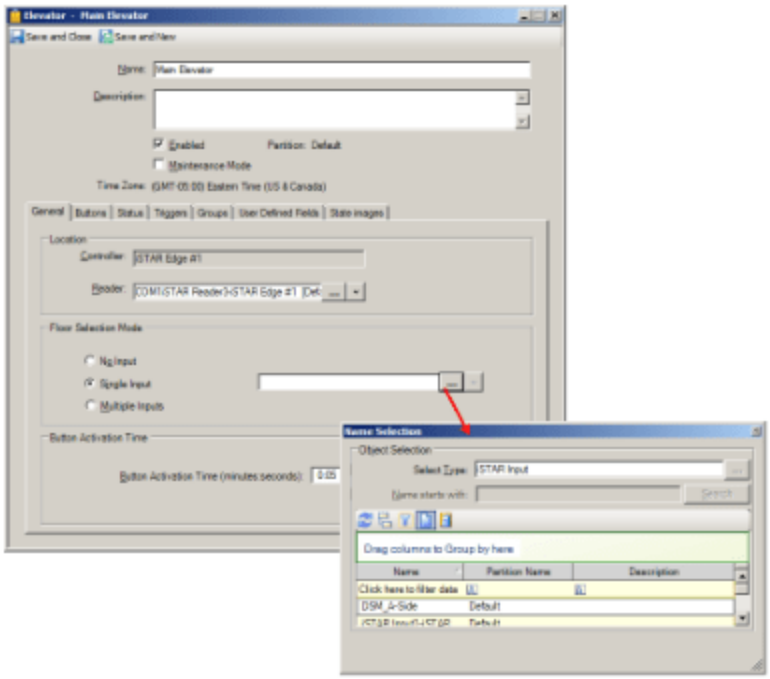
   The iSTAR Controller is displayed within the Location box.

Figure 200: iSTAR Elevator General Tab - Reader Selection



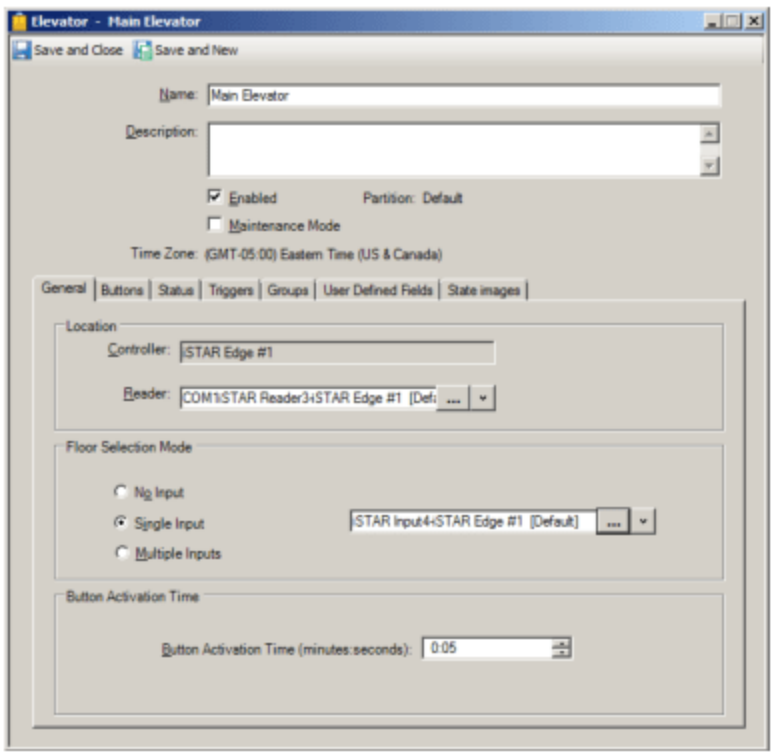
5. Click [...] to select a **Reader** in the **Location** area. The Reader list shown in the Reader browser is restricted to unassigned readers on the parent Controller.
6. Choose an Elevator **Floor Selection Mode** for the elevator from the listed options. The possible choices include:
   - **No Input**
   - **Single Input**
   - **Multiple Inputs**
7. If you choose the **Single Input** option, click the browse [...] button to select an Input from the Input browser (see Figure 201 on Page 509).

Figure 201: iSTAR Elevator General Tab - Input Selection



8. Enter a **Button Activation Time** in seconds.

Figure 202: iSTAR Elevator General Tab - Completed



9. Navigate to the **Buttons** tab or click **Save and Close**.

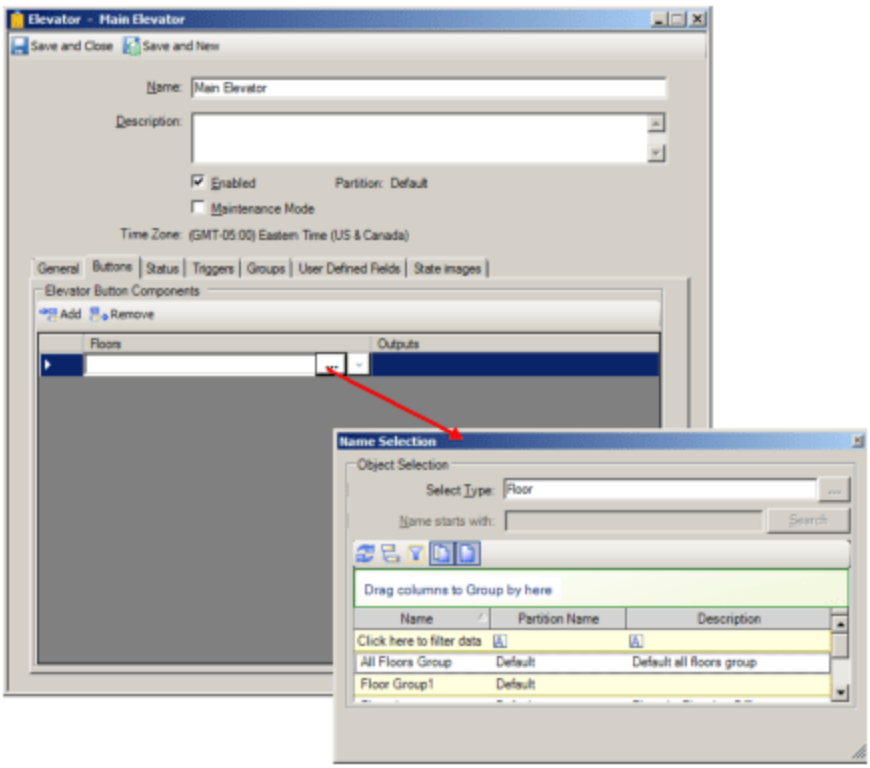
iSTAR Elevator Buttons Tab

Elevator Buttonscan be created in the Elevator Buttons tab to specify which floors, inputs, and outputs are connected to elevator buttons. See iSTAR Elevator Buttons Tab Definitions on Page 515 for more definitions of the Buttons tab.

To Configure Elevator Buttons for Floor Access

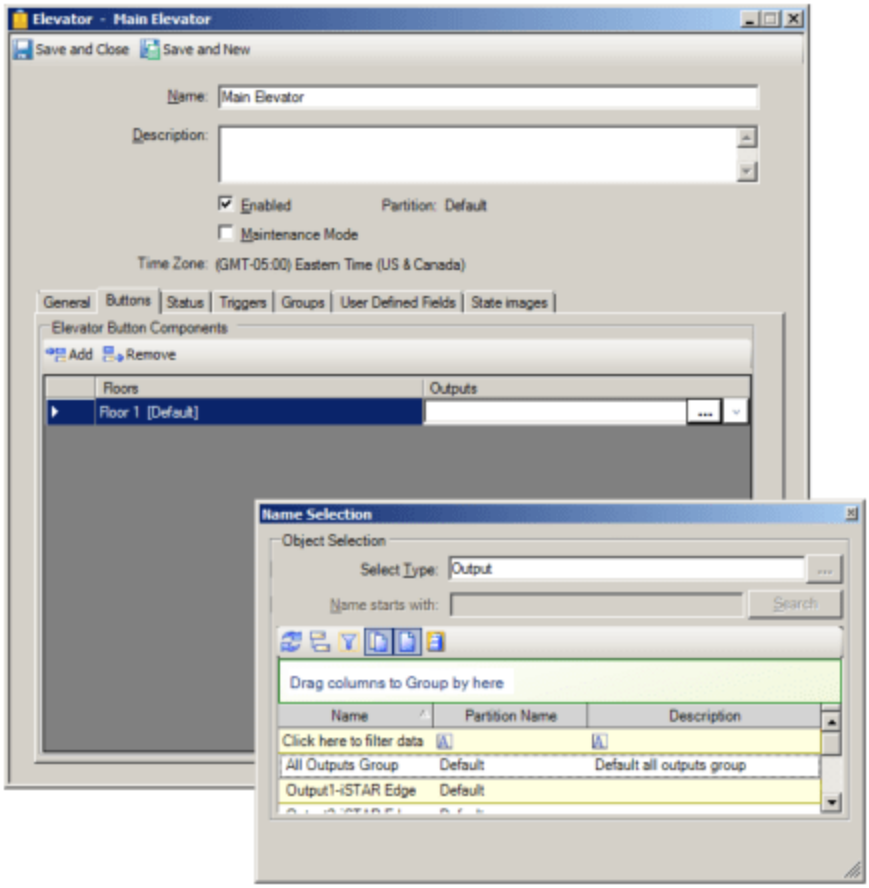
1. From the **Elevator** dialog box, click the **Buttons** tab. The **Elevator** dialog box - **Buttons** tab opens, shown in Figure 203 on Page 510.
2. Click **Add** to create a row under the **Floors** and **Outputs** columns.
3. Click within the **Floors** column to display the browse [...] button and select a **Floor** from the Floor browser, shown in Figure 203 on Page 510, that you want to associate with the iSTAR Elevator.

Figure 203: iSTAR Elevator Buttons Tab - Floor Selection



4. Click within the **Outputs** column to display [...] and select an **Output** from the Outputs browser, shown in Figure 204 on Page 511, that you want to associate with the iSTAR Elevator.

Figure 204: iSTAR Elevator Buttons Tab - Output Selection



5. Continue to add **Floors** and **Outputs** until you have finished creating Elevator Buttons for each floor that you want to manage with the iSTAR Elevator.
6. Navigate to the **Status** tab or click **Save and Close**.

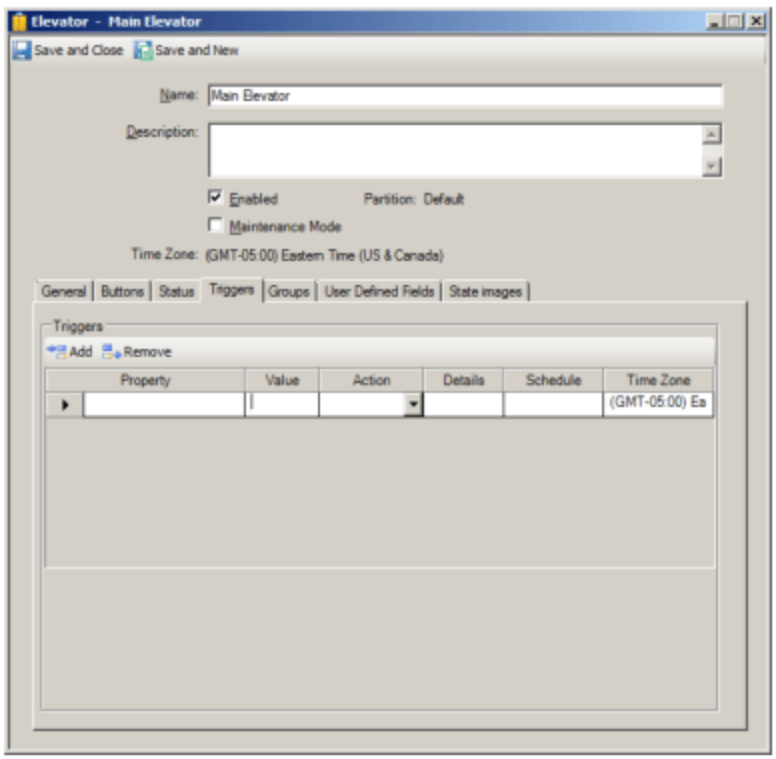
iSTAR Elevator Status Tab

The Elevator Status tab (see Figure 205 on Page 512) provides a read-only listing of critical information about the operational status of the selected Elevator including:

- **Communication Status** - displays the values Normal or Comm Fail.
- **Tamper Status** - displays the values True or False.
- **Admit Status** - displays the values Admit or Reject.

See iSTAR Elevator Status Tab Definitions on Page 516 for descriptions of the fields on this tab.

Figure 205: iSTAR Elevator Status Tab



Navigate to the **Triggers** tab or click **Save and Close**.

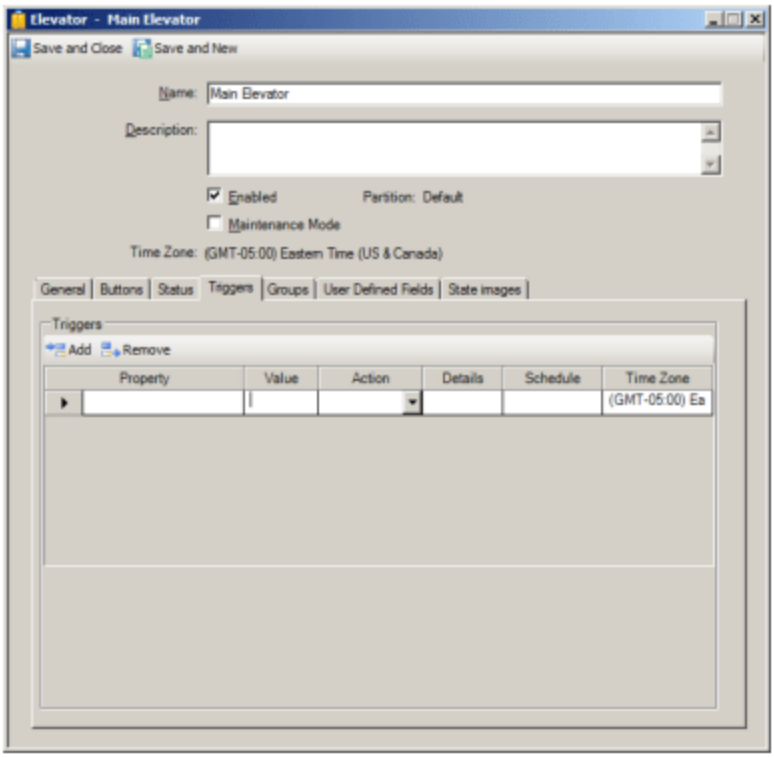
iSTAR Elevator Triggers Tab

You can create Triggers for iSTAR Elevators using the iSTAR Elevators Triggers tab. A Trigger executes a specified **Action** when a particular predefined condition occurs. When a Trigger is defined, the Actions available depend on the property selected (see Figure 206 on Page 513).

See Triggers Tab for iSTAR Devices on Page 270 for information on creating Triggers for an iSTAR device.

See iSTAR Elevator Triggers Tab Definitions on Page 516 for descriptions of the fields on this tab.

Figure 206: iSTAR Elevator Triggers Tab - Completed



iSTAR Elevator State Images Tab

The iSTAR Elevator **State Images** tab provides a means to change the default images used to indicate controller states (see Figure 207 on Page 514). These images appear on the Monitoring Station and change according to the state of the object that they represent.

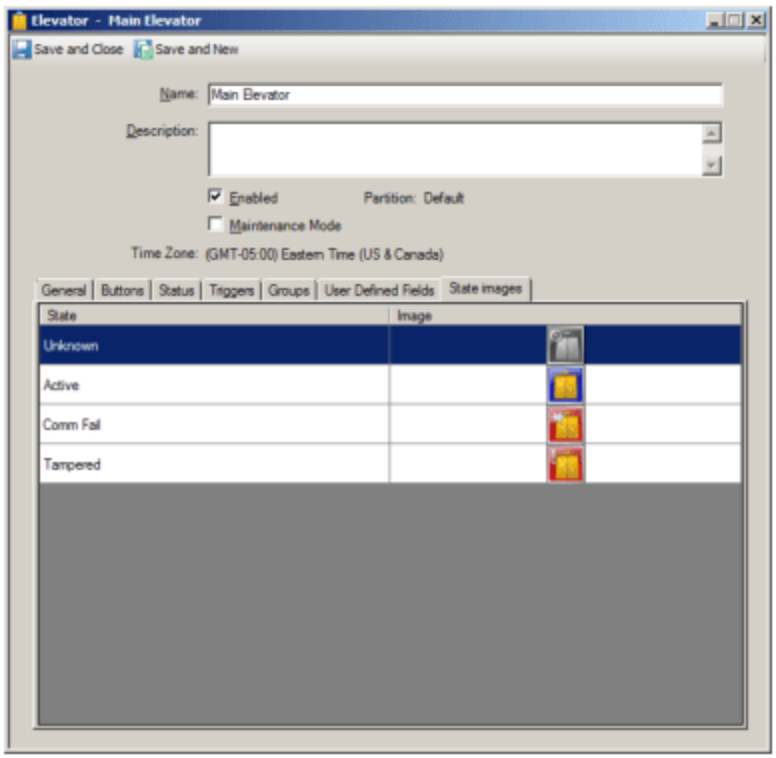
To Change an Elevator State Image

1. Double-click the existing image.

   A **Windows Open** dialog box appears allowing you to browse for a folder in which you have placed replacement images.

2. When you locate the replacement image, select it to add it to the image listing.
3. To restore the default image, right-click on the new image and select **Restore Default**.

Figure 207: iSTARElevator State Images Tab



4. Click **Save and Close** to finish the **iSTAR Elevator** configuration and return to the **Hardware Pane.**

iSTAR Elevator Definitions

The tables in the following sections provide definitions for the iSTAR Elevator editor tabs.

- iSTAR Elevator General Tab Definitions on Page 514
- iSTAR Elevator Buttons Tab Definitions on Page 515
- iSTAR Elevator Status Tab Definitions on Page 516
- iSTAR Elevator Triggers Tab Definitions on Page 516
- iSTAR Elevator Triggers Properties on Page 517
- iSTAR Elevator Triggers Actions on Page 517
- iSTAR Elevator State Images Definitions on Page 517

iSTAR Elevator General Tab Definitions

iSTAR Elevator General Tab Definitions

Field/Button	Description
Identification	

iSTAR Elevator General Tab Definitions (continued)

Field/Button	Description
Elevator Name	Enter a unique name for this elevator.
Description	Enter a brief description for this elevator.
Maintenance Mode	Click to put the elevator into Maintenance Mode. See Chapter 2: Maintenance Mode for more information.
Enabled	Select this check box to put the elevator online. For an elevator to be put online, it must selected.
Location	
Controller	The parent controller is displayed in this read-only field.
Reader	Click ... to select a Reader from the Reader browser.
Floor Selection Mode	
No Input	Click on No Input to indicate that no inputs are connected to the elevator buttons. However, the system cannot tell if a person presses a floor button after being granted access.
Single Input	Click on Single Input to indicate that one input is connected to all buttons on this elevator. Click ... and select an Input from the Input list that displays. When a person presses an elevator button, the system detects an elevator button has been pressed, but cannot determine which button.
Multiple Inputs	Click on Multiple Inputs to indicate that multiple inputs are associated with this elevator. Each elevator button will be connected to a different input. Select the inputs by clicking Elevator Buttons to open the Elevator Buttons dialog box. When a person presses an elevator button, the system determines which button the person pressed.
Button Activation Time	
Button Activation Time (seconds)	Enter the interval at which the Elevator button activates.

iSTAR Elevator Buttons Tab Definitions

Table 120: iSTAR Elevator Buttons Tab Definitions

Field	Description
Elevator Button Components	
Add	Fields are added to Elevator Button Components by clicking **Add**, which adds an empty row to the grid.
Remove	Click the row selector , then click **Remove** to delete a trigger.

Table 120: iSTAR Elevator Buttons Tab Definitions (continued)

Field	Description
Floors	This displays a list of available floors for the elevator. Use **Add** to add a floor to the list and click ... to display the Floor selection browser.
Outputs	This displays a list of available Outputs for the elevator. Click ... to select an Output from the Output selection browser.

iSTAR Elevator Status Tab Definitions

Table 121: iSTAR Elevator Status Tab Definitions

Field/Button	Description
Communication Status	Unknown, Normal, Comm Fail
Tamper Status	True, False
Admit Status	Unknown, Admit, Reject

iSTAR Elevator Triggers Tab Definitions

Table 122: iSTAR Elevator Triggers Tab Definitions

Field	Description
Add	Fields are added to Elevator Button Components by clicking **Add**, which adds an empty row to the grid.
Remove	Click the row selector , then click **Remove** to delete a trigger.
Property	Click within the Property column to display browse ... button. When you click this button, the Property browser opens, presenting properties available for the controller. Click a Property to select it and add it to the column.
Value	Click within the Value column to display a drop-down list of Values associated with the Property that you have selected. Click on a Value that you want to include as a parameter for the trigger to add it to the column.
Action	Click within the Action column to display a drop-down list of valid actions. Click on an Action that you want to include as a parameter for the trigger to add it to the column. When a Trigger is added, an Action must be configured in the Action column. This is the Action that will occur when the object's selected Property receives the selected Value. As the Action is selected, the lower pane in the Triggers box will show a corresponding entry field, or group of entry fields, specific to the selected Action. Click the browse ... button to select entries for these fields. Once the field (or group of fields) is completed, the Details column will show information about how the Action was configured.
Details	The Details column displays information about how the Action was configured. This field is read-only.
Schedule	Click within the Schedule column, then click ... to select a Schedule that you want to associate with the trigger. Schedules are created in the Configuration Pane.

iSTAR Elevator Triggers Properties

Table 123: iSTAR Elevator Triggers Properties

Property	Description
Admit Status Values are: - Admit - Reject - Duress - Noticed Admit - Noticed Reject	For any one of the Admit Status values (see the Value column drop-down list) you can choose one of the following Actions to create a Trigger: **Activate Event** – When this status occurs and the Schedule is Active (you can choose any Schedule). **Activate Event Outside Schedule** – An event is activated when this status occurs while the Schedule is Inactive (choose any Schedule). **Activate Output** – When this status occurs (only works with the Always Schedule). Only these three Actions are supported for Admit Status.
Comm Status Values are: - Normal - Comm Fail	1. Choose a value for the Property from the Value column. 2. Select an Action from the Action drop-down list: See Table 124 on Page 517. For example, if you chose Comm Fail as a Comm State Status for which you want to define an action, you could then select **Activate Event** if you wanted to send a command to a CCTV Switch, then in Details, select theEvent that you wanted to activate when a **Comm Fail** status occurs.
Tamper Status Values are: 	

iSTAR Elevator Triggers Actions

Table 124: iSTAR Elevators Triggers Actions

Action	Description
Activate Event	Select an Event to activate when this status occurs.
Activate Event Outside Schedule	Select an Event to activate when this status occurs while the Schedule is inactive.
Activate Output	Select an Output to activate when this status occurs. Must use the Always Schedule.

iSTAR Elevator State Images Definitions

iSTAR Elevator State Images Tab Definitions

Field/Button	Description
Unknown	

iSTAR Elevator State Images Tab Definitions (continued)

Field/Button	Description
Active	
Comm Fail	
Tampered	

apC Elevators

This section illustrates the configuration process for the apC - controlled elevator. The **advanced processing Controller** (apC), apC/8X, and apC/L are access control field panels that coordinate communication between the C•CURE 9000 server and the system security hardware.

NOTE Elevator controls have not been evaluated by UL.
The apC and apC/L Controllers have not been evaluated by UL.

The apC Elevator editor includes the following tabs:

- General
- Buttons
- Groups (this tab appears once you have created an Elevator Group)
- State Images

The function of these tabs is covered in the description of configuring the apC Elevator in the following sections. To configure an elevator controlled by a reader on an apC panel, you must first create and configure the following objects:

1. Floor (for more information see Floors Overview on Page 396)
2. apC panel(s) (for more information see apC Panel Overview on Page 296)
3. Readers, Inputs, Outputs

Once these parent and dependent objects are created, you can continue the elevator configuration process:

1. Elevator name (for more information see apC Elevator General Tab on Page 520)
2. Elevator Buttons (for more information see apC Elevator Buttons Tab on Page 522)
3. Personnel Clearance for cardholders who will use the Elevator (for more information see the *C•CURE 9000 Personnel Configuration Guide*).
4. Groups tab (see Groups Tab for Hardware Devices on Page 28).

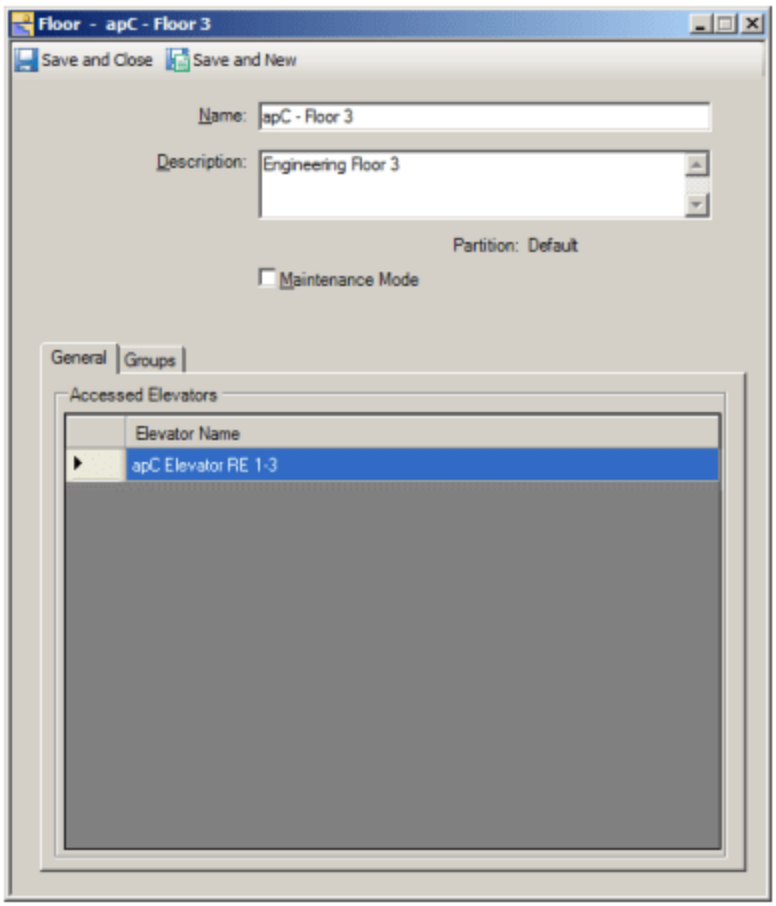
Configuring a Floor for an apC Elevator

You may create new floors or configure existing floors using the Floor folder displayed in the hardware tree. After you create the apC panel, you can configure outputs, readers, elevators, and buttons and associate the these objects with specific floors or elevators for access by authorized cardholders. When you create a Floor group, a Group tab will appear with the Floor General tab. For more information see Floors Overview on Page 396.

Configuring a Floor for an apC Elevator

1. From the default **Floor** directory of the **Hardware** tree, create a new floor, or edit the name or description of an existing floor.
   a. Highlight the **Floor** folder, right-click and select **New**. A Floor dialog box opens.
   b. Enter a **Name** and **Description** for the new floor and click the **Enabled** box if you want to set the floor online.

Figure 208: Floor Editor General Tab



2. Click **Save and Close**. The new floor name displays below the Floors folder in the Hardware tree.

   Continue this creation process until your facility's floors, which you want to access via an elevator, have been assigned to a C•CURE 9000 Floor object.

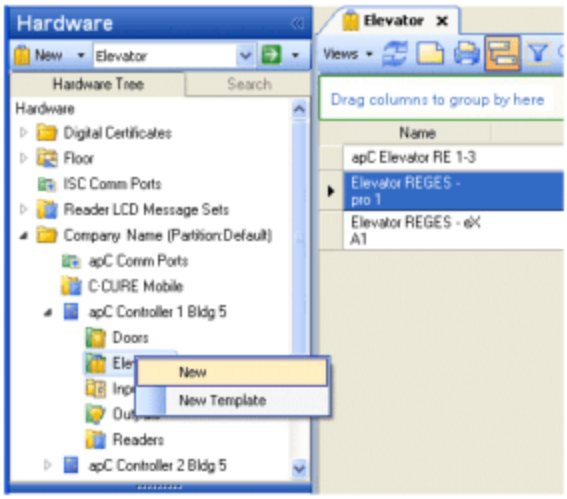
apC Elevator General Tab

You can access the Elevator editor from a configured apC Elevator object in the C•CURE 9000 Hardware pane.

To Access the apC Elevator Editor

1. In the C•CURE 9000 **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Click the apC Controller drop-down list and select **Elevator**.
3. Right-click the Elevator listing and click **New** or **New Template**.
4. If you have configured Elevators, double-click the Elevator listing for the selected controller to open a **Dynamic View** showing all existing **Elevator** objects (see Figure 209 on Page 521).
5. Double-click the **Elevator** in the list that you want to edit, and the **Elevator General** tab opens, shown in Figure 210 on Page 522.

Figure 209: Hardware Pane apC Elevator Selection

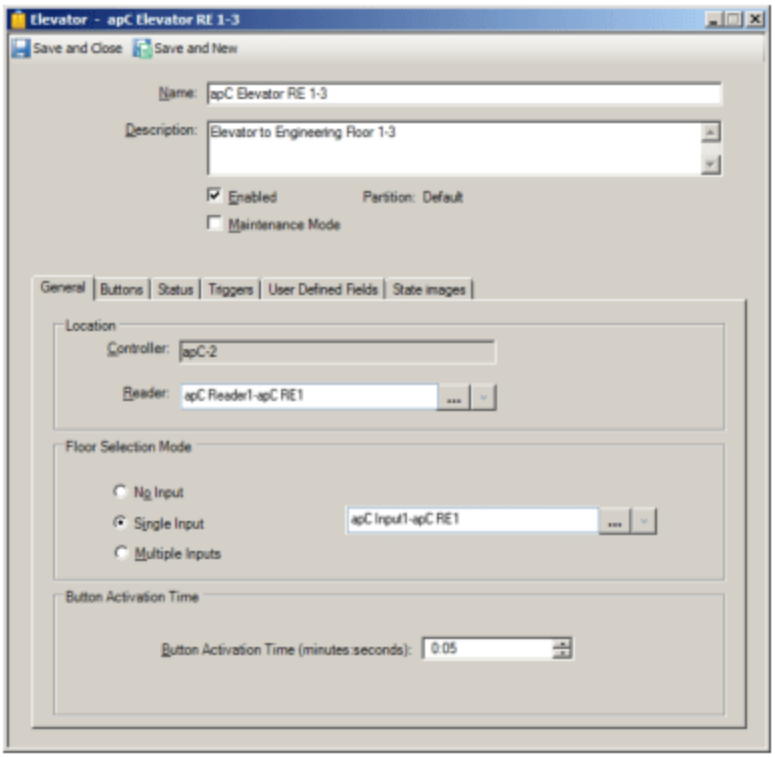


To Configure Elevators

1. In the **Navigation Pane** of the **Administration Workstation**, click **Hardware** to open the **Hardware** pane.
2. Right-click the **Elevators** folder in the **Hardware** tree and select **New** to create a new **Elevator**. The **Elevator - General** tab, shown in Figure 210 on Page 522 opens.
3. Enter a **Name** and description (for example, its location or function) for the elevator.
4. Select **Enabled** to put the **Elevator** online once you click **Save and Close**.

   The apC panel name is displayed within the Location box.

Figure 210: apC Elevator General Tab



5. Click ... to select a **Reader** in the **Location** area. The Reader list shown in the Reader browser is restricted to unassigned readers on the parent Controller.
6. Choose an Elevator **Floor Selection Mode** for the elevator from the listed options. The possible choices include:
   - **No Input**
   - **Single Input**
   - **Multiple Inputs**
7. If you choose the **Single Input** option, click the browse ... button to select an Input from the Input browser.
8. Enter a **Button Activation Time** in seconds.
9. Navigate to the **Buttons** tab or click **Save and Close**.

apC Elevator Buttons Tab

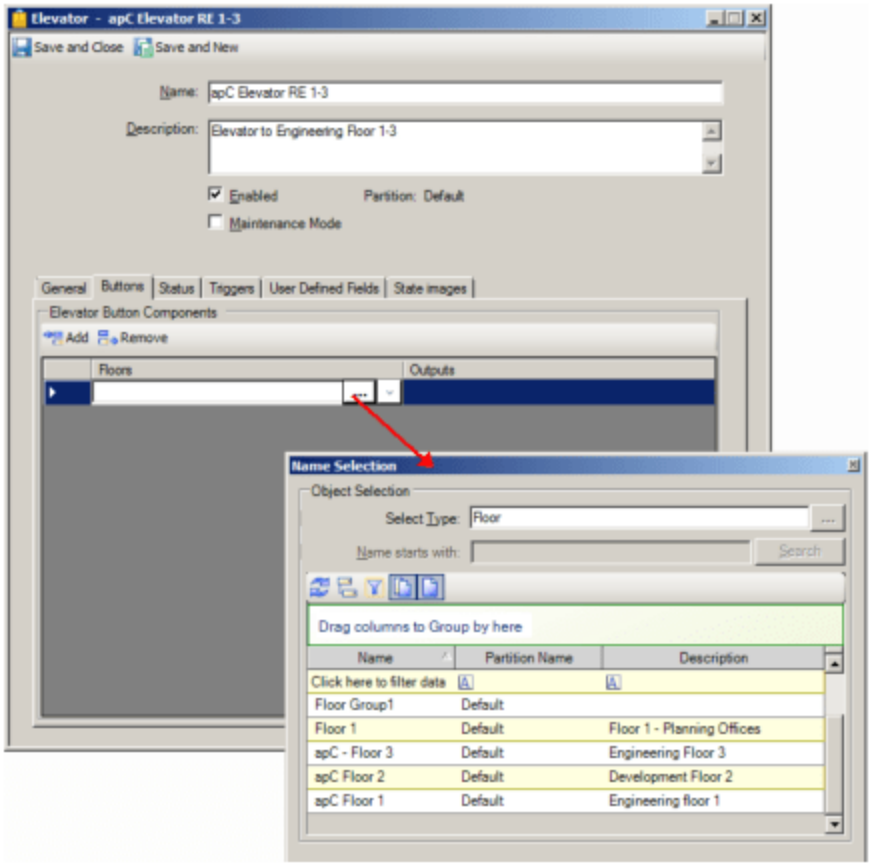
Elevator Buttons can be created in the Elevator Buttons tab to specify which floors, inputs, and outputs are connected to elevator buttons.

To Configure Elevator Buttons for Floor Access

1. From the **Elevator** editor, click the **Buttons** tab. The **Elevator Buttons** tab opens, shown in Figure 211 on Page 523.
2. Click the **Add** button to create a row under the **Floors** and **Outputs** columns.

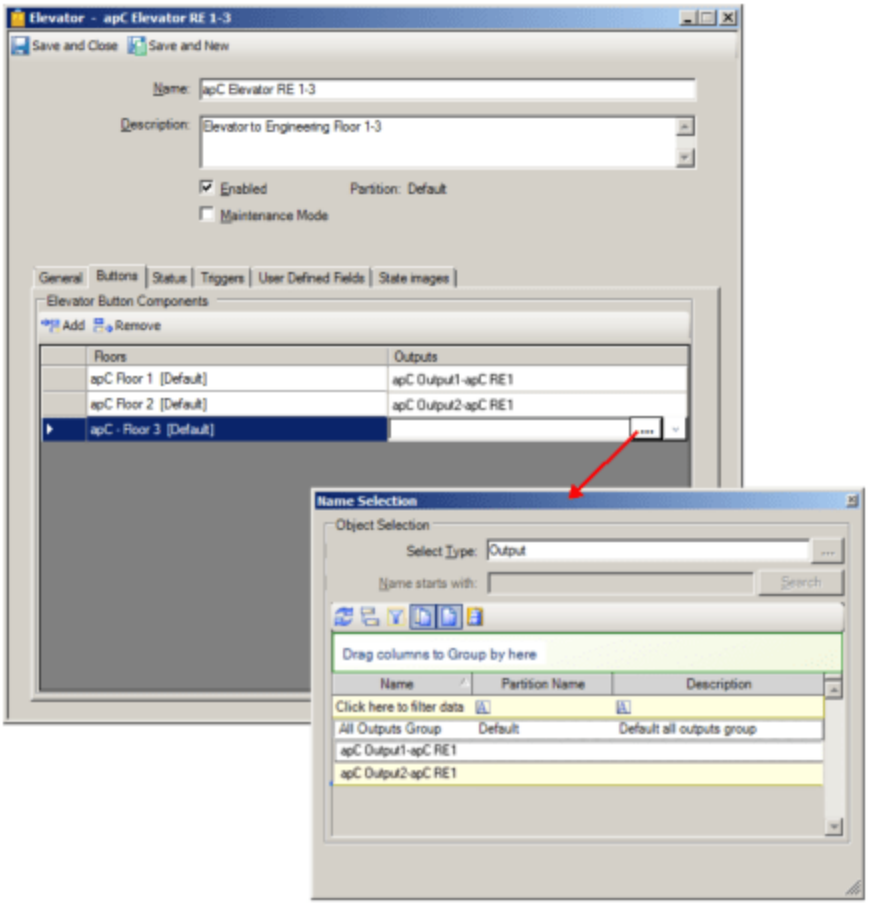
3. Click within the **Floors** column to display [...] and select a **Floor** from the Floor browser, shown in Figure 211 on Page 523, that you want to associate with the apC Elevator.

Figure 211: apC Elevator Buttons Tab Floor Selection



4. Click within the **Outputs** column to display [...] and select an **Output** from the Outputs browser, shown in Figure 212 on Page 524, that you want to associate with the apC Elevator.

Figure 212: apC Elevator Buttons Tab Output Selection



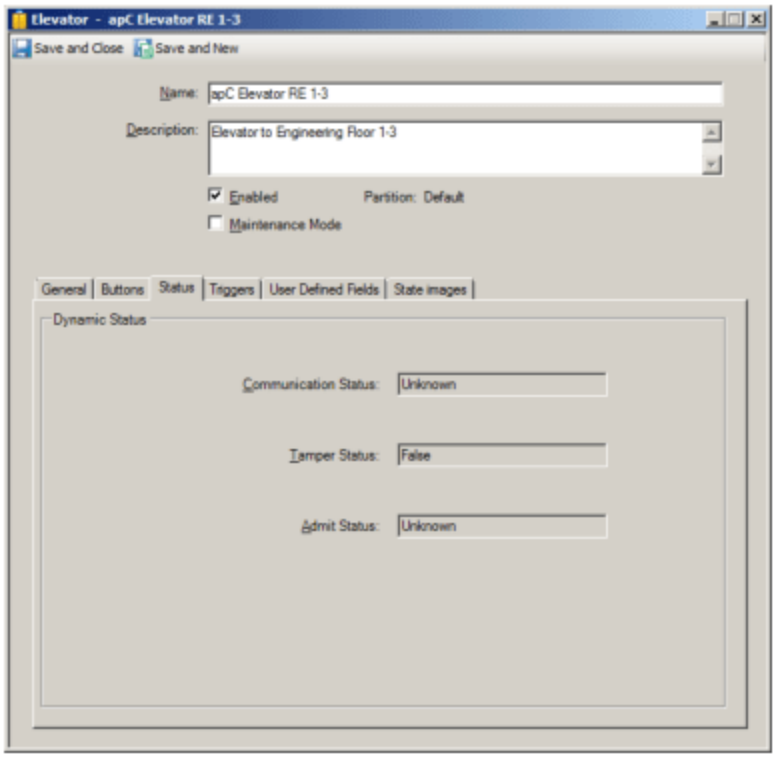
5. Continue to add **Floors** and **Outputs** until you have finished creating Elevator Buttons for each floor that you want to manage with the apC Elevator.
6. Navigate to the **Status** tab or click **Save and Close**.

apC Elevator Status Tab

The Elevator Status tab (see Figure 213 on Page 525) provides a read-only listing of critical information about the operational status of the selected Elevator including:

- **Communication Status** - displays the values Normal or Comm Fail.
- **Tamper Status** - displays the values True or False.
- **Admit Status** - displays the values Admit or Reject.

Figure 213: apC Elevator Status Tab



Navigate to the **Triggers** tab or click **Save and Close**.

apC Elevator Triggers Tab

You can create Triggers for apC Elevators using the apC Elevators Triggers tab. A Trigger executes a specified **Action** when a particular predefined condition occurs. When a Trigger is defined, the Actions available depend on the property selected

See the following for information on apC Triggers:

- Triggers Tab for apC Devices on Page 369.
- Defining a Trigger for an apC Device on Page 370.
- Removing a Trigger on Page 272.

You can click **Save and Close** after configuring apC Elevator triggers, or navigate to the Status tab.

apC Elevator State Images Tab

The apC Elevator **State Images** tab provides a means to change the default images used to indicate controller states (see Figure 214 on Page 526). These images appear on the Monitoring Station and change according to the state of the object that they represent.

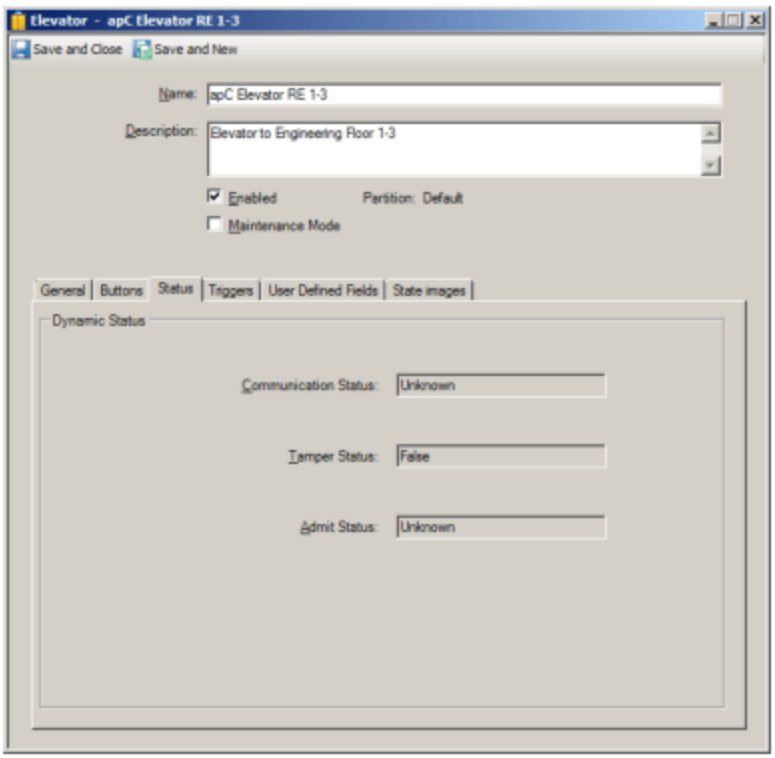
To Change an Image

1. Double-click the existing image.

A **Windows Open** dialog box appears allowing you to browse for a folder in which you have placed replacement images.

2. When you locate the replacement image, select it to add it to the image listing.
3. To restore the default image, right-click on the new image and select **Restore Default**.

Figure 214: apC Elevator - State Images Tab



4. Click **Save and Close** to finish the **apC Elevator** configuration and return to the **Hardware Pane**.

apC Elevator Definitions

Table 125 on Page 526 through Table 129 on Page 528 provide details about the fields and buttons on the General tab, Buttons tab, Status tab, Triggers tab, and State Images tab of the apC Elevator dialog box.

apC Elevator General Tab Definitions

Table 125: apC Elevator General Tab Definitions

Field/Button	Description
Identification	
Elevator Name	Enter a unique name for this elevator.
Description	Enter a brief description for this elevator.

apC Elevator General Tab Definitions (continued)

Field/Button	Description
Enabled	Select this check box to put the elevator online. For an elevator to be put online, it must selected.
Maintenance Mode	Click to put the apC Elevator into Maintenance Mode. See Chapter 2: Maintenance Mode for more information.
Partition	This read-only label shows what partition the elevator is in. If the system is not partitioned, the label indicates that the elevator is in the "Default" partition.
Location	
Controller	The parent controller is displayed in this read-only field.
Reader	Click ... to select a Reader from the Reader browser.
Floor Selection Mode	
No Input	Select this option when no inputs are needed for the apC Elevator.
Single Input	Click ... to select an Input from the Input browser.
Multiple Inputs	Select this option when more than one input is needed for the apC Elevator.
Button Activation Time	
Button Activation Time (seconds)	Enter the interval at which the apC Elevator button activates.

apC Elevator Status Tab Definitions

Table 126: apC Elevator Status Tab Definitions

Elevator Status Property	Values
Communication Status	Unknown, Normal, Comm Fail
Tamper Status	True, False
Admit Status	Unknown, Admit, Reject

apC Elevator Triggers Definitions

Table 127: apC Elevator Triggers Tab Definitions

Field	Description
Add	Fields are added to Elevator Button Components by clicking **Add**, which adds an empty row to the grid.
Remove	Click the row selector , then click **Remove** to delete a trigger.

Table 127: apC Elevator Triggers Tab Definitions (continued)

Field	Description
Property	Click within the Property column to display a [...] button. When you click this button, the Property browser opens, presenting properties available for the controller. Click a Property to select it and add it to the column.
Value	Click within the Value column to display a drop-down list of Values associated with the Property that you have selected. Click on a Value that you want to include as a parameter for the trigger to add it to the column.
Action	Click within the Action column to display a drop-down list of valid actions. Click on an Action that you want to include as a parameter for the trigger to add it to the column. When a Trigger is added, an Action must be configured in the Action column. This is the Action that will occur when the object's selected Property receives the selected Value. As the Action is selected, the lower pane in the Triggers box will show a corresponding entry field, or group of entry fields, specific to the selected Action. Click [...] to select entries for these fields. Once the field (or group of fields) is completed, the Details column will show information about how the Action was configured.
Details	The Details column displays information about how the Action was configured. This field is read-only.
Schedule	Click within the **Schedule** column, then click the browse [...] button to select a Schedule that you want to associate with the trigger. Schedules are created in the Configuration Pane.

apC Elevator Triggers Properties

Table 128: apC Elevator Triggers Properties

Property	Description
Admit Status Values are: Admit Reject Admit Duress Reject Duress Noticed Admit Noticed Reject	For any one of the Admit Status values (see the Value column drop-down list) you can choose one of the following Actions to create a Trigger: **Activate Event** - When this status occurs and the Schedule is Active (you can choose any Schedule). **Activate Event Outside Schedule** - An event is activated when this status occurs while the Schedule is Inactive (choose any Schedule). **Activate Output -** When this status occurs (only works with the **Always** Schedule). Only these three Actions are supported for Admit Status.

apC Elevator State Images Definitions

Table 129: apC Elevator State Images Tab Definitions

Field/Button	Description
Unknown	

apC Elevator State Images Tab Definitions (continued)

Field/Button	Description
Active	
Comm Fail	
Tampered	

Index

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W